

A. Cover Page

NASCIO 2008 Award Submission

Title: Multi-media, Web-based E-learning Security Training Program

Category: Information Security and Privacy

New York State

SECTION B: Executive Summary

The New York State Chief Information Officer/Office for Technology (CIO/OFT) recognizes the value of having all agency staff receiving security awareness training. Security training has always been a part of the CIO/OFT information security program. However three years ago CIO/OFT implemented a new multi-media, web-based E-learning training program.

The agency security policy requires all staff members to receive security training on an annual basis to keep security issues foremost in their minds. It was difficult and expensive to provide training to our large workforce (800+), which is geographically dispersed across the state and work multiple shifts at our data centers and network call centers which operate 24x7. We also wanted a measure to ensure that staff actually understood security best practices and that everyone actually completed training each year. Additionally, the security training materials needed to be kept current, which means frequent updates to the training program so that it remains relevant to the current threat landscape.

CIO/OFT implemented its multi-media web-based training program to meet the goals, overcome the challenges and provide a low cost solution to security awareness training. Security training is now available at any time from any computer with Internet access. All staff members have a Directory Services password protected user ID logon used to identify them to the system. There are two training tracks, one for managers and supervisors and one for all staff. Both have a competency testing component and the system records those who successfully complete the training.

Security subject area experts can create, revise, develop, modify, and manage the training content through an on-line content management system. Additional security training courses, such as specific security topics for network design staff or application developers can be developed and administered through this system.

Over the past three years, over 99% of the agency staff has kept current with their security training. This has raised the level of knowledge of security policies and good practices, and changed employee behavior.

During 2007 CIO/OFT made this system available to other state agencies. Agencies can use CIO/OFT's training and testing content or modify it to meet their specific agency needs. The on-line content management system is also available for agencies to create their own programs. Nine courses from four agencies are now available for sharing across state agencies ranging from the original security training course to an employee orientation program. All agencies participate in the State Directory Services and therefore can easily implement this secure application in their environments. This E-Learning initiative has become a statewide resource that is improving the level of information security awareness and good practices across the State with minimal cost to CIO/OFT or the other agencies.

SECTION C: Description of the business problem and solution

The State Chief Information Officer / Office for Technology (CIO/OFT) is required by statewide security policy, federal requirements such as Health Insurance Portability and Accountability Act (HIPAA), and contractual obligations to customers to establish an information security program in line with industry best practice. Such an information security program must include a robust user training and awareness component that encompasses CIO/OFT's entire workforce, which needs to be trained annually.

CIO/OFT needed an information security training program that could: 1) provide training to existing staff in a very short timeframe; 2) provide training to new staff as they are hired; and 3) provide annual recurring training for all employees. The training content would need to be updated frequently to include emerging security issues and the current threat landscape. CIO/OFT also needed to maintain documentation regarding who had received training and achieved a minimal competency level. These goals were complicated by the fact that:

- CIO/OFT has a staff of over 800 employees that include both State employees and contractors.
- The agency has multiple worksites across the State, including 11 main sites and various satellite locations.
- Employees work 5 different shifts providing 24x7 coverage.
- Data center staff assigned to critical infrastructure components cannot leave their work locations for any extended period of time.

We were constrained by: 1) limited funds for developing a training/awareness program; 2) managers were skeptical of the value of having large segments of their workforce leaving duty stations to attend training sessions and 3) traditional classroom training for the number of staff and locations was not feasible.

CIO/OFT determined that an E-learning approach was the best approach to reach all the employees in the timeframes needed, across the diverse locations and work hours and within the limited budget. A project was initiated in 2004, managed by the Security and Risk Management Office, with oversight from the agency's Project Management Office. The project team consisted of about 10 people from various CIO/OFT units. The on-line training system was developed in-house. CIO/OFT's State Technology Academy hosted the on-line training program and provided help desk support to staff while using the training program. A network of supervisors and administrative staff helped promote and market the training. In addition, the project team coordinated with CIO/OFT's Employee Newsletter Team and Executive Management for communication and marketing.

The project was completed within 6 months. In addition to in-house resources, some consulting services (\$15,000) were used to design the training course structure and to help prepare material for presentation on the web. The security training content was developed internally and based upon existing security policies and standards that were already in place. The initial project included the development of one user security training course. The consultant then transferred knowledge to in-house subject area experts and a second security training course for managers and supervisors was completely developed with in-house resources.

The project also utilized existing technical resources and process as well as leveraging existing CIO/OFT staff expertise. New York State Directory Services (NYS DS) which provides authentication and security services for web-based applications was used as the authentication service and means for tracking staff completion of training. Training users did not need to have an additional account or password to access the training. The New York State Technology Academy was used as the means to deliver the training, which also provided a vehicle for expanding the training to other State and local government agencies.

