Report

Of the

Office of the Chief Information Officer
And
The Office of Information Technology

To

The Joint Standing Committee on
Insurance and Financial Services

On

Public Law 2005, Chapter 379
"An Act to Protect Maine Citizens from Identity Theft"

Report of the Office of the Chief Information Officer
and
The Office of Information Technology

to

The Joint Standing Committee on Insurance and Financial Services

on

Public Law 2005, Chapter 379
"An Act to Protect Maine Citizens from Identity Theft"

February 1, 2006

Introduction & overview

As part of the Public Law, the CIO is required to report to the Joint Standing Committee on Insurance and Financial Services "regarding the State's current and planned-for policies, strategies and systems to protect the privacy and security of electronic personal information maintained by State Government."

The primary purpose of the information security strategy of the Office of Information Technology (OIT) is to protect the electronic data managed by the state's information systems. All OIT security policies and procedures are aimed at 1) keeping the data confidential and assuring that it is accessed only by those who are authorized to access it, 2) maintaining the integrity of the data, assuring that is not modified or deleted except by those persons authorized to do so, and 3) keeping the data available, but only to those authorized to access it. This strategy can be categorized as the **C-I-A** approach, aimed at ensuring the **confidentiality**, **integrity**, and **availability** of data.

The state employs a **layered approach** to information security, often referred to as a **defense in depth** strategy. OIT employs a number of defenses against unauthorized access to the state's data network, and constantly monitors the network for signs of attacks and attempts to compromise the network.

Overall protection strategy for the network infrastructure:

Personnel security, physical security, access control

Information technology employees, who are the ones with the most potential access and control of the resources that manage electronic data, are subject to background checks

before they are hired. Upon hire, all employees who handle sensitive data are provided with basic confidentiality training and sign non-disclosure agreements. Departments that are accustomed to handling confidential and sensitive material (e.g., taxpayer information in Maine Revenue Services) have detailed departmental policies regarding privacy, security, and confidentiality. Breach of confidentiality and non-disclosure agreements is grounds for dismissal from state employment.

A primary component of data security is the physical security of the critical components of the network. The most critical data processing facilities are the most secure buildings in the state. The main data processing center is attended by security guards 24 hours a day, 365 days a year. There are card key access systems to protect the most secure areas of the buildings where data processing systems are operated. Network routers and voice and data switching equipment are kept in locked rooms with card key access, keypad and pin number access, or under lock and key. Card key access systems assure that only those who have job responsibilities that require them to physically access the systems have access to secure areas where equipment is kept.

Access to components of the data processing network (network routers, servers, desktop computers, etc.) is through userID and password. The security policy requires the use of complex passwords to access system resources (minimum length of eight characters, including at least two of the following: an upper case letter, a number, or a special symbol). Policies also require that passwords be changed regularly and cannot be immediately reused. Agencies typically offer employees training in creating complex passwords that are easy to remember, but difficult to crack. In some circumstances, biometric devices are used to provide logon access to authorized employees, but this has not been deployed throughout the state system.

Security through Design: Network Architecture

DMZ or MZ – The state essentially maintains two networks, one that handles internal traffic between state agencies and another that faces the outside world. The network uses a DMZ or demilitarized zone – which could better be described as a "militarized zone" where critical defense systems are concentrated – to separate the internal network from the outside world. Publicly accessible servers are located in a "militarized zone" protected by software on dedicated server. Users do not connect directly to servers on the state's internal network and do not have direct access to state resources.

Firewall - Access to the state's network is through logical communications ports which are open for certain defined purposes. The firewall inspects not just the header information on incoming network traffic but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. In this manner, the firewall can determine whether incoming message matches the purpose for which the port is intended. If not, the packet is rejected. This prevents hackers from sending commands to commonly used communications ports in order to compromise state resources.

