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

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

Presented by: Marcus Zambrano

What is an Insider?

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

Study Background

- Report examines 23 incidents carried out by 26 insiders in the Banking and Finance sector
- Study cites 7 findings of Insider attacks

Finding 1: Most Incidents required little technical sophistication

- Insiders usually exploited non-technical vulnerabilities such as business rules or organization policies and were usually carried out by individuals with little or no technical expertise
- The Insider usually carried out the incidents by simple, legitimate user commands
- Few cases employed the use of advanced programs or scripts

Finding 2: Perpetrators planned their actions

- Most incidents were thought out and planned in advance
- Individuals close to the perpetrator usually knew of their activity

Finding 3: Financial gain motivated most perpetrators

- Most insiders were motivated by financial gain
- Few were motivated by revenge

Finding 4: Perpetrators did not share a common profile

- Insiders came from a diverse background
- Money the greatest equalizer?
- Most were not known to be difficult employees
- Common perceptions about insiders could be false

Finding 5: Incidents were detected by various methods and people

- Most were detected by non-technical staff such as customers and supervisors
- Insiders were caught by manual procedures, inability to log in, customer complaints, and audits
- System logs were used to obtain identities of insiders

Finding 6: Victim Organizations suffered financial loss

- Insider can cause an organization financial harm by direct and indirect means

Finding 7: Perpetrators committed acts while on the job

- Suspicious activity includes accessing someone else's computer, attempts to download company information to personal computer, and increasing combativeness with co-workers
- Some insiders used remote access to perform incidents (no longer felt they were being watched over their shoulder)
- Organization could offset with closer logging and audits of remote activity

Questions

- Can you really trust a study with such a small sample?
- Paper states: "Many believe that insider attacks are under-reported to law enforcement agencies or prosecutors. Companies may fear the negative publicity or increased liability that may arise as a result of the incidents."