NASCIO
Representing Chief Information Officers of the States

Insider Security Threats: State CIOs Take Action Now!

NASCIO Staff Contact:
Mary Gay Whitmer
Senior Issues Coordinator
mwhitmer@amrms.com

Could This Happen in Your State?

Her reputation for being cheerful and cooperative had always preceded her during her nine-year tenure with the state. Staff at the state revenue department knew that, if they ran into a problem with the state's tax records database, they could call on Jennifer. She was known to work long hours and even be in the office on weekends. On September 28, 2006, though, her co-workers were taken aback upon opening the morning paper. Jennifer had been arrested on multiple criminal charges. The article read as follows.

"Yesterday, police arrested a state revenue department employee on charges of identity theft, computer trespass, and tax fraud. Authorities revealed that, for three consecutive years, Jennifer Adams, 45, an IT systems administrator, allegedly orchestrated a tax fraud scheme that scammed the government—and taxpayers—out of over $50,000.

A source close to the investigation said that Adams is believed to have asked for and received a user ID and password from an employee with a computer issue. She then allegedly used other employees' computers when they were away from their desks, including an IT contractor's company laptop, to access the state's database that contains the tax records of all individuals and businesses. Stealing the personal information of countless individuals who were listed as dependents on individual tax claims, she then filed returns that claimed the fraudulent dependent exemptions.

The source also said that abnormal computer logs dated after Adams was placed on administrative leave suggest that she continued to access taxpayers' personal information from her home using her state-issued laptop. Adams could face additional charges for that under the state's newly amended computer trespass law, which makes it illegal to access government or business information systems without the proper authorization. The law closes a loophole that required a computer trespasser to cause damage or harm.

Adams is expected to plead not guilty on all counts."

Months later, Jennifer pled guilty to all charges in hopes of a light sentence. At the sentencing, her attorney argued she was "a good, upstanding citizen" who had simply "hit on hard financial times" as a result of a messy divorce twelve years earlier which had left her saddled with a portion of her ex-husband's gambling debt—a fact that the criminal background check prior to her employment had failed to reveal. No one had a clue.[1]

The Overlooked Threats from Within

Media attention has primarily focused on external threats with FBI and industry reports revealing alarming hacking and identity theft statistics. Yet, threats from within both public and private sector organizations have been surprisingly numerous in recent years (see chart on page 2)[2] and can be equally if not more serious than external threats. Threats from the inside of state organizations may not have received the attention that they deserve because of the sensitivities that are present in the state government environment. Due to the high level of public scrutiny of state employees regarding legal and ethical concerns, states may not be as aggressive in their oversight and compliance efforts regarding insider security threats.

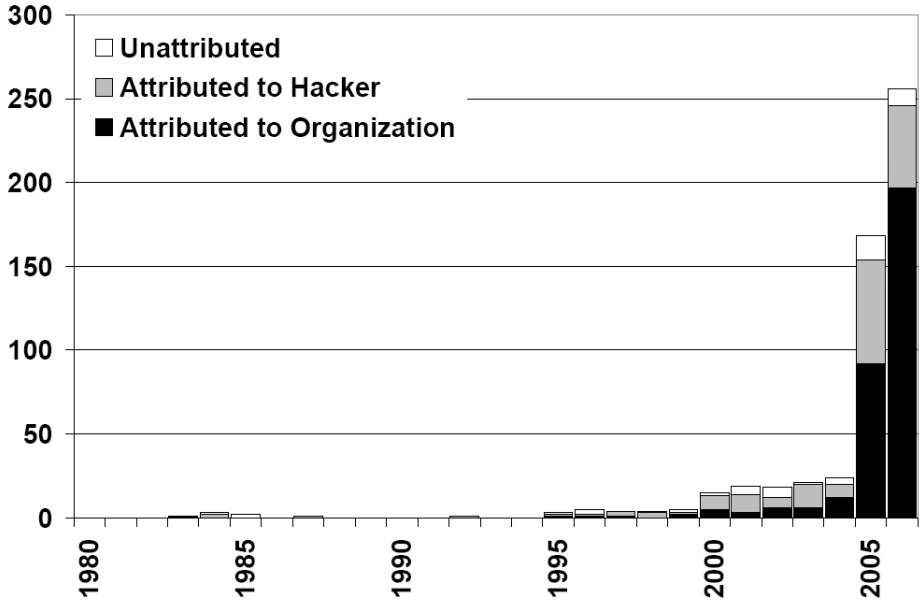
NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
Email: NASCIO@AMRms.com

1 This scenario is based on a true story. "Former IRS Employee Sentenced for Identity Theft Scheme," Press Release, U.S. Attorney's Office, Northern District of Georgia, August 29, 2005, <http://www.usdoj.gov/tax/usaopress/2005/txdv0508-29-05b.html>.

2 Erickson, Kris, and Philip N. Howard. "A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records, 1980-2006." Journal of Computer Mediated Communication 12, no. 4 (2007). The pre-publication draft is available at: <http://www.wiareport.org/documents/jcmcfullpaper.pdf>.

Hacker and Organizational Culpability in Reported Incidents of Compromised Records, 1980-2006



SOURCE: Erickson, Kris, and Philip N. Howard. "A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records, 1980-2006." Journal of Computer Mediated Communication 12, no. 4 (2007).

A cooperative approach among the state CIO, executive management, human resources, and programmatic agencies is needed to address a problem rooted in employee behavior that is inconsistent with state policies and also has implications for state IT.

While the insider threat issue must be addressed, it is not an issue that CIOs can address by themselves. A cooperative approach among the state CIO, executive management, human resources, and programmatic agencies is needed to address a problem rooted in employee behavior that is inconsistent with state policies and also has implications for state IT.

Although the information in this brief may be back-to-basics for many, such threats could be ignored to a CIO's peril. It is critical to take action on insider threats before they compromise a state's overall IT security. This brief discusses five significant insider threats and provides suggested actions for addressing them. Although the threats are listed below numerically, they are not in order of priority, as they are all important and warrant effective CIO action.

CAUTION! Top Five Insider Threats

PEOPLE:

THREAT 1: Malicious Employees (with or without IT knowledge)

THREAT 2: Inattentive, Complacent or Untrained Employees

THREAT 3: Contractors and Outsourced Services (IT and non-IT)

PROCESSES:

THREAT 4: Insufficient IT Security Compliance, Oversight, Authority and Training

TECHNOLOGY:

THREAT 5: Pervasive Computing—Technology is Everywhere and Data is on the Move

PEOPLE—GETTING TO KNOW YOUR EMPLOYEES

The insider threat begins with the people on the inside of an organization, whether they are full-time employees, student interns or even contractors. While this brief focuses on three types of individuals who are of particular concern, there are distinct categories of "insiders". Some possess varying degrees of malicious intent while others are inattentive to security and standard business processes or lack training. The list below is not intended to encompass all types of insiders, but to identify those who pose the most common risks to state IT. **Note that, at the outset of an investigation or recognition of a problem, state IT staff may not know which category or categories may be applicable to a suspect.**

Individuals with Malicious Intent to Cause Harm

- The IT Expert with a Hacker Mentality
- The Dissatisfied or Disgruntled Employee
- The Terminated or Demoted Employee
- The Fraudster Motivated by Financial Gain
- The Employee Who Wants Unauthorized Access to Information

Individuals Who are Inattentive (Non-Malicious Intent) or Complacent

- The Tech-Savvy Employee Who Gets Around Security Measures
- The One Who Just Doesn't Pay Attention
  - IT Staff
  - Non-IT Staff
- The Untrained New Guy
- The Employee without Adequate Training

THREAT 1: MALICIOUS EMPLOYEES

There are two notable types of malicious employees who may have the potential to cause significant harm or damage—one is the IT expert with a hacker mentality and intent to cause harm and the other is the disgruntled employee who causes harm typically out of the desire to "get even" with his or her employer. Let's meet them.

(a) The IT Expert with a Hacker Mentality: This person is perhaps the most dangerous of all due to his or her expertise and resulting ability to exact a significant amount of damage which could garner unfavorable headlines. This employee (or contractor) possesses a malicious, corrupt intent along with some degree of technical competence. The ill-intent may originate from a desire to cause harm for harm's sake or from an egotistical belief that IT expertise is tantamount to a get-out-of-jail-free card regarding IT security requirements.