The program developed has the following features and functionality:

- Two online Information Security training courses:
 - User Responsibilities for Protecting CIO/OFT Information Assets; and
 - Managers' and Supervisors' Information Security Training.
- A training experience that keeps the employee engaged with the security content through a visual and intuitive system with easy navigation and a self-paced user experience.
- A method and functionality for automatically documenting all staff members who successfully completed the training by passing a basic competency quiz.
- A Table of Contents feature that is available from anywhere within a course and takes you to a site map of all the modules and pages. This allows you to jump to any page in the course
- The ability to print a hardcopy version of the entire course content.
- Two ways to authenticate into the system – NYS Directory Services or a built-in database with password encryption.
- A content management application that makes it possible for non-technical content specialists to develop, modify, and manage sophisticated online, multi-media, interactive training courses.
- An online course for administrators of the system to learn how to use the design and administration features.
- Content authors can include interactive modules anywhere within the flow of a course. These modules are page components such as quizzes, exams, interactive learning displays, multimedia, etc.
- Content authors can view courses they are creating in the view of the student with the click of a button, at any point in the course.
- The quiz builder function allows creation of questions and answers (single choice and multiple choice), and settings for each quiz to determine if the quiz is required, if the score is recorded, and what the minimum passing score is.
- Content authors can define glossary terms and definitions. When the eLearning system renders the content, it automatically generates a list of terms found in the content at the bottom of the display with a callout of the term's definition.

The application was written in Adobe ColdFusion using a Microsoft SQL Server database. The ColdFusion logic manages all of the content and produces an interface made up of HTML, JavaScript, and CSS. Web 2.0 technologies were utilized in this application, in the following ways:

- Clean layout, neutral background, plenty of whitespace
- Sharper colors and 3D effects
- Centered orientation
- Design for the content, not the page
- Nice large font
- Interactivity and responsiveness by using AJAX (Asynchronous JavaScript And XML)

- Use of DHTML (Dynamic HTML) leverages browser functionality providing a more enhanced and intuitive user experience present

Several features in the application, such as in-place WYSIWYG editing of the course, module and page titles, reordering of pages and modules, and portions of the Quiz Builder, all implement AJAX. This allows quick response for the content author since the webpage does not have to be reloaded when a change occurs. A single interface is used both for editing and viewing, allowing content authors and administrators the ability to experience the work they are doing as if they were the student.

The E-learning security training program has been in full operation for three years including:

- Part of each new employee's orientation process, both State employees and contractors.
- An annual training/recertification cycle from June to December each year when all employees are required to test out of or successfully complete the appropriate security training course (User or Manager/Supervisor).
- Annual content review and revision cycle by the Security and Risk Management Office to take into account changes in technology, policy, law and regulation, and to address new security issues in the current threat landscape.

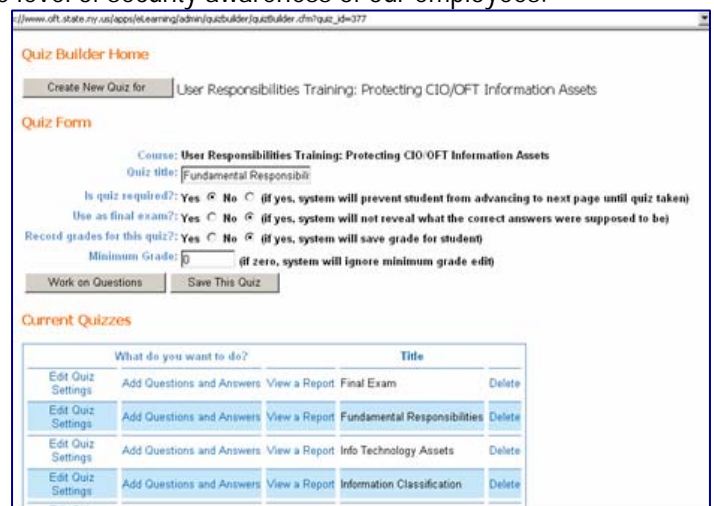
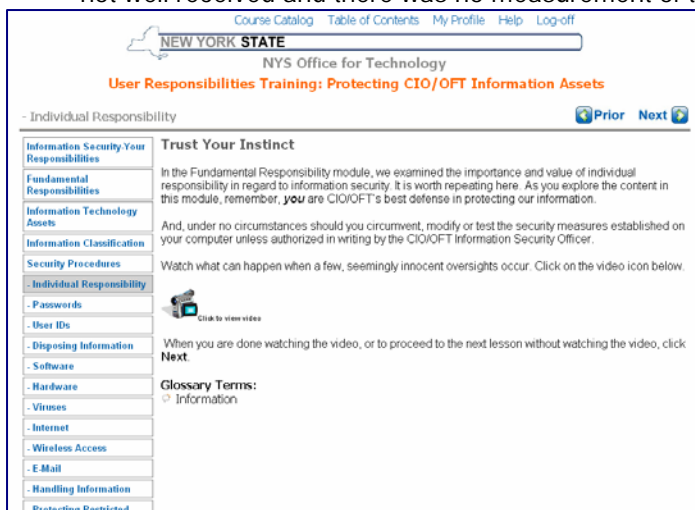
The security training application has been marketed throughout the agency through a multi-pronged approach. Employees were directly contact via e-mail and posters throughout the agency buildings when the training was first launched. Continuing marketing is achieved through the CIO/OFT employee newsletter and employee Intranet portal. Supervisors are encouraged to support and promote the training. E-mails are sent from the CIO/Director and senior managers during the training cycle at regular intervals reminding employees of the need to take the training and recertify.

