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
  - 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

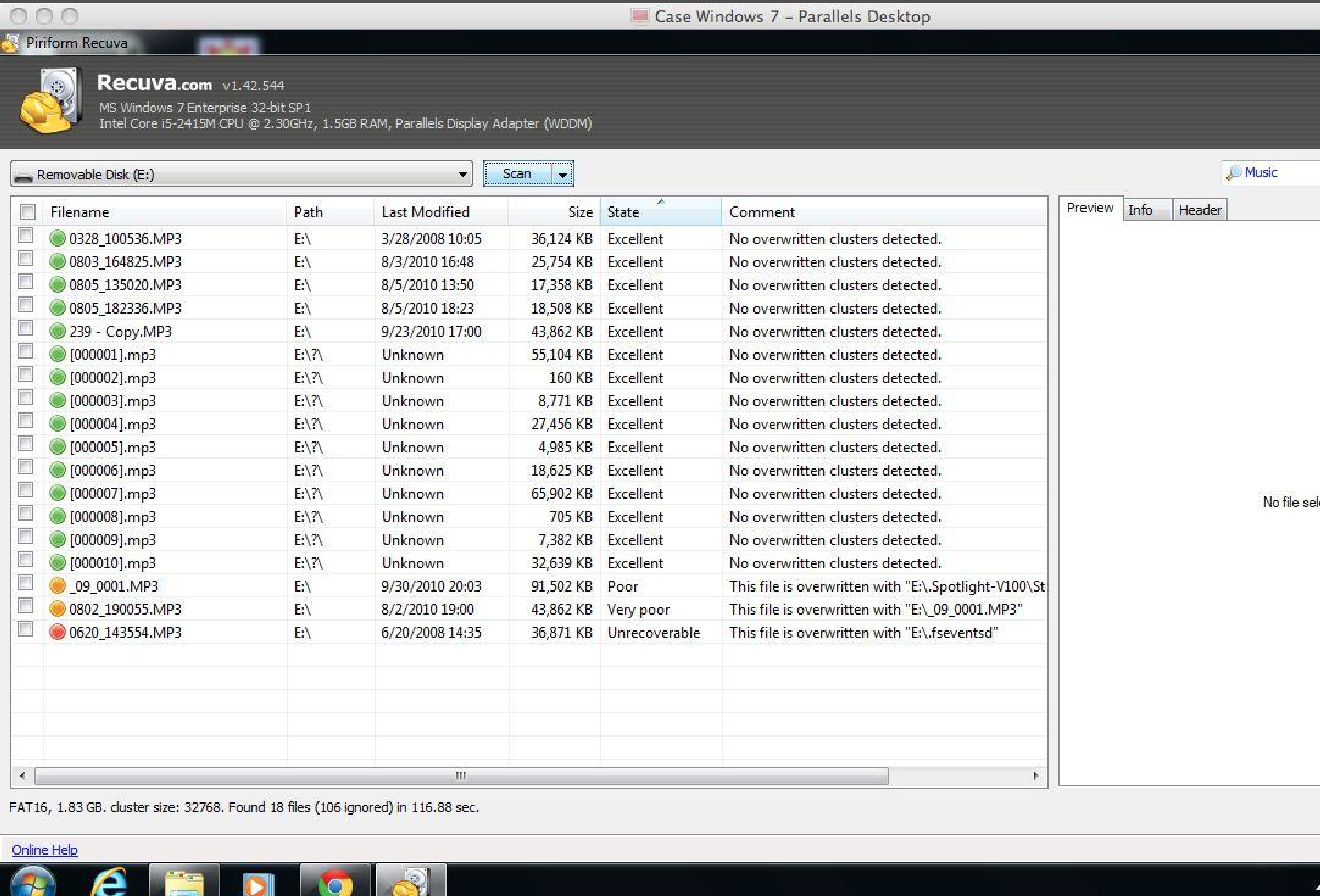
- Computer, equipment theft
- Researcher notifes PI
- PI notifies IRB
- IRB notifies HIPAA Security at Metro Health
- Metro notifies CWRU Research Admin
- CWRU Information Security notified
- Incident investigation begins
- Coordinated risk evaluation between organizations

Facts

- Data gathering procedure
  - 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



Recuva.com v1.42.544
MS Windows 7 Enterprise 32-bit SP1
Intel Core i5-2415M CPU @ 2.30GHz, 1.5GB RAM, Parallels Display Adapter (WDDM)

□	Filename	Path	Last Modified	Size	State	Comment
□	● 0328_100536.MP3	E:\	3/28/2008 10:05	36,124 KB	Excellent	No overwritten clusters detected.
□	● 0803_164825.MP3	E:\	8/3/2010 16:48	25,754 KB	Excellent	No overwritten clusters detected.
□	● 0805_135020.MP3	E:\	8/5/2010 13:50	17,358 KB	Excellent	No overwritten clusters detected.
□	● 0805_182336.MP3	E:\	8/5/2010 18:23	18,508 KB	Excellent	No overwritten clusters detected.
□	● 239 - Copy.MP3	E:\	9/23/2010 17:00	43,862 KB	Excellent	No overwritten clusters detected.
□	● [000001].mp3	E:\?\	Unknown	55,104 KB	Excellent	No overwritten clusters detected.
□	● [000002].mp3	E:\?\	Unknown	160 KB	Excellent	No overwritten clusters detected.
□	● [000003].mp3	E:\?\	Unknown	8,771 KB	Excellent	No overwritten clusters detected.
□	● [000004].mp3	E:\?\	Unknown	27,456 KB	Excellent	No overwritten clusters detected.
□	● [000005].mp3	E:\?\	Unknown	4,985 KB	Excellent	No overwritten clusters detected.
□	● [000006].mp3	E:\?\	Unknown	18,625 KB	Excellent	No overwritten clusters detected.
□	● [000007].mp3	E:\?\	Unknown	65,902 KB	Excellent	No overwritten clusters detected.
□	● [000008].mp3	E:\?\	Unknown	705 KB	Excellent	No overwritten clusters detected.
□	● [000009].mp3	E:\?\	Unknown	7,382 KB	Excellent	No overwritten clusters detected.
□	● [000010].mp3	E:\?\	Unknown	32,639 KB	Excellent	No overwritten clusters detected.
□	● _09_0001.MP3	E:\	9/30/2010 20:03	91,502 KB	Poor	This file is overwritten with "E:\.Spotlight-V100\St
□	● 0802_190055.MP3	E:\	8/2/2010 19:00	43,862 KB	Very poor	This file is overwritten with "E:_09_0001.MP3"
□	● 0620_143554.MP3	E:\	6/20/2008 14:35	36,871 KB	Unrecoverable	This file is overwritten with "E:\.fseventsd"

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 fuear 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