

Employee Security Education

Patrick Dooley: Wisconsin Department of Revenue

Synopsis

The electronic world presents today's worker with a totally new set of security problems. The ability to duplicate, store, and transport vast amounts of data is rarely preceded or combined with training on how to protect these data. Our goal is to erase that gap.

The purpose of this research was to review current practices and tools, and to provide recommendations for strengthening the employees' ability to work properly with electronic data. The educational effort will be ongoing. Although certain modules will be given as part of new employee orientation, many of the modules will be presented on a yearly basis. This is both because of IRS demands and the changing landscape of the environment.

The agency needs to consider improving the use of data and applications so that we can meet today's security standards. In order to achieve this, secure application writing must become a primary goal for technical staff.

We must implement a system of security awareness and best practices modules with a goal of improving end user understanding and awareness. As part of that system the business managers need to become an active member in security, by reviewing reports on current accesses and regularly reviewing security practices with employees.

Issues

- 1 For most people the concept of moving, using, and securing data is still tied to the moving and using paper. The fluidity of electronic data; how it needs to be secured, and disposed of is relativity unknown to the business user as well as the application developer.
- 2 IRS mandates that all users of federal tax information (FTI) go through yearly security awareness training and that training be specific to the person's job.
- 3 Security needs to keep pace with evolving computer architecture.

Findings

- 1 General perceptions and understanding of computer security vary considerably.
- 2 Software flaws are everywhere and need to be properly understood and dealt with by all employees.
- 3 Employees, as well as people in general, want to know more about the proper way to treat electronic data.
- 4 The public demands that all governments, as well as private entities, do a better job of securing their Private Personal Information.

Customer Impact

- 1 All employees will need to be given time to attend specific modules that apply to their job. The goal will be to develop modules that will be completed in 30 to four hour increments.
- 2 If computer based training (CBT) is developed, employees will need to be given desk time to complete it.

Recommendation

Security Awareness Training should not be treated as a one time event. Although this report is nearly exclusively based on the classroom, security awareness events and notices must be a continuing part of each employee's environment.

Security advisory E-mails, posters CBTs, intranet sites and computer based interactive security games should be an ongoing part of security education within the department. Security will be tasked with developing these with input from all divisions.

Goal: To make employees the first line of defense in securing taxation data.

Training rules:

First rule: Business users are not, and should never be expected to be computer experts.

Second rule: An employee must feel that the subject matter is relevant to their environment.

Third rule: Teaching security relevant to home use creates better work practices.

The syllabi below are for 13 separate modules in security awareness that I've mapped out. Modules length can be any where from 30 minutes to four hour increments depending on the need. Development of online as well as in person classes for each of these modules should be considered. Our intent is to give training that is pertinent to the employee's position. No employee will need to attend all modules.

Syllabi

Note: These are top level outlines of what we are planning or doing for Wisconsin Department of Revenue.

1. Basic Access Concepts
 - a. All access is defined by a business need.
 - b. Access granted to Individuals.
 - c. Access is sponsored. (Somebody else besides you needs to ask for and approve the access.)
 - d. Access is logged such that the specific who, what, where, and when are captured and reported.
2. Logon ID / Password
 - a. Nobody, including security has access to your password.
 - b. Distribute and discuss a "Good Password Pamphlet".
3. Two Factor Authentication

- a. RSA Fobs (a physical security device to access network. The concept of something you have and something you know should be explained.)
4. Social Engineering
- a. Term that describes ways to trick people into revealing passwords or other information that compromises a target system's security.
 - b. Classic scams include phoning up an individual that has the required information and posing as a field service tech or a fellow employee with an urgent access problem.
 - c. Highly deceptive domain names. All of the following are not what they would seem to be:
 - i. vísa.com
 - ii. pàypal.com
 - iii. paypàl.com
 - iv. chasebank-online.com
 - v. citi-bank.com
 - vi. bankofameriuca.com
 - d. Opening unknown E-Mail
 - e. Downloads
5. Law
- a. Laws (Anti-browsing power point and Employee Handbook)
 - b. The basic meanings of the laws are these.
 - i. Discuss your state laws here.
 - ii. IRS CODE SECTION 7213
 - 1. It is unlawful for any person to disclose to any other person, except as authorized in this title, any return, or return information.
 - 2. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than five years, or both, together with the costs of prosecution.
 - iii. IRS CODE SECTION 7213A
 - 1. Unauthorized willful disclosure is a felony punishable by a fine not exceeding \$5,000 or imprisonment of not more than five years, or both (sec. 7213). An action for civil damages also may be brought for unauthorized disclosure.
 - iv. Public Law 105–35 105th Congress, H.R. 1226
 - 1. Unlawful for any state employee to willfully inspect, except as authorized, any return or return information.
 - 2. Applies To All Employees.
 - 3. Any Violation Must be reported to the IRS.
 - 4. Taxpayer is notified if employee is criminally charged
 - 5. Taxpayer may file lawsuit against you for civil damages.
6. Policies Procedures and Work rules.
- a. Discuss your state policies procedures and work rules. In Wisconsin we have an “Employee Handbook” that describes all of the laws that the employee must operate under. It is discussed in this module.
7. Personal Security
- a. Identity Theft
 - b. Don’t give information when asked by cashiers at stores
 - c. Online purchase tips
 - d. Check your credit reports

