NASCIO
Representing Chief Information Officers of the States

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

IT Security Awareness and Training: Changing the Culture of State Government

ATTENTION STATE CIOS: IT SECURITY AWARENESS AND TRAINING MAY AVERT YOUR NEXT CRISIS!

One crisis can result in the following for state elected leaders:

- Unflattering headlines about the way the state conducts business littering the daily news
- The expenditure of taxpayer dollars for costly remedial actions, such as credit monitoring for a data breach
- Lower utilization of e-government services due to a lack of public trust in government's ability to protect citizens' security and privacy
- Approval ratings of the Governor or other elected state officials may suffer due to a security or data breach crisis that was not properly managed

The act of a single state employee, who may not intend to cause any harm at all, can result in these dramatic consequences and send the state into full-on crisis mode.

The Security and Data Breach Problem for Elected State Leaders: In an era of data and security breaches, these incidents have demonstrated that the expenditure of millions of dollars in credit monitoring fees and other remedial services can be only a part of the overall disastrous impact of a large scale data breach. Public and private sector entities have suffered humiliating headlines casting doubt on their ability to provide the most basic protections for citizens' personal information.

For state elected leaders, they have the added concern of a data breach creating a negative view of their ability to lead and of state government in general. One high profile incident can cause citizens to distrust government and be wary of its competence, credibility and integrity.

IT Security Awareness and Training as Crisis Prevention: Continuous and ongoing awareness and training activities for state employees (and contractors) could help prevent a major state crisis. For example, adequate awareness and training could have the following positive impact:

- A state health and human services agency employee learns through periodic training to always lock her computer when she leaves her desk, thereby preventing a curious co-worker from accessing sensitive government information.

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

- Another state employee who has been made aware of the sensitivity of publicly releasing Social Security Numbers, avoids posting a document to a state webpage that contains citizens' Social Security Numbers.
- A long-time state employee avoids having her bank account information stolen through an attempted phishing attack, because she attended an identity theft prevention session provided by the CIO's Office during National Cyber Security Month.

Providing continuing IT security awareness and training is also relatively cost-effective given the fact that a large data breach caused by one state employee could cost the state millions in resources and diminish citizens' trust in their government.

Since a holistic approach to security revolves around people, cultural change is needed to truly ensure that employees and contractors understand their IT security responsibilities and take them seriously.

Awareness and Training: Often-Overlooked but Effective Security Solutions

While not all security incidents and breaches are preventable, many are. Today, there are technological solutions to solve some problems created internally by state employees and contractors. Password-protected screensavers and configurations that require employees to use complex passwords are a few. However, when technology solutions reach their limitations, adequate and ongoing IT security awareness and training efforts for all state employees become an important part of improving a state's overall IT security posture.

Avoiding the Overlooked Threats from Within

In its April 2007 Research Brief entitled "*Insider Security Threats: State CIOs Take Action Now!*", NASCIO highlighted the fact that many security breaches in the states originate from within state government, as opposed to externally as a result of hackers or identity thieves. In fact, according to recent research conducted by the University of Washington, the number of incidents of compromised records originating from within far outweighs those incidents caused by external sources by a margin of 4-to-1.[1] Suggesting that insider threats may be overlooked by leaders in the states, the brief discussed common internal threats such as inattentive, complacent or untrained employees and contractors. The brief also suggested that much of the insider threat is not caused by malicious employees' intentionally destructive acts, but by those who may not understand the importance of IT security. Part of the solution suggested by the brief is sufficient and ongoing IT security awareness and training efforts at all levels of government.

This brief will examine important aspects of awareness and training that every CIO should know and will provide examples of awareness and training efforts that are working in other states.

Security and Cultural Change

One goal of IT security awareness and training is ensuring that state employees recognize IT security issues when they arise and know how to protect the state's IT resources and themselves when carrying out their daily duties. However, the ultimate goal of sufficient security awareness and training involves a holistic effort to ensure that every state employee has an understanding of his or her responsibility and accountability for the protection of state IT resources. Such awareness and training efforts also are much broader than just IT and involve protecting citizens' and other sensitive data as well as physical facilities security. Since a holistic approach to security revolves around people, cultural change is needed to truly ensure that employees and contractors understand their IT security responsibilities and take them seriously.

Technology has become ubiquitous not only in state government but also in society at large. Most state employees are familiar with what technology does to make their work and lives easier and more efficient. However, the awareness of the security risks posed by the vast array of readily available technologies has not kept

pace with state employees' use of technology. In order to ensure that state employees properly use state IT resources as well as their personal devices that they may use partially for work purposes, IT security must become as much of a part of society's fabric as technology has become.

Within the state government context, state CIOs must view IT security awareness and training as an ongoing and continuous effort that will require a cultural shift in the way state employees perceive IT security and take it on as part of their responsibilities. The distributed nature of state IT systems and networks, and the prevalence of technology in society have made one simple principle clear: IT security is everyone's job. It only takes one weak link to compromise the entire state network or a critical IT system.

Employee Performance Evaluations and IT Security: One way that state CIOs may consider driving the point home to state employees that IT security is part of everyone's job is to make compliance with IT security policies and procedures part of an employee's performance evaluation. This effort would likely stem from a partnership between the state CIO and the state's human resources or personnel department.

