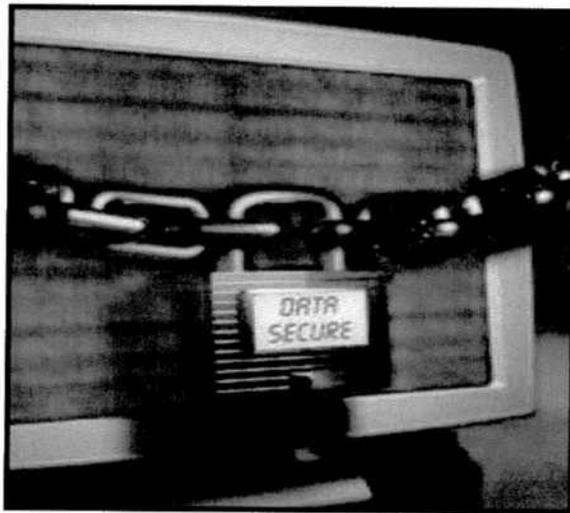


CITY OF HOUSTON
Public Works & Engineering
Student Intern, Research paper, summer 08



Data Security
Government Agencies

Prepared by:

Mamadou Malle

Supervisor:

Bryant Bragail

LAN Specialist

Rodrigue Michelon
7/24/2008

Data Security - Government Agencies

Outline

- I. Introduction
- II. Necessity of Data Security
 - a. Vulnerable Data
 - b. Internal and External Threats to Data
 - c. Counter Measure
- III. Security Management
 - a. Policy Consideration
 - b. Procedures
 - c. Physical Data Protection
- IV. Consequences: National Security Issue
 - a. Homeland Security
 - b. Cyber terrorism
 - c. Identity Theft
- V. Conclusion
- VI. Resources

I. INTRODUCTION

The purpose of this paper is to discuss data security issues in America. Weak data security systems and policies can cause major losses to confidential information of people, businesses, and the government. In section two, this paper will start of discussing the need for strong data security and will also point out some of the most vulnerable data targeted by internet hackers and thieves. Next, internal and external data will be defined and some statistics offered to show the frequency of data security breaches. The section will then conclude with countermeasures against internet hackers and thieves. Section three discusses policies and procedures implemented by the government. Section three will also suggest ways that individuals and private businesses may protect against breaches of data security. Section four will end the discussion with specific national security issues to both the public and the government, including homeland security, cyber terrorism, and identity theft.

It is important to define some common terms used in the field of data security. Data security is defined as the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data. [http://en.wikipedia.org/wiki/Data_security] Hackers are people who breach the data security systems of other people, businesses, or the government to gain access to classified or confidential information for illegal use.

II. THE NECESSITY OF DATA SECURITY

A. Vulnerable Data

Data security provides protection for personal, business, and government data on the internet. Many people have a misconception regarding the safety of their personal information on the internet. Although there are ways to increase the privacy of information stored on computers, there is no absolute protection against the most skilled internet hackers and thieves. This is a serious issue for the U.S. government. Now, more than ever, government agencies need data security solutions. Lost equipment could mean catastrophic financial losses or national security invasions by terrorists. Government and business documents of interest to local intelligence services are highly targeted.

[<http://www.checkpoint.com/products/datasecurity/solutions/government/index.html>http://en.wikipedia.org/wiki/Data_security]

Business web pages are one of the most targeted by identity thieves. The increase in E-commerce, retail shopping or conducting business over the internet, has fueled the problem of identity theft. Retail shopping usually requires paying with a credit card for an immediate transaction. Although businesses request verifying information from the shopper, such as billing address, and verification number, this does nothing to protect against the hacker able to gain access into the most secure areas of a business web page. A difficult issue for web businesses is they are not able to compare signatures on the receipt and card or ask for photo identification for verification the shopper is the true owner of the credit card used.

Generic email providers are also heavily targeted by internet snoops and thieves. Most internet web pages, with the exception of AOL, are not encrypted to protect the content of an

email. [[Http://www.worldtraderef.com/WTR_site/data_security.asp](http://www.worldtraderef.com/WTR_site/data_security.asp)] Thus, this information is not only one of the most targeted, but is the easiest to attain. However, even encrypted sights, such as AOL, do not provide full security against hackers.

[[Http://www.worldtraderef.com/WTR_site/data_security.asp](http://www.worldtraderef.com/WTR_site/data_security.asp)]

B. Internal and External Threats to Data

Threats to data security may be classified as internal and external. These threats are to people, businesses, and the government. The Federal Bureau of Investigation (“FBI”) and the Computer Security Institute (“CSI”) have conducted an annual survey, the CSI and FBI survey, reporting computer crime and security issues for the past twelve years. Respondents to the survey are employees of governmental agencies and private businesses. The 2007 survey reported a decrease in the incidences of security breaches overall. [Richardson, 2007: 5] The following will briefly discuss key findings of each threat classification.