- e. Know your rights
8. Physical Security
- a. Building Security
 - b. Key Card Badges
 - c. Tailgating
 - d. Laptops
 - e. Portable Data storage (Stress the temporary aspect)
 - i. Floppies
 - ii. PDA
 - iii. Telephones
 - iv. Memory Sticks
 - f. Paper
 - g. Disposal Processes of both Paper and Electronic Data
 - h. Clean Desk Policy
 - i. White boards
 - j. Fax Machines
9. Data Security
- a. Duplication of data is not desirable and may be illegal
 - b. Proper backups
 - c. Proper storage
 - i. On portable devices
 - ii. On internal systems
 - iii. On local workstation
 - d. Encryption
 - i. Data in transport
 - ii. Data at rest
10. System Security
- a. Defining the boundaries.
 - i. Department
 - ii. Enterprise
 - iii. Public
 - 1. Individuals
 - 2. Business
 - 3. other governments
 - b. Ownership (All data has an owner)
 - c. Firewalls
 - d. Anti-Virus software
 - e. Automatic Lockup
 - f. Warning Banner
 - g. Installing Software
11. Data Security II (intended for application staff)
- a. Version Control
 - b. Use of Application Logon ID
 - c. Application designs must be done in accordance with OTS design standards
 - i. Systemic boundaries are a primary
 - d. Separation of granting a request for application/data access and granting system access.
 - i. Use of an application/data is a business decision.

1. The authority for granting access to an application/data resides with the business owner and is accomplished through a formal DOR process.
2. Business personnel should never request that an OTS application developer grant application/data access. It is a conflict of good security for application staff to be involved in the process.

12. Application Security (Specific to the use of end user applications)

- a. E-Mail
- b. Internet
- c. Intranet
- d. Internal Applications
- e. External Applications
- f. Logging
- g. Log Reports

13. Application Business Ownership (Given to both application staff and business owners)

- a. Systems comprise three major components: data, display (screens & reports) and software (code). Decisions relating to data and display accesses reside with the business owner. Decisions relating to the management of software reside with the Office of Technology Services (OTS). The following rules pertain to DOR internal applications only. State enterprise or public applications will be covered in a later module.
 - i. OTS must manage its operations in compliance with State and Federal standards.
 1. OTS Application staff should not be involved in the process of granting an employee permission to access a production application/data. To do so is in conflict with security best practices.
 2. An application developer should never place a program directly into production. Code must pass a formal review process, usually performed by OTS Configuration Management
 3. An application developer should never have independent access to production data.
 - ii. Data ownership is with a business defined owner. Authority to grant access may be delegated by the owner to subordinate managers/supervisors.
 1. Best practice for an employee to obtain access to an application or data is as follows:
 - a. The employee's request is reviewed and approved by both the employee's immediate supervisor/manager (first tier) and the next higher level of management (second tier). (Be prepared to answer questions on how the Secretary or their direct reports get access and has the access approved)
 - b. The above process should be used irrespective of the employee's location in DOR's organization.
 - iii. Owners should be informed of accesses to their systems and review that information on a regular basis. As owners you should demand this.
- b. Discussion of management reports for all accesses.
 - i. Reports on access to applications and data are generated and reviewed by the owners or their appointed surrogate.
 - ii. Discussion of what management reports should be created and what currently exist.
 - iii. Who should do the checking?
 - iv. How often?
 - v. This is an important check on employee usage of the system.
 - vi. What should managers look for?

- vii. How to get changes done when problems are found.

Note on Background checks.

The following is from a discussion with the IRS.

Agencies are required to have personnel screening policies and procedures in place. The screening is to encompass their employees and their contractors who have or will be given access to federal tax returns and/or return information. In January 2007, IRS office will begin reviewing agencies personnel screening processes; those agencies who have none in place will be asked about their plans to implement, what that will be, date will be implemented. Those agencies that have this in place will be asked for copies of their policies, procedures, screening packages so we can ascertain what's being done. IRS safeguard review reports will write up what they find, but this will not be written in a negative manner; it will be written from an observational point of view and to obtain information for our files. We will use that information to assist our Office in reaching sensible, good business decisions as to how we want agencies to meet the requirement for personnel screening.

Documents Reviewed

	Title	Date	Source
1	Correspondence and Research Papers	August , November, 2006	California DOR Kansas DOR IRS
2	Noticebored (Is that really the right spelling of bored? YES) News Letter and Blog	August , November, 2006	ISECT, IT governance consultancy
3	Safeguarding Taxpayer Information	August 2006	Lili Crane
4	Study: Customers don't want data handled by outside vendors They'll likely go elsewhere if a data breach occurs	August 2006	Computer World
5	How to Raise Information Security Awareness.	August 2006	European Network and Information Security Agency,
6	Cyber Security Training and Awareness Through Game Play	November, 2006	US Navy
7	NIST Special Publication 800-50, Building an Information Security Awareness and Training Program	November, 2006	NIST (National Institute of Standards and Security)
8	NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model	November, 2006	NIST