Effective Victim Interview Techniques for Incident Responders

Alison Naylor

Principal Information Security Analyst

Red Hat, Inc.

Overview

- Interview Basics
  - Why interview as part of Incident Response?
  - Subject (victim or person of interest) interviewing techniques
  - Quality Questions
  - Active Listening and Emotional Intelligence
- Structure of an Incident Response Interview
- Case Studies

Why Interview for Incident Response?

- Gather more information (obviously)
  - You may already know *what* happened, now find out the *how* and *why*
- Opportunity for user education
  - Incidents are a memorable experience!
- Positive PR for security team
  - Show your users how you keep their data safe
  - Security folks are people too!

Why this talk?

- Many of us are introverts
  - Less than comfortable talking to strangers
- Our questions aren't that good
  - We tend to focus on the tech, not the person
  - Often miss the information gaps
- Interviewing is a skill we can develop
  - Guidelines to build confidence
  - Plan, practice, and put into use!

Types of Subjects

- Victim
  - The incident happened "**to**" them
  - Was scammed, or perhaps just made a mistake
  - Usually cooperative
- Adversarial subject
  - Person of interest
  - May (or may not) be the actor behind the incident
  - Less than cooperative

"**Subject**" refers to either case − the person we are interviewing

Types of Questions

Closed-ended Questions

- Usually elicit a short, one-word answer (usually yes or no)
- Useful to confirm facts
- Often begin with “Do you..” “Can you..” “Who” “When” “Where”
- Might make victims anxious
- Could make adversarial subjects hostile or clam up
- Can imply judgment, or an expected answer

Types of Questions

Open-ended Questions

- Encourage a full, meaningful answer using both the subject's experiences and feelings
- Usually begin with "Tell me.." "What do you think.." "How" or "Why"
- Are reassuring to victims
- Can make adversarial subjects nervous and chatty
- More objective, less leading

Closed-Ended vs. Open-Ended

“Can you tell me what happened?”	“Okay, tell me what happened.”
“Do you know the sender of this email?”	“How do you know this person?”
“Do you have any problems with your boss?”	“Tell me about your relationship with your boss.”

When to use them?

As a general rule:

- Open-ended questions to start a conversation
- Closed-ended questions to clarify, confirm details
- Back to open-ended to continue a narrative

Organizing a Narrative Flow

For particularly involved incidents, a traditional four-stage interrogation can help. We ask the subject to describe:

- The entire incident, as they remember it *(mostly open-ended questions)*
- The period before the incident took place *(some open, some closed)*
- Details about the incident *(mostly closed)*
- The period following the incident *(some open, some closed)*

Quality Questions

- Objective
  - Specific and Direct
- Non-Judgmental
  - Don't play Stupid vs. Evil
- Adapt to the subject
  - Show that you're listening
- Tone of voice
  - Matter-of-fact
  - Supportive

Interviewing Tips

Establish rapport

- Take time for introductions
- Set expectations for the interview
- Offer reassurances
- The magic words: "**You're not in trouble.**"

Be patient! Don't rush

- Repeat and rephrase as needed
- **Book more time** than you think you need

Interviewing Tips

Use Active Listening

- Paraphrase – restate the subject's information with different words
- Summarize – concisely reiterate main points to identify overall progress
- Clarify – allow for unclear portions to be restated until intended meaning is clear
- Reflect – be attuned to and reflect feelings

Be Mindful of Body Language

- Make eye contact
- Relaxed, open
- Neutral expression

Interviewing Tips

Consider the Interview Environment

- How will the setting affect the subject?
- Boardroom vs. Comfy Chairs vs. Cubicle Ambush

Bring a Partner

- One of you can focus on the subject
- The other can focus on capturing data, fact-checking
- Good to have a witness (especially if adversarial)