Doing What's Right—The Ethical Side of IT

Included in creating a more IT security-conscious state workforce is building within state employees a sense of the ethical use of state IT resources.

A step beyond issues related to compliance with state IT security policies, cyber-related ethics issues deal with whether certain behaviors using IT resources are appropriate in the state government workplace. The ethics questions differ depending upon where a state government employee stands. For state Chief Information Security Officers, these questions revolve around how strictly to enforce acceptable use and IT security policies and deciding which behaviors are definitely over the line. On the other hand, for most state employees, the question is whether their online behaviors, such as carrying-on in-office flirtations via their state email accounts, checking personal email accounts, online shopping or visiting a social networking website at work, are appropriate for the state workplace.

While ethics connected with cybersecurity issues has been a somewhat controversial topic within the IT security community regarding its effectiveness, it could be an emerging line of training that states may consider in concert with other awareness and training activities. Instead of dealing with high-profile topics like spam, spyware and data protection, cybersecurity ethics examines the underlying philosophical questions that impact lifestyles and employees' online behaviors. It would likely blend values, ethics and cybersecurity training and encourage proactive steps employees can take in the pursuit of better IT security.[2]

Consistency—A Key to Cultural Change

Cultural change to the fabric of the state government workforce is needed to make IT security and the ethical use of state IT resources as ubiquitous as technology. Since that cultural change involves changing the way that state employees perceive IT security, consistency and patience are necessary ingredients. Isolated presentations or training sessions, while a good start, will not lead to the creation of a long-term culture of IT security. After all, state employees, like everyone else, have many plates to juggle and may not retain the entirety of the awareness and training content to which they have been exposed, especially upon the passage of months or years. Hence, regularized and constant reminders in many forms are needed to enact this cultural shift. *Such holistic, multi-channel efforts will likely be multi-year initiatives with visible results that may not be evident until a year or two into the project.*

In addition to regular and ongoing awareness and training efforts, state CIOs must

ensure the vitality of the state's awareness and training efforts. This involves the ongoing review and assessment of awareness and training efforts' effectiveness and responsiveness to emerging threats.

However, with many competing priorities, states may have to implement IT security awareness and training on a piecemeal basis. Many of the examples contained in this brief can be implemented as standalone efforts that could later become part of a more holistic approach to IT security awareness and training.

Creating the Security Baseline

Awareness and training efforts come into play after risk assessments are completed and policies and security measures have been implemented. However, preliminary steps to assess the current status of a state's security awareness and training efforts may provide a foundation for the later implementation of awareness and training programs. Some of these preliminary steps include:

- **Know What You've Got:** Inventorying all state IT systems and networks and identifying the sensitive or personal information within them, so the right individuals handling that information and using those systems get the right training
- **Know What Awareness and Training Activities are Already Taking Place:** Assessing (possibly through a risk assessment) when and how state agencies are conducting IT security awareness and training and whether those efforts appear to be effective and where awareness and training gaps may exist
- **The Enterprise Architecture Piece:** As part of a state's overall Enterprise Architecture (EA) program, awareness and training should be addressed within the state's EA security domain
- **The Policy Piece:** Crafting and implementing policies that support awareness and training programs across the enterprise
- **The Use of Available Technology Solutions:** From configurations that require employees to select complex passwords to encryption to data leakage technologies, there are solutions that states can implement to take the "human factor" out of the equation. This not only helps to ensure IT security compliance but also helps to protect employees from violating state IT policies and practices.
- **Audit, Compliance and Enforcement:** Audit, enforcement and compliance efforts will help determine where additional training may be needed or if training is not effective for some employees, such as those who are persistent violators of state IT policies.

With an established baseline, a state CIO may then draw observations from the baseline in order to identify areas of need regarding security. For example, security policies may be in place but are not vigorously enforced or taken seriously by state employees. From identified gaps in awareness and training, state CIOs may then develop targets for which to aim in terms of improving the state's overall IT security posture. These gaps in awareness and training will also be helpful in reaching out to partners in state government, such as the state's human resources department, to make the point that increased awareness and training efforts deserve additional attention and resources.

What Are Other States Doing?

IT Security Assessments—State of Kansas: During agencies' annual security self-assessments, they must identify training efforts that have taken place and opportunities for future training.

Risk Assessments Regarding Social Engineering—State of Texas: The State's Department of Information Resources conducted penetration testing of many agencies to determine if agency employees were vulnerable to phishing and other types of attacks that use social engineering. This helped to identify agencies' training

needs and build the business case for funding that training.

The Policy and Enforcement Pieces—State of Alabama: Alabama has enacted a training and awareness policy based on the standards of NIST (the National Institute of Standards and Technology). It applies to contractors and employees, and includes enforcement provisions and content and procedural guidance for awareness and training programs.

The Multi-Branch Policy Piece—State of Delaware: This state's broad information security policy includes awareness and training provisions and covers all three branches of state government in addition to 19 public school districts and 17 charter schools.

Enterprise Security Architecture—Commonwealth of Pennsylvania: Awareness and training are included as a critical part of Pennsylvania's overall Enterprise Security Architecture.

