CRJS475 Unit 5 Discussion Board – Considerations for Cyber Interviews

The first thing that a cyber-investigator must do is to determine if a crime occurred – and exactly what that crime is – and whether the laws in his or her jurisdiction will support a prosecution. For example, with the global nature of the Internet, a cybercrime may have happened elsewhere, to include in a foreign country (IACP, n.d.). The examples below may or may not be a crime in your jurisdiction (alphabetized):

Online Fraud for Financial Gain

- Compromised passwords
- Cyber extortion
- Data breaches
- Debit or credit card fraud
- Distributed Denial of Service (DDoS) using Botnets
- Identity theft
- IOT hacking
- Internet piracy
- Malware
- Phishing
- Ransomware
- SIM swapping
- Smishing attacks
- Trafficking passwords
- Unauthorized system access
- Website spoofing

Online Personality Issues

- Cyberstalking
- Invasion of privacy
- Online impersonation
- Online harassment
- Social network fraud
- Unauthorized email and social media access

Online Sex Crimes

- Child pornography: creating, distributing or possessing
- Soliciting for underage sex

Cybercrime interviews will involve the basic investigative steps that are used to identify and preserve digital evidence. When conducting a cybercrime investigation, basic questions that still apply will include (IACP, n.d.):

- Who, what, where, when, where, why and how?
- Where is the physical and digital evidence located, if any?
- What types of physical and digital evidence were involved?

The investigator must also consider who the interviewee is going to be because that will determine the type of questions that should be asked. For example, interviewees can be classified into three investigative categories: (1) victims, (2) witnesses and (3) suspects. Additionally, prior to conducting an interview, an investigator should try to determine if the suspect is a:

- Current or former employee.
- Complete stranger who was seeking internet or computer vulnerabilities.
- A computer expert who was hired by a competitor for espionage or other malicious intentions.

Technical Considerations during Cyber Interviews

According to Yerukala (2021), the following technical issues should be ascertained, preferably before an interview takes place – or at least during an interview:

- Ascertaining threats, vulnerabilities and risks
    - Threat – Someone who has the potential to cause harm by damaging data to or in a system, such as a phishing attack, etc.
    - Vulnerability – Weaknesses that are in a system, which makes threats possible.
    - Risk – It is the probability of loss. For example, potential damage is when a threat exploits a vulnerability
- Possibility of Botnets – A Botnet is a group of internet-connected devices, such as servers, computers, cellphones, etc., that are affected and controlled by malware. Botnets can do the following things:
    - Steal data
    - Send spam
    - Perform distributed denial-of-service attack (DDoS attack).
    - Enables unauthorized users to gain access to devices.
- Symmetric verses Asymmetric encryption
    - Symmetric Encryption – uses a single key to encrypt and decrypt information.
    - Asymmetric Encryption – uses a pair of public and private keys to encrypt and decrypt information.
- Two-factor authentication – Uses a two-step verification, in addition to a password, where a user must provide two authentication factors to gain access to something, such as getting access to:
    - Online bank accounts
    - Emails
    - Websites, etc.
- Firewalls – A security system that controls and monitors network traffic. It protects a system or a network from:
    - Malware
    - Viruses
    - Worms, etc.

Vulnerability assessment and penetration testing

- **Vulnerability Assessment** – A process used to define, detect and prioritize vulnerabilities in systems, network infrastructure, applications, etc. It gives an organization information that can then be used to fix flaws.
- **Penetration Testing** (or ethical hacking) – You hire someone to hack into your own network to identify vulnerabilities that malicious attackers could also exploit.
- **Brute Force Attack** – It is a trial-and-error method that is used to decode passwords or encrypted keys by using brute force. For example, it identifies passwords by repetitively attempting all possible matches. It can be avoided by:

    - Creating password-complexity by using different characters and formats.
    - Limit the number of login failures that are allowed.
    - Use two-factor authentication to completely avoid brute force attacks.
- **Port scanning** – Identifies open ports that are accessible on a host network.
    - Security administrators can use open ports to identify vulnerabilities.
    - Hackers can also use open ports to identify and exploit vulnerabilities.

Identify types of possible data leaks

- *Accidental breach* – Most data leaks are accidental.
- *Employee with bad intentions* – Example: An angry employee sends confidential data to unauthorized people.
- *Electronic devices* – Almost all electronic devices are capable of being used to leak confidential information over the internet.

References

IACP. (n.d.). *Cybercrime Investigations*. International Association of Chiefs of Police.

https://www.iacpcybercenter.org/officers/cyber-crime-investigations/

Yerukala, M. (2021). *Cybersecurity interview questions* [Cyber Investigations]. Mind Majix.

https://mindmajix.com/cyber-security-interview-questions