Special Considerations for Victims

- Victims may feel traumatized—look for signs of distress
- Recognize the victim's fears, embarrassment, guilt, or confusion
- Establish a safe space—physical and otherwise
- Offer reassurances prior to asking uncomfortable questions
  - Particularly around browser history, emails, photos, chat logs, etc.
- Avoid getting bogged down speculating about the adversary
- Share a personal story if you've experienced something similar

Effects of Cybercrime

- Trauma can lead to long-lasting psychological effects:
  - Self-blame, guilt, anger
  - Feeling vulnerable, powerless
  - Isolation, inability to trust
- Physical effects can include:
  - Difficulty concentrating
  - Appetite changes
  - Insomnia
  - Absenteeism

Source: https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/

Before Your Interview

- Plan out your questions
  - Determine what background data you must record for every incident. Ask your subject only for the facts you can't discover through other means.
  - Develop questions tailored to the particular incident
    - You may already have the answers (that can be a good thing)
  - Try out questions on a teammate—rewrite closed questions as open!
- Choose a time and place
  - Select a location appropriate for your subject
  - Book more time than you think you'll need

Background Data

- **Subject profile**: name, userid, email address, phone number, job title, hire date, department, location
- **Device profile**: type, manufacturer, revision, operating system, patch level, status of backups, status of disk encryption
- **Software profile**: packages installed, versions, what AV or endpoint protection software is present, what MDM profile is present, what classification of data may be stored on the system or pass through the system, etc.

IOC/Artifact Collection Checklist

Collect the following to correlate with system logs, network traffic records, packet captures, IDS logs, AV reports, forensic tools, and third-party analysis sites:

- **Device vitals**: IP address, MAC address, FQDN, local computer name
- **Email metadata**: To, From, Date, Subject, Attachment name
  - Copy of the email with full headers and attachment payload preferred!
- **Phone call metadata**: Phone numbers, CallerID, timestamps, and durations
- **External entities**: IP Addresses, ports, domain names, URLs, ASNs
- **Forensic artifacts**: Files, hashes, payloads, memory dumps, disk images, backups

Beginning Your Interview

- Introduce yourself, give them a chance to do the same
- Explain the purpose of the interview
- Offer reassurances—this is about information, not blame
  - "We need your help to understand what happened."
- If appropriate, use the magic words:
  - ***"You're not in trouble!"***
- Set expectations—what you'll be asking, whether you are taking notes or recording, if you'll be examining any artifacts in their presence
- Smile, use eye contact, and speak calmly!

Subject History

- Ask your subject to recount what happened. Encourage them to take their time, start at the beginning, include as much detail as they can.
- Record detailed notes on all statements provided by the victim.
- Correlate with your incident timeline as much as possible. Include timestamps from event logs, emails, chat logs, etc. when available.
- Gently ask for additional information and clarification as needed.

Panic Mode?

- Ask the subject what steps they took once they suspected a problem.
  - Did they try to do any cleanup on their own before engaging the security team?
  - What specific actions were taken?
    - Passwords changed? History cleared? System unplugged? Software uninstalled?
  - Who else might have they spoken to about the incident?
  - What protective measures did they already have in place, and what was their effectiveness?
  - Have they experienced a similar incident before?

Additional Data

- Usual physical location(s) of device
- Who owns the device? Is it company-provided, or personal?
- Who else has access to the device / account?
  - You've ***never*** let your assistant / teammate / partner / child / parent use it?
- Is any suspicious activity ongoing?
- Is the device currently connected to any network?
- Has the device been powered off or rebooted?
- Have any changes been made to the device?

