

slide1



slide2



Introduction

Lance Morgan

Lead Investigator

Office of the Chief Information Officer
Investigations and Forensics Unit

2



The slide features a decorative banner at the top with the British Columbia flag on the right and a sun/mountain logo on the left. The word "BRITISH" is above "COLUMBIA".

Investigator

Common Traits

- Unbiased
- Flexible
- Alert / Observant
- Organized
- Creative Thinker
- Tactful / Understanding
 - *And know when to not be*
- Professional and Thorough

3



Investigation

What are the Key Elements?

- Issue / Complaint / Allegation
- Person(s) of interest
- A definitive resolution
- RESPONSIBILITY / AUTHORITY to investigate

4

slide5



Investigation

Process Terms

- Reasonable and Probable Grounds
- Mandate and Scope
- Investigative Interview
- Standard of Proof
- Continuity of Evidence
- Exhibit

5



Common Investigation Types

- Human Resource
 - Inappropriate Use
- Internal Threat
 - Compromised / Unsophisticated Employee
 - Malicious Employee
- External Threat
 - Nefarious Actors

6

slide7



Conducting an Investigation

Initiation

- Identify Issue
- Identify actors / key assets
- Plan the investigation
 - Open Case - Documentation
 - Identify Resources required to successfully review the situation

7



Conducting an Investigation

Documentation

- Initial Report
- Ongoing Documentation
- Interim Reporting
- Concluding Report
 - Recommendations?



8

slide9



Conducting an Investigation

Documentation - Elements of a report

- Administrative
 - Who's involved
- Narrative
 - What I did
- Summary
 - What I found
- Concluding Report
 - Recommendations ?

9





Conducting an Investigation

Coordination

- Coordinate response
 - Who is part of the investigative team?
 - Who needs to be notified / kept apprised
- Each investigation is unique

10



Data Collection

'Evidence'

- Physical assets
 - Devices
- Documentary
 - Logs
- Testimonial
 - Statements

11

slide12



Standard Evidence Principles

- Standard of Proof
 - Criminal
 - Civil
- Entrapment
- Admissibility of Evidence
 - Chain of Custody
 - Non Repudiation of Data

12

slide13



Interviewing



13



The slide features a decorative header with the British Columbia logo on the left, which includes a sun rising over mountains, and the Canadian flag on the right, with a stylized yellow floral or leaf motif at the bottom.

Interviewing

2 Key purposes

- Determine facts
- Detect Deception

14

slide15



The slide features the official logo of British Columbia in the top left corner, which includes a stylized sun rising over mountains. To the right of the logo is the Canadian flag, with the British Columbia provincial crest superimposed on it. The background of the slide is white.

Interviewing

Determine Facts

Key Questions to ask yourself

- What do I know
- How do I know it
- Why is it important

15



Interviewing *Actors*

- Witnesses
- Suspects
- Corroborative persons

16

slide17



The slide features the official logo of British Columbia on the left, which includes a stylized sun rising over mountains. To the right of the logo is the British Columbia flag, which consists of the Union Jack in the canton and the Canadian coat of arms in the center, surrounded by a blue border. Below the logo and flag is a decorative banner featuring a landscape scene with mountains and water.

Interviewing

Traditional

- What Happened?
- Chronological in nature
- Isolates the event in the interviewee

17



Interviewing

Cognitive

- Re-establish environment, mood, setting & experiences
- Non linear
- Non specific – enjoy the journey ...

18

slide19



The slide features the official logo of the British Columbia government in the top left corner, which includes a stylized sun rising over mountains and the text "BRITISH COLUMBIA". To the right of the logo is a decorative banner featuring the Canadian flag, the Royal Coat of Arms, and a golden crest. The main title "Cognitive Interview" is centered in large, bold, yellow font. Below the title is a photograph showing two men standing in a doorway, looking out onto a bright outdoor area. The number "19" is printed in blue at the bottom left of the slide.

slide20



Cognitive interview

- <http://www.ctvnews.ca/a-deeper-look-into-the-interrogation-of-russell-williams-1.565832>

20

<http://www.ctvnews.ca/a-deeper-look-into-the-interrogation-of-russell-williams-1.565832>



Forensic Interview

Used with Suspects

Part 1: Information Gathering

- Understand the circumstances
- Have suspect commit to their “story”