The IT expert with a hacker mentality may hold a system administrator or other position with high-level access privileges. This can make it a fairly simple task for such an employee to drop a logic bomb (a piece of malicious code intended to cause harm to IT systems or information) into a critical state system or construct a back-door to be used in an attack after the revocation of access privileges. They also may use state IT resources for personal gain, such as running a personal business from a state office, or may prey upon other unsuspecting or untrained employees for passwords or other sensitive information.

Dealing with the IT Expert with a Hacker Mentality: Note that, with this type of insider, their lack of ethics and moral underpinnings may be no match for typical security measures, such as roles-based access and security awareness training.

- **Trust, but Verify:** Diligent monitoring and auditing of employee access to IT systems, email and the Internet may turn up abnormalities that are warning signs of such activity.
- **Swift and Severe Consequences:** Deal with such offenders in a swift and severe way, making consequences (including criminal charges) known and enforced.
- **Applicability of State Criminal Laws:** Review state criminal laws regarding computer trespass and unauthorized access for applicability to state employees and then educate state employees regarding their responsibility to abide by any such laws.
- **Focus on Professional Ethics:** Training in ethics, especially for those with greater access privileges, may play an emerging role in this area. It could serve as a reminder of the importance of integrity and the level of responsibility that accompanies IT access privileges. This training would focus on identifying and analyzing ethical problems that system administrators and others may face in carrying out their day-to-day duties.

(b) The Disgruntled Employee: While the conniving insider with a hacker mentality may be difficult to identify, the disgruntled employee who also possesses malicious intent may be easier to identify. He or she may be more apt to open displays of concerning behaviors that may be signs of IT trouble ahead. **A recent study of private sector and government IT entities revealed that most insiders acted out in a concerning manner in the workplace prior to committing their IT violations or crimes.** This highlights the important role that watchfulness by trained supervisors or other vigilant staff members can play in recognizing and reacting to a problem before an incident ever occurs.[3] Warning signs[4] for disgruntled

[3] "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," U.S. Secret Service and U.S. CERT, May 2005, <http://www.secretservice.gov/ntac/its_report_050516_es.pdf>.

[4] "10 Signs an Employee is About to Go Bad," darkreading.com, February 14, 2007, <http://www.darkreading.com/document.asp?doc_id=117323&page_number=1>.

employees may include:

- Frequent absence from work
- Changes in temperament (sometimes due to a family or other personal crisis)
- Unusual behavior in the office
- Frequent efforts to access unauthorized systems
- Changes in computer behavior or configurations (suddenly working late nights)
- Negative employee performance review
- Signs of financial distress
- An office romance gone wrong
- The termination or voluntary resignation of an employee

Some simple steps can address the bulk of the insider threats, since security breaches tend to stem from a general lack of attention to standard business processes rather than from a malicious intent to cause harm.

Dealing with the Disgruntled Employee:

- **What's in Their Background?** Background checks of all job candidates, including interns and contractors, can identify those with a record of acting out inappropriately or using questionable judgment and could prevent their hiring in the first place. A credit and financial background check can help to identify job candidates in financial difficulty. They could have an incentive to use IT to defraud the state, especially if a position has financial responsibilities or access to financial IT systems.
- **Vigilance Pays Off:** Management should be aware of the signs of a disgruntled employee who could cause damage with or to state IT resources.
- **Open Communication Channels with Management:** A reporting system for employees who witness or know of a disgruntled employee with ill-intended plans can serve as an early-warning system to management. In addition, allowing employees an official channel for the expression of grievances may prevent them from taking their anger out behind management's back.
- **Watch Them:** For problem employees, managers may consider coordinating with state IT staff to monitor their access to email, the Internet and state IT systems.
- **The Value of Audits:** Regular and ongoing audits may identify ill-intended behaviors of employees that management may not immediately recognize as disgruntled. Audits can include the review of access, activity and facilities logs.
- **The Exit Strategy:** Employees who resign or are terminated may take one last swipe at their employer through sabotage or data theft. A formal and thorough exit process can prevent such occurrences. This includes cutting off access privileges before an employee is terminated or immediately after an employee resigns if the employee appears to be disgruntled and escorting an employee out of the office.