Interview Wrap-Up

At the conclusion of the interview, it's important to:

- Thank the subject for their time and cooperation
- Offer an opportunity for them to ask any questions
  - e.g. next steps, what will happen with their case
- Ask if they have any concerns arising from the incident
- Provide your contact information, in case they remember something else

User Education

- Help the user understand ways to prevent future incidents:
  - When in doubt, confirm identities via another method
- Passwords
  - Change any suspect passwords
  - Use good passphrases, 2FA wherever possible
  - Don’t re-use passwords
  - Use a password manager
- Prepare for possibility of re-victimization
  - Compromised data can be re-sold, used again

Additional Support

- Offer suggestions for additional support:
  - Employee Assistance Programs
  - Credit monitoring services
  - National Identity Theft Victims Assistance Network
  - Cybercrime Support Network
- Encourage the subject to reach out if they recall any further details
  - An overall positive interaction will increase likelihood of re-contact

Case Study: Cryptominer Chris

- Tracking down a cryptominer in an office building
- Unknown system, hadn't authenticated to anything official
- Found the MAC address on a switch, traced out the cable
- Approached the associate at their desk
- "WHAT'S YOUR MAC ADDRESS?!"
- The associate promptly clams up and becomes uncooperative
- "Let's start over" ☺

Case Study: Cryptominer Chris

This interview started out *really* poorly, but we were able to turn it around

- Really had to calm down the associate—sitting at eye level, soothing voice, etc.
- Explained who we are, that we're trying to understand data, and needed his help
- Asked about his company-issued laptop first, but it didn't match what we'd seen
- Then I noticed another PC on the desk—he said it wasn't his
- Lots of open-ended questions later, admitted he'd lifted it from an e-waste bin
- He had brought it to his desk, plugged it in, turned it on, and walked away
- He was used to re-using every scrap of hardware, thought that was standard
- Excellent opportunity for user education about plugging in unknown devices!

Case Study: Photo Phil

- Threatening tweets with photos from inside a company event
- Triangulating who took the photo from shots of the crowd
- We found a low-resolution crowd shot posted on an internal blog that could potentially solve the mystery
- Approached the photographer: “Did you take this photo? We’re going to need you to hand over the original!”
- Photographer freaked out!
- **“Oh my god, who even *are* you guys? I don’t have to give you anything! Nobody gets my photos, they’re mine!”**

Case Study: Photo Phil

The magic words: “You’re not in trouble. We really need your help to figure out what’s going on. Can you help us solve this mystery?”

- Time was of the essence, unfortunately planning was non-existent
- Another case of an overly-intimidating start to the conversation
- Always lead with who you are, why you’re talking to them, and that they’re ***not in trouble***.
- This associate was super happy to help once he realized it *wasn’t about him*, very excited and proud that he could help us crack the case!

Case Study: Scammer Fiction, Double Feature

1. Associate's Amazon account was credential-stuffed and compromised
2. She wanted to talk to tech support, so Googled it and called the first number
3. *Of course* it was a scammer—asked her to join a WebEx session for help
4. He took control and "showed" that 87 evil IP addresses were connected
5. Said she could take the PC to a "Cisco Store" or pay $350 for online help
6. Asked her to check her bank details while connected and she refused
7. The scammer got belligerent and threatening, and she eventually hung up
8. The associate was so unsettled, she worried she was being watched

Case Study: Scammer Fiction, Double Feature

This interview went really well! We were able to do some things right:

- Small, comfortable interview space
- One interviewer, one scribe
- We absolutely needed double the time we'd booked with her
- Letting her speak about her feelings—she'd been terrified for days, wasn't sleeping
- We were able to explain she'd been scammed twice, by unrelated actors
- User education helped her understand what actually happened, vs. the frightening lies the scammer had told her
- She left feeling relieved and empowered to resist future scams!

Questions?

Thanks for attending!

Acknowledgements

- The Question of Question Types in Police Interviews: A review of the literature from a psychological and linguistic perspective (2010: The International Journal of Speech, Language, and the Law: Oxburg, Myklebust, and Grant)
- Interviewing Techniques in Domestic Violence Cases (New Jersey Division of Criminal Justice)
- #ISC2Congress: Cybercrime Victims Left Depressed and Traumatized
  - https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/
- A Lasting Impact: The Emotional Toll of Identity Theft
  - https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf