Stanhope Conference - Cybercrime

Scenario Discussions:

- Government Data on the Dark Web
- Ransomware & Data Breach

Presented by:
Det/Cst. 2520 Robert Merriott
Technological Crime Unit
Vancouver Police Department

Presentation Goals

Show you that:

- Cybercrime can be complex to investigate, but investigations can often involve ‘old school’ policing techniques to solve the crime. *(Sources, Surveillance, Interviews, etc.)*

- Data Breaches are often a result of human errors and NOT advanced hacking techniques.

Email Compromise

Email accounts

- Contain personal and private communications
- Email address are often used to access other sensitive online applications
- “Forget My Password” reset links are sent to your email

If someone gains access to your email account, what other online applications can they access?

Email Compromise

- Have you ever forgotten a password?

Could your account have been compromised?

Security Tip:

Always Use Multi-Factor Authentication (MFA)

Social Engineering

WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES

Scenario #1 – Government Data

Role of Audience: Lead Investigator

Type: Technology-as-instrument

Incident: Identity Theft Unit (ITU) recently arrested an individual ("JOHN") who completed a $150,000 fraud.

Scenario Setting #1

- **JOHN states:**
  - He buys info from "JoseKMan" (*name, dob, credit info, etc.)*
  - Communicates with JoseKMan on the Dark Web
  - JoseKMan can get info on any Canadian citizen
- JOHNs lawyer advises him to stop talking to police

Open Discussion

- What steps can you take to identify JoseKMan?
- What sections in your department would you involve?
- What training would members need in order to identify JoseKMan?

- Sub-event to follow this initial discussion -

Government Data - Sub-Event

Cybercrime team confirms:

- “JoseKMan” is advertising on the Dark Web
  - Selling personal information of Canadians – confirmed via Dark Web purchase (w/ Bitcoin)

Identity Theft Unit:

- A Source identifies “JoseKMan” as Jose Manfake
  - No previous police interactions

Open Discussion

- What steps can you take next?

Additional Things to Consider…

- Do your investigators have enough technical knowledge to confidently state that their opinions regarding cybercrimes are accurate?
- What happens if you arrest JOSE without knowing how the Personal Information is being obtained?

Complex Passwords

- Complex passwords are secure if…

You keep your password a secret!

What Is Your Password?

Scenario #2 – Ransomware / Breach

Your Role: Senior Manager of a Investigative Unit

Type: Technology-as-target

Incident: You just received a phone call from the CEO of large corporation advising you of a major cybercrime incident to his organization.

Scenario Setting #2

- Company hit by Ransomware
  - All 300+ computer systems encrypted & offline
- Hacker group is demanding $500,000 in Bitcoin to:
  - Decrypt the computer systems
  - Not release sensitive corporate & employee info
- Hackers plan to release corporate data in 72 hours

Tabletop Discussion

- What steps can you take next?
- Does your police agency have the proper resources to assist?
  - Which unit leads the investigation?
- Should they pay the ransom?

- Sub-event to follow this initial discussion -

Ransomware / Breach - Sub-Event

48hrs later, the company reports that it is:

- Working with local law enforcement who WILL:
    - Help correct the issue to the business
    - Ensure private information is not released
    - Arrest the “Hackers”

1 HR later, the CEO:

- Advises you that the backups are corrupted
- Demands police assistance for this criminal act!

Open Discussion

- What can your department do to assist?
  - Should the cybercrime team go ‘hands on’ to analyze the company system?
- What suggestions will you have for the company?

- Conclusion to follow this discussion -

Ransomware / Breach - Conclusion

CEO advises:

- $500,000+ to hire a cyber security firm to determine the "how" and "when" of the incident
- 9-week old backups – Dormant ransomware possible
- Hackers have SIN and personal banking information for all current and past employees
- Company may go bankrupt due to pre-existing financial issues if they can't resolve the incident

Single Solution Not Suitable for Complex Scenarios!

Scenario #2 - Final Thoughts

Will your department be prepared to respond both professionally and effectively to a large breach or ransomware attack?

How will your department respond if they are the victim of a ransomware or breach attack?

Final Thoughts

Majority of future investigations will require both technical and old-school investigative techniques.

All investigators need to have a solid fundamental understanding of cybercrime and technology.

Departments need to invest in advanced cybercrime training and have dedicated experts to help with complex technical investigations.