Statewide Data Privacy

August 1, 2007 to August 15, 2008
The Honorable Jon S. Corzine  
Governor of New Jersey

The Honorable Richard J. Codey  
President of the Senate

The Honorable Joseph J. Roberts, Jr.  
Speaker of the General Assembly

Mr. Albert Porroni  
Executive Director  
Office of Legislative Services

Enclosed is our report on the audit of Statewide Data Privacy for the period of August 1, 2007 to August 15, 2008. If you would like a personal briefing, please call me at (609) 292-3700.

[Signature]
Stephen M. Eells  
Assistant State Auditor  
December 10, 2008
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>1</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Portable Storage Devices</td>
<td>4</td>
</tr>
<tr>
<td>Encryption</td>
<td>5</td>
</tr>
<tr>
<td>Data Classification</td>
<td>6</td>
</tr>
<tr>
<td>Third Party Connections</td>
<td>7</td>
</tr>
</tbody>
</table>
Statewide Data Privacy

Scope

We assessed the adequacy of internal controls over data privacy at selected state agencies for the period August 1, 2007 to August 15, 2008 and evaluated policies and procedures in place to process, store, and maintain the data captured in a secure manner. The Judiciary, the Legislature, and colleges and universities were excluded from the scope of this review.

Objectives

Our objective was to determine whether personal information or other confidential information is collected by the agencies and whether adequate policies, guidelines, and procedures were in place to protect this data.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with Governmental Auditing Standards issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was issued by the International Organization for Standardization (ISO), the US National Institute of Standards and Technology (NIST), and the IT Governance Institute.

In preparation for our testing, we studied legislation, executive orders, procedural guidelines and flow charts, and industry and governmental standards for computer security and operation.

We sent surveys to 50 agencies and received back 49. The Department of the Treasury failed to respond to our repeated requests. The survey was used as a tool to gather information by asking each agency to provide details on which state and federally funded programs produce confidential data and identifying where the data is stored,
whether at the agency, at the Office of Information Technology (OIT), shared between both agencies, or held at a third party. We also inquired about the measures employed for data security such as encryption, data classification, and the existence of security policies and procedures. We also asked what legal and regulatory requirements applied to the information, such as the Health Insurance Portability and Accountability Act (HIPAA), the Open Public Records Act (OPRA), and the Federal Education Rights and Privacy Act (FERPA).

We selected seven agencies for further review to evaluate the accuracy of their responses and the strength of their controls. We reviewed the existing policies and procedures governing data security and confidentiality. We also evaluated the adequacy of policies and procedures regarding portable storage devices and determined compliance with the data security requirements of the applicable federal and state regulations.

Conclusions

The Office of Information Technology has taken significant steps in providing for the privacy of confidential data. They have named a director of IT security who is responsible for the oversight and coordination of data security, and they are working with all parties that have a responsibility for data security to coordinate privacy efforts. They continue to develop and promulgate IT security policies that provide direction for state agencies. However, more needs to be done and all state agencies must work in conjunction with OIT to protect personal and confidential information.

Per the New Jersey Identity Theft Prevention Act, "Personal information (PI) means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.” Confidential information (CI) for the purposes of this review
means any information, other than PI defined above, that the entity deemed as critical or sensitive in nature.

Thirty-seven percent (237) of the 649 programs/systems contained either PI or CI. The following chart shows the distribution of these programs/systems based on the physical location of the database.

<table>
<thead>
<tr>
<th>Location of IT Resources</th>
<th>Total</th>
<th>WITH PI</th>
<th>%</th>
<th>WITH CI</th>
<th>%</th>
<th>TOTAL PI AND CI</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agencies</td>
<td>495</td>
<td>160</td>
<td>32%</td>
<td>28</td>
<td>6%</td>
<td>188</td>
<td>38%</td>
</tr>
<tr>
<td>OIT Facilities</td>
<td>103</td>
<td>31</td>
<td>30%</td>
<td>2</td>
<td>2%</td>
<td>33</td>
<td>32%</td>
</tr>
<tr>
<td>Shared between OIT and Agency</td>
<td>36</td>
<td>13</td>
<td>36%</td>
<td>3</td>
<td>9%</td>
<td>16</td>
<td>44%</td>
</tr>
<tr>
<td>Third Party Organizations (Vendors, Partners)</td>
<td>15</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>649</strong></td>
<td><strong>204</strong></td>
<td><strong>31%</strong></td>
<td><strong>33</strong></td>
<td><strong>5%</strong></td>
<td><strong>237</strong></td>
<td><strong>37%</strong></td>
</tr>
</tbody>
</table>

As indicated above, no personal information or confidential information was held with third parties.

