SANS INCIDENT RESPONSE TACTICS PANEL

Tom Liston & Mike Poor InGuardians, Inc

Panel Question 1

How do you answer the following questions from clients after confirming an incident has occurred:

- What type of data loss should we be more concerned with PII or PCI?
  - Good consultant answer: It depends…
  - Within what domains does your company operate?
  - PII/PCI-centric thinking - problematic
- What should our first priority be? Detailed descriptions of the data that was stolen OR a detailed description of how the break in occurred?
  - If you have prepared for attack, answering the “how” should answer the “what”
- If we hire an outside firm to help us with IR: What are the 3 questions that we should ask?
  - Experience w/this type of incident?
  - Who will be doing the actual work?
  - Teaching experience/ability in this area

Panel Question 2

What are the top three incident response/forensic mistakes that organizations routinely make? Are there public examples?

1. Trying to handle incidents themselves
   - Using personnel w/o knowledge, training, or experience
   - Destroying more evidence than they gather…
2. Being "unprepared" for compromise
   - All budget focused on avoiding compromise
   - Failure to architect and deploy proper monitoring
   - Want to know "what happened?" but have no logging we can use to determine the story…
3. Having all the needed info, but doing *NOTHING* to stop the attack
   - Investigated a breach at a large government contractor
   - Found 10 BILLION lines of log from a 1.5 year compromise
   - *THEY **HAD** THE LOGS!!*

Non-Panel Question :-)

Why were Rob Lee, Harlan Carvey, Ovie Carrol, and Richard Bejtlich asked for a DNA sample and invited to a recent episode of the *Maury Povich* show with an unnamed female Smurf?

Well…