Using IT Asset Management Solutions as Investigative Tools

Lance Mueller
Director of Forensics
Executive Forensics
lance@execforensics.com

Scenario #1

- Scott
  - Scott works for a major technology company as an engineer for the past 2 years

Scenario #1

- Scott
  - Scott was traveling and accidently left his laptop in the airline lounge.
  - Once he realized he left his laptop behind, Scott notified the IT help desk per the company policy.
  - The IT help desk conducted their normal defined process:
    - Corporate Security notified
    - Asset Management notified
    - Account/Identity management team notified to disable/force reset passwords
    - Network/Domain trust revoked
    - Device had full disk encryption installed
    - Police Report?

Scenario #2

- Shayne
  - Shayne works for the same company as Scott, but in a different building and they do not know each other.
  - Shayne has worked for the company for three years as a sales representative.

Scenario #2

- Shayne
  - Shayne's car was broken into while at a restaurant one night after work and his laptop was stolen.
  - Shayne contacted the IT help desk per the company policy and notified them it was stolen.
  - The IT help desk conducted their normal defined process:
    - Corporate Security notified
    - Asset Management notified
    - Account/Identity management team notified to disable/force reset passwords
    - Network/Domain trust revoked
    - Device did not have full disk encryption installed
    - Police Report?

Scenario #3

- Resh
  - Resh works for the same company as Scott and Shayne, but also works in a different building and department unrelated to the other two.
  - Resh is a telecommuter. He comes into the office once a week and does everything else from home and communicates with his manager/team via email and phone.

Scenario #3

- HR was notified that Resh may also be working for a competitor and would like an investigation to be conducted.
- Since Resh is a telecommuter, he is not on the corporate network very often.

What is missing?

- All the proper processes were followed and notifications were made.
  - How valuable is your data?
  - Do you feel you are not a target?

- Where is the follow-up and follow-through on these incidents?
  - Proactive research can be resource intensive, but is it important?

What are we missing?

- We are missing some ***context and overall perspective*** with these incidents.
  - Scott
    - Lost Computer
  - Shayne
    - Stolen Computer from vehicle
  - Resh
    - Potentially working for competitor

What tools do you already have in the enterprise that may help?

- Leverage existing IT infrastructure (are any public facing?)
  - SMS/SCCM
  - Active Directory logs
  - Mail/Webmail access logs
  - VPN logs
  - Asset Management tools (persistent tools like Computrace)
  - Antivirus Console (Symantec/EPO)
  - DLP

EXCLUSIVE | CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents

Electronic snooping was part of a trial run for U.S. NSA and other foreign services

By Greg Weston, Glenn Greenwald, Ryan Gallagher, CBC News Posted: Jan 30, 2014 8:59 PM ET | Last Updated: Jan 31, 2014 6:38 PM ET

Trial run for NSA

The document indicates the passenger tracking operation was a trial run of a powerful new software program CSEC was developing with help from its U.S. counterpart, the National Security Agency.

In the document, CSEC called the new technologies "game-changing," and said they could be used for tracking "any target that makes occasional forays into other cities/regions."

Sources tell CBC News the technologies tested on Canadians in 2012 have since become fully operational.

CSEC claims "no Canadian or foreign travellers' movements were 'tracked,'" although it does not explain why it put the word "tracked" in quotation marks.

Deibert says metadata is "way more powerful than the content of communications. You can tell a lot more about people, their habits, their relationships, their friendships, even their political preferences, based on that type of metadata."

The document does not say exactly how the Canadian spy service managed to get its hands on two weeks' of travellers' wireless data from the airport Wi-Fi system, although there are indications it was provided voluntarily by a "special source."

What kind of metadata could you get from within your organization, if needed?

- Public facing vs. internal availability (many security and investigative tools focus on internal connectivity only)
  - IP network information
  - Connection history
  - Geo-location information
  - Windows Logon events/details
  - Webmail logons

