Three Ways To Lose Data And One Way To Stop It

Joji Montelibano

CERT

Session ID: DAS-202

Session Classification: Intermediate

Notices

Agenda

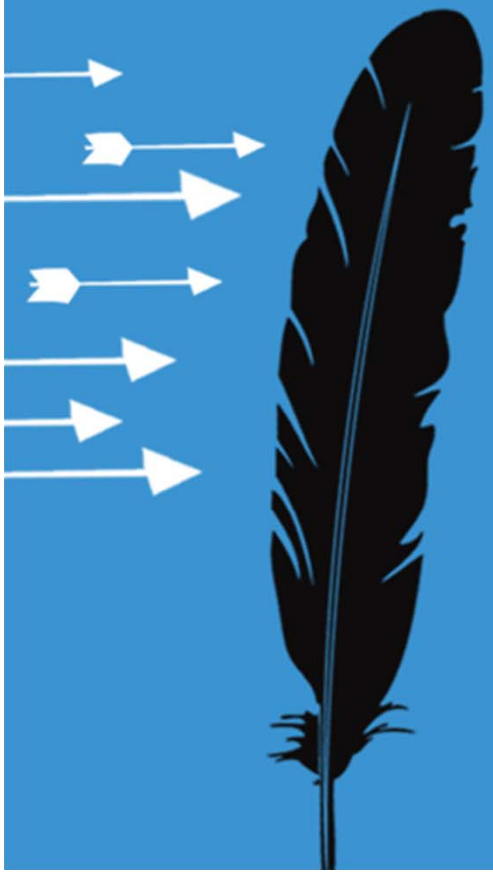
- Introduction to CERT
- Data Theft – How bad is it?
- Case Studies of Data Theft
  - Insider
  - Outsider
  - Malware
- Mitigation Strategy
- Application to your organization

What is CERT?

- Center of Internet security expertise
- Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today
- Located in the Software Engineering Institute (SEI)
  - Federally Funded Research & Development Center (FFRDC)
  - Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

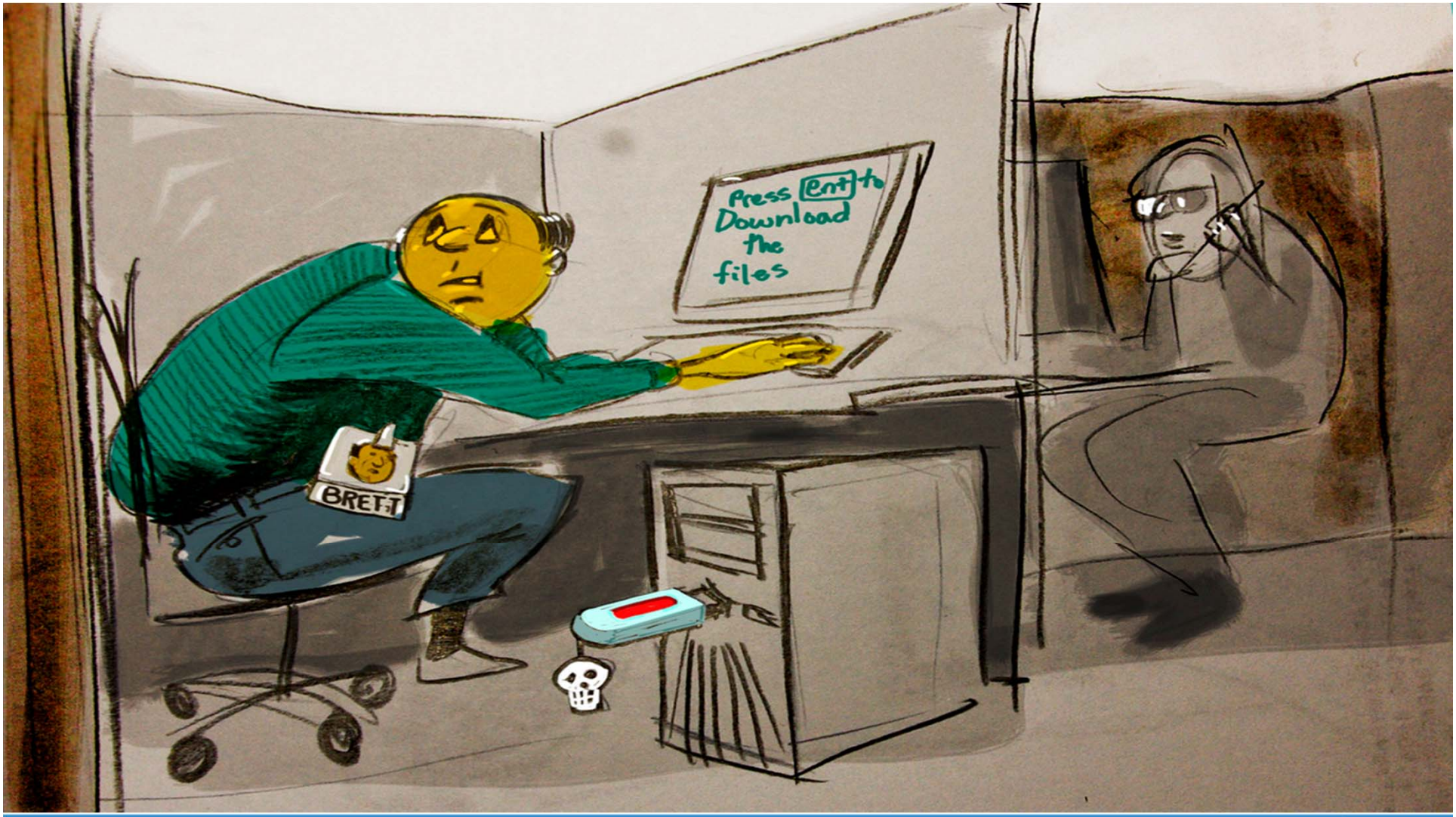
Data Theft – How bad is it?