Part 2: Interrogation

- Break down their “story” by identifying inconsistencies, lies, etc.
- Have the suspect provide an admission and confession

21

slide22

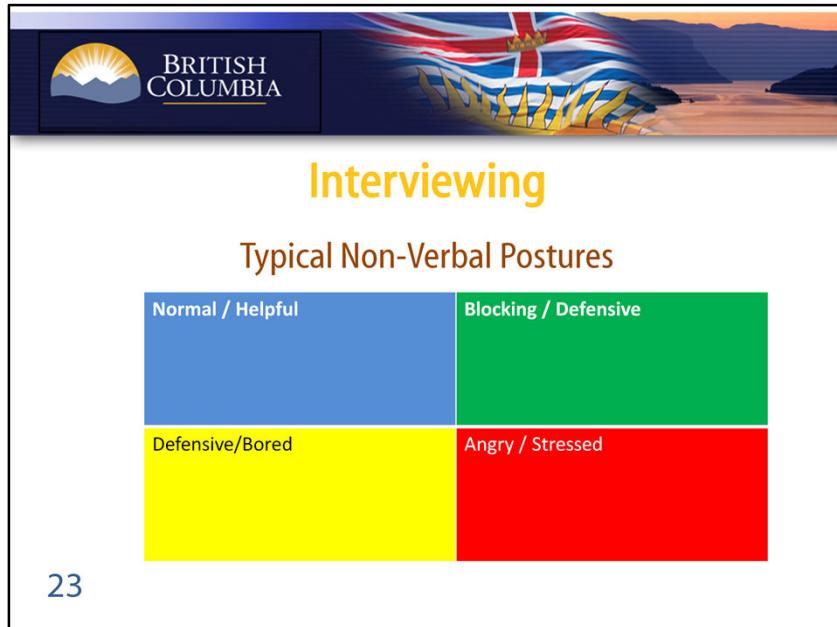


Interviewing

- Various Techniques:
 - Open ended
- Goal:
 - Develop as clear a picture as possible

22

slide23



The slide features the British Columbia logo in the top left corner, which includes a sun rising over mountains. The background is a scenic landscape with a flag. The title "Interviewing" is centered in yellow, and the subtitle "Typical Non-Verbal Postures" is below it. A 2x2 grid diagram is shown, divided into four colored quadrants: blue (top-left), green (top-right), yellow (bottom-left), and red (bottom-right). The blue quadrant contains "Normal / Helpful". The green quadrant contains "Blocking / Defensive". The yellow quadrant contains "Defensive/Bored". The red quadrant contains "Angry / Stressed". The number "23" is at the bottom left of the slide area.

Normal / Helpful	Blocking / Defensive
Defensive/Bored	Angry / Stressed

23

slide24



Interviewing

Typical Non-Verbal Postures

Normal / Helpful <ul style="list-style-type: none">• Feet Flat• Relaxed• Engaged	Blocking / Defensive
Defensive/Bored	Angry / Stressed

24

slide25



Interviewing

Typical Non-Verbal Postures

Normal / Helpful <ul style="list-style-type: none">• Feet Flat• Relaxed• Engaged	Blocking / Defensive <ul style="list-style-type: none">• Crossed Arms• Challenging Stare• Head Back
Defensive/Bored	Angry / Stressed

25

slide26



Interviewing

Typical Non-Verbal Postures

Normal / Helpful <ul style="list-style-type: none">• Feet Flat• Relaxed• Engaged	Blocking / Defensive <ul style="list-style-type: none">• Crossed Arms• Challenging Stare• Head Back
Defensive/Bored <ul style="list-style-type: none">• Rolling Eyes• Crossed Arms• Sighing	Angry / Stressed

26

slide27



Interviewing

Typical Non-Verbal Postures

Normal / Helpful <ul style="list-style-type: none">• Feet Flat• Relaxed• Engaged	Blocking / Defensive <ul style="list-style-type: none">• Crossed Arms• Challenging Stare• Head Back
Defensive/Bored <ul style="list-style-type: none">• Rolling Eyes• Crossed Arms• Sighing	Angry / Stressed <ul style="list-style-type: none">• Hands Clenched• Tapping Heels• Narrowing Eyes