A Word about the Differences Between Awareness and Training

While "awareness" and "training" are often combined together much of the time, they are distinct and separate concepts and are both integral parts of an effort to improve a state's IT security posture.

- **Awareness:** These efforts are meant to focus attention on IT security and help the recipients to recognize common risks and to respond appropriately. For example, awareness presentations may address ways to recognize phishing attacks. The audiences for awareness efforts are normally recipients of information, as opposed to being active participants. The goal of awareness is to reach a broad audience. Marketing tactics may be used to accomplish this goal.
- **Training:** This is more formal and has the goal of building knowledge and skills to help employees do their jobs in a way that will not compromise a state's IT resources. In training, participants are expected to take an active role and may be asked to engage in exercises meant to help them apply the concepts introduced in the training.[3]

The relationship between awareness and training is that awareness is the foundational level upon which training efforts can be rolled-out.

Making State Executives Aware

Raising awareness among high-level government officials, including Governors and legislators, is likely the first critical step when embarking upon increased IT security awareness and training efforts. While awareness presentations will assist high-level government officials in making informed decisions regarding a state's IT resources, it will also help to garner their buy-in for making the business case for the expenditure of state resources on awareness and training efforts. Visible support from the Governor and even legislators will also signal to all state employees as well as citizens the importance of paying attention to IT security.

Visible support from the Governor and even legislators can also signal to all state employees as well as citizens the importance of paying attention to IT security.

Although the approach will vary from state-to-state, common success factors include finding innovative ways to demonstrate the importance of IT security and what may happen if the state does not take appropriate awareness and training actions. An example is a presentation that begins with the scenario of a state data breach and includes an attention-getting slide with a "ripped from the headlines" feel that will provide government officials with an understanding of how inadequate awareness and training can easily translate into unfavorable headlines. Part of the challenge is to show state executives in clear terms the cascade of negative consequences that will likely result from being in "reactive" instead of "proactive" mode.

Other important points for a presentation to executive-level officials include the following:

- Security incidents caused by those inside state government undermine citizens' trust in government
- The credibility of government in citizens'

eyes to conduct business in a competent fashion can be greatly diminished by one act of an untrained or unaware state employee
- Substantial disruptions to the state's daily business operations may occur in some cases as a result of a single security incident
- The consequences of security incidents resulting from the actions of state employees necessitate action on IT security awareness and training—it should be mandatory—not optional.

State CIOs also should be cognizant of conducting these presentations in a way that dispenses with the use of technical jargon so that non-IT officials can easily understand the value of IT security awareness and training.

Visible support from the Governor and even legislators can also signal to all state employees as well as citizens the importance of paying attention to IT security.

To foster trust early-on with state executives, state CIOs may consider proposing measures of effectiveness, such as scorecards or other types of reports to measure where awareness and training gaps exist and where progress has been made. This builds-in accountability to awareness and training efforts and sets the stage for an ongoing, long-term focus on awareness and training to improve the state's IT security posture.

Finally, consistency is a key factor. One isolated presentation does not make for adequate awareness. Presentations on an annual or more frequent basis can help to keep IT security at the forefront of government officials' agendas so that executive and legislative support does not wane over the long-term.

What Are Other States Doing?

Executive-Level Awareness—State of Delaware: Delaware conducted an executive-level IT security awareness presentation that started with the Governor's cabinet. The Governor then requested that the state CIO cascade the presentation to all department leaders. Over 3,000 employees have seen the presentation, which is anticipated to focus on all employees and not just senior and middle-management.

Agency Head Awareness—State of Alabama: This state's policy requires that each agency have an awareness and training plan that is approved by each agency head. Through this requirement, agency heads are involved and ultimately responsible for plan implementation. Thus, responsibility can quickly elevate the importance of this issue for agency leaders. The state CIO's office also provides high-level security briefings for the upper management of agencies.

Legislative Awareness—Commonwealth of Pennsylvania: To build awareness among legislators and citizens, Pennsylvania conducts an annual "Security Awareness Day" at the state Capitol to raise awareness.

The Results of Awareness—North Carolina: Discussing the results of an IT security risk assessment with government officials and legislators, the state CIO obtained enterprise funding for IT awareness and training. North Carolina's CIO now offers free training for executive branch agencies. Local governments and universities can also participate in the training for a nominal fee.

Building the Business Case

While there are low cost steps that states can take towards improving awareness and training, obtaining enterprise-level funding for such efforts is ideal. Funding helps to provide not only resources for awareness and training but also serves as a signal of state executive leadership's support for a culture of IT security.

While the business case for awareness and training funding will be state-specific, it is important to point out that awareness and training can substantially reduce the security risks caused by untrained, inattentive or complacent employees or contractors. Moreover, the cost of a single data breach incident holds the potential to be very high. As reflected in a 2006 study by

the Ponemon Institute across 15 industry sectors, the average cost of a data breach totaled $4.8 million.[4]

In addition, targets, goals and measurable objectives identified by the creation of a baseline and observations made therefrom can play a part in supporting a business case to show what actions the state CIO proposes to take to address employee awareness and training needs. This also helps to build accountability into an awareness and training business case. Finally, the use of technology to conduct awareness and training efforts can support a business case through making those efforts cost effective. For example, online training or streaming videos can save both time and financial resources.

