Crossing Borders: Conducting a Multiple Org Incident Response

Tom Siu, CISO
Case Western Reserve University

SANS Data Breach Summit 2018
New York, NY
Higher Education
Risk and Exploration

EARTH, SEA AND THE STARS
Risky Ventures
Looking Back
Future View
The Endurance
Sailing to Survival
James Caird sails to South Georgia
24 April - 10 May 1916
Exploration Risk

- Success and failure often overlap
- Explorers had to know what there was to know
- They assumed there would be discoveries along the way
- They needed skills and tools to “live off the land”
- There was a reward worth the risk
Looking Back

- Incident details and scope
- Failures and findings-
- What we did - looking outside the IR box
- What we all should be doing
Future View

- Lessons
- Prepare for the next one...it may be tomorrow
- Map out communications
- Team Of Teams and ISAOs
Clinical Research

- Patient care evaluation
- Recording provider-patient meetings
- Assess provider communications
The Tools

- Using digital audio recorder, SD Cards
- Transfer audio files to encrypted USB
- Upload .wav files to NAS in office
Scope

- CWRU Principal Investigator (PI)
- Consented data collection
- 3 participating hospitals (A, B, & C)
- Data collection kit: laptop/audio recorder/encrypted USB
- 8 kits for data collection
Failure #1

- In a meeting...
- The phone rings.
- CISO at “Hospital C” asks me, “Did you hear about the data breach from the stolen university laptop?”
Research group staff had laptop bag stolen from car on a Friday

Reported theft to supervisor on Monday

Supervisor contacted Hospital A’s Institutional Review Board (IRB)

Supervisor contacted other three affected hospitals

I’m the last to know...

Thursday
Study Protocol

Researchers leave recorder in patient exam room.

When recording complete- connect SD card from digital voice recorder to laptop

“Drag and Drop” audio file from SD Card to encrypted USB drive

Delete file from SD Card, they assume no data on (unencrypted) laptop

Failure #2
Who is Affected?

- One of 8 collection devices
- Sent sample to forensic investigator
- Assessed impact of SD Cards
  - Audio WAV files - no obvious identifiers
- Started reaching out to peer CISOs
Tech Findings

- Laptop slack space
- SD Card slack space
- USB integrity
- Don’t know if audio files actually have sensitive info
- Don’t know who was on the affected kit

Failure #3
The Fun Begins

- Internally- Inform and brief local management (Dean, CIO, President, Provost)

- Held first inter-organizational management response meeting
  - CISOs, InfoSecurity Mgr., Privacy Officials

- Conference calls, then meeting venues: complexity

Failure #4
Confusion- Regulation?

- HIPAA or not HIPAA mandates
- CWRU Researcher not Covered Entity (CE)
  - All 3 Hospitals are CEs
- Not clear actual impact/content
- Judgment calls on possible data in slack space
Notify vs. Not-Notify?

- Unknown data in slack space
- IF the thief uses data forensics/recovery tools...
- Risk of undue alarm by warning study participants of vague data loss
  - You *may* be affected
  - Data *might* be accessible
  - IF, if, if,
Who Is In Charge?

When boundaries are crossed, each org has their own strategy:

- CWRU took the lead to organize response
- Could not affect various decisions of other institutions
- Risk tolerance differences

Failure #4
Varied Responses

- Hospital A decided they wanted to notify participants from their cohort
- Hospital B decided it was not clearly impactful (slack space data) and would not notify their participants
- Hospital C agreed with Hospital A
- CWRU agreed with Hospital B

Failure #5
Additional Impact
Lessons
Failure #1

- Leadership: You need to use your internal relationships to get incident reporting to YOU first.

- Backup plan: your external relationships with information security management (CISOs) will keep you from being surprised.
Failure #2

• Get some workflow analysis and security evaluation of cross-org data handling.

• If this user group knew what ‘drag and drop’ operations did, they would have been able to use full disk encryption and disk wipe tools we had readily available.
Failure #3

- SANS/CIS Critical Controls 1 & 2 say “inventory” prominently

- If project team had inventoried which ‘kit’ had been used for each data collection event, they could have saved hundreds of hours reviewing all the other files for potential PHI
Failure #4

• If you might have a cross-border incident - you need to have InfoSec team relationships and communications in place BEFORE it happens
  • Plan communications exercises with industry partners. Learn from each other’s mistakes.
  • Foster relationships between responders.
  • Agree to authority beforehand.
I know
INFOSEC-FU
Developing TRUST?

• A great way to foster these (trust) relationships is to join an ISAO

• Example in CLE: Northeast Ohio Cyber Consortium (NEOCC)

• Example in AZ: Arizona Cyber Threat Response Alliance (ACTRA)

• These are cross-industry relationships
Failure #5

- Consistent response in this type of incident was due to language and tech misunderstandings
- All these hospitals now have more robust IR teams
- Terminology jail: they don’t say
  - “data breach” or “reportable incident”
Lesson from Team of Teams

What we were designed for

What we are facing
Failure #5, part 2

Lesson from Team of Teams by McChrystal

Liaison staff with other organizations

Senior leader

Representative of the best of your org.
“Information sharing was key, because ultimately, that was what we might one day turn around and request from the host agency in return.”

-McChrystal, Team of Teams, p 179.
Looking Ahead

- Plan for a cross-organizational Incident
- Know your neighborhood and neighbors
- Set standard secure communications methods/platforms
  - Prepare to host them on your platforms
- Up-to-date contact information vital
Pre-Made Decisions

- Who will lead the incident?
- Understand and agree upon risk tolerances and involve both privacy and security leadership
- Conduct an exercise, use past ‘real scenario’
- Agree to disagree, but still to follow the lead
Conclusions

Shackleton's string of failures led to his ultimate success:

- He brought all of his crew home
- He told his story

Our incident had a string of failures

- We overcame those failures, and
- We are prepared for the next one...
References

[Image of "Endurance: Shackleton's Incredible Voyage" by Alfred Lansing]

[Image of "Team of Teams: New Rules of Engagement for a Complex World" by General Stanley McChrystal]
References


You Don’t Go It Alone