27

slide28



Common Investigation Types

- Human Resource
 - Inappropriate Use
 - Threatening Behaviour
 - Misuse of Time
 - Bringing employer into disrepute / exposure of data
 - Copyright Infringement

28

slide29



Common Investigation Types

- Internal Threat
 - Unsophisticated Employee
 - Compromised Employee
 - Malicious Employee
 - Key loggers / introduction of malware
 - Data Leak
 - Hacking
 - Social Engineering
 - Hacktivists

29



Common Investigation Types

- External Threat
- Nefarious Actors
 - Hackers, Phishers, Hacktivists
 - Social Engineers (Mitnick)

30

slide31



The slide features the British Columbia logo in the top left corner, which includes a sun rising over mountains. The background is a scenic landscape with a flag overlay. The title "Social Networking" is in yellow, and the subtitle "SOCIAL SABOTAGE?" is in red. A bulleted list follows, and a red quote at the bottom right is in italics.

Social Networking

SOCIAL SABOTAGE?

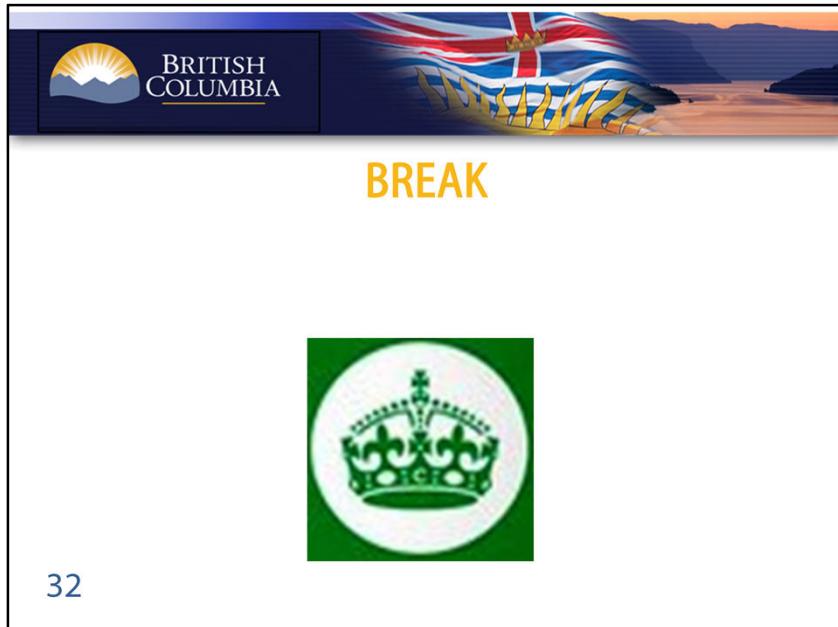
- MySpace
- YouTube
- Facebook
- LinkedIn
- Flickr

You are what your 'friends' post!

31

<http://www.azfamily.com/news/Tempted-to-vent-about-work-online-You-could-get-fired-188133881.html>

slide32

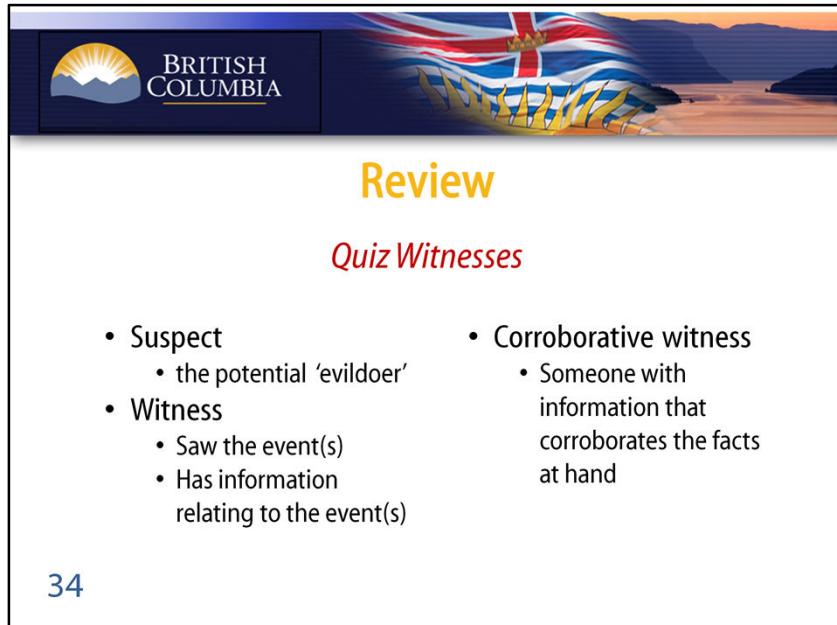




Review

- Types of Actors?
 - Suspects
 - Witnesses / Corroborative Witnesses
- Types of Data Sources (Evidence)
 - Logs
 - Devices
- Documentary Requirements
 - Reports / Communications Trail