A Note on State Homeland Security Grant Funding: A successful business case might even be incorporated into a plan to use a portion of the State Homeland Security Grant (SHSG) funding from the U.S. Department of Homeland Security for IT security awareness and training.

What Are Other States Doing?

Business Case for Online Training Tool—State of Utah: This state supported its business case for an enterprise online IT security training tool by citing the time that would be saved by employees in terms of travel time to in-person training and reduction of time spent by agency security personnel providing awareness and training and answering employee questions. In addition, online training saves costs in terms of travel, facilities and dedicated trainer costs.

Business Case for Overall Security Program that Includes Training and Awareness—State of Michigan: Michigan's Department of Information Technology identified that citizens want web 2.0 transactions. However, a survey of Michigan citizens indicated that they were more afraid of identity theft than job or home loss or a terrorist attack. These findings supported Michigan's "Security 2.0: Next General Security" program that includes awareness and training efforts.

Making It a Group Effort

Improving, enhancing or even building an awareness and training program from the ground-up may present opportunities for the state CIO to partner with other agencies or even branches of government. In building a culture of IT security across state government, creating or leveraging relationships with other agencies and entities can help to spread the word about awareness and training opportunities. As previously mentioned, an example of partnering on IT security awareness and training may involve the state CIO's coordination with state human resources officials to include compliance with IT security as an element of every state employee's performance evaluation. Such an effort would help to ensure end user compliance and identify and address instances of non-compliance.

Improving, enhancing or even building an awareness and training program from the ground-up may present opportunities for the state CIO to partner with other agencies or even branches of government.

NIST encourages "broad cross-organizational strategy at the executive level bringing together various functions and organizational entities that may not have worked together."[5] To this end, the state CIO may consider partnering with the state's human resources department, risk management office and/or the state attorney general's office to identify awareness and training needs and develop programs to address those needs.

The state CIO also should consider opportunities for partnerships with the private sector. For example, a state IT contract may be drafted to include security training for state employees provided by the private sector vendor. Such training efforts could focus on security as it relates to the vendor's products or services or the training could focus on IT security more generally. Either would be of benefit to state employees as well as the state's IT security program.

While making state employees aware of IT security is paramount, so is providing the same awareness and training for state contractors.

Keeping the Agency Security Officers in the Loop: Agency-level IT staff may include security officers. Keeping them apprised of awareness and training opportunities and IT security-related issues can help them raise awareness with agency employees. For example, Alabama provides a listserv for agency information security officers. The state's Information Security Officer in the CIO's Office provides updates on security-related information as it becomes available. Similarly, the Commonwealth of Pennsylvania also holds CISO Roundtables as learning sessions with guest speakers.

Other states' efforts to engage agency-level security and other IT staff include the State of Texas, which provides periodic cyber-security forums and conferences, including an Annual Cyber Security Forum, and information on security-related educational opportunities that might interest agencies' Information Security Officers. The State of Nebraska also provides a guide for agency Information Security Officers that contains detailed guidance for setting up an information security program at the agency level.

What Are Other States Doing?

Collaborating with Human Resources/ Personnel Departments—State of North Carolina: This state CIO's Office coordinated with the state's personnel department for IT security training as part of a larger executive assistant training course. Topics included spam, phishing and spyware, security and online collaboration tools, and telephone communications.

Forging New Partnerships—State of Utah: Through its new online training tool for IT security, Utah's CIO forged new relationships with the state's Risk Management and Surplus Property Departments, and the Bureau of Criminal Identification.

Participating with State Security Officials: The state of Florida's CISO is a member of the Florida Domestic Security Law Enforcement Terrorism Committee and has partnered with the state's Domestic Security initiative to build a business case for Cyber-funding that includes training on awareness and basic training for security managers.

Marketing the IT Security Awareness Message to State Employees

Again, innovative approaches may serve to spark IT security awareness in the minds of many state employees. By starting with a marketing campaign of sorts for IT security, a state can start to build a culture of IT security vigilance.

Don't Forget About Contractors! While making state employees aware of IT security is paramount, so is providing the same awareness and training for state contractors. Regardless of whether a contractor will be performing IT or non-IT related tasks, most contractors will use a state's IT resources, including handling state government information, in some capacity. Therefore, awareness and training programs should apply to contractors. Requiring contractors to sign IT security and acceptable use acknowledgements as well as crafting contractual provisions requiring compliance with state IT awareness and training requirements are ways to guard against security incidents that originate from contractors' use of state IT resources.

Starting the Awareness Process: To begin the process, some states have built their awareness efforts around a recognizable logo or brand. Whether crafted in-house or professionally, all security awareness and training materials, including pens, notepads or post-its, can be embossed with the logo or brand. For states that do not have adequate resources to retain an advertising firm and that do not have on-staff expertise, the state CIO may consider requesting input and assistance from state marketing officials, such as public information officers, even if those officials are located in other departments.

