November 15, 2012

DHR/DT/eMerge Technology Forum
Agenda

eMerge Updates

- Changes Since Last Meeting
- CanAudit Assessment
- Workstation Security
- Policy and Best Practices
- A note on Passwords

Active Directory

Matt Reeves, DT

Q&A

- Lessons Learned
- Feedback
- Issues
eMerge Updates
Changes Since Last Meeting

- **eMerge Security Time-Out**
  - Increased from 15 minutes to 1 hour
  - Portal security time-out remains at 15 minutes
  - More info: [http://sfcontroller.org/emerge](http://sfcontroller.org/emerge)

- **eMerge Read-Only Period**
  - Last 3 pay periods system returned to users Friday AM

- **Communications**
  - Email distribution list created to notify users of changes
  - Increased Portal content: timely updates and reference

- Query database available to trained users

- Business Continuity site operational Dec 2012
Changes Since Last Meeting (Cont)

- **Reporting**
  - **EIS/Cognos: Budget and PeopleSoft Data**
    - Controller’s AOSD division owns this data warehouse
    - Dept CFOs currently confirming security access
    - Planned launch this week or next
  - **eMerge Reports**
    - Issue encountered: users running multiple versions of the same large report (Payroll Register)
    - Solution: eMerge now runs reports over weekend
Canaudit Assessment

- Canaudit Inc.
  - Conducted an “Internal Network Penetration Testing and Vulnerability Assessment”
  - Assessment was requested by eMerge
  - Assessment was managed by Controller’s City Service Auditors Division

- Assessed:
  - Web Application
  - Network
  - Windows
  - Unix Linux
  - Databases
  - Network Devices
Canaudit Process

- Map the Network
- Connect to systems and services to gain info
- Scan systems and devices for vulnerabilities
- Exploit vulnerabilities to gain access
- Attempt to escalate access to administrator
- Document security vulnerabilities/audit issues
Findings and Next Steps

- Extensive findings and recommendations
- eMerge and DT are responsible for addressing most findings and recommendations
- Department IT have a major security role
  - Workstation Security
  - Enforcing eMerge’s "least privilege" principle:
    The principle of least (or minimal) privilege is to give users the least amount of authority or privilege that is necessary to do the task. That way they are less likely to do something they are not supposed to do - either accidentally or on purpose.
Work Station Security

According to recent studies...

- As much as 80% of data breaches are result of human error not the failure of technology systems.
- Often, these errors are because individuals who handle information do not fully understand:
  - the sensitivity of the information
  - the legal requirements to protect the data
  - the threats to that information

Ask yourself:

- If this were confidential information about me, would I feel secure about the way it was being handled?
Workstation Best Practice Guidelines

- Install latest Operating System (OS) security patches.
- Set OS updates automatically download install.
- Enable OS firewall or equivalent.
- Disable local administrative or power user privileges.
- Change the default account passwords (inc. Administrator).
- Disable and remove all unnecessary and unused accounts.
- Disable ‘save password’ feature in browsers, if applicable.
- Implement strong OS password rules: 8 or more characters in length including mix of alphanumeric and special characters. Update Password Quarterly.
Workstation Best Practice Guidelines

- Enable password protected screen saver with inactivity threshold of 10 minutes. **Update Password Quarterly.**
- Install and actively monitor managed version(s) of virus, spyware, malware protection software (e.g., Symantec).
- Disable LM Hash on all Windows systems.
- Enable account lockout on all Windows systems.
- Install and actively monitor Management Agent software.
- Restrict access to shared drives and understand the kind of information that is stored in them.
A Note on Passwords

- Anyone who knows or can guess your password can see or do whatever you can. **Do not share passwords.**
- Passwords should be at least 8 characters, and a mix of letters, numbers and symbols.
- Avoid dictionary words in any language, obvious sequences (abcd1234) and simple alterations of common words (p@ssw0rd).
- Never set a blank password or use a default or initial value password.
- Use different ID and password combinations for different applications.
- Phrases can be the basis for an effective and easy to remember password, e.g., “I am one happy person at Controller Office!” could become the password “Im1hp@CO!”.
- Change your password regularly to limit the time a hacker has to discover it. **At least quarterly.**
- Avoid writing passwords down, but if you must, mask it, keep the piece of paper in a safe place and do not include related data (e.g., ID, site name).
eMerge PeopleSoft Log-In

- AD Infrastructure
  - Audit
  - Restore

- Login Improvements
  - Multi-Server Support
  - Library Checking
Q/A

- Lessons Learned
- Feedback
- Issues