Retirement Board Information Security Concerns

- Maintain fairly significant amounts of confidential and personal information pertaining to its members (in both paper and electronic formats):
  - Social Security Numbers
  - Bank Account Numbers
  - Tax Returns
  - Medical Information
- Boards "own" their own applications and data – security not overseen by municipal IT departments.
- Many day-to-day processes involve activities that can expose personal information.
- Lack "formal" Information Security Programs.

Retirement Board Information Security Concerns

Applicable Regulations and Laws:

- MA Data Security Law - 207 CMR 17
- M.G.L. Chapter 66A. Fair Information Practices
- PERAC Regulation - 840 CMR 6.00 - Standard Rules for Disclosure of Information
- M.G.L. Chapter 30, Section 42 (Standards for the management and preservation of records– sale and destruction)
- New PERAC Disability Retirement Process and the New Treating Physician’s Statement (Memorandum #21, 2009)

Why is Information Security Important?

- PII is a primary target for data thieves – because it is VERY valuable to them.
- Identity theft is one of the fastest growing crimes in the country (has surpassed drug dealing).
- Data breaches occur frequently:
  - TJ Maxx
  - Heartland Payment Processing (Most recent large breach)
  - Veteran's Administration
  - Many, many more… (See: Open Security Foundation's Data Loss Database - http://www.datalossdb.org/)
- Most breaches are avoidable through reasonable controls.
- Due to the economy there will likely be an increase in incidents.
- Very costly to the organizations that are entrusted with confidential data:
  - Regulatory fines, civil actions, lawsuits, and reputation

Emerging Cyber Threats

Strengths such firewalls are no longer the focus for attackers. The current focus is on known weaknesses (human factor – un-patched systems).

- **Phishing**
  - Use of email or telephone to trick someone into providing information or to go to a malicious Web site by falsely claiming to be from a known entity. These attacks are becoming more and more sophisticated. Use of social networking sites has become an issue.
- **Malware**
  - Sophisticated software that is covertly installed and used to mine personal data, record keystrokes, or enlist machines into botnets. Infection can come from email attachments, instant messages, or even legitimate WEB sites. (10 fold increase in 2008)

Critical Risk Management Activities

Make protecting critical and confidential information a priority:

- Start by asking three questions. First, where is your most critical data, who has access to it, and how is it used?
- Second, consider the various ways the data could be exposed and where the possible weaknesses in your security controls lie.
- Reduce the amount of PII you maintain to only what is needed to conduct business.
- Limit access (both logical and physical). Consider vendors and other third parties that may have access to your PII.
- Keep up to date with system patches.
- Browse safely. Limit browsing to only what is necessary for business.
- Be prepared for an incident. Know how to react, who to engage and when to notify.
- Without adequate security awareness training all else will fail.

Recommended Risk Management Activities

- Periodically test controls and safeguards.
- NEVER open email attachments unless you are absolutely sure of the source.
- Use and maintain firewalls.
- Utilize virus and spyware protection and keep it up to date.

Recommended Risk Management Activities

- NEVER send confidential information in an email (unless it is encrypted).
- Obscure confidential information on forms, reports, and other paper documents if it isn't required before faxing or sending out in regular mail. Request that the recipient of any confidential information is aware that you are sending via fax and email and request confirmation of receipt if at all possible.
- Validate the identity of individuals over the phone and in person before divulging any confidential information.

Questions?

Thank you.

I appreciate the opportunity to have this discussion with you today.

John DeMauro, President

CISSP CISM CISA

JDeMauro@practicalsecuritysolutions.com

508-614-0719