To signal support for a culture of IT security, some states have made security awareness and/or training mandatory either by policy or by Executive Order. While this does ensure that state employees must engage in the required awareness-raising activities, awareness programs that are not mandatory can still be effective.

Whether required or not, there are a variety of methods of raising IT security awareness. These can include reminders about the importance of IT security with posters or trinkets. Other ways to provide more detailed information are through IT security newsletters, paycheck inserts or email subscription services for IT security alerts and news. State CIOs should also keep in mind that they may be able to leverage existing resources in order to raise awareness. An example would be including an IT security-related article in an agency's newsletter.

To cover a wider range of IT security topics and to gain an even more memorable impact, in-person presentations provide a means of allowing a more interactive experience during which state employees can ask questions and begin to think about IT security as it applies to their respective corner of state government. However, more cost-effective methods, such as online videos or even conference calls, provide mechanisms for spreading the IT security awareness message. Some states also hold Annual IT Conferences, which likely include IT security awareness presentations. Attendees to such conferences normally include state government employees as well as local government and university employees.

States seeking to raise awareness may consider implementing a multi-channel approach to reach citizens through a combination of mechanisms that have a broad reach into the state government employee population.

What Are Other States Doing?

A Multi-Channel Approach to Employee Awareness—State of Delaware: The Department of Technology and Information worked with state marketing officials on a multi-channel awareness-raising campaign that included: a "latrine" poster campaign (posters in restrooms that are available to agencies and change regularly), paycheck inserts, an email subscription service, and the development of a logo and brand by an outside advertising firm

Brand It! Three States' Branding Efforts: digiKnow (Delaware), SecureFlorida.org (Florida), and SecurITy (Wisconsin)

Gotta Do It—Making it Mandatory—States of Alabama and Pennsylvania: Either through policy or Executive Order, IT security awareness for state employees is mandatory in some states, including Alabama and Pennsylvania.

IT Security Websites Abound: Many states have developed IT security and cybersecurity websites with tips, newsletters, resources and even videos. For examples of state IT security websites, please see Appendix B.

IT Security Newsletters—States of Arkansas and South Dakota: Some states have security newsletters that are available online, including South Dakota and Arkansas' State Security Office, that cover topics ranging from safeguarding data to cyberbullies.

Posters with IT Security Reminders—States of Delaware, Iowa, Pennsylvania, and Nevada: States such as the ones listed above use posters with catchy slogans and pictures that serve as security reminders. While some states may create their own, sample posters are available from the MS-ISAC, private sector sources and NIST.

Beyond the usual focus of IT security awareness and training on state employees, some states are now broadening those efforts to encompass IT security awareness for citizens, businesses, local governments and even children.

Beyond State Employees—Building Citizen Security Awareness

Beyond the usual focus of IT security awareness and training on state employees, some states are now broadening those efforts to encompass IT security awareness for citizens, businesses, local governments and even children. These efforts tend to focus on the basics to help citizens secure their personal IT resources, such as desktop and laptop computers, and to help them identify and deal appropriately with scams they may encounter on the Internet.

Through raising awareness with the citizenry at large, a state CIO will facilitate an overall culture of IT security, which will help everyone use technology to their benefit, not their detriment. Moreover, citizens who are made aware of IT security's importance are likely to pay closer attention to IT security if they join the state workforce.

A common mechanism that some states are using to reach citizens is a specially designed website with resources intended for citizens. ***Written in understandable language that is not technical in nature, much of these websites contain information for citizens on how they can protect their computers and stay away from Internet predators and scams.*** Common elements of many of these websites include:

- Tips on securing personal computers
- Tips for spotting scams and avoiding identity theft
- Sections on how children can safely explore the Internet
- IT security newsletters
- IT security alert email subscriptions
- Links to and information about tools for "cleaning" computers infected with viruses, spyware and the like
- Information for those who have become victims of identity theft
- Online video training for citizens
- State IT security laws, policies and recommended best practices
- Quizzes to test citizens' IT security knowledge

Please see Appendix B for examples of state IT security websites.

In addition to IT or cyber security websites, other methods of delivering the message of IT security awareness to citizens include posters, T-shirts, crawls on the Weather channel local forecast, stickers on the front-page of the newspaper with the IT security brand or logo, and Public Service Announcements (PSAs) on the radio, TV and even movie screens prior to the showing of the previews.

To leverage existing IT security awareness efforts, state CIOs may consider linking state awareness activities to National Cyber Security Awareness Month, which takes place in October. A program of the National Cyber Security Alliance (NCSA), it encourages organizations to place a banner on their websites about National Cyber Security Awareness Month and hold a cyber security awareness day, among other activities. States as well as NASCIO have participated with this effort through issuing press releases, proclamations and conducting other activities to raise awareness of security with state employees as well as citizens. Schools and educational institutions are also encouraged to participate in National Cyber Security Awareness Month.

What Are Other States Doing?

Taking it to the Streets—State of Delaware: The state's Department of Technology and Information worked with a local design firm on a "wrap" for an intra-county transit bus that focused on the theme of personal computing safety. Thousands of citizens saw the bus each day.

Taking it to the Citizenry—State of Michigan: In fall 2007, the state will hold a town hall meeting on cybersecurity and protecting children online. This activity is being conducted at the request of a state legislator.

