Tutorial: Cloud Computing Security

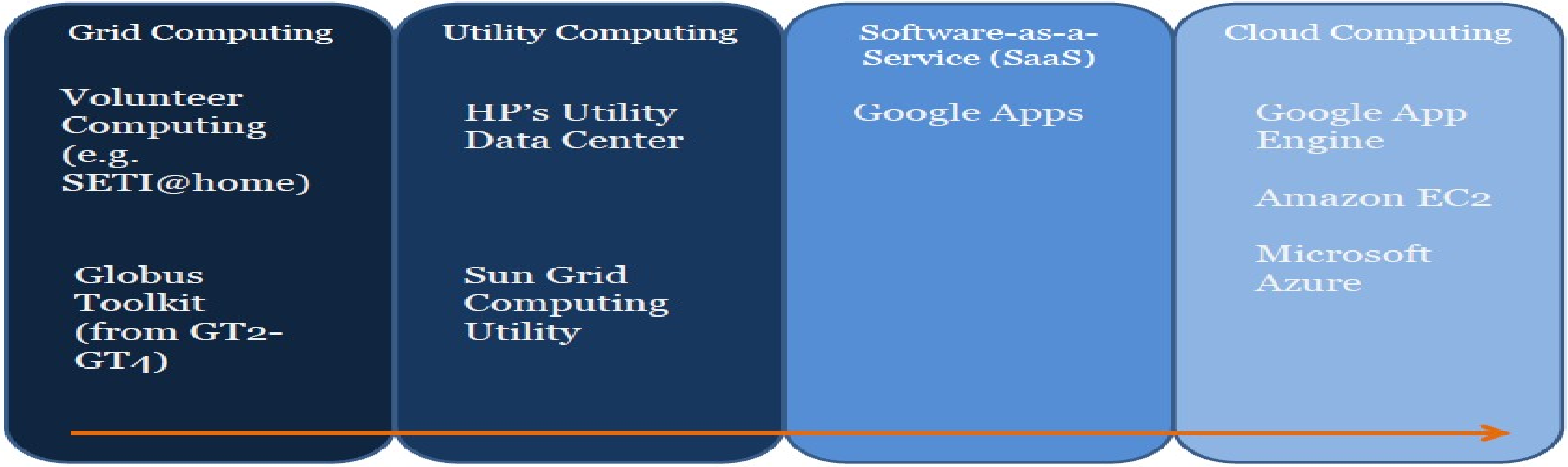
William R. Claycomb, PhD.
Lead Research Scientist
CERT Enterprise Threat and Vulnerability Management Team

Agenda

- Background: Cloud Computing
- Threats to Cloud Security
- Insider Threats in the Cloud
- Present, Past, and Future Attacks
- Threats to Cloud Security 2.0
- Future Research

What is Cloud Computing?

- It’s internet computing
  - Computations are done through the Internet
  - No worry about any maintenance or management of actual resources
- Shared computing resources



Grid Computing

Volunteer Computing (e.g. SETI@home)

Globus Toolkit (from GT2-GT4)

Utility Computing

HP’s Utility Data Center

Sun Grid Computing Utility

Software-as-a-Service (SaaS)