Sample Training

Sample Content Management System

SECTION D: Significance to the improvement of the operation of government

Until the development of this E-Learning solution CIO/OFT's security training and awareness program was not well received and there was no measurement of the level of security awareness of our employees.



Since the implementation of this E-Learning training program CIO/OFT has achieved over 99% compliance with security training requirements that all employees are trained each year. In addition, the robustness and flexibility of the system has given CIO/OFT the adaptability to respond to new security training requirements and to ensure all employees are aware of new security threats and protective measures.

During 2007 CIO/OFT made this system available to other state agencies to administer within their agency. Agencies can use CIO/OFT's training and testing content or modify it to meet their specific needs. The on-line content management system is also available for agencies to create their own programs. Information Security Officers throughout NYS agencies have been offered access to CIO/OFT's online security training system and content. Some agencies are using the complete security training applications while others have adopted the content in part.

Access to the system is available through the CIO/OFT Technology Academy (www.oft.state.ny.us/apps/eLearning/welcome.cfm) which coordinates technology training among state agencies. The system has had great significance beyond information security. It has been further developed to allow agencies to develop, administer and share E-Learning training on any subject. Currently, nine courses from four agencies are available for sharing across state agencies ranging from the original security training course to an employee orientation program. All agencies participate in the State Directory Services and therefore can easily implement this secure application in their environment. This has become statewide resources that is improving the level of information security awareness and good practices across the State with minimal cost to CIO/OFT or the other agencies.

Some notable and immediate improvements include:

- A number of state agencies who had not yet complied with statewide information security training mandates were able to immediately copy our security training and customize it for their own use.
- CIO/OFT developed and implemented a new employee orientation course using this system.
- Agencies are experimenting with using this tool for other uses, such as for knowledge management, which is an important issue in the state workforce these days.

SECTION E: Benefits of the Project

The benefits of this project for CIO/OFT include a workforce that is more aware and knowledgeable of information security issues and best practices which translates into a more secure environment overall.

Prior to the E-Learning system, information security training was delivered through two hour training sessions, held multiple times to try to reach all employees. The average time to complete the E-Learning security training is about 50 minutes because of the streamlined course approach, easy navigation and ability for a person to test out of sections where they are already knowledgeable. Additionally, instructor time and logistical planning for delivering a classroom course multiple times has been eliminated.

Savings Summary				
Prior to E-Learning System		With E-Learning System		Savings
2.5 hours for 800	2000 hrs.	50 minutes per	666 hrs.	1334 work hrs. per

employees (if they all attended)		employee		year (67% reduction in staff hrs. spent in training)
----------------------------------	--	----------	--	--

The most dramatic results have been the increased awareness of security issues and practices on the part of all CIO/OFT staff. This has increased the level of protection for customer information and critical CIO/OFT infrastructure, which contributes greatly to CIO/OFT's mission of delivering quality IT services to other state agencies. Prior to the E-Learning system, the only measure of the level of employee security awareness and knowledge were attendance records on the number of employees that attended training sessions. The E-Learning system with its testing and tracking components provides a more accurate measure of the level of awareness and knowledge of information security issues that staff members have retained.

The system has similarly helped other state agencies to improve and provide savings in their security training programs. It has provided a generic E-Learning training tool for all agencies to use and share training that will continue to provide huge time and resource savings across the state government.

Using this system as a low-cost solution to mandated security training saves taxpayers in the long run, since more expensive training solutions would come out of agency budgets or agencies would not be in compliance with State security policy and Federal requirements, which might jeopardize Federal funding.

Online learning authoring tools can cost many thousands of dollars for an enterprise solution. Self-hosted solutions require additional resources to learn how to configure the software, plus how to set up the system to allow for shared access of courses created internally – again, many thousands of dollars, as well as the cost to learn how to use these solutions. CIO/OFT only spent \$15,000 in consultant services in addition to the in-house work on this system.

Organizations that never thought of using customized online security because of the costs involved and the expertise required can now take advantage of this free service opportunity offered by CIO/OFT.

Over a dozen organizations have been experimenting with the system, and some have created course content that they plan to offer within their organization. It will be open to any organization that sees benefits in it use, and will in turn be available to users in the agency to take these custom training courses.