THREAT 2: INATTENTIVE, COMPLACENT OR UNTRAINED EMPLOYEES

Although technology has advanced to the point that the average citizen (and state employee) has access to powerful technologies, such as PDAs, smart phones, and laptops, the culture of sensitivity to IT security has yet to mature to meet the sophistication of available technologies. However, some simple steps can address the bulk of the insider threats, since security breaches tend to stem from a general lack of attention to standard business processes rather than from a malicious intent to cause harm. Let's meet three of these well-intentioned yet problematic employees.

(a) The Inattentive Employee: Many state employees may not realize the risks that go along with having access to state IT resources. They may enter state government with a comfort-level regarding technology and may be desensitized to the gravity of the risks associated with even simple email applications and Internet access. Moreover, with the lines blurred between home use of technology and use in the workplace, some employees may not have a realistic appreciation for the risks to the state network that can result from checking a personal email account or just doing some random Internet surfing while on the job. Employees also are operating in a network-centric environment, which creates the possibility that a virus downloaded to one computer could infect a myriad of other computers connected to the same network.

(b) The Complacent Employee: Some employees' jobs may be somewhat routine. They may enter data into a database that contains information on AIDS patients within the state. As the task of data entry becomes more rote and mundane, the likelihood will increase that an employee may not fully appreciate what could happen if the wrong data is entered or if a mistake leads to the leaking of an AIDS patient's name.

(c) The Inadequately Trained Employee: With a vast array of decentralized agencies, it is likely that states have training and awareness practices that are inconsistent across the state enterprise. Even employees who use

technology on a regular basis in their personal lives, may not have an appreciation for security risks. These may be employees who don't understand the value of updating anti-virus signatures on a regular basis. For untrained employees, it is not a matter of intending to do harm, it is a matter of not having the requisite knowledge about IT security and standard business processes. These and other insiders have the potential to open up the state to legal liability stemming from copyright or intellectual property infringement or even illegal music downloads.

Dealing with Employee Inattentiveness, Complacency and Lack of Training:

- **Start at the Top—The Governor and Executive Management:** Educating executive management, including the Governor's office, about the importance of IT security and consequences of not supporting it can help to develop a culture of sensitivity to security. Providing management with anecdotes about the seriousness of a data breach or deletion of critical files may quickly get their attention. Garnering the support of executive management and developing a culture of IT security could help to avoid a high-profile security incident that would embarrass the Governor or other cabinet-level state officials.
- **Marketing the Message—Training and Awareness Programs:** These programs for state employees (and contractors) may range from annual IT security events to specialized training and certification for IT security staff members. They may include ongoing monthly or quarterly newsletters circulated by email or enclosed in employee paychecks or security posters taped to restroom stalls.
- **Partner with HR:** The CIO may coordinate with the state's Human Resources (HR) department to include IT security as part of broader educational programs for certain classes of employees, such as administrative assistants. Educating on topics such as phishing and social engineering can help employees secure state and personal IT.
- **Getting to Know State IT—Adequate Orientation:** A significant gap may be the lack of a consistent level of IT security orientation across the state enterprise. IT security orientation programs should be developed by the CIO's office and attended by a CIO staff member to ensure quality control. No state employees, such as executive management, should be exempt. Content may include lists of do's and don'ts. Ideally, this training should take place before an employee is permitted to access state IT resources, and new employees (and contractors) should sign security and acceptable use statements.
- **Trust but Verify:** Monitoring of email, Internet, and application use can help to identify frequent offenders in order to correct problems before they result in actual consequences. Also, security controls, such as those found in the Federal Information Security Management Act (FISMA) and publications produced by the National Institute of Standards and Technology (NIST), can prevent employees from taking actions that will result in security breaches. These security controls may include access controls, automatic screensavers, content filtering, and anti-spam applications.
- **Reporting Structure:** Mistakes will happen. However, implementing a reporting structure that encourages employees to disclose innocent mistakes (especially state IT staff) can help to identify problems at the earliest point to minimize risks.