- "It is inherently difficult to assign an economic value to some types of information that are subject to theft."
  - ONCIX Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (October 2011)



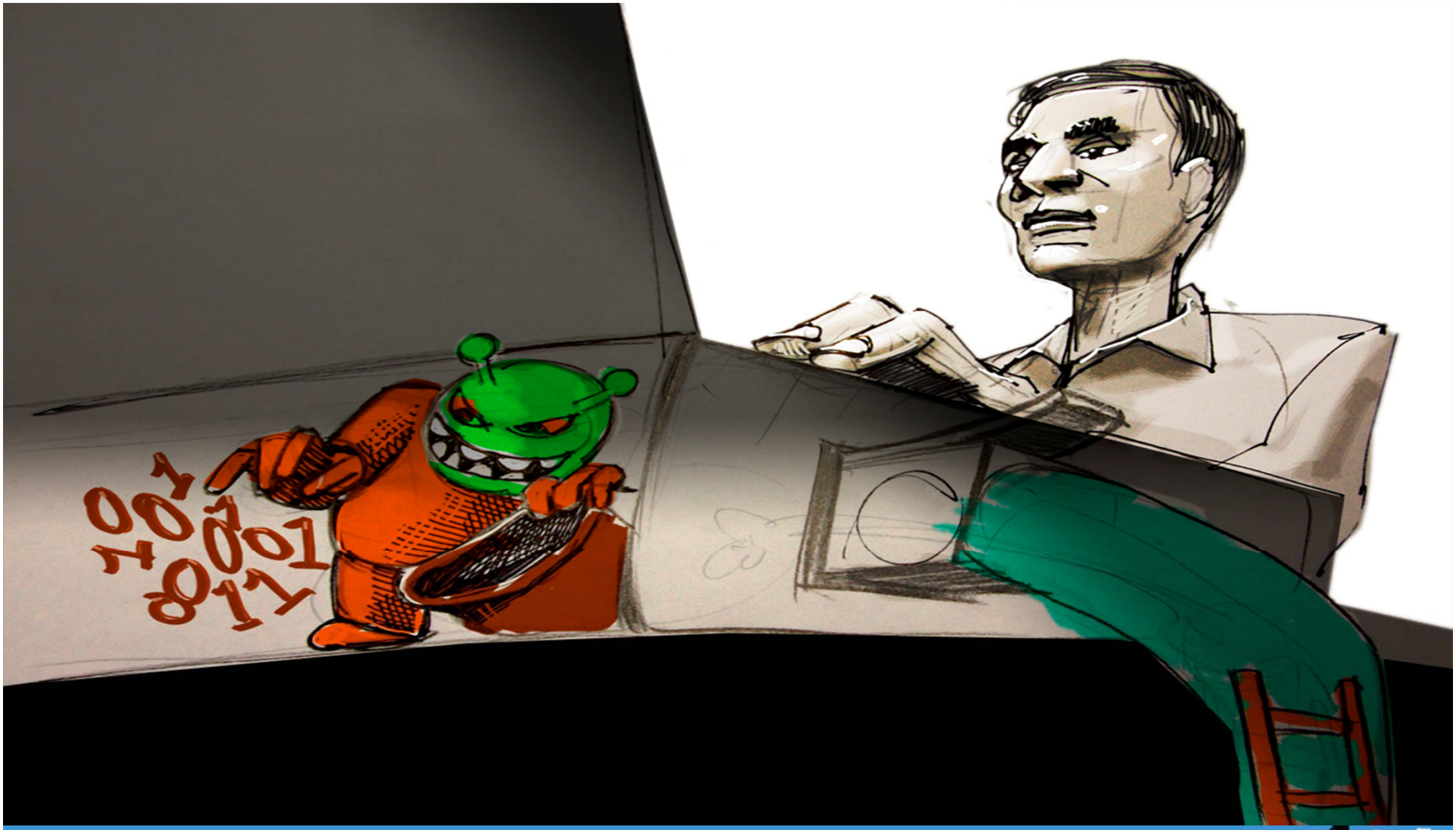
Case Studies

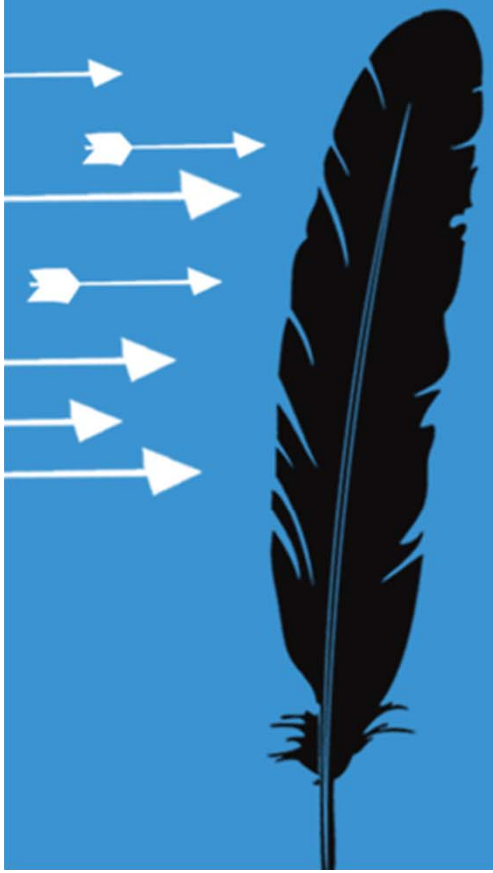
Case Study 1 – Insider Demo



Case Study 2 – Outsider/Hacker Demo

Case Study 3 – Malware Demo

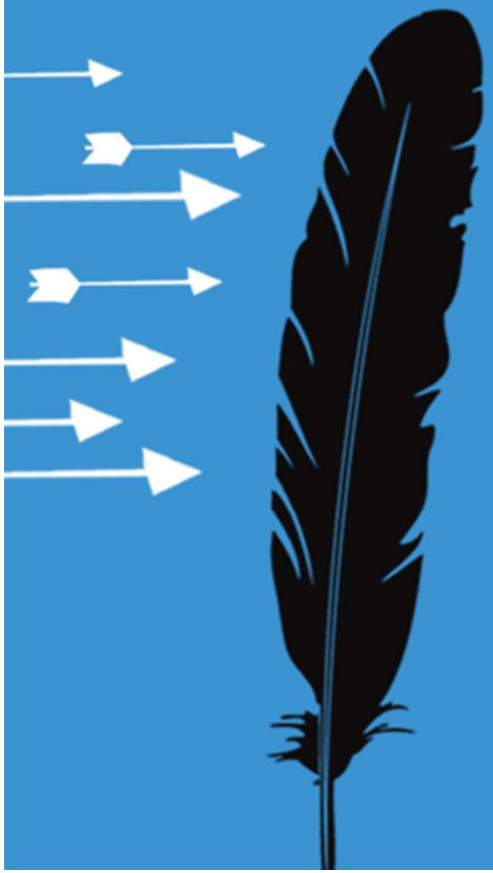




Common Failures

Failures

- We are afraid to use the right tools the wrong way
- We don't know what we're looking for…
  - …so we try to look at EVERYTHING
- Security devices are not generating efficient and analyst-friendly indicators, and warnings



How to stop it?

Mitigation Demo

How to Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Baseline your network activity
  - Baseline your host activity
  - Decrypt encrypted traffic, especially https!
- Within six months you should:
  - Create network and host-based signatures that can capture any deviations from that baseline
    - Network volume anomalies
    - Regular Expressions (e.g. “CONFIDENTIAL”)
    - Use of shared privileged accounts

Useful Tools

- Splunk – http://www.splunk.com
- SiLK – http://tools.netsa.cert.org/silk/
- Snort – http://www.snort.org
- Insider Threat Controls - http://www.cert.org/insider_threat/

Caveats

- Consult with Legal counsel to ensure legality of monitoring measures.
- Make sure you have policies in place that define employer/employee rights and responsibilities!
- Awareness – make sure employees know what is company proprietary information.

Points of Contact

Joji Montelibano
Team Lead, Insider Threat Technical Solutions
CERT Insider Threat Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-6946 – Phone
jmm137@cert.org – Email

Mike Hanley
Information Security Analyst
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-8145 – Phone
mhanley@cert.org – Email