Google Apps

Cloud Computing

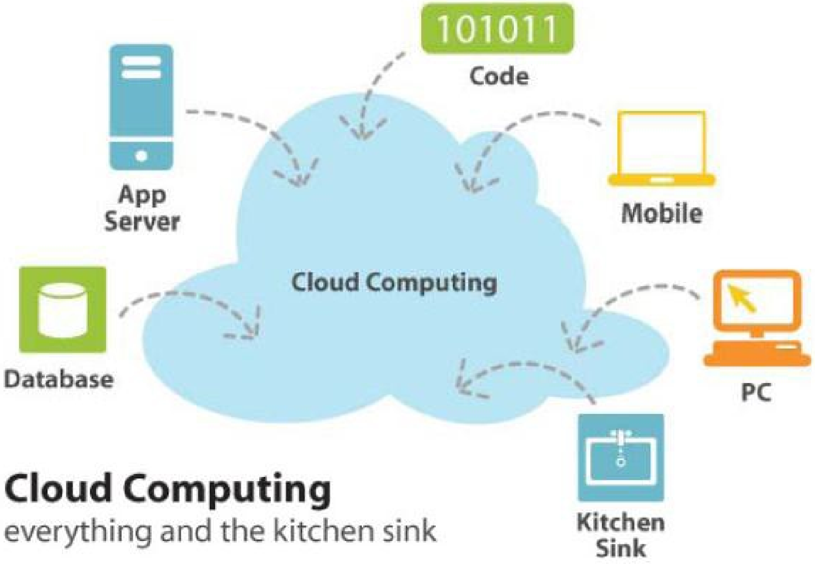
Google App Engine

Amazon EC2

Microsoft Azure

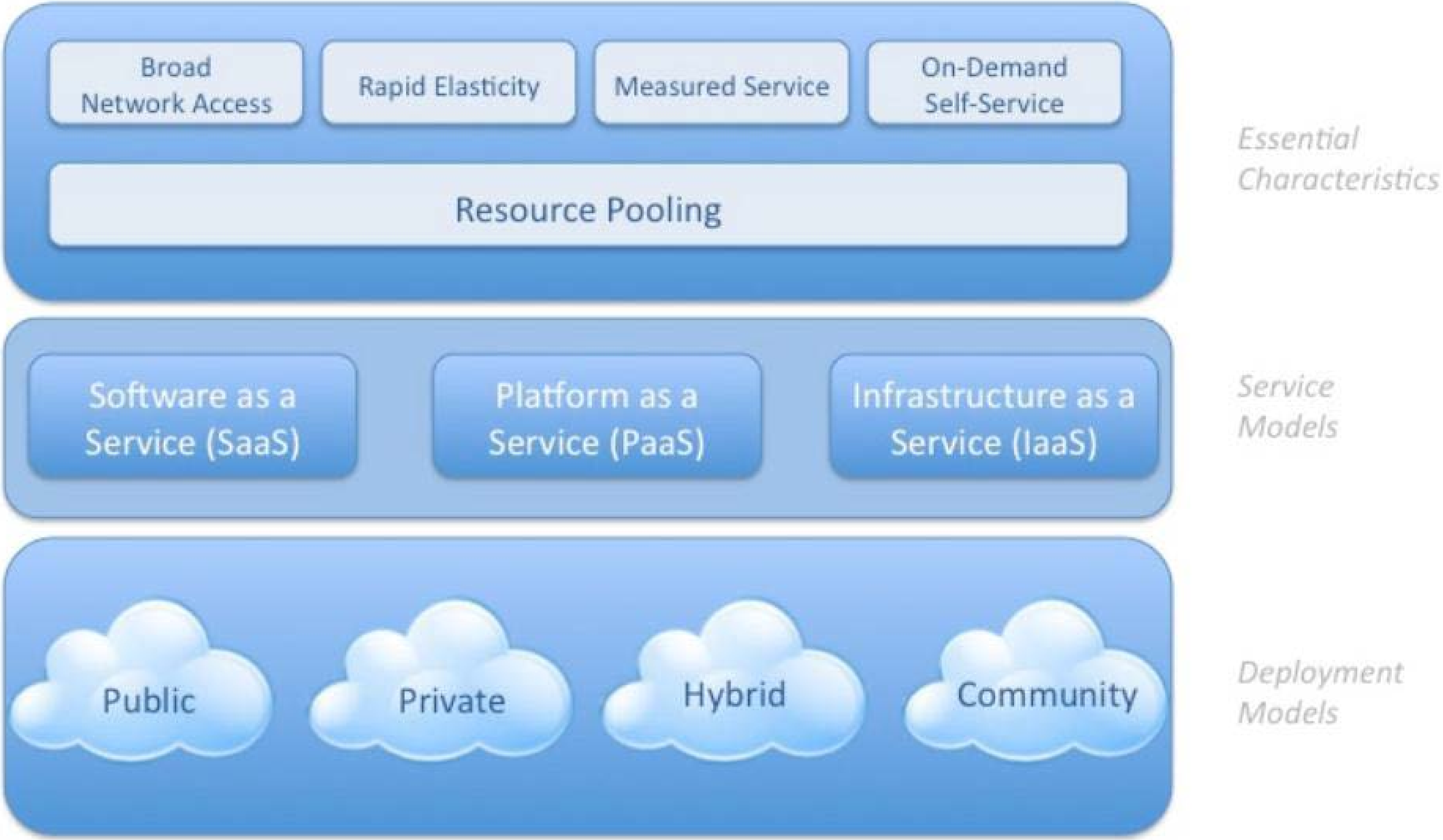
So, Cloud Computing is:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (from NIST)



Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Five Characteristics

- On-demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Measured service

Four Cloud Deployment Models

- Private cloud
  - Enterprise owned or leased
- Community cloud
  - Shared infrastructure for specific community
- Public cloud
  - Sold to the public, mega-scale infrastructure
- Hybrid cloud
  - Composition of two or more clouds

Agenda

- Background: Cloud Computing
- Threats to Cloud Security
- Insider Threats in the Cloud
- Present, Past, and Future Attacks
- Threats to Cloud Security 2.0
- Future Research

Threats to Cloud Computing

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service, and Traffic Hijacking
7. Unknown Risk Profile

From Cloud Security Alliance, 2010

Abuse and Nefarious Use

- Password and key cracking
- DDOS
- Launching dynamic attack points
- Hosting malicious data
- Botnet command and control
- Building rainbow tables
- CAPTCHA solving

- Exploits exist already

Insecure Interfaces and APIs

- Could expose more functionality than intended
- Policy could be circumvented
- Credentials may need to be passed –is the interface secure?

Malicious Insiders

- Particularly poignant for cloud computing
- Little risk of detection
- System administrator qualifications and vetting process for cloud services provider may be different that that of the data owner

Shared Technology Issues

- **Underlying architecture (CPU cache, GPU, etc.) not intended to offer strong isolation properties**
- **Virtualization hypervisor used to mediate access between guest OS and physical resources**
- **Exploits exist (Blue Pill, Red Pill)**

Data Loss or Leakage

- Data is outside the owner’s control
- Data can be deleted or decoupled (lost)
- Encryption keys can be lost
- Unauthorized parties may gain access
- Caused by
    - Insufficient authentication, authorization, and access controls
    - Persistence and remanance
    - Poor disposal procedures
    - Poor data center reliability

Account or Service Hijacking

- Exploits phishing attacks, fraud, or software vulnerabilities
- Credential reuse

Unknown Risk Profile

- **How well is the cloud being maintained?**
  - **Many companies are unwilling to release details**

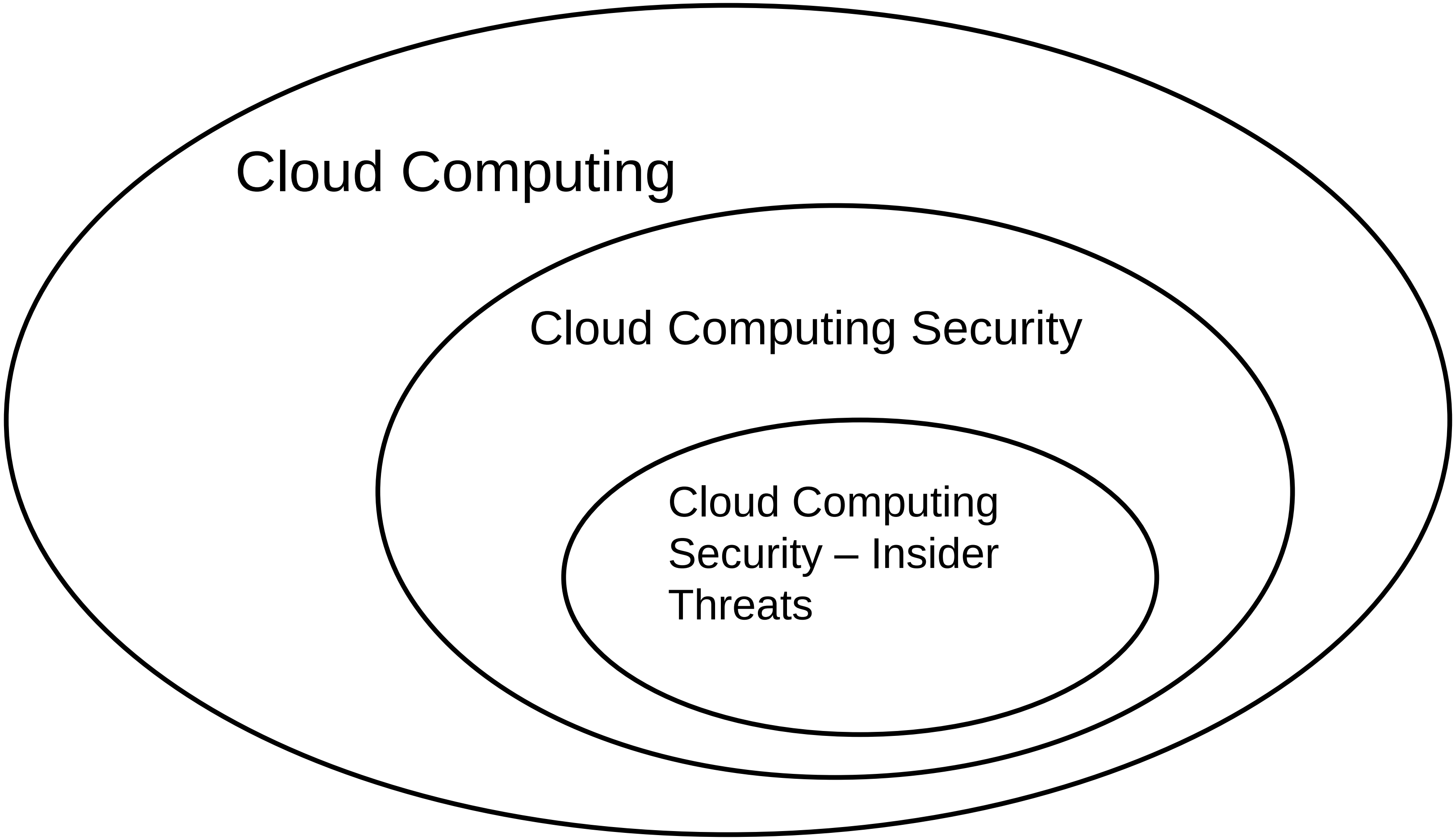
- **Is the infrastructure up to date**
  - **Patches**
  - **Firmware**