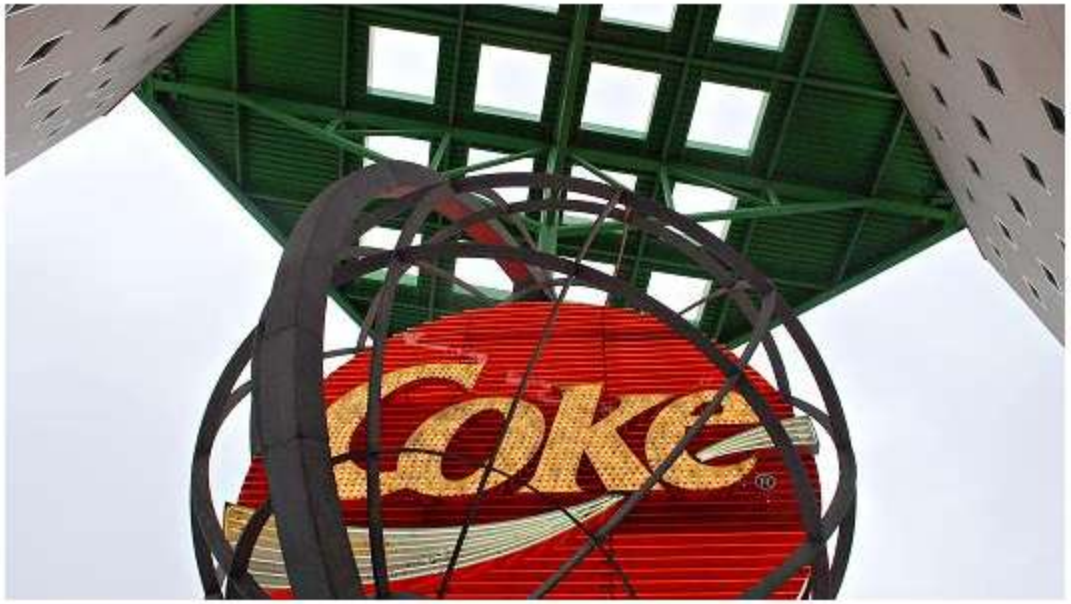
FOOD AND BEVERAGE

Coca-Cola laptop theft could have compromised info for 74,000

REUTERS

Text Size

Published: Monday, 27 Jan 2014 | 8:57 AM ET



Chris Rank | Bloomberg | Getty Images

A Coke logo sculpture is suspended outside the World of Coke in Atlanta, Georgia.

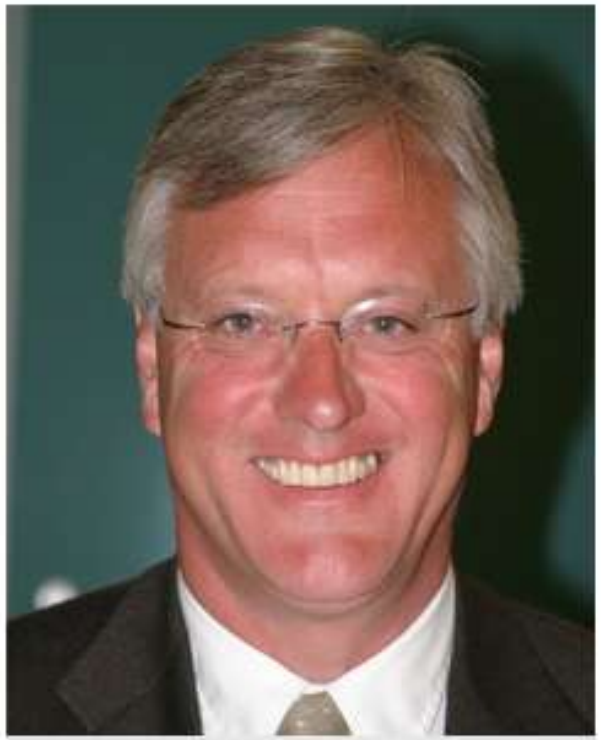
Beverage maker **Coca-Cola** on Friday said company laptops had been stolen from its headquarters in Atlanta and could have compromised information of about

Loss of 388 council laptops described as 'not a big security breach'

Published: 25 Nov 2013 13:30

2 comments

THE loss of hundreds of council laptops potentially containing council taxpayers' confidential information has been dismissed as 'not a big security breach'.



Share this image

THE loss of hundreds of council laptops potentially containing council taxpayers' confidential information has been dismissed as 'not a big security breach'.

The Observer exclusively reported last week, an Interim Progress report from the Royal Borough's internal Audit and Investigation Unit revealed 388 council-owned laptops were unaccounted for in a survey of council IT assets.

The missing laptops range from devices owned and used in council-maintained schools to assets kept in council buildings.

Daniel Whiteway

Social networks...

Facebook

Twitter

Questions/Discussion

Lance Mueller

Director of Forensics

Executive Forensics

lance@execforensics.com