

# UTAH'S SECURITY AWARENESS PROGRAM

Information Security and Privacy

State of Utah

NASCIO Awards

2009

# SECURITY AWARENESS PROGRAM

## B. EXECUTIVE SUMMARY

The Utah Department of Technology Services (DTS) launched its cyber-security awareness training for State employees in conjunction with National Cyber-awareness Month. The event was sponsored by the Multi-State Information Sharing and Analysis Center with the participation of all 50 states and the District of Columbia. This effort was in support of the President's National Strategy to Secure Cyberspace.

The State of Utah was the first to administer such broad-based awareness training with statewide participation in such a short amount of time. In October 2006, more than 16,000 State employees completed online awareness training (over 90% of Executive Branch employees). In addition, the Judicial and Legislative branches also had significant participation—resulting in more than 75% of all State employees completing the training. By the end of 2006, 96% of all Executive Branch employees had completed the training. Since that time, annual training has regularly exceeded 95%

The training curriculum covers topics such as PC user habits, online safety, appropriate use of IT resources, and the risks and vulnerabilities of information security. The training concluded with test and a minimum pass rate.

The success of this training moved information security beyond the technical realm, engaging the user on issues beyond IT. State governments bear a higher risk than federal and municipal governments in securing information, since state agencies collectively maintain the broadest spectrum of highly sensitive and personal data, such as records on drivers' licenses, criminal activity, business and professional licensing, and taxes, among others.



## C. DESCRIPTION OF PROJECT

### Descriptions of the Business Problem

Information security is most often considered an IT-only problem, where users assume that it takes only an IT solution to fix it. However, the pervasiveness of technology, especially the rapid increase of online resources providing government services in the last decade, illustrates how the Internet and technology have become tightly integrated into everyday society. Now governments must take more dramatic measures than ever to protect their systems and networks from the ever-changing security threats and the headlines and publicity that are generated any time security incidents are reported. Additionally, the State of Utah receives periodic Federal and State legislative audits that require employees to certify that they have been formally instructed on information security issues.

### Purpose and Objectives

The two primary objectives of the DTS Security Awareness program are to emphasize awareness of the potential dangers and vulnerabilities of losing sensitive data and help employees understand the critical roles and responsibilities they each bear in keeping the State's information safe. From credit card scanners to PCs, technology devices are widely used for a variety of functions, thus increasing a government's liability as data is made more accessible. Despite the perception that data breaches are presumably committed by highly trained hackers, most breaches are a result of unauthorized physical access to data through portable devices such as PDAs and laptops or when data is inadvertently placed in the public domain (e.g., on a Web site).

### Solution Description

The security awareness training focused especially on the critical role users play in keeping data secure through seemingly mundane precautions, such as locking a workstation as one leaves his or her work area, formulating complex passwords, or how to recognize potential scams online.

The Web-based training is an accessible method for almost all employees, and was developed so users could complete the training in stages, accommodating an employee's time constraints. Upon passage of the exam (requiring a score of 75% or higher), a notification is automatically attached to the employee's Human Resource file. Several hundred employees in the State's Department of Alcoholic Beverage Control that work in retail outlets were required to complete the training manually, since they handle personal credit card information. A record of this training is maintained, just as other mandatory training—such as defensive driving or unlawful harassment, by the State's Department of Human Resource Management. The training has two curriculum

tracks: technical training for DTS employees, and non-technical training for all other general users. The technical training was completed by all 900+ DTS employees during the month previous to rolling out the non-technical training to all State employees. This allowed DTS employees to be knowledge resources, available to assist all other State employees in completing their training.

#### Length of Time in Operation

The online training program was in operation for a year within the Department of Technology Services and then pushed to all state employees in 2006. It has been in use for three years on a statewide basis. Each year, new topics and information are added to increase the overall knowledge that state employees have.

---

### D. SIGNIFICANCE TO IMPROVED GOVERNMENT OPERATION

#### Operational Maturity

The State of Utah has recognized the importance of information security for many years. In the past, the State has held an annual conference which has regularly been supported by the Governor and attended by upwards of 300 state employees. Individual departments have also had their own awareness programs. The implementation of this statewide program indicates the degree of support that has been achieved for information security. With a large share of what the state does happening online, it was important for every employee to recognize they have a role. This program has allowed this to happen more than ever before.

#### Predictable Results

There are many issues that have measures that can be indirectly and directly impacted by the success of this program.

- Employees and business managers throughout the state now have a better understanding of the importance of security as they put services online. Since 2004, the number of online services offered by the State of Utah has grown from 200 to over 850. As these services are put online, agencies have implemented them with secure payment services and privacy measures already in place.
- An audit of surplus state computers taken prior to this program discovered many systems still had confidential or private data. This has significantly improved following implementation of this program.
- State employees do a much better job today managing private data than prior to this program's implementation.