- **Does the combination of different service providers create previously unseen vulnerabilities?**

Agenda

- Background: Cloud Computing
- Threats to Cloud Security
- Insider Threats in the Cloud
- Present, Past, and Future Attacks
- Threats to Cloud Security 2.0
- Future Research

Scope



Cloud Computing

Cloud Computing Security

Cloud Computing Security – Insider Threats

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

Part of the Software Engineering Institute (SEI)

- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

What is the CERT Insider Threat Center?

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

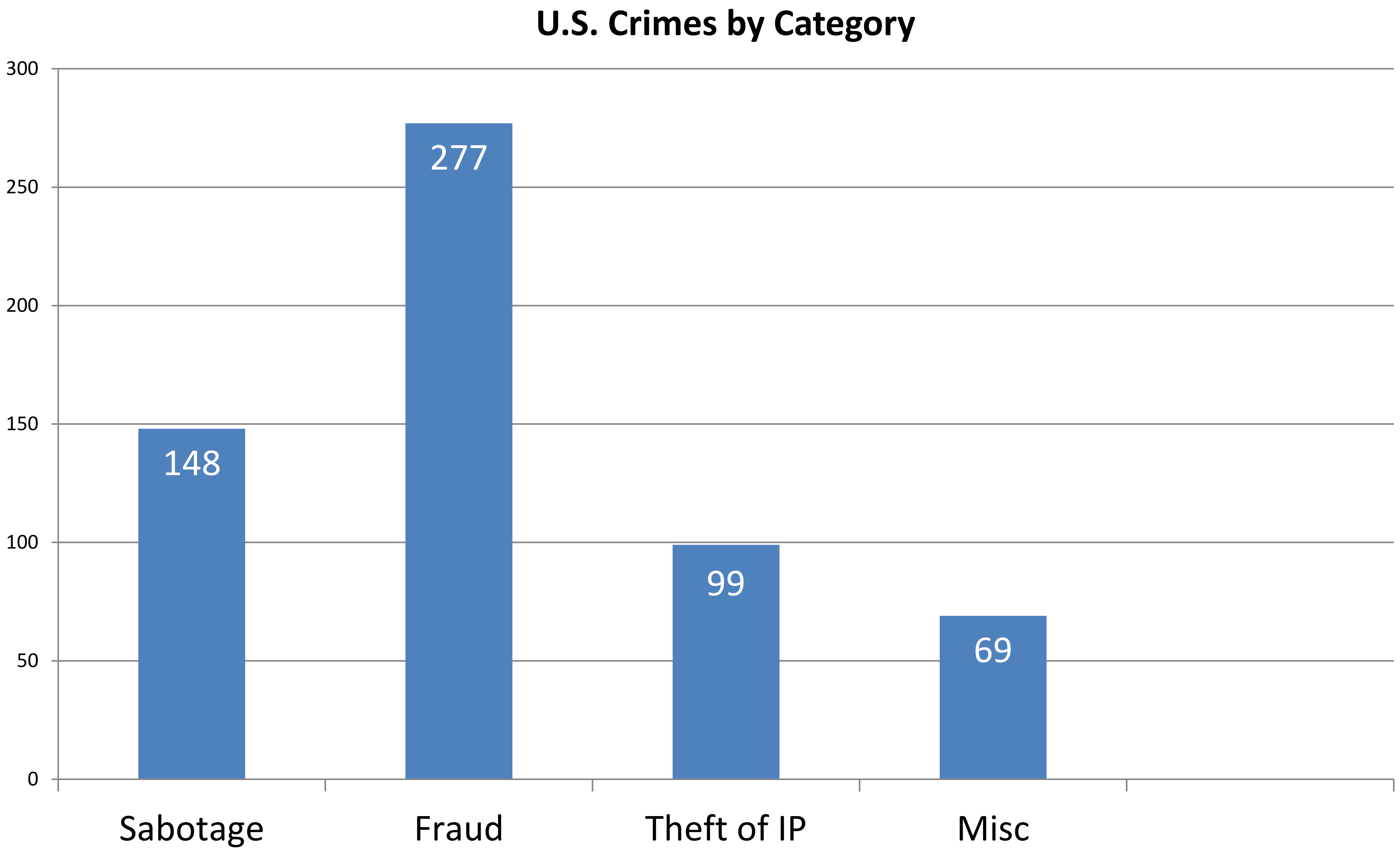
Our mission: *The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.*

