Lessons Learned from a Cross-Organizational Data Loss Security Incident

Tom Siu
Chief Information Security Officer
Welcome to a Compliance Brown Bag Lunch Presentation

- Information about these events:
  - *Informal (bring your lunch!)* Training or informative sessions that cover a variety of compliance related topics.
  - Open to all University community members, but each event typically has a target audience.
  - If you like what you hear don’t be afraid to ask for a repeat presentation in your own department.
  - E-mail notifications of future events available – please contact boyd.kumher@case.edu to be added to distribution list.
About the Compliance Program

• Purpose
  • Outline, document, assess, and support the University’s compliance efforts
  • Encourage compliance by providing support, training, and educational resources.

• More Information
  • Brochures available at door.
  • [www.case.edu/compliance](http://www.case.edu/compliance)
  • Contact Boyd Kumher, the University Compliance Officer, at 216-368-0833.
Lessons Learned from a Cross-Organizational Data Loss Security Incident

Lessons Learned:
Thomas Siu
CWRU, Oct 23, 2012
Overview

• Novel Incident
• Changed CWRU response process
• Case Study
• Policy and Procedure Implications
• Lessons Learned
Background

• Researcher collects digital audio recordings in research protocol
• Subjects given study numbers
• Field data collection from non-campus location
• SOP is to return equipment to CWRU after field data collection
• Study includes subjects from UH, CCF, Metro
Incident Summary

- Computer, equipment theft
- Researcher notifies PI
- PI notifies IRB
- IRB notifies HIPAA Security at Metro Health
- Metro notifies CWRU Research Admin
- CWRU Information Security notified
- Incident investigation begins
- Coordinated risk evaluation between organizations
Facts

• Data gathering procedure
  o CWRU initially determined negligible risk of disclosure from computers
• Paper records also lost
• Laptop not using encryption
• Equipment not in our possession
Investigation

• Forensic analysis of representative laptop

• Evaluated the (remaining) SD cards used

• Possibility that some audio files could be exposed to thief
<table>
<thead>
<tr>
<th>Filename</th>
<th>Path</th>
<th>Last Modified</th>
<th>Size</th>
<th>State</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0328_100536.MP3</td>
<td>E:\</td>
<td>3/28/2008 10:05</td>
<td>36,124 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>0803_164825.MP3</td>
<td>E:\</td>
<td>8/3/2010 16:48</td>
<td>25,754 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>0805_135020.MP3</td>
<td>E:\</td>
<td>8/5/2010 13:50</td>
<td>17,359 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>0805_182336.MP3</td>
<td>E:\</td>
<td>8/5/2010 18:23</td>
<td>18,508 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>239 - Copy.MP3</td>
<td>E:\</td>
<td>9/23/2010 17:00</td>
<td>43,862 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000001].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>55,104 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000002].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>1,60 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000003].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>8,771 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000004].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>27,456 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000005].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>4,985 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000006].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>18,625 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000007].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>65,902 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000008].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>705 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000009].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>7,382 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>[000010].mp3</td>
<td>E:\Unknown</td>
<td></td>
<td>32,639 KB</td>
<td>Excellent</td>
<td>No overwritten clusters detected.</td>
</tr>
<tr>
<td>09_0001.MP3</td>
<td>E:\</td>
<td>9/30/2010 20:03</td>
<td>91,502 KB</td>
<td>Poor</td>
<td>This file is overwritten with &quot;E:\Spotlight-V100\St...</td>
</tr>
<tr>
<td>0802_190055.MP3</td>
<td>E:\</td>
<td>8/2/2010 19:00</td>
<td>43,862 KB</td>
<td>Very poor</td>
<td>This file is overwritten with &quot;E:\09_0001.MP3&quot;</td>
</tr>
<tr>
<td>0620_143554.MP3</td>
<td>E:\</td>
<td>6/20/2008 14:35</td>
<td>36,871 KB</td>
<td>Unrecoverable</td>
<td>This file is overwritten with &quot;E:\fseventsd&quot;</td>
</tr>
</tbody>
</table>

FAT16, 1.83 GB. cluster size: 32768. Found 18 files (106 ignored) in 116.88 sec.
Complications

• Probability of sensitive data on the lost SD card
• Decision to review ALL data
• Time crunch to meet mandated reporting time window
• Different organizations have differing opinions on "breach" status
• CWRU is not a Covered Entity, not subject to HIPAA/HITECH
Lessons Learned

• Relationships: Engage conversations with UH, Metro, CCF before incidents
• CWRU has higher risk tolerance threshold
• HITECH audits spawn fear of HHS audit and fines
• Researchers need to inform CWRU Research Admin when a theft of data or devices occurs
• Collaboration: Counsel, Compliance, Information Security, Research Admin