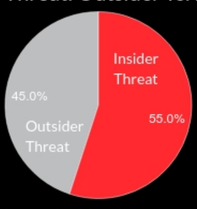
COMBAT INSIDER THREAT

The Government's Most Under Estimated Risk: Espionage

Avatar: The Last Bit

Abdoul Barry, Melissa Chan, Harrison Fernandez, Kristy Li, Mutasem Sayeedi, Randy Rosario, Faisal Khan

Cyber Threat: Outsider vs. Insider



55% of attacks are insider threat
32% of which were caused by malicious insiders
23% were inadvertent actors

*Source: IBM 2015 Cybersecurity Intelligence Index

85% of cases of espionage were discovered by an outside third party.

*Source: 2014 Verizon Data Breach Report

In 62% of espionage cases, the breach went for months before being detected, and in 5% it went on for years.

4

*Source: 2014 Verizon Data Breach Report

Espionage on a Global Level

*Source: FECIE 2008 Industrial Espionage Report

Who is Recruited?

- Students
- Employees

How are they Recruited?

Red Flags of an Insider

Behavioral

- Disgruntlement in company
- Greed
- Personality Problems
- Record of Violating Rules
- Difficulty engaging in social interactions and making decision.
- Vulnerability

Technical

- Encryption software
- Foreign IP traffic
- Foreign Contact
- Foreign preference / loyalty
- Mishandling classified information
- Repeated Violations

Detecting Malicious Insiders

- Implement a behavioral monitoring program

- Use secured tools to decrease detection time of incidents

- Run tests on network by sending "false" requests for information. See if employees will respond.

- Use computer forensic tools to look for signatures or analyze systems.

How to Prevent an Insider Threat

- Take away ex - employee privileges immediately
- Assign right on a need-to-know basis
- Provide employees with online security training to prevent insider threat.
- Urge employees to report something if they see something say something.
- Protect data to prevent data leakage.
- Block all social media use in the company.
- Prevent use of personal devices.
- Monitor networks and software.