Who is a Malicious Insider?

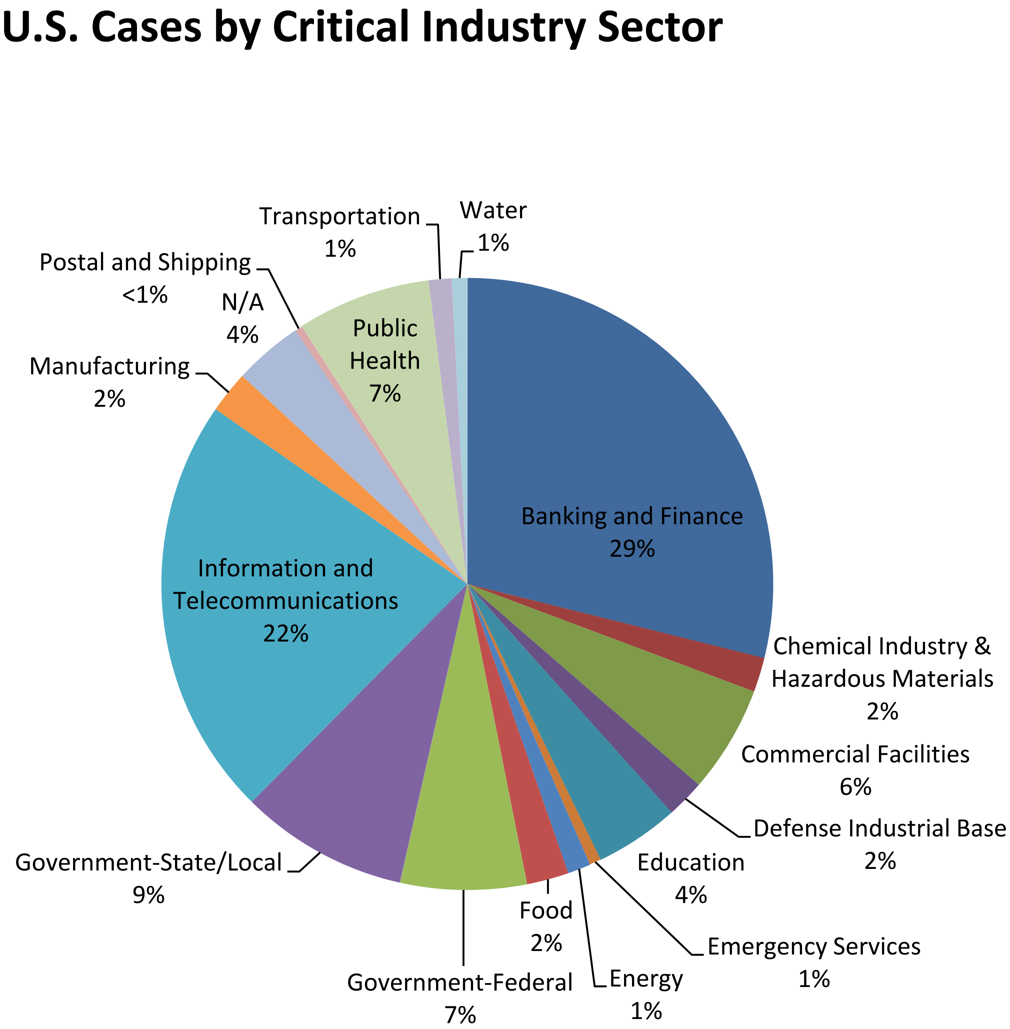
Current or former employee, contractor, or other business partner who

