Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector

D. Cappelli, M. Keeney, E. Kowalski, A. Moore, M. Randazzo

CERT Coordination Centre, Software Engineering Institute, Carnegie Melon University (PA, USA)

US Secret Service Report, August 2004

Available at: http://www.cert.org/archive/pdf/bankfin040820.pdf

Presented by: Samantha Daniels

Parties Involved

- American study
- Collaborative study between the **United State Secret Service** and the **CERT® Collaboration Centre**

Goal

"to develop information to help private industry, government, and law enforcement better understand, detect, and ultimately prevent harmful insider activity."

Definition 1

<u>Insiders</u>:

"Individuals who were, or had previously been, authorised to use the information systems they eventually employed to perpetrate harm."

- Note: An "Insider" is someone who does harm, not someone with the potential to do harm.
- The authors interchange "insider" and "perpetrator"

Definition 2

<u>Banking and Financial Sector</u>:

Included such areas as:

- Credit unions
- Banks
- Investment Firms
- Credit Bureaus
- Other (unspecified)

Components of Study

- Case Study Analysis
  - In-depth look at insider incidents that have occurred between 1996 and 2002
- Review
  - A review of the prevalence of insider activity over a 10-year time frame
- Survey
  - A survey of recent insider activity experienced by a sample of public and private organisations.

Overview Cont.

7 major findings were observed:

- Most incidents required little technical sophistication
- Perpetrators planned their actions
- Financial gain motivated most perpetrators
- Perpetrators did not share a common profile
- Incidents were detected by various methods and people
- Victim organisations suffered financial loss
- Perpetrators committed acts while on the job

Appreciative Comments

- Easy to read
  - Flowed well
  - Used layman's terms – non-technical
- Study was justified

  “gaps in the literature have made it difficult for organizations to develop a more comprehensive understanding of the insider threat…”
  - Previous studies focused on convenience samples and specific organisations
  - Previous studies did not look at behavioural and technical angles together
  - This study was a unique study looking at both behavioural and technical perspectives.

Appreciative Comments Cont.

- Limitations

  “this report and others from the study will articulate only what we found among these known cases, but can say nothing about cases not known or reported. This uncertainty limits the ability to generalise the study findings and underscores the difficulty other researchers have faced in trying to better understand the insider threat.”

  - Unknown cases due to:
    - Jeopardizing reputation
    - Harm suffered would not be sufficient to warrant criminal charges
  - Does not diminish the value of the study as still proves insiders have attacked systems and still provides some insight.

Appreciative Comments Cont.

- Avoided potential for bias
  - Investigation only looking banking and finance sector
  - Could be biased towards insiders only after financial gain
  - Provided examples of cases with motivations for attacks:
    - Financial gain
    - Prestige
    - Revenge

Critical Comments

- Review
  - 10 year period – from when to when?
- Survey
  - Sample of public and private organisations – how was the sample done?
  - Where was the list of organisations from?
- Too easy to read – not enough detail provided by being non-technical
- Review and survey???
  - Where did they go?

Critical Comments Cont.

- Parameters
  - No detail or description
  - How did they come to their conclusions?

  Example:

  - Most incidents required little technical sophistication
  - 87% of insider attacks used simple commands
  - What is simple?
  - Result of being too non-technical and writing for any reader?

Critical Comments Cont.

- Vague and/or impractical suggestions
  - Goal: To develop information to help detect and prevent harmful insider activity

  Example 1:

  - Incidents were detected by various methods and people
  - 61% of incidents were detected by people not responsible for security
  - 35% of incidents were detected by customers
  - Recommendation: Increase employees security awareness and train staff on security policies
  - Could open up more loop holes
  - How would this affect customers?

Critical Comments Cont.

- Vague and/or impractical suggestions

  Example 2:

  - Recommendation: Train staff and suggest they report suspicious co-workers.
  - Large emphasis on the human factor
  - 85% shared their plans with others

Question

7 findings:

- Most incidents required little technical sophistication
- Perpetrators planned their actions
- Financial gain motivated most perpetrators
- Perpetrators did not share a common profile
- Incidents were detected by various methods and people
- Victim organisations suffered financial loss
- Perpetrators committed acts while on the job

Within an area not included in the banking and finance sector, for example the movie production and distribution process, how could the above points be applied?