THREAT 3: CONTRACTORS AND OUTSOURCED SERVICES

Contractors who provide both IT and non-IT-related services to the state routinely have access to the state's IT resources. With anticipated increases in the use of contractors as state employees retire, addressing IT security issues associated with contractors will become an even greater challenge than it is today. Essentially, many of the concerns regarding contractors stem from the fact that the state may not have as much control over its contractors as it does over its employees. For example, while state personnel laws are well-defined concerning employees who fail to follow state IT policies, state procurement laws that govern contractors may not be as well-defined. It also can be a challenge to ensure that a contractor who has failed to follow IT security policies at one agency will not re-appear at another agency.

Moreover, background checks and IT security training and awareness can be even more difficult to ensure, given a fairly constant churn of contractors in most states. A state may not be fully informed about an outsourced service provider's background check and IT security training practices. The fact that contractors may bring their own laptops and PDAs into the state workplace can further complicate matters by creating issues of whether the state can seize a contractor's company laptop or other mobile

Educating executive management, including the Governor's office, about the importance of IT security and consequences of not supporting it can help to develop a culture of sensitivity to security.

IT security is an issue for all of state government, because the agencies and branches are part of the larger state enterprise.

device if the contractor is deemed to be placing the state network or other IT resources at risk.

Dealing with Contractors:

- **The Rules Apply to Them, Too:** Ensure that state background checks, IT security training, and roles-based access policies apply to contractors. In particular, a state may perform background checks on contractors to ensure that a contractor's company is not relying on an incomplete or dated background check.
- **Make Sure Contracts Include IT Security-Related Provisions:** To ensure that IT security policies and procedures are legally binding, all contracts for services, whether IT-related or not, should include boilerplate language to ensure contractor compliance. Other provisions can address the security measures for data handling and audits. In the event of a security incident, the contract should address the rights and responsibilities of each party and provide the state with termination rights in the event of a particularly egregious security event. A contractor should be required to notify the state immediately upon the occurrence of a security breach.
- **Make Them Sign on the Dotted-Line:** All contractors who have access to state IT resources should be required to sign a non-disclosure agreement in addition to an acknowledgment and agreement to follow all state IT security requirements.
- **HIPAA**: For agencies that must comply with the Health Insurance Portability and Accountability Act (HIPAA), they should have business agreements with any contractors, even those working on facilities-related projects, who could have access to personal health information.

PROCESSES

THREAT 4: INSUFFICIENT IT SECURITY COMPLIANCE, OVERSIGHT, AUTHORITY AND TRAINING

Through Enterprise Architecture (EA) programs, CIO Councils, and other governance mechanisms, states have formally adopted IT security policies and processes to ensure common expectations on the part of all state employees. However, the process of documenting policies is only a first step and must be accompanied by compliance efforts and appropriate response measures for those who fail to do what they should. **Important elements for ensuring compliance are:**

- **Oversight (including Monitoring and IT Security Audits)**
- **CIO Authority**
- **Employee and Contractor Training**

(a) Oversight: The "trust but verify" model of IT compliance recognizes that verification is needed to determine if employees are meeting their IT security-related responsibilities. Various monitoring and auditing practices serve as important verification tools.

(b) CIO Authority: In addition to oversight, a state CIO needs adequate authority with respect to executive branch agencies and even other branches of government. IT security is an issue for all of state government, because the agencies and branches are part of the larger state enterprise. In a network-centric environment, many IT systems and networks are interconnected. Within this environment, a malicious employee with a hacker mentality may be surprised that his attempt to disrupt the state court system's network has just disrupted IT across the state in all three branches. **Hence, state IT security deserves to be treated in a holistic fashion across the state enterprise. The CIO's authority with respect to compliance should include the ability to work with all agencies and branches of government to ensure that an instance of non-compliance does not lead to serious IT troubles for the entirety of state government.**

For those employees who have failed to meet their IT security responsibilities, they should be met with a response process involving the CIO and other agencies, such as the human resources department and the Attorney General's office, as warranted. This process should ensure that state employees understand that IT security is part of their jobs and serious and/or continuing violations can cause termination or even result in criminal charges.

(c) Training: To reduce the number of non-compliant employees, training is the best way to communicate with clarity what employees must and must not do when using state IT. Under the purview of the state CIO, more consistent IT security training methods will produce more consistent employee expectations and skill levels across the state enterprise. That fact alone will serve to bolster a state's overall IT security posture.

