WHITE PAPER

KEEPING CUSTOMER DATA SECURE: DOES YOUR COMPUTING SYSTEM VIOLATE THE CONSTITUTION?

Michael J. Mellor, CPA, DiSanto, Priest & Co.

DiSanto Priest & Co.
Certified Public Accountants

The Fourth Amendment of the U.S. Constitution's Bill of Rights established our freedom from "unreasonable search and seizure" and unlawful entry, resulting in the requirement for search warrants and, thus, securing our right to privacy. Fast forward to the 20th century, when every man's or woman's house becomes his or her "castle" and we find the U.S. Privacy Act of 1974, which was enacted to protect the privacy of personal data that is collected by the government.

PRECEDENT FOR PRIVACY

This law, although strong and broad in scope, only applies to the government, but it could be considered the precursor of subsequent laws such as:

- **The Financial Modernization Act of 1999**, also known as the **Graham-Leach Bliley Act or GLBA**, which addresses the protection and privacy concerns of personal financial information and applies to all financial institutions
- **The Health Insurance Portability and Accountability Act of 1996***,* or **HIPAA**, which specifies the privacy and security requirements related to personal health information and applies to all health care providers and similar entities
- **Children's Online Privacy Protection Act of 1998**, or **COPPA**, which specifies the rules and notification requirements related to the online collection of personal information of children under the age of 13

So how can you be sure the computing systems at the organization you work for, and others you interact with on a daily basis, don't violate these and numerous other privacy regulations?

Consider the definition of *computing systems* as defined by Pfleeger & Pfleeger (Security in Computing, 4th ed., 2007)[1]: A *computing system* is a "collection of hardware, software, storage media, data and people that an organization uses to perform computing tasks." When we use terms such as *privacy, protection* and *computing* what often comes to mind is *security* and, in the context of this article, *computer security*.

At this point, two recurring themes or concepts should be apparent; *protection of information and privacy*. Although the general rule of **no expectation of privacy** applies to employees within the workplace while using employer resources, it is reasonable to assume the goal of any organization in this modern era of electronic data interchange is to protect sensitive information. The establishment of a good security plan should provide assurance that unwanted access to sensitive data is restricted.

YOUR ORGANIZATION'S RESPONSIBILITY

Given the importance placed on organizational privacy, let us re-phrase the titular question:

- Are you confident your security plan provides adequate protection of your organization's private data as required by law?
- Do you have a good security plan?
- How do you establish a good security plan for your organization?
- What is a good security plan?

Simply stated, a good security plan is a carefully written set of security policies and practices that are supported by management, executed throughout all levels of the organization by each employee, periodically monitored and measured for its successes or failures, and, most importantly, contain a logical methodology for improvement.

According to recommendations published by the National Institute of Standards and Technology (NIST) in *Special Publication 800-30 (Risk Management Guide for Information Technology Systems)*[2], there are five goals for a good security plan:

- *Integrity* is the requirement to protect data against intentional or unintended manipulation with access restricted to only authorized users
- *Availability* is the requirement to ensure data is accessible to authorized users at the appropriate times
- *Confidentiality* ensures data is only accessed by authorized users
- *Accountability* ensures that procedures and practices are followed by authorized users
- *Assurance* helps to remediate issues regarding human error or oversight, reducing system vulnerabilities

Finding the proper balance between the intersection of the first three of these goals (*integrity*, *availability*, and *confidentiality*) is the challenge faced by all information technology security professionals. To accomplish this task, you must determine the types of vulnerabilities and threats that exist within your computing environment.

Threats to your computing system can be described as a set of actions or circumstances that can accidentally or intentionally cause harm through the exploitation of vulnerabilities (flaws and weaknesses) in your system's security plan.

Not all threats are so easily recognized, particularly threats that exist within your *computing systems* environment. Threats to your computing systems can be categorized into four specific classes – *interception, interruption, modification,* and *fabrication*:

- *Interception* is the unauthorized access of a program, file, data, or asset
    - **Example:** A hacker gains access to your organization's payroll file which is used for direct deposit transmission.
- *Interruption* is the unavailability or loss of a program, file, data, or asset
    - **Example:** The server which operates your database application has been infected with a computer virus and corrupts your payroll data table. You are unable to create the payroll file for transmission to your financial institution by the required deadline.
- *Modification* is the alteration of a program, file, data, or asset by an unauthorized individual or entity
    - **Example:** A hacker intercepts your payroll file during transmission and changes several of the account and routing numbers, thereby redirecting some of the deposit amounts.
- *Fabrication* is the unauthorized creation of fictitious programs, files, or data within your computing systems
    - **Example:** An unauthorized individual fabricated employee records within your payroll database and these records are subsequently used to generate illegal payment.

By recognizing the vulnerabilities within your organization's computer system security strategy, you will be better able to analyze, identify, and moderate the types of threats that may exist within your computing environment. This type of analysis, otherwise referred to as *risk assessment*, is just one component of a comprehensive risk management program that should be deployed throughout your organization.

As part of the development of a successful computer security plan, NIST recommends conducting a preliminary study to gain an understanding of the operational characteristics of your organization. A suggested sample of some of the information needed might include:

- Who are the valid users?
- What is the mission of the user organization?
- How important is the system to the organization's mission?
- What is the system's availability requirement?
- What information (both incoming and outgoing) is required by the organization?
- What information is generated by, consumed by, processed on, stored in, and retrieved by the system?
- How important is the information to the organization's mission?
- What are the paths of information flow?
- What types of information are processed by and stored on the system (e.g., financial, personnel, research and development, medical, command and control)?
- What is the sensitivity (or classification) level of the information?
- What information handled by or about the system should not be disclosed and to whom?
- Where specifically is the information processed and stored?
- What are the types of information storage?
- What is the potential impact on the organization if the information is disclosed to unauthorized personnel?
- What are the requirements for information availability and integrity?
- What is the effect on the organization's mission if the system or information is not reliable?
- How much system downtime can the organization tolerate? How does this downtime compare with the mean repair/recovery time? What other processing or communications options can the user access?

COMPREHENSIVE COMPUTER SYSTEM CONTROLS

It is clear, given some of the recent high-profile data breaches at Target and Equifax, that securing private information and keeping it safe from unauthorized access is currently front and center in our national dialogue. Having comprehensive computer system controls in place is critically important for conducting business in this digital age, as insufficient controls can not only negatively impact your organization's day to day operations but can have a drastic impact on your organization's reputation.

[1] *Pfleeger, C. P., Pfleeger, S. L. (2007). Security in Computing (4th ed.). Upper Saddle River, NJ: Prentice Hall.*

[2] *NIST – National Institute of Standards and Technology. (2006, December). Special Publication 800–30: Risk Management Guide for Information Technology Systems. Retrieved February 24, 2011 from* **http://csrc.nist.gov/publications/ PubsDrafts.html**.

About DiSanto, Priest & Co.

DiSanto, Priest & Co. is a full service public accounting firm headquartered in Warwick, Rhode Island with expertise in assisting companies evaluate the current risk assurance needs. Please give us a call if you need assistance, and we would be glad to talk with you about your organization's goals and objectives in this area.

Headquarters

117 Metro Center Boulevard
Suite 3000
Warwick, Rhode Island 02886
Telephone 401.921.2000
Facsimile 401.921.2010
www.disantopriest.com