Internal threats to data involve someone who is authorized to access secure information of a government agency or business, but who abuses this authority by misusing the information themselves or selling it to identity thieves and terrorists. Overall, 46 of the 2007 survey respondents reported they believed they were victims of insider security breach. [Richardson, 2007: 13] However, this group did not detect any actual incidences. A narrower finding of the survey is five percent of respondents believed that eighty percent of their security breaches were committed by insiders and about thirty-six percent of the respondents believed that none of their security breach issues were attributable to insiders. [Richardson, 2007: 13] All of these findings were down from the 2006 survey’s findings of the 2006 survey. [Richardson, 2007: 13] Overall, insider security breaches occurring less frequent.

External threats to data are internet hackers and thieves not authorized to access the data intending to steal a person's identity or breach the U.S.'s national security by accessing classified documents. Other types of external threats are theft of the data storing device (i.e. laptop, computer, or mobile phone), and use of unsecured wireless networks in public places [http://www.worldtraderef.com/WTR_site/data_security.asp] The CSI and FBI survey reported percentages for numerous types of external threats. The most frequent for the 2007 survey is laptop or mobile device theft. [Richardson, 2007: 14]

C. Counter Measures

Counter measures are needed by all, including the consumer, businesses, and governmental agencies. Consumers need to be more aware when retail shopping online and all three are wise to invest in computer security software, such as firewall. Many businesses and government agencies are also investing in computer security trainings for employees.

Some ways consumers can protect their identities online are listed below. [Http://www.worldtraderef.com/WTR_site/data_security.asp]

- Install firewall on all data devices, including mobile devices and PCs
- Never save password or use credit card information on public or shared device
- Only transact on sites with a secure connection; these sites will have “//https:” beginning their web address
- Use of “scrambling” software, thus if data is intercepted, it is undecipherable

III. SECURITY MANAGEMENT

A. Policy Consideration

Numerous federal agencies have proposed and are implementing policies to solve the complex and difficult issues of data security as it relates to the average person, businesses, and

government agencies. These agencies implement policies for employees and make proposals to the legislature on how to best solve the issues of data security and national protection. However, many of these policies will take years to implement, meanwhile, data security is still heavily breached in one of several ways.

There are several areas relating to the setup of personal and company devices that are authorized to access business or government networks that policy makers would be wise to address. Considerations should include the use and authorization of, wireless local area networking, public hotspots, home networks, corporate networks, mobile phones, reporting theft or loss of devices, approved connections, authentication credentials and their use, notifying human resources and IT departments when staff are laid off or leave the company. Laws requiring these issues are addressed are crucial to improving data security and should be implemented.

B. Procedures

The E-Government Act [Public Law 107-347], passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (“FISMA”), included duties and responsibilities for the Computer Security Division in Section 303, “National Institute of Standards and Technology. [NCIS/CS WEB, CRSC home>about] The Computer Security (“CS”) division of the National Institute of Standards and Technology (“NIST”) publicizes encryption standards for use by all federal agencies. These standards or legal requirements are called Federal Information Processing Standards (“FIPS”). [http://en.wikipedia.org/wiki/Federal_Information_Processing_Standard] Many FIPS standards

are modified versions of standards used in the wider community by private businesses (ANSI, IEEE, ISO, etc.). However, some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g. country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46) and the Advanced Encryption Standard (FIPS 197) were developed by the government. [http://en.wikipedia.org/wiki/Federal_Information_Processing_Standard]

The above FIPS do not regulate private sectors and are no help there. Thus, private businesses should implement a procedure for data handling and protection that is very specific. Furthermore, rules should be established to deal with incidents of lost and stolen data. Managers, supervisors, and all employees should undergo frequent training for the purposes of enforcement of procedures, and to give updates of new issues in data security and their resolutions.

C. Physical Data Protection

Data protection by an individual with a website or personal information online must be proactive in securing their online data. Although there are laws governing data security and most legitimate businesses install security software on their websites, to receive the most protection, an individual must follow precautions they perform themselves. In some areas, the precautions are not enough, and an individual must weigh the risk of security breach against the desired online transaction.

There are several precautions provided by governmental agencies. The precautions include, installing firewall to divide internal network from external network; installing anti-virus program on all machines within the network in addition to servers; making sure all updates and patches are installed on the operating system that is hosting the website and database application; at

regular intervals, backing up all data onto a removable storage device; ensuring that all transactions are done over a minimum of a 128-bit encrypted SSL (secure socket layer) connection; and purchasing security certificate authority to assure that site is authentic and SSL encryption secures all transactions.

