



Three Ways To Lose Data And One Way To Stop It

Joji Montelibano

CERT

Session ID: DAS-202

Session Classification: Intermediate

RSACONFERENCE2012

Notices

© 2011 Carnegie Mellon University

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT ® is a registered mark owned by Carnegie Mellon University.



Software Engineering Institute

Carnegie Mellon

RSACONFERENCE2012



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?

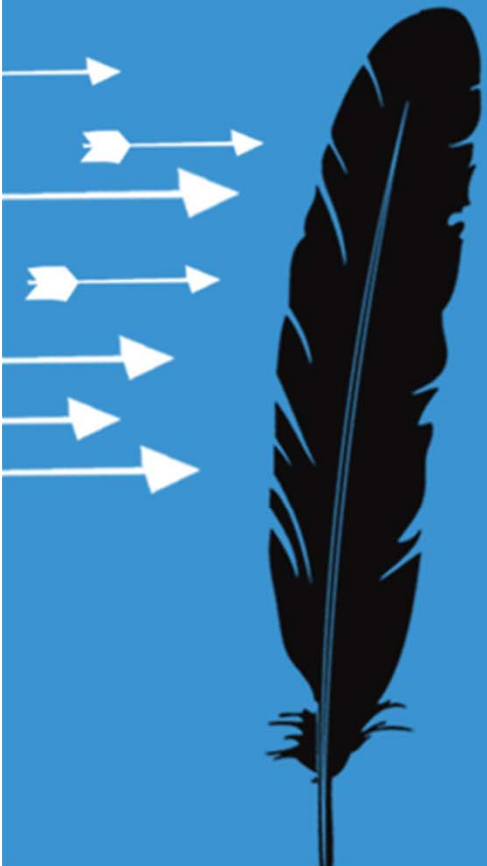


- Center of Internet security expertise
- Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today
- Located in the Software Engineering Institute (SEI)
 - Federally Funded Research & Development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



Data Theft - How bad is it?

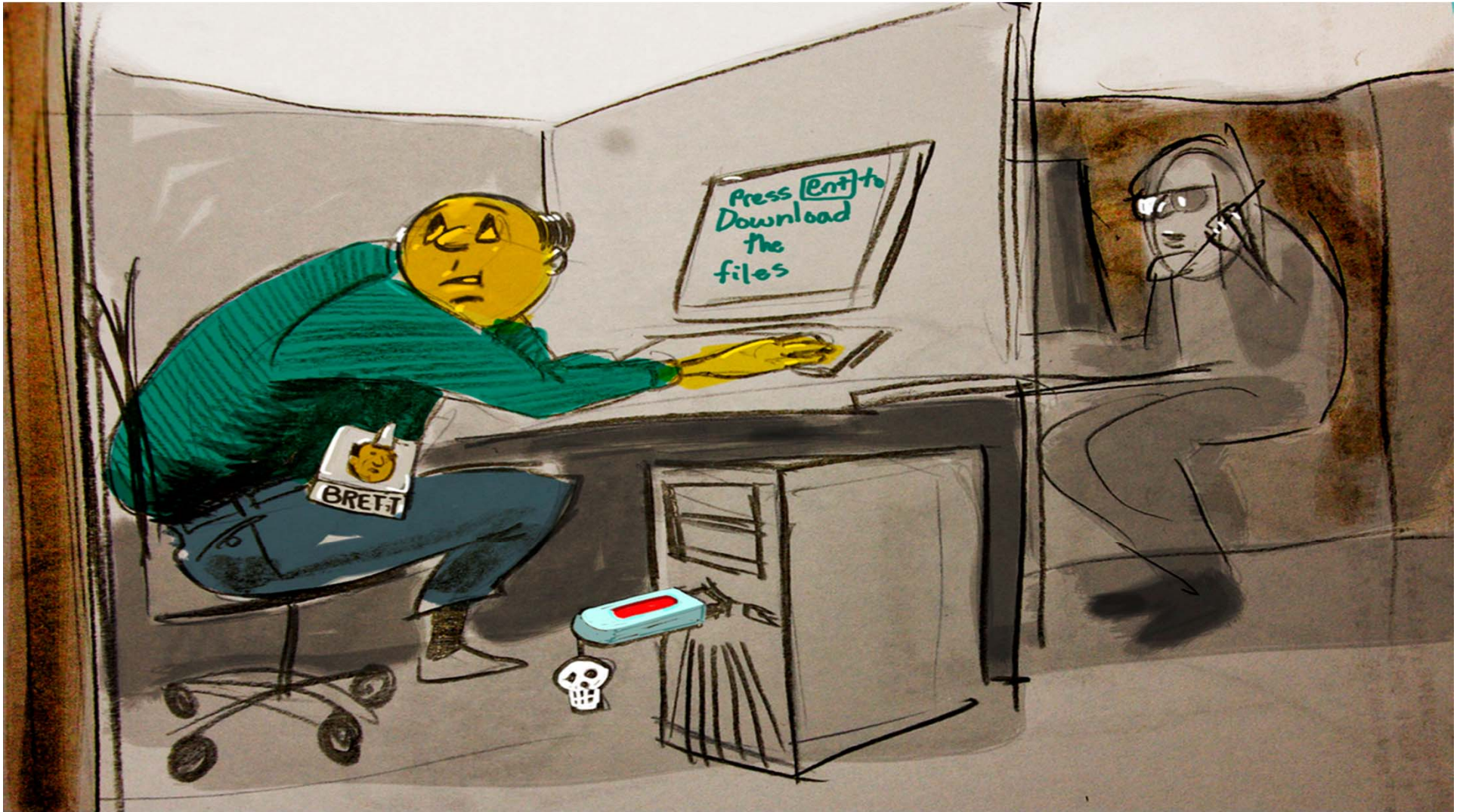
- “It is inherently difficult to assign an economic value to some types of information that are subject to theft.”
 - ONCIX Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (October 2011)