Taking it to the Schools—State of Wisconsin: The state's Department of Enterprise Technology has conducted awareness-raising presentations to educators, principals, and others on teachers' in-service days. The state is currently examining possibilities for rolling awareness activities into school children's computer classes.

Taking it to the Locals—the MS-ISAC: The Multi-State Information Sharing and Analysis Center (MS-ISAC), an organization of the states that provides mechanisms for cyber security readiness and response for state and local governments, has many cyber security awareness materials that can be tailored to specific states and, in particular, to local governments.

Taking it to Those Who Want to Learn More—State of Florida: This state has developed the C-Safe in-person security awareness and training program that can be tailored to individual business' and organizations' needs.

Making It Formal—IT Security Training

The approach that NIST has taken is to emphasize training criteria or standards rather than content or curricula and focus on job functions, roles and responsibilities as opposed to job titles and classifications. Training is broken out into beginning, intermediate and advanced levels. The NIST guidance recognizes that some employees may need several different levels of training because they have multiple roles to fulfill to perform their job duties.[6]

State CIOs may begin by examining what training is currently taking place and where the gaps that need to be addressed are. Common examples of gap areas include training for both IT and non-IT contractors as well as training for employees and contractors that takes place before access can be granted to any state IT resources.

A Note on Paper vs. Electronic Information: State CIOs also may consider whether training should encompass only electronic resources or include paper resources that may contain sensitive or personal information. While a data breach that exposes electronic information may impact more individuals, data breaches involving paper have the potential to occur more often. For example, a common gap is that employees may not know to shred printed documents that hold individuals' credit card or Social Security Number information. Leaving such information in a garbage dumpster leaves it open to exposure to those with ill-intent (such as "dumpster divers"). Since some information that is initially in electronic form may find its way into paper form, there is a close connection between security training regarding sensitive electronic information and sensitive information in paper form.

Training, with a more in-depth focus on IT security and steps employees (or even citizens) can take to protect themselves and IT resources, can cover a broad range of areas depending upon the audience. See Appendix D for lists of potential topics and delivery mechanisms. Content can range from an emphasis on data protection, such as with Utah's online training tool, to courses that focus on incident response training, risk management and state information security manual training, which are available through North Carolina's state CIO Office.

Important state CIO considerations for any IT security training program include:

- What are the target areas of the state government employee population? New employees? State IT staff? All employees?
- How will training be "cycled" through state employees? How often will they receive training?
- How will employees who work night shifts or irregular schedules receive training?
- How will uncooperative agency employees be handled if they refuse to participate in training? Will agency

supervisors have the authority to require the training?

Finally, the state CIO may look to strategic partners, such as universities, which can be helpful in providing content as well as innovative training delivery mechanisms that may include online training or training by streaming video.

What Are Other States Doing with Online Training Tools?

Michigan: Michigan Online Security Training (MOST) has four parts: at work, at home, government laws, and business issues. It can be taken anonymously by anyone, including citizens. State employees can register to take the training and receive a certificate if they obtain a sufficient score and can sign-up for notices of MOST updates.

North Dakota: Security Training, Awareness and Reference Tool (START) is for state employees and others who want to use it and includes common IT security terms, vulnerabilities, and ways to protect IT resources. The tool includes a wide range of topics from PC security to Internet usage to telephone issues.

South Dakota: This state's online security training system includes an Information Technology User Security Guide with IT security policies and procedures for state employees and contractors. All current state employees were required to take this course and each new state employee takes the course at his or her new employee orientation period.

Tennessee: This state's Cyber Academy is an online tutorial that includes lessons on all types of computer security issues with quiz questions interspersed throughout. Anyone can take this online quiz, although it is geared to state employees.

Other States with Online Training Tools: Indiana, Oregon, Utah, and West Virginia.

What Are Other States Doing with Other Types of Training Tools?

Training by Video:
Michigan: *Protecting State of Michigan Sensitive Information* is a 4 minute data breach training video that anyone can view.
Delaware includes videos from a variety of sources

In-Person Training:
Delaware
Florida
North Carolina

Specialized Training:
Delaware and Michigan: Both states coordinate CISSP training and certification of IT security staff.

Training/Tabletop Exercises:
Delaware: An annual interactive full-day tabletop exercise designed to simulate a real-world cyberattack on the state's information resources. The 2006 exercise covered technical implications of a pandemic and what it means for Delaware government and citizens.

Pennsylvania: The Commonwealth held a cross-agency cyber security training exercise in which eleven agencies participated over two days in the table-top exercise. A lessons learned discussion followed resulting in a formal report. Pennsylvania also participated in the MS-ISAC's Cyber Tempest (a regional effort with five states participating). In addition, the Commonwealth will be participating in DHS's Cyber Storm II in 2008.

In the Final Analysis—Are They Working? Measuring Effectiveness and Accountability

Since funding for many state IT security priorities, including awareness and training, may be limited, it is important to demonstrate the effectiveness of such efforts. Measuring effectiveness may focus on measuring progress on desired outcomes or progress in cascading training and awareness through the state government employee population or a combination of the two.