- *has or had authorized access to an organization’s network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.*

CERT's Insider Threat Case Database



Critical Infrastructure Sectors



** *This does not include espionage cases involving classified information*

How bad is the Insider Threat problem?

Insider Threat Issue -1

Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers' systems and/or databases.

Insiders can bypass existing physical and electronic security measures through ***legitimate*** measures.

Insider Threat Issue -2

Has your organization been the victim of an insider attack?

Can you ***confidently*** say you have ***not*** been the victim of an insider attack?

2011 CyberSecurity Watch Survey - 1

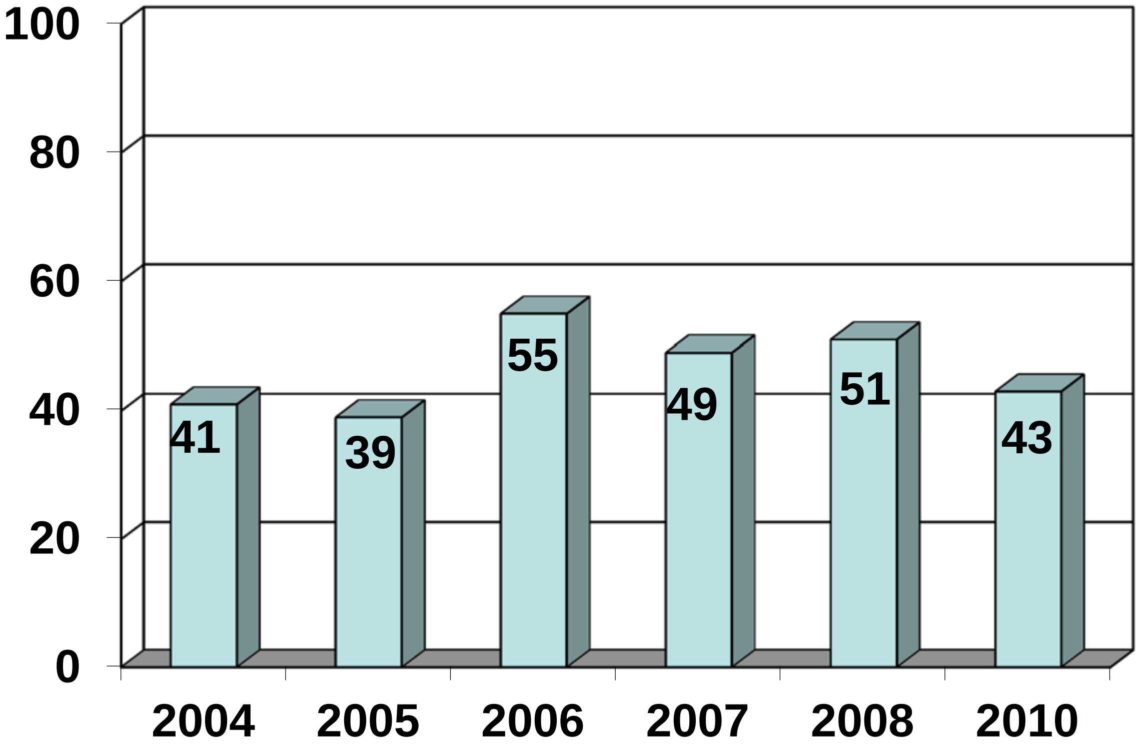
CSO Magazine, USSS, CERT & Deloitte

607 respondents

38% of organizations have more than 5000 employees

37% of organizations have less than 500 employees

Percentage of Participants Who Experienced an Insider Incident



Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