Intrusion Prevention System (IPS) – Dedicated hardware is placed in two key locations to monitor and control remote access to the state's wide area network. One device inside the firewall monitors traffic from users accessing the network using broadband connections (i.e. at home using cable modems and *any* access through the Internet). Another hardware device monitors the dial-in connections for users accessing the network from home or when traveling. The IPS identifies a computer virus and quarantines [blocks] the sending device, preventing it from sending further infected traffic.

Email anti-virus protection – The state has two email gateway servers that process all mail coming into the state's network from the Internet. Antivirus software is used on these servers -- and on all the state's mail servers – to assure that all mail, internal and external, is examined for harmful viruses and prohibited file types. The mail servers use antivirus software to scan email messages and attachments for viruses, worms, and other malicious code. The software is also used to block certain types of attachments and prevent them from arriving in user mailboxes. Blocked attachments are those file types most often used to contain [often in disguised format] programs that can attack the infrastructure.

Desktop and server anti-virus protection – Antivirus software on the desktop and the servers works similarly to the antivirus that scans email traffic. Installed on the desktop or server, the antivirus software scans *all* files on the hard drive for malicious code. It can remove infected files that arrive at the desktop by means other than email (loaded manually by a diskette or USB device or downloaded from the Internet, for example). It cannot repair damage caused by malicious code. The antivirus software is centrally managed across the enterprise to assure the software is kept up-to-date with the most current fixes available from the vendor. Fixes for known viruses become available almost daily, and a centralized management tool is an important part of the protection strategy.

Remote access – Although remote access was partially explained under the Intrusion Prevention section above, the state has additional measures for securing access to the state's resources from outside the wide area network. Anyone who needs to be able to log onto the network remotely has been issued a card which provides strong authentication. These cards generate an access code which changes every few minutes and is coordinated with the remote access control system on the network. The user must enter a valid access code and a personal PIN number to access the network. Then, when the user is authenticated and connected to the state's network over a broadband connection, a secure communications channel called a Virtual Private Network (VPN) is created. All traffic over the VPN is encrypted for extra security while it travels over the public data network (i.e. the Internet). Then, as explained above, the data stream is inspected by the Intrusion Prevention System to assure that it does not contain a virus or other malicious code.

Patch management – OIT uses the most current version of the Windows Software Update System to proactively push the most current software updates and security patches to the

Windows operating systems on the state's desktop computers. Hackers who want to compromise state resources are becoming quicker at exploiting known vulnerabilities of computer operating systems. Typically, when Microsoft discovers a vulnerability in its software, it prepares a patch that addresses the problem. It announces the vulnerability and makes the patch available. Hackers then have "inside information" on how to attack computers that haven't been patched. Keeping operating systems and antivirus software up-to-date is an important component of the security strategy.

Routers, switches – Network hardware is secured by userID and password. Network administrators have unique logon IDs and passwords. Default settings for network community names have been changed to make it more difficult for hackers to gain access.

Wireless – Wireless connections to the state's internal network are encrypted. Building perimeters are inspected to assure that there is a minimum of signal leakage that might allow unauthorized users to access the state's network. The network is monitored to identify activation of any unauthorized wireless access points. Default configurations of wireless access points are changed upon installation.

Agency-specific protection of personal information

The Department of Public Safety, Maine Revenue Services, and the Department of Health and Human Services [to name only three agencies] have long been concerned about confidentiality of their data and the right to privacy of the citizens whose records are being kept. All Executive Branch agencies have been polled and have conducted a recent review of their applications to determine which of them handle personal information about Maine Citizens. Across the board, state agencies have taken measures to secure their applications: password protection, restricted access to data, encrypted web access, application firewalls, audit logs of all access to servers, and other security practices have been widely implemented.

All **Department of Public Safety** internet applications are protected through the use of encrypted Secure Socket Level (SSL) browser sessions. Access to the application services requires the use of a userID and password. Application services are further protected by a set of permission rules. Credit card information is not retained by DPS applications.

