Usability and Healthcare Data Breaches

M. Eric Johnson
Tuck School of Business
Dartmouth College
Types of Security Failures

Technical

Social Engineering

Awareness

Direct (active) attacks
- Hackers
  - Break-ins
  - Virus and worms
- Denial of service
  - Bot Networks
- Deceptions
  - Phishing/pharming

Leaks: Inadvertent disclosure
- Conversations/email/messaging
  - Deceptions
- Blogs
- Misdirected communication
  - email/Fax sent to the wrong person
- Paper
  - Poor disposal practices
- Electronic leaks
  - Web postings
  - Lost storage devices (laptops/tapes)
  - Peer-to-peer networks

Memorial Hospital Loses Laptop Containing Sensitive Employee Data
by Leanne Tokars (tokars@wbbt.com)
UPMC patients' personal data left on Web

This chest scan of a 60-year-old Homestead woman, complete with clinical examination notes, was part of a file on the UPMC's radiology department Web site that was accessible on the Internet until this week. The woman's family agreed to let the Post-Gazette reproduce the image if the paper removed information that reveals her identity. Other patients had their names and Social Security numbers posted on the Web site without their permission, in what UPMC officials acknowledge was "a mistake."

By Steve Tweet, Pittsburgh Post-Gazette

Names, Social Security numbers and other personal information for nearly 80 UPMC Health System patients were posted on the medical center's radiology department Web site possibly for as long as two years, apparently without the patients' permission.

"It looks like they made a training video and instead of blanking out the information, they left it in there for some stupid reason," said Robert Ewlat, 38, of Erie, after seeing his name and Social Security number on the Web site.

"I didn't agree to let them put my personal information on the Internet, that's for
Memorial Hospital Loses Laptop Containing Sensitive Employee Data

by Leanne Tokars (tokars@wsbt.com)

Memorial Hospital has notified employees that it has lost a laptop containing the personal information of 4,200 full and part-time employees and retirees. (WSBT photo)

Story Created: Feb 7, 2008 at 6:53 PM EDT
Story Updated: Feb 7, 2008 at 7:10 PM EDT

SOUTH BEND — Missing information at one of the area’s largest employers could put thousands at risk.

An employee lost the laptop while traveling in November.

This week employees received a letter warning them that the missing
Patients’ Data on Stolen Laptop
Identity Theft Not Likely, NIH Says
By Ellen Nakashima and Rick Weiss
Washington Post Staff Writers
Monday, March 24, 2008, Page A21

A government laptop computer containing sensitive medical information on 2,500 patients enrolled in a National Institutes of Health study was stolen in February, potentially exposing seven years’ worth of clinical trial data, including names, medical diagnoses and details of the patients’ heart scans. The information was not encrypted, in violation of the government’s data-security policy.

NIH officials made no public comment about the theft and did not send letters notifying the affected patients of the breach until last Thursday -- almost a month later. They said they hesitated because of concerns that they would provoke undue alarm.

The handling of the incident is reminiscent of a 2006 theft from the home of a Department of Veterans Affairs employee of a laptop with personal information about veterans and active-duty service members. In that case, VA officials waited 19 days before announcing the theft.

South Shore Hospital data breach may affect up to 800,000; contractor named
22 July 2010

Earlier this week, Massachusetts-based South Shore Hospital informed patients, employees, and others affiliated with the institution that personal information may have been exposed when it contracted a data management firm to dispose of outdated files. Now comes news that the contractor used was Archive Data Solution according to publicly filed records from the Department of Health and Human Services.
Usability and Healthcare Data Breaches

Ritu Agarwal
University of Maryland

Eric Cowperthwaite
Providence Healthcare

Khaled El Ersam
University of Ottawa

Paul Connelly
Hospital Corp of America
Breakout: IT Security Breaches and Implications for the Enterprise

• Environment - public opinion and legislation
  – How is security and privacy different in healthcare?

• Changing breach landscape.

• Opportunities for breakthroughs.

• How to incent adoption.