IV. Consequences: National Security Issue

A. Homeland Security

The Protected Infrastructure Information Program (“PCIIPP”) Program, part of the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), is designed to encourage private industry to share its sensitive security-related business information with the Federal government.

[[Http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm](http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm)] PCIIP is an information-protection tool that facilitates information sharing between governmental agencies and the private sector. DHS and other federal, state and local government analysts use PCIIP in pursuit of a more secure homeland. The primary focus is, analyzing and securing critical infrastructure and protected systems; identifying vulnerabilities and developing risk assessments; and enhancing recovery preparedness measures.

[[Http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm](http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm)] The private sector, by submitting information to PCIIP, requests protection under the Critical Infrastructure Act of 2002 (“CIA”). If information submitted satisfies the requirements of the CIA, it is protected from public disclosure under the Freedom of Information Act and state and local disclosure laws. Also protected is use of the information in civil litigation.

http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm

B. Cyber Terrorism

According to the FBI, cyber terrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents". Cyber terrorism is utilized to cause physical harm or extreme financial hardship. Possible cyber terrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Cited by an assistant secretary of DHS, the world we live in, "... is a world that operates on a vast infrastructure of information and communications systems – an interconnected network that supports and operates virtually everything we do—and everything we need—to keep our economy growing and our citizens secure. Financial services, transportation, government, emergency services, online commerce, health care, manufacturing, and process control systems. These are all functions of a robust economy and are critical to the nation. IT and communications networks support these critical infrastructures and must be protected." [http://www.dhs.gov/xnews/speeches/sp_1171386545551.shtm] It is commonly understood, protection of this system is imperative to the U.S.'s national security.

Several proposals for security have been offered by government officials. A plan to be implemented within the next ten years is to have a single, advanced integrated IP network to handle the majority of the world's communications needs.

C. Identity Theft

Identity theft occurs when someone uses someone's personally identifying information, such as, their name, social security number, or credit card number. The use is without permission and for the purpose of committing fraud or other crimes.

[[Http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf](http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf)]

The Federal Trade Commission (“FTC”) estimates that as many as 10 million Americans have their identities stolen each year.

[[Http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf](http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf)] A common type of identity theft is Government Documents Fraud where a thief is able to receive or have made a driver's license or official ID card issued in with their picture. Another act classified as GDF is where a thief gains access to another person's social security number and applies for government benefits, or files tax returns with the number fraudulently.

There is no guaranteed way to avoid identity theft, however, the risk of and damage by identity theft can be reduced by, deterring identity thieves by safeguarding personal information, detecting suspicious activity by always monitoring your financial accounts and billing statements, and defending against ID theft as soon as you suspect a problem.

[[Http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf](http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf)] Effective online safety tactics include protecting your information, knowing who you're dealing with; using anti-virus, spyware, and firewall software and updating them regularly properly setting up operating system and web browser properly; backing up important files; protecting passwords; and contacting OnlineOnGuard.gov if problems occur while online.

[[Http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf](http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf)]

Identity theft is a serious issue. Many victims suffer the loss of hundreds of dollars and hours spent just correcting the effects of identity theft.

[[Http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf](http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf)] Effects on a victim resulting from identity theft is a drop in credit score, rejection of loans and mortgages, lost job opportunities, arrest for crimes they did not commit, and extreme stress.

[[Http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf](http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf)]

V. Conclusion

Data security remains a difficult issue to solve for businesses and government agencies. Implementing training programs and awareness of the law governing data security is crucial in terms of reducing the risks and grave financial damage resulting from data security breaches. Private individuals, as well, must be proactive and aware of the precautions to reduce risks of breach and its resulting damage. Awareness of the laws regarding data security by individuals is imperative to the protection of personal data. Lastly, outside or physical threats to data security are also important, and must be proactively fought by the owner of the mobile device for full protection to exist.

VI. Ressources

1. http://en.wikipedia.org/wiki/Data_security
2. <http://www.checkpoint.com/products/datasecurity/solutions/government/index.html>
3. http://www.worldtraderef.com/WTR_site/data_security.asp
4. Richardson, R. (2007). CSI – Computer Crime and Security Survey. 5, 13, 14.
5. http://www.dhs.gov/xinfo/share/programs/editorial_0404.shtm
6. <http://www.ftc.gov/bcp/edu/pubs/consumer/general/gen20.pdf>. p. 31, 34
7. http://en.wikipedia.org/wiki/Federal_Information_Processing_Standard