DATA EXPOSURE UPDATE TO UCIST

February 28, 2014

UNIVERSITY OF WATERLOO

DATA EXPOSURE

- Description of exposure – Extra menu item was made available due to an implementation error, which allowed applicants to use a search page to view data of other applicants
- Contributing Factor – Because of how the search page was designed, this functionality was available to forceful browsing
  - » In security terms, forceful browsing is the act of accessing parts of a web application without using provided navigation
- One applicant noted the issue

IMMEDIATE ACTIONS THAT WERE TAKEN

- Exposed extra menu item was removed on Feb 18th
- A query was created to identify potentially similar scenarios
- Query results lead to the identification and hardening of three additional components
  - » Functional resources are in the process of testing these additional fixes
  - » Feb 28th implementation planned; signoffs in process

FURTHER ACTIONS

- All UW self-service components will be assessed to determine whether they are vulnerable to forceful browsing (Feb 28th)
- Security Admin will identify and label “restricted permission lists” (Feb 28th)
  - » A “restricted permission list” is defined as a permission lists containing multi-purpose components OR any permission list assigned to a self-service student role
- System configuration changes include:
  - » Disabling menu caching (for security changes to be reflected in a timelier manner) (Mar 5th)
  - » QA environment caching changes to mirror production (Feb 28th)
  - » Migration procedures will be extended to run correcting SQL when permission lists are migrated (immediate)
- A program will be created to remove invalid navigation entries at the database level; this program will be accessible to Security Admins, App Admins, and Functional Power Users (Mar 7th)
- Changes to all permission lists will be audited and emails will be generated when restricted permission lists are changed (Mar 17th)

INITIAL CHANGE MANAGEMENT PROCEDURES

- **Option 1** – Enable Use of the Delivered Navigation
  - » Once hardened, revert to default menu items
- **Option 2** – Implement Changes to Restricted Permission Lists during the Maintenance Window
  - » Continue to mask menu items
- Option 1 is recommended, as it is consistent with the de-customization of Quest, which is our long term ERP direction

LONGER TERM RESPONSE

- IST will provide an effective and simple change management process allowing security changes to confidently occur without the risk of data exposure
- This revised process will be developed and implemented collaboratively with our business partners from the RO, GSO, and Finance departments to support their business needs
- Immediate, short-term, and long-term actions will follow

LONGER TERM SECURITY CHANGE MANAGEMENT RECOMMENDATIONS

Jason Testart

UNIVERSITY OF WATERLOO

DEFINITIONS FOR CHANGE MANAGEMENT

- Role – a job function, either in a business process or a department
- Function (system) – a page, a component, an object, a system capability (e.g. ability to query), or a collection of these things
- Change Advisory Board (CAB) – a group of stakeholders that must approve certain changes before they can be implemented
- Permission list – a Peoplesoft construct that defines the capabilities of roles to functions (security enforcement)

SUCCESS FACTORS

- Data steward maintains a list of roles, business processes and functions as per Peoplesoft Security
- Security considerations must be made as early as possible in the System Development Life Cycle
- All security changes in test, QA and production are made by the security administrator, with the exception of the assignment of a role to a user
- The re-use of functions for more than one business process should be avoided
- A permission list enforces security policy on what a role can do to/with a function
- There shall be a standard for role security

ROLE ASSIGNMENTS/REMOVALS

- While no CAB approval is required, changes must be logged in RT – this is operational
- Log must contain (more than today):
  - » Date and time of request
  - » Name of target account
  - » Name of role
  - » Reason for change
  - » Approver (with evidence of approval)
  - » Date and time of change
  - » Date of revocation (if applicable)

ROLE AUDITS – MORE FORMALIZATION FOR CHANGES

- Role audits need to take place every 6 months
- Security administrator, together with appropriate functional lead perform the audit and identify potentially inappropriate role assignments for further investigation
- Audit findings reported to CAB before actions/remediation steps taken

CHANGES WITH SECURITY IMPACT - PROPOSAL

- All changes are initiated with a change request
- All changes must be tested in a pre-production environment before being introduced into production
- Functionality for a new business process requires CAB approval
- Re-use of functions for more than one business process requires CAB approval. All security changes to re-used functions require CAB approval.
- New functions for an existing business process does not require CAB approval if and only if the new functionality is an extension/evolution of existing functionality (and function is not re-used)

EXISTING FUNCTIONALITY

- Part of an existing business process that the system already implements
- No additional roles needed while upholding the principle of least privilege
- No changes to permissions needed for roles in the business process

CHANGE REQUEST

- Description of Change with reasons why needed
- Type of Change
- Change Window (start/end date/time)
- Business Criticality
- Impact
- Impact of not making change
- Test Plan
- Rollback plan
- Communications Plan
- Originator’s Name
- Sponsor’s Name
- Approval Date

CAB COMPOSITION FOR QUEST

- CIO as Chair
- Quest Security Administrator
- Quest Tech Lead
- Peoplesoft Application Admin
- GSO Representative
- RO Representative
- Finance Representative

EMERGENCY CHANGES

- In our experience, only occurrence is in the context of assigning/removing roles to/from users
- Defined process for these changes should be sufficient.
- Role audit should capture potential “undoing” that may be required.

UNIVERSITY OF WATERLOO