The Department of Public Safety uses a set of manual and electronic procedures to protect personally sensitive information. Electronic records are protected while in transit by data encryption technology and firewalls. Most public safety computer systems maintain an audit log of all information access events. The Department of Public Safety presently operates a private data communications network to exchange criminal justice records. The Public Safety data network is in the process of being upgraded to use hardware data encryption technology to further protect information as it is exchanged between a client PC and the information storage server.

The **Department of Health and Human Services** is guided and regulated by provisions of the Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996. Although HIPAA establishes many substantial regulations for securing medical, financial, and personal records of patients and health care consumers, HIPAA does not require that providers notify patients in the event of a breach or exposure of their personal, financial, or medical information.

HIPAA makes a distinction between confidentiality, privacy, and security, but in practice, strong security measures are what keeps data confidential and ensures the privacy of the citizens.

Maine Revenue Services provides the most comprehensive employee training in the state on privacy, confidentiality, and security of the information in their trust. A culture of confidentiality has long been in place at MRS and it is reinforced by numerous federal guidelines and regulations for secure handling of taxpayer information. The Internal Revenue Service requires a formal memorandum of understanding that covers the transmission of taxpayer data to and from the IRS. The IRS provides the software to secure the transmission and underwrites the cost of a dedicated transmission.

Current/past practice in cases of data breach

In a recent incident in which a state agency discovered that personal information of employees had been exposed to the public on an Internet site, that agency notified the employees of the breach of security and offered to pay for two credit checks in the next year so that the employees can monitor activity against their financial accounts. The agency was not able to confirm that anyone had viewed the data, nor did it attempt to assess potential harm to the employees. It notified the employees of the *possibility* that their personal information had been viewed and offered a method to assure that any potential damage could be minimized. [No employee involved in this incident has reported any damage or loss.]

Plans to improve data security

Increase deployment of biometric authentication. Two agencies (Labor, PFR) are currently using biometric authentication.

Expand use of Windows Software Update System (WSUS) to deploy software security updates. We currently push current patches to the Microsoft Windows operating system to the desktop computers on the wide area network. We plan to use the newly upgraded WSUS to push out patches to the Microsoft Office products as well.

Increase use of certificates on internal network. The current architecture that supports certificate authentication of computers, users, and network components on the state's internal network will be re-designed to support wider (and more secure) deployment.

Improve hardening of network appliances and servers by creating policies and procedures for removing unused services, shutting down unused ports, and restricting use of administrator privileges.

Increase the ability for forensic analysis of desktops and servers.

Select and deploy a standard anti-spyware software product to all personal computing devices.

Improve wireless encryption technology.

Establish a data identification and data classification scheme to ensure that the state knows precisely which of its applications contain the most critical information to assure that appropriate actions may be taken in the event of data compromise.

Assign additional resources to Information Technology auditing. Perform regular information security audits of our highest-value systems. Review information handling procedures and controls.

Continue efforts to reduce reliance and/or eliminate the use of SSN# for employee identification in state's financial systems to reduce the impact of a data compromise.

Provide additional employee awareness training for information workers and for IT professionals in regards to security and for handling confidential information.

Assure that information security is integrated into all planned IT projects at inception to ensure that all new applications contain the proper controls and protection for critical data.

Recommendation/policy for breach events

The CIO and the Office of Information Technology will develop a policy that governs response to a data breach in the Executive Branch. The policy will take into account the state agencies' past practices and will adopt the same standard as that imposed upon financial institutions ("the financial institution standard" – notification of consumers if a breach has occurred and if a reasonable investigation reveals that personal information has been misused, or if there is a reasonable possibility that such information will be misused).

The CIO does not recommend statutory action to assure implementation of a policy that formalizes actions now being taken by state agencies. Further, implementation of any

private cause of action would conflict with existing sovereign immunity provided constitutionally to State Government. In January, 2007, when the 123rd Maine Legislature convenes, the CIO will deliver the completed Breach Notification Policy to the Standing Committee and make himself and his staff available for questions or discussion of the issue.