Getting Your House in Order—Compliance, Oversight, Authority & Training:

- **Got a CISO?** A state's Chief Information Security Officer (CISO) understands the threats facing state IT and available options for addressing them. In fact, the state CISO is established as an IT security leader in most states. According to a summer 2006 NASCIO survey, eighty-three percent of responding states have a state CISO or the equivalent. Most state CISOs have at least some level of IT security policy responsibility and should be involved in compliance, oversight and training efforts.
- **Got EA?** A state's Enterprise Architecture program can provide a governance structure for this endeavor.
- **Got a Relationship with HR?** The misuse of state IT resources is an employee behavior problem with IT implications. The state CIO should make state Human Resource (HR) officials aware of the severity of the risks resulting from IT security violations. The CIO may also recommend that HR include guidance in the state employee handbook regarding the use of IT resources.
- **The Role of the Risk Assessment:** This can serve as a mechanism for identifying gaps in compliance and even gaps in current IT security policy and processes.
- **The Role of Automated Tools:** Identity management solutions and/or software used to monitor regulatory compliance with HIPAA and similar laws can help to ensure compliance with internal policies and procedures. Automated log reviews and software to correlate security events across the enterprise may be options as well.
- **IT Audits:** Audits of account and password practices, access privileges, configuration management, physical facility security, and IT asset inventories can provide verification of compliance. Both random and ongoing audits can maximize the potential for detecting problematic employee activity early. Note that scheduling variations for periodic audits protects against vigilant employees who scale back prohibited activity in anticipation of regularized audit schedules.
- **Training:** As discussed previously in relation to averting employee inattentiveness and complacency, IT security training should ideally start on an employee's (or contractor's) first day. Awareness and additional training should be an ongoing effort that has the full support of executive agency management.
- **Planning for the Inevitable:** Employees (and contractors) will inevitably violate state IT security requirements. A strong incident mitigation plan should have a decision-tree for when and with whom to coordinate upon the occurrence of an event. For example, the plan may provide that the CIO should notify and coordinate with the state Attorney General's Office as well as with federal law enforcement if an employee's activities rise to the level of criminal activity. Less egregious employee activities may only constitute personnel matters and could warrant disciplinary proceedings, requiring the notification and involvement of the state's HR department. A Memorandum of Understanding can be a useful tool in documenting when and how the CIO will coordinate with other agencies and departments.

TECHNOLOGY

THREAT 5: PERVASIVE COMPUTING—TECHNOLOGY IS EVERYWHERE AND DATA IS ON THE MOVE

(a) Technology is Everywhere: Technology has become a common convenience for most state employees, and they use it to manage both their personal and work-related matters. Standard interfaces to make consumer devices interoperable have provided great benefits but have also blurred the lines of technology at work and technology at home. **The ubiquity of technology in the state workplace has increased the risk of the human element exploiting risks associated with both personal and professional technologies. To counterbalance this effect, IT security must become ubiquitous, too.** It must be woven into new technologies and IT systems from their inception and be a high-priority responsibility for those using state IT resources (or using their own personal devices in a way that will not compromise the state's IT assets).

IT Security—Making it Ubiquitous:

- **Securing New Technologies and Systems:** Security must be a component in evaluating new technologies, developing new applications, and deploying new IT systems and technologies. It must be a consideration from beginning to end of an

The misuse of state IT resources is an employee behavior problem with IT implications. The state CIO should make state Human Resource (HR) officials aware of the severity of the risks resulting from IT security violations.

IT project and, where time is needed, timelines must yield to security considerations.

- **Training:** In addition to general IT security training, employees must be required to take part in training for new technologies or systems.

(b) "Take It With You" Technologies: The mobility of technology has contributed to its omni-presence in society. Mobile devices, such as PDAs, laptops and smart phones, allow state employees to conduct both professional and personal business on the go. While these technologies provide immense convenience in terms of twenty-four-seven communication and information access, they also present consequences for state IT systems and the potentially sensitive information within them. Mobile devices also can store more information than ever before. High-priority risks include:

- Theft of workplace data via mobile devices with storage capability
- IT network and system infections transferred from mobile devices or employees' home computers while telecommuting
- Unauthorized access to the state network via a remote device that is improperly authenticated or stolen
- Attacks on state IT systems carried out remotely, which provides perpetrators with more privacy than in the state workplace and less risk of immediate detection

Citizens who are placed at risk for identity theft have limited options, such as continued credit report monitoring, and may be kept wondering for years on end if they will become identity theft victims.