After reviewing the responses from the surveys and the results of our follow-up work at the seven agencies, we determined that the confidential data maintained at each of the agencies, including personal information, may be at risk of unauthorized disclosure. Our conclusion is based on a lack of existing policies and procedures governing data security, confidentiality, and portability. We have provided the seven agencies reviewed with a management letter containing a more detailed discussion of data security specifics.
Portable Storage Devices

Our survey addressed the use of portable data storage devices such as flash or jump drives, portable hard drives, floppy disks, compact discs (CDs), and digital video disks (DVDs) and how those devices are controlled. The results of the survey disclosed that of the 237 systems that contain personal or confidential information, 114 (48%) of these systems are in agencies that have portable storage devices in use. Our additional field work at the seven agencies revealed that two had no policy governing their use and three had a policy that was in draft form only. In addition, no statewide policy governing the use and control of portable storage devices has been drafted.

With the storage capability and transfer rates of the current portable devices, large amounts of personal or confidential data could be easily transferred to a portable storage device and removed from the workplace. In addition, a lack of proper disposal procedures could also place personal or confidential information at risk if data is not properly removed or the device is not adequately disabled. Any sort of uncontrolled data leakage could put the citizens of New Jersey at risk for identity theft. Industry standards require that adequate procedures be in place for the management of removable media. The procedures should cover the use, restriction, control, and disposal of these portable storage devices. Agencies have not taken the initiative to develop and implement these policies and procedures, and the lack of a statewide policy leaves agencies without guidance in the area.

Recommendation

We recommend agencies either approve and implement existing draft policies or refer to industry standards to create policies and procedures. A well constructed policy would include assignment and tracking of portable devices, encryption strategies for data stored on these devices, and proper disposal of devices to prevent data leakage. In the long term, a
Adequate policies are not in place concerning the encryption of personal or confidential information.

statewide policy on portable storage devices should be drafted and approved, and agencies should then ensure their specific policies and procedures are in compliance with OIT guidelines.

Encryption

Our survey inquired as to the agency’s encryption strategy and whether confidential data is encrypted. We found that 176 of the 237 (74%) systems containing personal or confidential information do not encrypt the information, whether at rest or in transit. The follow-up audit work performed found that six of the seven agencies visited had no encryption strategy in place and only one of those was in the process of implementing an encryption strategy. There is also currently no statewide policy in effect or in draft form requiring encryption of personal or confidential information.

Industry standards state that a policy on the use of cryptographic controls that considers the use of encryption or suitable compensating controls for the protection of sensitive information should be developed. In addition, the New Jersey Administrative Code currently states that encryption is one of the safeguards that must be in place to prevent unauthorized access to electronic files, media, or data from being considered a breach of security. It currently requires encryption on all stored or transmitted files containing personal information, with the required standard being the Advanced Encryption Standard 128-bit to 256-bit. Agencies have not taken the initiative to put encryption standards and requirements into place, and no statewide policy exists to guide agencies as to what data should be encrypted or the complexity of the encryption required. If a breach of security were to occur, the data that was accessed would be readable by anyone, greatly increasing the risk of identity theft occurring from the breach.
Recommendation

We recommend that agencies develop and implement policies requiring encryption of an adequate type, strength, and quality for data classified as personal or confidential, whether the data is at rest or in transit. In addition, a statewide policy on encryption or other compensating controls in compliance with statutes should be drafted and approved, and agencies should then ensure their specific policies and procedures are in compliance with OIT guidelines.

Data Classification

Adequate policies are not in place concerning the classification of data.

A data classification strategy is a systematic method of classifying data in terms of its value, legal requirements, sensitivity, and criticality to the organization. Our survey asked if the agency had classified its data and, if so, how the data was classified. Of the 237 systems that contain personal or confidential information, 188 (79%) have not had a formal data classification performed. OIT has issued a policy defining the classification levels for information assets and requiring all agencies to appoint a data steward and classify those assets.

Industry standards state that a data classification system should be used to define an appropriate set of protection levels and communicate the need for special handling based on the criticality and sensitivity of the data. In addition, the Identity Theft Prevention Act requires agencies to protect personal information, which would require the agency to first determine if they maintain such data elements. Subsequent to the end of our field work, OIT released IT Circular 130, Information Asset Classification and Control Policy, which adequately covers all of the necessary elements of data classification.
We recommend that data classifications in compliance with the OIT policy be performed at all agencies as soon as possible.

Third Party Connections

Our survey asked each recipient if there were any third parties that accessed, processed, or managed information systems for state programs. Of the 237 systems that contained personal or confidential information, 72 (30%) have third parties that are connected to these systems for various reasons. The additional field work found a lack of security agreements with third parties and no statewide policy has been drafted to address the security requirements for third party connections.

Industry standards state that third parties accessing (beyond read capability), processing, communicating, or managing the organization’s information should be required to enter into data access agreements covering all relevant security requirements.

Opening a connection to a third party which allows that third party to access data on state systems or to transfer data to and from state systems could make the state vulnerable to security weaknesses of the third party. Consistent and comprehensive agreements with third parties that include relevant security requirements should be developed and enforced.
**Recommendation**

We recommend that state agencies obtain agreements with third parties that have more than just read capabilities on their systems to ensure that security at the third party is adequate to protect the confidentiality, integrity, and availability of the data. We also recommend that a statewide policy be drafted and approved that sets out all relevant information security requirements for third parties entering into agreements with state agencies.