## Cost Effective Development

The State realizes substantial savings by implementing a standardized, online security awareness program. Agencies have the opportunity each year to provide input on how to improve the system to meet the constantly evolving needs of information security. The elimination of duplicate effort in developing individual department-level programs has saved tens of thousands of dollars. All efforts are coordinated through a two-person team, an information security specialist and web developer.

## Reliability and Timeliness

The security training handled as many as 9,000 simultaneous users. All site users were tracked through their employee identification number so that completion of their exams were automatically recorded in their personnel files.

It was important for DTS to introduce this training in conjunction with National Cyber Security Month to for two reasons. First, it helped encourage employees to complete the training during within the month. Also, it communicated the measures the State is taking to efficiently protect taxpayer resources.

The security training program has been in place for over three years. The 2009 program covers the following categories of information:

1. Authentication and Password Management
2. Security Threats and Menaces
3. Internet Security and Malicious Code
4. Awareness of Social Engineering
5. Identity Theft and Fraud

Each year, the program is updated to reflect the most current security issues and to build on the awareness that was presented in the prior year.

---

## E. PUBLIC VALUE OF THE PROJECT

### Stakeholder Participation

According to the 2005 FBI Computer Crime Survey, the average cost incurred by public and private organizations due to one laptop theft is \$89,000 (when considering losses in productivity, data, work product, and assets). There are many other similar statistics that strongly make a case that the strongest deterrent to data losses is user awareness. Few technologies can provide the security and safety gained simply by making users aware of information security

dangers and how they can be mitigated. Not only does this training help keep the State's information secure, but it also helps employees protect themselves.

It is difficult to substantively quantify the results of this training, as little or no measurements of data loss or theft were being monitored or reported on an enterprise level previous to the creation of the Department of Technology Services in 2006. However, this awareness training is one of the major functions of the State's Enterprise Security Office which, under the direction of the Chief Information Officer (CIO), administers enterprise-wide programs and enforces security policies to keep State networks and systems secure. The high visibility of this training within the State has forged new relationships between DTS and various departments and agencies, such as Risk Management, Surplus Property, and the Bureau of Criminal Identification, to further secure the State's data and its work environments.

The State of Utah holds a unique position in information security since the CCIO has statutory authority to implement statewide security policies. The Enterprise Security program will also perform an enterprise-wide security assessment to define agency security requirements and identify vulnerabilities. Other security measures include a surplus property process that ensures proper removal of all State-owned information from surplus IT equipment and an upcoming policy requiring criminal background checks for all technology employees. This enterprise approach to technology services makes Utah the only state that has administered statewide security awareness training on such a broad scale in such a short period of time.

Utah's Governor issued an Executive Order in support of National Cyber Security Awareness Month, requiring all Executive Branch employees within the State to complete this training. The Order helped put this effort into the local media spotlight as well as prompting tremendous support from all of the Governor's cabinet members and agency directors.

## Public Policy Benefits

As one of the State's largest employers, this training has set the standard for other large companies throughout the state. Moreover, many other states have requested copies of the training curriculum for their own use.

This program supports the following public policies:

- Ensuring that confidential data remains secure.
- Supports the privacy of personal information.
- Supports on overall public environment that engenders trust in government services.
- Ensuring that public employees are competent and well-trained

## State and Agency Benefits

Agency information security personnel are able to spend less time on awareness and responding to questions because many issues are addressed on a broad

scale across the state. Individual agencies no longer spend time developing this type of awareness because it is now coordinated centrally and administered on a statewide basis.

---

## REALIZED RETURN ON INVESTMENT

### Adoption

As stated previously, the training was completed by over 16,000 State employees in just 30 days (an average of approximately 800 users per business day). The Web-based training was developed by DTS staff at no cost to its customers, using information from a variety of national cyber-security resources.

### Savings and Cost Avoidance

DTS is an internally funded agency relying on funds generated by the services it provides. FY 2007 is the first year in which these enterprise rates were implemented. DTS was able to offset the cost of all Enterprise Security activities through cost savings realized from other services—resulting in added services at no additional costs to DTS customers. All entities that utilize the State's network systems by DTS are required to participate in the security program.

### Return on Investment

Prior to this statewide program, each agency was conducting their own information security programs with mixed results. Training sessions often required that employees travel to a central location and also dedicated trainers. Physical restrictions limited these programs from reaching out to employees across the entirety of state government. By the time this program was implemented and extended statewide, benefits had already exceed the costs as agencies were able to divert existing training and development resources to other tasks and opportunities.

### Continuing Operational Benefits

DTS, with the endorsement of the Governor and his cabinet, will continue administering this training on an annual basis. The training is now required for all new hires to the State of Utah. Due to the rapid pace of change in technology and the ever-changing cyber threats, an updated, ongoing training curriculum will help users understand the most pertinent and current threats.