Securing Mobile Technologies:

- **Configuration Management:** Using configuration management to close off USB ports and other access points allows employees to bring personal devices into the office while protecting state IT systems and information assets.
- **Using State-Issued Devices:** If an employee has a business need to use a PDA or laptop, issuing a state-owned one to an employee provides the state with more control over the security measures and access controls to protect those devices. IT asset inventories and audits can ensure compliance and detect theft or issuance abnormalities.
- **Encrypt It:** For mobile devices that transmit or store sensitive information, encryption of sensitive information both in transit and at rest may be a viable option.

(c) Easy Accessibility of Sensitive and Personal Information: Citizens' personal information has been placed at risk by the fact that it is more easily accessible through technology. Gone are the days in which personal information was locked away within the obscurity of state government file cabinets. The massive storage capabilities of small, often mobile devices, such as USB drives and memory cards, have compounded this risk. As the cost of storing gigabyte after gigabyte of information has decreased, the amount of information that can be stored on a single device has drastically increased.

Moreover, even within the perimeter of the state workplace, those who become accustomed to handling personal information, especially in jobs that are somewhat routine, may be subject to forgetting about the potential impact of an inadvertent disclosure of personal information. These concerns have been compounded by headlines that are littered with news of both public sector and private sector data breaches. Citizens who are placed at risk for identity theft have limited options, such as continued credit report monitoring, and may be kept wondering for years on end if they will become identity theft victims.

Protecting Personal Information:

- **Security Measures Provide Protection:** Encryption, roles-based access, identity management systems, physical facilities access management and frequent monitoring, auditing and training—all of these measures play a role in maintaining the confidentiality, integrity and availability of personal information.
- **Executive Buy-In:** Given the high-profile risks, obtaining buy-in from executive agency management as well as from the Governor's office can be made easier by demonstrating the costly effects of major data breaches in terms of lost money, time and organizational reputation.
- **Training, Awareness and Consequences:** Employees must have a clear understanding of what a breach of citizen privacy can mean for a citizen and the steps that they must take to prevent that. They also must understand that consequences will follow for failure to comply with IT privacy protections. State HR officials must be informed of the importance of appropriately consequencing employees for such failures.

Appendix A: Insider Threat Best Practices

State Employee Awareness

Arkansas—State Security Office's Newsletter: Recent issues address protecting your data and cyberbullying and are available at: http://www.itsecurity.state.ar.us/news/newsindex.htm.

Delaware—Latrine Poster Campaign: Involved the placement of cybersecurity posters in agency restrooms. Bi-monthly distribution has grown from 40 to over 500 in the last 6 months.

Delaware—Cyber Security/Disaster Recovery Executive Briefings: These are provided to Cabinet Secretaries, Division Directors, and Elected Officials, as directed by the Governor and State CIO. Ninety-four sessions have been conducted involving 2,800 employees to date.

Delaware—Cyber Security Awareness Fact Sheet: This is in paycheck envelopes for 25,000 state employees four times per year.

Nevada—Downloadable Security Posters: Titles of posters include "Choose Cyberpals Carefully" and "Carelessness Causes Security Incidents". They are available at: http://infosec.nv.gov/Security_Awareness.htm.

Washington—Education by Video: "IT Protect it" video for state employees.

Employee Training Opportunities

California—State Employee Awareness Website: Includes resources to assist state agencies in complying with security and privacy mandates. See the webpage for a recently published brochure entitled "Top Ten Information Security Practices You Should Know". Security practices are listed separately for executives, managers and supervisors, IT staff, and employees: http://www.infosecurity.ca.gov/.

Michigan—Online Security Training (MOST): This website is for Michigan state employees. It allows them to review information and take an online quiz to measure the knowledge they obtained from training. A high enough score allows an employee to print off a certificate of accomplishment. This tool is available at: http://www.michigan.gov/cybersecurity/0,1607,7-217—108238—,00.html.

Nebraska—Security Officer Instruction Guide: Complete guide to the creation of a successful information systems security program. It includes details from creating a security team, to security audits to security awareness and training and is available at: http://www.nitc.state.ne.us/standards/security/so_guide.pdf.