33



The slide features the British Columbia logo in the top left corner, which includes a sun rising over mountains. To the right is a decorative banner with the Canadian flag and a landscape scene. The main title "Review" is centered in large yellow font. Below it, the subtitle "Quiz Witnesses" is in red italicized font. The content is organized into two columns of bullet points:

<ul style="list-style-type: none">• Suspect<ul style="list-style-type: none">• the potential 'evildoer'• Witness<ul style="list-style-type: none">• Saw the event(s)• Has information relating to the event(s)	<ul style="list-style-type: none">• Corroborative witness<ul style="list-style-type: none">• Someone with information that corroborates the facts at hand
--	---

34



Review

Quiz Evidence Types

- Statement
 - Testimonial
- Logs
 - Demonstrative
- USB Key
 - Physical
- Network Diagram
 - Demonstrative
- Cell Phone
 - Physical

35



Review

Quiz Evidentiary Principles

- Standard of Proof
 - Beyond a reasonable doubt
 - Criminal
 - Civil
 - The Balance of Probabilities
- Admissibility of Evidence
 - Chain of Custody
 - Entrapment

36

slide37



Review

Documentation - Elements of a report

- Administrative
 - Who's involved
- Narrative
 - What I did
- Summary
 - What I found
- Concluding Report
 - Recommendations ?

37





The slide features the British Columbia logo in the top left corner, which includes a sun rising over mountains. To the right is a decorative banner with the Canadian flag and the British Columbia coat of arms. The main title "Current Events" is centered in yellow text. Below it, a bold orange subtitle reads "It's a wild wild world....". A bulleted list follows, detailing various actors in the cyber world:

- Hacktivists
- Script Kiddies
 - Useful idiots....
- Hackers
- Criminal Elements
- National Actors
- Co-opted elements.

38

slide39



The slide features a decorative header with the British Columbia logo on the left, which includes a sun rising over mountains, and the Canadian flag on the right, set against a background of a coastal landscape at sunset.

Espionage / Exploits

Nothing New

- Social Engineering
- USB Techniques
- Flame

39

slide40



The slide features a decorative banner at the top with the British Columbia flag on the right and a sun/mountain logo on the left. The title 'Espionage / Exploits' is centered in yellow, and a subtitle 'Nothing New' is in red.

Espionage / Exploits

Nothing New

- Social Engineering
 - Officers, Agents & Spies
 - Covert agendas
 - Not what it appears to be
 - Prays on human nature to be 'helpful'

40

slide41



The slide features a decorative banner at the top with the British Columbia flag on the right and a sun/mountain logo on the left. The main title 'Espionage / Exploits' is centered in large yellow font, with the subtitle 'Nothing New' in red italic font below it. A bulleted list of espionage techniques follows.

Espionage / Exploits

Nothing New

- USB Techniques
 - Stuxnet
 - Key loggers
 - Other viral implants
 - Data Extraction

41

slide42



Espionage / Exploits

Nothing New

- Flame
 - Data Extraction
 - Network exploitation
 - High degree of sophistication
- Mini-Flame
 - Follow on for precision strikes

42

slide43



The slide features the British Columbia logo in the top left corner, which includes a sun rising over mountains. The background is a landscape with a flag. The title 'Cyber War' is in yellow, and the subtitle 'Future is Now' is in italicized black. A bulleted list follows:

- Estonia 2007
 - Strictly non kinetic - Infowar
- Georgia 2008
 - Supported Kinetic activity
- South Korea 2011
 - 10 Days of Rain
- Iran Stuxnet / Duqu

43

<http://www.youtube.com/watch?v=M4V3BwTIN0A>

RU Television

<http://www.youtube.com/watch?v=M4V3BwTIN0A>

47 MInute

US Naval War College ILD 2012 Panel Discussion Cyber Attacks: The Law

Published on Oct 10, 2012

International Law Conference, U.S. Naval War College

June 25-27, 2012

http://www.youtube.com/watch?v=oz_NPGqNIqo

PBS Great Decisions 2012 Excerpts: How to Protect Against Cyber Attacks

Published on Jun 11, 2012

From Great Decisions 2012, Episode 4 "Cybersecurity: Defense in the Digital Age" - Originally aired on PBS

As cyber attacks continue to occur at a breakneck pace, is the U.S. at risk?

