Data Security:
Central Registry Perspective

Missouri Cancer Registry

This project was supported in part by a cooperative agreement between the Centers for Disease Control and Prevention (CDC) and the Missouri Department of Health and Senior Services (DHSS) (U58/DP000820-02) and a Surveillance contract between DHSS and the University of Missouri.
J. Jackson-Thompson, MSPH, PhD
Operations Director,
Missouri Cancer Registry
and
Research Associate Professor,
Health Management & Informatics,
University of Missouri- Columbia

jacksonthompsonj@health.missouri.edu
573 882-7775
Nancy Cole, BS, CTR
Assistant Project Manager, Missouri Cancer Registry

colen@health.missouri.edu
573-884-2491
MCR: Background & Overview

- Subcontractor to state health dept.
- Housed in academic setting (SoM).
- Challenges of physical location.
- Key access.
Data & Software

• Process > 50,000 records/year.
  – 28,000+ MO incident cases
  – Data exchange w/ 20 states
• In late 2007, switched to CRS Plus.
  – Already used Abstract Plus, Web Plus.
• Database c. 1 million records (1972-2009).
  – NPCR reference year (high-quality data): 1996.
Data Security

• We approach data security the way we approach reporting of cancer cases to MCR:
  – Report not because there is a law that says you must; instead, report so we can work together for better patient outcomes.
  – Be vigilant about data security not because we have statutory & contractual obligations but because it is the right thing to do.
• Reporting facilities & cancer patients trust us.
Data Security Measures

• Includes all data, electronic or paper.
• Policies and procedures in place, updated as needed. Examples:
  – No PHI on thumb drives.
  – No PHI in e-mails or attachments.
  – File cabinets & offices locked.
  – Charts/records sent to P.O. Box or by FedEx.
  – Mail & data carried in locked bags.
Data Security Measures - continued

• Ongoing training for staff.
• All MCR staff reminded annually by signing:
  – Confidentiality agreement;
  – Acknowledgment of state and federal laws about penalties; and
  – MCR security policy.
• “The Security Mouse was here.”
Weather alert changed MCR’s paper-handling policies

• Tornado drill – staff from another unit directed to a 4-person MCR office – OOPS!!!

• Led to changes:
  – More locking cabinets
  – Lock doors if leave
  – No papers visible
  – Cross-cut shredder
  – Change in drill location
Data Security Structure

• MU
  – IT: department, campus and hospital.
  – Servers housed off-site in an IT facility.
  – Most reporting facilities use Web Plus.

• DHSS and State Office of Administration
  – SFTP site folder restrictions at DHSS.
  – BCCCP data.
  – Some path lab data.
VA Data Security

• We were satisfied w/ security of incoming data but VA wasn’t.

• Spent two months locating source for FIPS 140-2 compliant file transfer software.
  – Advantage of University setting.
  – MoveIT.
  – No charge to MCR.

• “They seem to be available on a ‘who’s screaming loudest’ basis.”
MU Information Security Program

• System initiative working with all campuses.
• Meeting to review issues:
  – Data classification systems.
  – General security procedures (strong passwords, encryption, etc.).
  – Workplace security manual.
  – Audits.
MCR Concerns

• Minimal IT input on MCR software, hardware or data flow since 2005.
• No strong passwords on Web +, CRS+, Abs+, Prep+ and some laptops.
• Passwords taped to some laptops.
IT Audit Requested

- MCR offered to be “guinea pig” unit.
- New MU IT initiative:
  - Usually audit systems.
  - Not accustomed to performing dept. audits.
- “We need to cover a higher-level of analysis of your systems and business practices.”
- Few trained/certified auditors (which they are).
- No charge!!!
Steps for each phase of security inspection program

• Identification.
• Coordination.
• Inspection.
• Evaluation.
• Recommendation.
• Repetition.
What IT Audit Includes

- Data flow/business practices (ongoing).
- Applications (Web Plus complete).
- Hardening operating systems (in process).
- Laptop encryption.
- Hard drive security.
- Security training for MCR staff (initial training complete; ongoing).
Audit priorities established

• Web Plus – most vulnerable area.
• Concern about text fields – places where hackers could include hazardous characters.
First phase: Applications – Web Plus Audit

- Facility abstractoruploader & central administratorcentral abstractorreviewer.
- 52 hours of testing using an automated vulnerability scanner & manual inspection of web pages.
- Results: 4 high-risk vulnerabilities, several moderate risks.
- Auditor comments:
  - “Went better than expected.”
  - “Web Plus is a good application.”
Web Plus Audit - continued

• Results sent to CDC.
• Fixed high-risk vulnerabilities immediately, requested re-scan; tested fix for moderate-level issues.
• Second scan – No high-risk vulnerabilities; fixed moderate-level issues.
Second Phase: Hardening operating systems

• Server audit issues related to:
  – Configuration.
    • proper port use, etc.
  – Management.
    • Managing administrative infrastructure.
    • Controlled access to file system & resources.
• Preliminary results only.
Future Steps

• Increase security on mobile devices (Laptops, external hard drives, etc.):
  – Identify & purchase encryption software
    Time frame - September 2009.

• Consider alternatives
  – Remote access reduces need for abstracting software (and PHI) on laptops.
Future Steps – continued

• Research and identify FIPS 140-2 software to use for database and servers. Time frame – 1 December 2009.

• Research use of encryption software for desktop computers, including TruCrypt (an open-source software) Time frame – 1 April 2010.
Future steps – continued

- Determine security level of networked drive.
  Time frame - 1 April 2010.
Recommendations

• Start with your institution’s P&Ps.
  – CCR’s may need to be more restrictive.
• Use the NPCR guidance.
• Annually, require that CCR staff sign:
  – confidentiality agreement;
  – Acknowledgments of state and federal laws about penalties; and
  – CCR security policy.
Recommendations — continued

• Look for opportunities to further employee awareness.
  – Items in the news, etc.
  – Computer stolen from unsecured work station.

• Learn from other organizations’ practices and mistakes.
Causes of Data Breaches

- Private files available in public spaces.
- Unused files with personal information.
- Lost or stolen laptops.
- Old or unused equipment without updated security protection.
- Sending files/allowing file access to wrong (reporting) facility.
You think you are secure!

• “...no matter how secure you are you fundamentally still are at risk.”

• “The only way to 100 percent protect yourself from attacks is to turn off your computers.”
  – Dan Chenok, chairman of the Information Security and Privacy Advisory Board, an advisory panel to NIST. February 23, 2009 – fcw.com
Resources

• NPCR Data Security.
  http://www.cdc.gov/cancer/npcr/tools/security/

• For complete details about MU’s Information Security program:
  http://doit.missouri.edu/security/

• Federal Computer Week - Complimentary paper subscriptions, also available on-line. Variety of topics, including security.
  http://www.fcw.com
MU IT security team
http://doit.missouri.edu/security/

- Manager - Brandon Hough
- Auditors -
  - Tyler Hargis
  - Michael Morrison
  - Caine Henderson
  - Sara Rohrs
- Audit coordinator - Becky Fowler
- Safety awareness - Kristy White
- Account management:
  - Megan Hartz
  - Joanne Boomer