For states seeking to measure ultimate outcomes, they may examine how close the state is to having no security incidents or compromised computers resulting from employee mistakes or malfeasance. Actual outcomes may also be measured against the state's IT security goals.

States also may measure their progress on training targeted segments of the state government employee population. It is important to note the difference between measuring the number of state employees who have received one or more types of IT security awareness or training and the number of seats filled at each awareness or training session. Some state employees may attend multiple sessions, while others may attend no sessions at all.

The results of compliance measurement efforts may be helpful, too. These could include instances of noncompliance as identified in employee performance evaluations or instances of noncompliance identified through "walk-arounds" by state IT staff during off hours.

While some state CIOs may not currently have responsibility for IT security awareness and training, state CIOs typically will be attributed at least some measure of responsibility in the face of a security incident created by the conduct of one or more state employees. Given this, a state CIO may consider requesting the responsibility for awareness and training efforts and that the Governor support efforts to make such activities mandatory for state employees.

With clearly defined targets and measurable objectives, the state CIO can track and demonstrate the ongoing effectiveness of awareness and training initiatives and identify areas in need of attention. Progress on IT security awareness and training may also become a part of the state CIO's scorecard or report on agency compliance.

Conclusion—Creating a Culture of IT Security is an Ongoing Journey

Since the threats are ongoing and ever-evolving, state IT security awareness and training activities must be ongoing as well. The state CIO has an important role to play from getting the initial executive buy-in for such efforts to ensuring that state employees are using what they have learned and are complying with state IT security policies.

Important points for all state CIOs to take with them when embarking on this continuous journey include:

- Understanding that IT security awareness and training efforts must be continuous, multi-year efforts
- Following-through on measuring the effectiveness of awareness and training efforts will help to maintain the continuing vitality of such activities
- The state CIO cannot "go it alone". From executive buy-in to the support of other state agencies, such as the human resources department, and the private and academic sectors, partnerships among interested stakeholders can prove to be invaluable.

A final point for state CIOs to remember is that the states as a collective and others are taking innovative, cost-effective approaches to IT security awareness and training. This brief is a step towards helping the states to share these innovations with each other.

Appendix A: Additional Resources

NASCIO Resources
"Insider Security Threats: State CIOs Take Action Now!" April 2007

"Keeping the Citizen Trust: What a State CIO Can Do To Protect Privacy," October 2006

"Born of Necessity: The CISO Evolution—Bringing the Technical and the Policy Together," July 2006

View these NASCIO Research Briefs at: http://www.nascio.org/publications/researchBriefs.cfm.

A Current View of the State CISO: A National Survey Assessment, September 2006

View this NASCIO survey at: http://www.nascio.org/publications/surveys.cfm

Other Resources
"Building an Information Technology Security Awareness and Training Program," the National Institute of Standards and Technology (NIST), Special Publication 800-50, October 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

"Information Security Training Requirements: A Roles- and Performance-Based Model," the National Institute of Standards and Technology (NIST), Special Publication 800-16, April 1998, http://csrc.nist.gov/publications/nistpubs/index.html#sp800-16

Publications of the U.S. Computer Emergency Readiness Team (US-CERT) may provide useful background for the development of awareness and training materials. They are available at: http://www.us-cert.gov/reading_room/

National Cyber Security Alliance (NCSA) organizes National Cyber Security Awareness Month and provides a toolkit and other resources to participate in that event. It takes place each October. More information is available at: http://www.staysafeonline.info/index.html

The Multi-State Information Sharing and Analysis Center (MS-ISAC) Cyber Security Awareness has resources that include brochures, newsletters, a toolkit, and links to state homeland security programs at: http://www.msisac.org/.

"The National Infrastructure Protection Plan," U.S. Department of Homeland Security, 2006, http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm

"Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan as input into the National Infrastructure Protection Plan," May 2007, http://www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf

Appendix B: Select State Security Websites

Alabama:
http://www.alabama.gov/portal/secondaryContent.jsp?page=Standard_Security

Arkansas:
http://www.dis.arkansas.gov/security/cybersecurity_toolkit.htm

California:
http://www.infosecurity.ca.gov/

Delaware:
http://dti.delaware.gov/information/cybersecurity.shtml

Florida:
http://www.secureflorida.org/

Georgia:
http://gta.georgia.gov/00/channel_title/0,2094,1070969_84340779,00.html

Idaho:
http://idaho.gov/cyber/

Iowa:
http://secureonline.iowa.gov/

Louisiana:
http://www.doa.state.la.us/oit/securityoffice/sec_tips.htm

Michigan:
http://www.michigan.gov/cybersecurity

Missouri:
http://www.cybersecurity.mo.gov/

Nebraska:
http://www.nebraska.gov/cybersafe

Nevada:
http://infosec.nv.gov/

New York:
http://www.cscic.state.ny.us/

Pennsylvania:
http://www.cybersecurity.state.pa.us/portal/server.pt

Rhode Island:
http://www.doit.ri.gov/security/

South Carolina:
http://www.secure.sc.gov/site/default.asp

Virginia:
http://www.vita.virginia.gov/security/

West Virginia:
http://www.wv.gov/Offsite.aspx?u=http://www.state.wv.us/scripts/admin/isc/default.cfm (see "IT Security" link to the left on the state's homepage)