Category

[News & Politics](#)

License

Standard YouTube License

<http://www.youtube.com/watch?v=3V8w5yDEY84>

Published on Oct 1, 2012

Posted 9/22/2012

slide44



'Cyber War'

Future is Now

- Estonia 2007
 - Strictly non kinetic – Infowar
 - Used by 'non-national' forces against Estonian Government and Financial targets
 - Suspected involvement of Russian Authorities but no proof

44



The slide features a decorative banner at the top with the British Columbia flag on the right and a sunburst/mountain graphic on the left. The text 'BRITISH COLUMBIA' is printed in white on a dark blue background.

'Cyber War'

Future is Now

- Georgia 2008
 - Supported Kinetic activity
 - Active DDOS against Georgian Government Sites
 - Experts believe involvement of Russian Military Intelligence and Federal Security highly likely.

45



The slide features a decorative banner at the top with the British Columbia flag on the right and a sun/mountain logo on the left. The title 'Cyber War' is prominently displayed in yellow.

'Cyber War'

Future is Now

- South Korea 2011
 - 10 Days of Rain
 - Brilliant use of cultural knowledge in creating the exploit tool
 - Major assault against S. Korean Government sites and US Forces Korea network
 - Self destruct feature
 - Very sophisticated for a 'simple' DDOS strike
 - A test for something later????

46

slide47



'Cyber War'

Future is Now

- Iran Stuxnet / Duqu
 - The next level
 - Multi-nation effort – *Operation Olympic Games*
 - Highly specific
 - Huge Effort
 - An example of asymmetric warfare
 - Supply Chain issues

47

slide48



slide49



The slide features the British Columbia logo in the top left corner, which includes a sun rising over mountains. To the right is a decorative graphic of the Canadian flag and some yellow reeds. The title "SCADA" is centered in large, bold, yellow capital letters. Below it, the subtitle "The not so hidden threat" is written in red italicized font. A bulleted list follows, detailing various SCADA-related incidents:

- 2008 Polish Tram attack
 - Modified TV Remote
 - 14 Year old hacker
 - Low cost / High impact event
- Nearly every week some report of hard coded 'backdoors' into scada systems are being reported

49

http://threatpost.com/en_us/blogs/malware-infects-two-power-plants-lacking-basic-security-controls-011413

http://www.theregister.co.uk/2008/01/11/tram_hack/

STUXNET

Cyber Defence Units Announced Recently:

India

Turkey

Brazil

Romania recently attacked through Red October vulnerability



Privacy and Investigations

Regina v. Cole

- Unreasonable Search and Seizure
 - Device was provided for personal use as well
 - Device transferred to Law Enforcement
- Employer Policies of Use must be clear
- Personal Use allowances invite risk and uncertainty

50

slide51



slide52



Guided Case Study

THE CASE OF THE LEAKED EMAILS

52

slide53



The Case of the Leaked Emails

Initial Report

- Compromised Credentials
 - What questions come to mind?
 - Reporter is evasive in his answers
 - What does this tell you?
 - Finally provides two emails of interest
 - What are your next steps?

53

slide54



The Case of the Leaked Emails

- What are you as the investigator looking for?
- What logs are available?
- What data sources can / should be reviewed

54

slide55



The Case of the Leaked Emails

PIXIE Logs

- What is the question you are trying to answer?
- What questions come to mind?
- How will you address the issue?

55

slide56



The Case of the Leaked Emails

Outlook Web Access Logs

- What is the question you are trying to answer?
- What questions come to mind?
- How will you address the issue?

56

slide57



The Case of the Leaked Emails

What are the next steps?

- What is the question you are trying to answer?
- What questions come to mind?
- How will you address the issue?

57