Case Studies

RSACONFERENCE2012

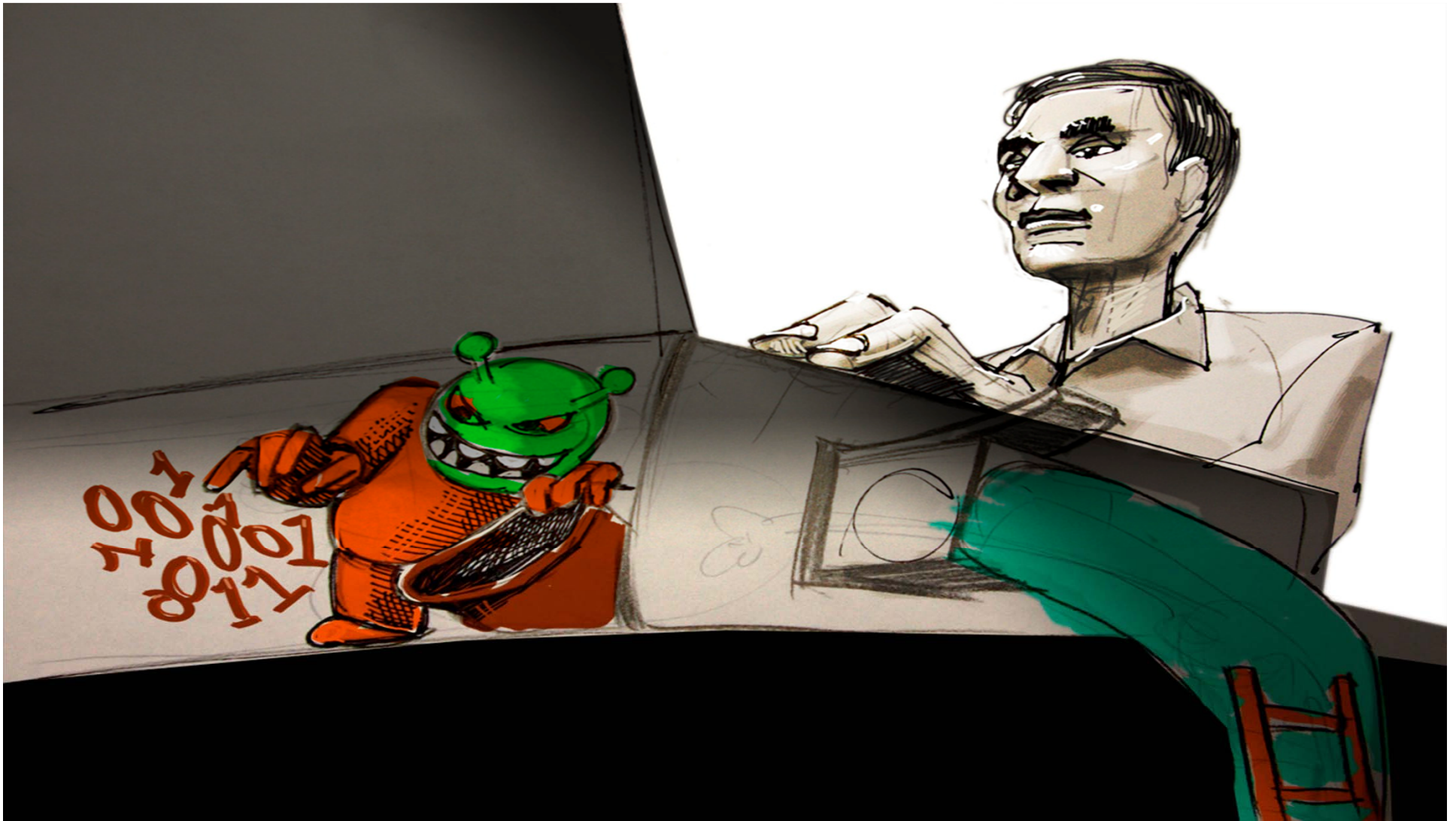
Case Study 1 - Insider Demo



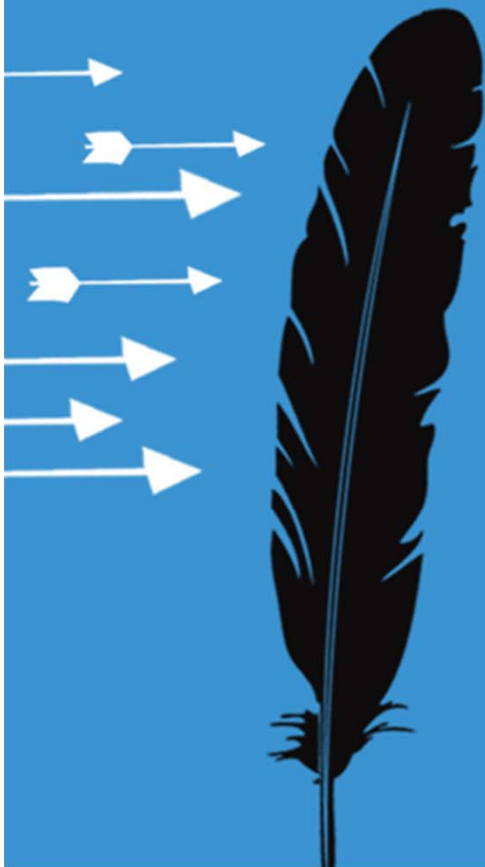
Case Study 2 - Outsider/Hacker Demo



Case Study 3 - Malware Demo



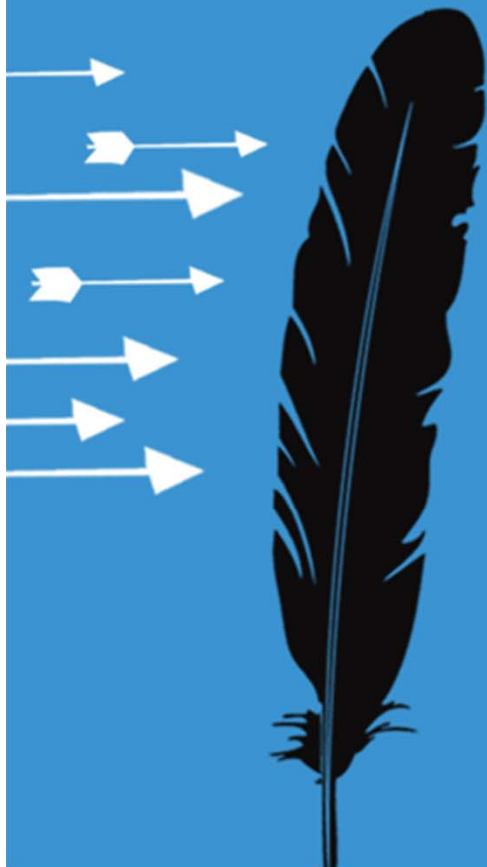
Common Failures



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



Software Engineering Institute | Carnegie Mellon

13

RSACONFERENCE2012



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



Software Engineering Institute

Carnegie Mellon