Wisconsin:
http://itsecurity.wi.gov/

Appendix C: Potential Awareness Raising Topics and Delivery Methods

The following lists are excerpts from state examples and also ***"Building an Information Technology Security Awareness and Training Program,"*** *the National Institute of Standards and Technology (NIST), Special Publication 800-50, October 2003,* http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Topics for Awareness-Raising Sessions:

- Password usage and management—including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions
- Policy—implications of noncompliance
- Unknown email/attachments
- Web usage—allowed versus prohibited; monitoring of user activity
- Spam
- Data backup and storage—centralized or decentralized approach
- Social engineering
- Incident response—contact whom? "What do I do?"
- Shoulder surfing
- Changes in system environment—increases in risks to systems and data (e.g. water, fire, dust or dirt, physical access)
- Inventory and property transfer—identify responsible organization and user responsibilities (e.g. media sanitization)
- Personal use and gain issues—systems at work and home
- Handheld device security issues—address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance
- Laptop security while on travel—address both physical and information security issues
- Personally owned systems and software at work—state whether allowed or not (e.g. copyrights)
- Timely application of system patches—part of configuration management
- Software license restriction issues—address when copies are allowed and not allowed
- Supported/allowed software on organization systems—part of configuration management
- Access control issues—address least privilege and separation of duties
- Individual accountability—explain what this means in the organization
- Use of acknowledgement statements—passwords, access to systems and data, personal use and gain
- Visitor control and access to spaces—discuss applicable physical security policy and procedures, e.g. challenge strangers, report unusual activity
- Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems
- Protect information subject to confidentiality concerns—in systems, archived, on backup media, in hardcopy form, and until destroyed
- Email list etiquette—attached files and other rules

Techniques for Delivering Awareness Material:

- Message on awareness tools (e.g. pens, key fobs, post-it notes, notepads, first aid kits, clean-up kits, diskettes with a message, bookmarks, Frisbees, clocks, "gotcha" cards)
- Posters, do and don't lists, and checklists
- Screensavers and warning banners/messages
- Newsletters
- Desk-to-desk alerts (e.g., a hardcopy, bright-colored, one-page bulletin—either one per desk or routed through an office—that is distributed through

the organization's mail system)
- Agency-wide email messages
- Videotapes
- Web-based sessions
- Computer-based sessions
- Teleconferencing sessions
- In-person, instructor-led sessions
- IT security days or similar events
- "Brown bag"/"lunch and learn" seminars
- Pop-up calendar with security contact information, monthly security tips, etc.
- Autosignatures of IT security staff
- On-hold messages for phone system
- Mascots
- Crossword puzzles
- Awards program (plaques, mugs, letters of appreciation)

Appendix D: Potential Training Topics and Delivery Methods

The following lists are excerpts from ***"Building an Information Technology Security Awareness and Training Program,"*** *the National Institute of Standards and Technology (NIST), Special Publication 800-50, October 2003,* http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

High-level bodies of IT security knowledge to consider for training and awareness purposes are:

- Laws and regulations
- IT security program
- System environment
- System interconnection
- Information sharing
- Sensitivity
- Risk management
- Management control
- Acquisition/development/installation/implementation controls
- Operational controls
- Awareness, training, education controls
- Technical controls

Methods of Training Delivery:

- Interactive video training
- Training by streaming video
- Web-based training (e-learning platforms)
- Non-web, computer-based training
- Outside, instructor-led training (includes peer presentations and mentoring and use of university learning management systems)

Appendix E: Endnotes

[1]"Insider Security Threats: State CIOs Take Action Now!", NASCIO, April 2007, http://www.nascio.org/publications/researchBriefs.cfm.

[2]This section is based upon entries by Dan Lohrmann, Chief Information Security Officer, State of Michigan, in the CSO Magazine Blog. For more about cyber ethics, please see the following entries: "Why Security Staff Struggle Implementing Cyber Ethics", January 26, 2007, http://blogs.csoonline.com/understanding_employee_conduct_trends

"Can CSOs Learn Anything from the Foley Email Scandal?" February 2, 2007, http://blogs.csoonline.com/can_csos_learn_anything_from_the_foley_e_mail_scandal

"Can Cyber Ethics Training Work for Adults?" February 11, 2007, http://blogs.csoonline.com/can_cyber_ethics_training_work_for_adults

[3]"Building an Information Technology Security Awareness and Training Program," the National Institute of Standards and Technology (NIST), Special Publication 800-50, October 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[4] "2006 Annual Study: Cost of a Data Breach," Ponemon Institute, 2006, http://download.pgp.com/pdfs/Ponemon2-Breach-Survey_061020_F.pdf.

[5] "Information Security Training Requirements: A Roles- and Performance-Based Model," the National Institute of Standards and Technology (NIST), Special Publication 800-16, April 1998, http://csrc.nist.gov/publications/nistpubs/index.html#sp800-16.

[6] "Building an Information Technology Security Awareness and Training Program," the National Institute of Standards and Technology (NIST), Special Publication 800-50, October 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.