North Carolina—Security Training Programs: These were part of North Carolina's broader security initiatives program that won a 2005 NASCIO Recognition Award. For more information on this state's Enterprise Security and Awareness Training Program, please see: http://www.iso.scio.nc.gov/SecurityTraining.htm. The four training programs were:

- How to Become an Effective Security Liaison
- Creating Information Security Awareness
- Certified Information Systems Security Professional (CISSP) Training
- Defense in Depth Conference

Public Outreach

Delaware—Cyber Security Email Subscription Service: This is a no-cost notification service of Information Security News, Alerts, and Advisories, including viruses, worms, phishing scams, and cyber security news from other state and local governments.

Delaware—Cyberbus: A public transit bus with a "wrap" regarding cybersecurity, it was used as a visual at the Governor's press conference on National Cybersecurity Awareness Month (October) and an estimated 15,000 citizens have seen the bus each weekday.

Delaware—School Outreach: This initiative includes outreach to administrators, teachers, and students.

Michigan—IT Security Awareness Web Portal: This solution hosts a website providing IT security information for computer users throughout the state. Launched in April 2005, this website reaches out to all citizens of Michigan, state employees, and home computer users everywhere and has received extensive national press coverage. The cybersecurity portal educates leaders on business continuity, personal privacy and the physical security of IT assets. The web portal is available at: http://www.michigan.gov/cybersecurity/.

Multi-State Information Sharing and Analysis Center (MS-ISAC): This organization of states has an education and awareness subcommittee that is working on tools for outreach to citizens, which include brochures, posters and calendars. More information can be found at: http://www.msisac.org/awareness/.

Enterprise Architecture Security-Related Resources

NASCIO Enterprise Architecture Committee Resources:
http://www.nascio.org/committees/ea/

Missouri Enterprise Architecture Security Domain:
http://www.oa.mo.gov/itsd/cio/architecture/domains/security/index.htm

Other Best Practices for Addressing the Insider Threat

Massachusetts Enterprise Security Board & Security Vulnerability Awareness, Monitoring and Remediation Group:
http://www.mass.gov/?pageID=itdmodulechunk&L=1&L0=Home&sid=Aitd&b=terminalcontent&f=organization_enterprise_security_office&csid=Aitd

North Carolina Memorandum of Understanding (roles and responsibilities for addressing security breaches):
http://www.iso.scio.nc.gov/pdf/MOU.pdf

North Carolina Administrative Assistant Training Program (includes IT security):
http://www.osp.state.nc.us/trancata/hrd-oe/Classes/AdminProfProg.html

NASCIO Award Winners

Michigan's Email Consolidation Program (including email scanning):
http://www.nascio.org/awards/2006awards/index.cfm#compendium

North Carolina Wireless Security Program:
http://www.nascio.org/awards/2005Awards/security.cfm and
http://www.scio.nc.gov/sitPolicies.asp

Appendix B: Additional Background Resources

NASCIO Resources:

Born of Necessity: The CISO Evolution—Bringing the Technical and the Policy Together, July 2006:
http://www.nascio.org/publications/documents/NASCIO-CISO_Brief_071006.pdf

A Current View of the State CISO: A National Survey Assessment, September 2006:
http://www.nascio.org/publications/documents/NASCIO-CISOsurveyReport.pdf

NASCIO Research Brief Series "The Year of Working Dangerously: The Privacy Implications of Wireless in the State Workplace—Parts I & II", 2005

Part I (*identifies wireless privacy implications*):
http://www.nascio.org/publications/documents/NASCIO-WirelessPartI.pdf

Part II (*identifies privacy policy and security measures for wireless technologies*):
http://www.nascio.org/publications/documents/NASCIO-WirelessPartII.pdf

Other Resources:

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, U.S. Secret Service and U.S. CERT, May 2005:
http://www.secretservice.gov/ntac/its_report_050516_es.pdf

Common Sense Guide to Prevention and Detection of Insider Threats, U.S. CERT, April 2005:
http://www.us-cert.gov/reading_room/prevent_detect_insiderthreat0504.pdf

Other U.S. CERT Insider Threat Research:
http://www.cert.org/insider_threat/