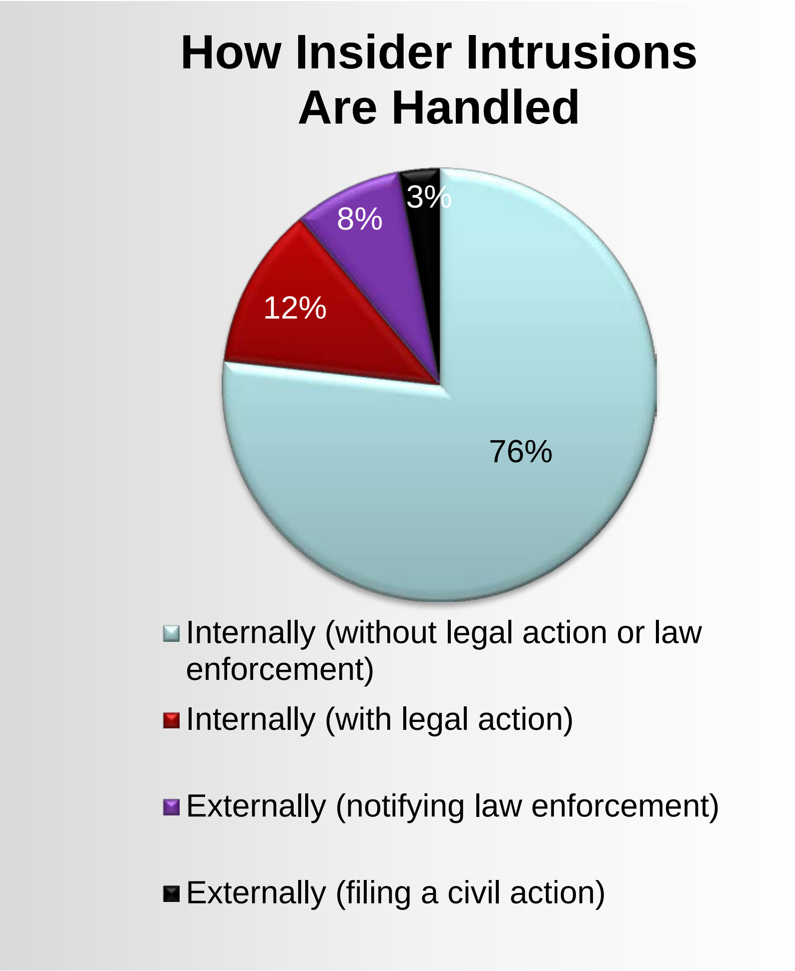
2011 CyberSecurity Watch Survey - 2

46 % of respondents	Damage caused by insider attacks more damaging than outsider attacks
Most common insider e-crime	

Unauthorized access to / use of corporate information	(63%)
Unintentional exposure of private or sensitive data	(57%)
Virus, worms, or other malicious code	(37%)
Theft of intellectual property	(32%)

Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011

2011 CyberSecurity Watch Survey - 3



Reason(s) CyberCrimes were not referred for legal action		
	2011	2010
Damage level insufficient to warrant prosecution	42%	37%
Could not identify the individual/ individuals responsible for committing the eCrime	40%	29%
Lack of evidence/not enough information to prosecute	39%	35%
Concerns about negative publicity	12%	15%
Concerns about liability	8%	7%
Concerns that competitors would use incident to their advantage	6%	5%
Prior negative response from law enforcement	5%	7%
Unaware that we could report these crimes	4%	5%
Other	11%	5%
Don't know	20%	14%
Not applicable	N/A	24%

Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011

IT Sabotage

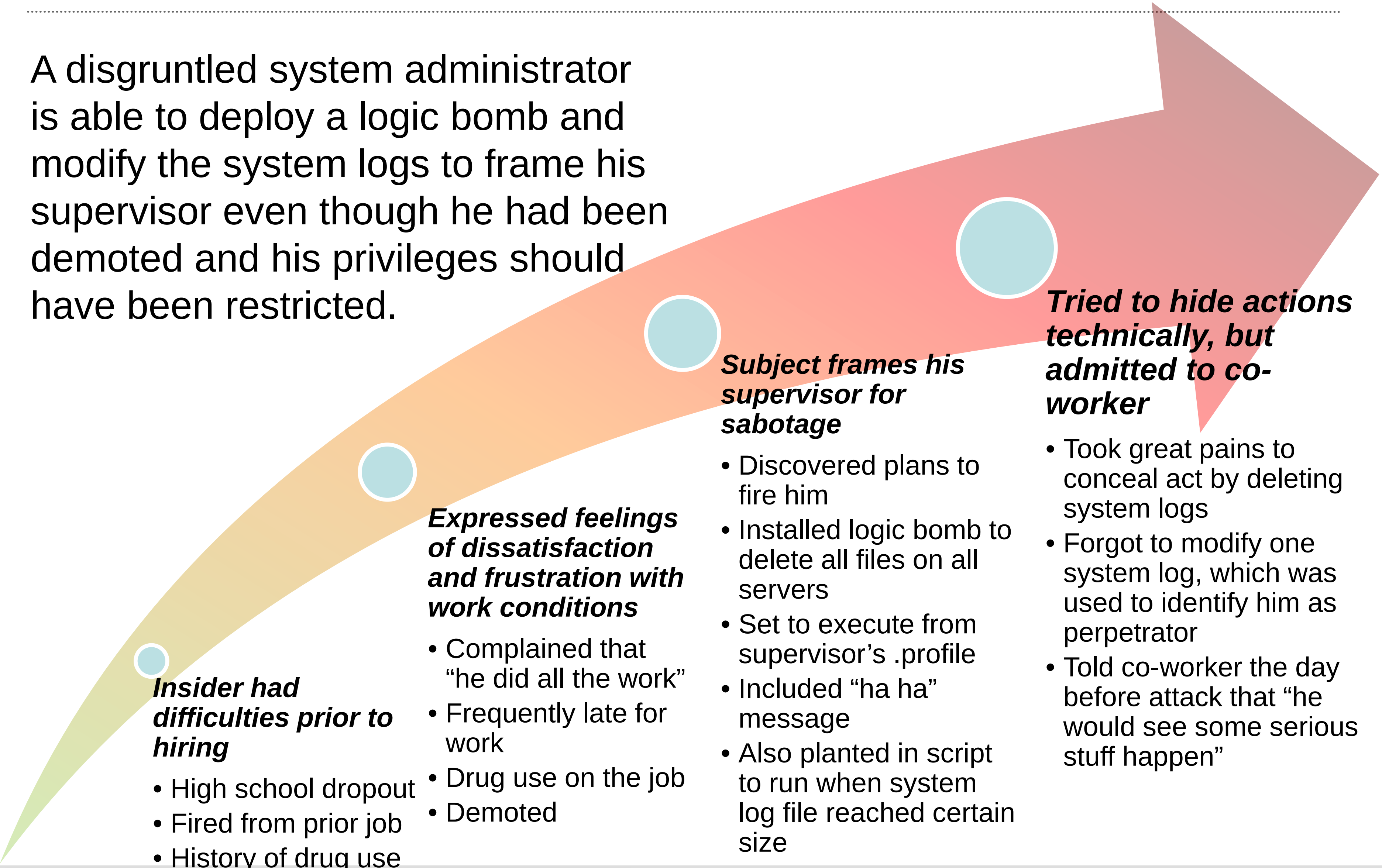
DAN
DAN
SLAM!
Attach File(s)
Do you want to attach DAN_BACKDOOR.EXE?
YES
NO

911 services disrupted for 4 major cities

Disgruntled former employee arrested and convicted for this deliberate act of sabotage.

Insider IT Sabotage: True Story

A disgruntled system administrator is able to deploy a logic bomb and modify the system logs to frame his supervisor even though he had been demoted and his privileges should have been restricted.



Insider had difficulties prior to hiring

- High school dropout
- Fired from prior job
- History of drug use

Expressed feelings of dissatisfaction and frustration with work conditions

- Complained that “he did all the work”
- Frequently late for work
- Drug use on the job
- Demoted

Subject frames his supervisor for sabotage

- Discovered plans to fire him
- Installed logic bomb to delete all files on all servers
- Set to execute from supervisor’s .profile
- Included “ha ha” message
- Also planted in script to run when system log file reached certain size

Tried to hide actions technically, but admitted to co-worker

- Took great pains to conceal act by deleting system logs
- Forgot to modify one system log, which was used to identify him as perpetrator
- Told co-worker the day before attack that “he would see some serious stuff happen”

Other Cases of IT Sabotage

Financial Institution customers lose all access to their money from Friday night through Monday

- Fired system administrator sabotages systems on his way out

A logic bomb sits undetected for 6 months before finally wreaking havoc on a telecommunications firm

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

- Installed malicious code on hospital computers, accessed patient medical records

SCADA systems for an oil-exploration company is temporarily disabled

- A contractor, who's request for permanent employment was rejected, planted malicious code following termination

System administrator at a manufacturing plant, passed over for promotion, deployed "logic bomb" prior to resigning, deleting critical software required to run operation

- Financial damage $10M; Forced to lay off 80 employees

Summary of Findings

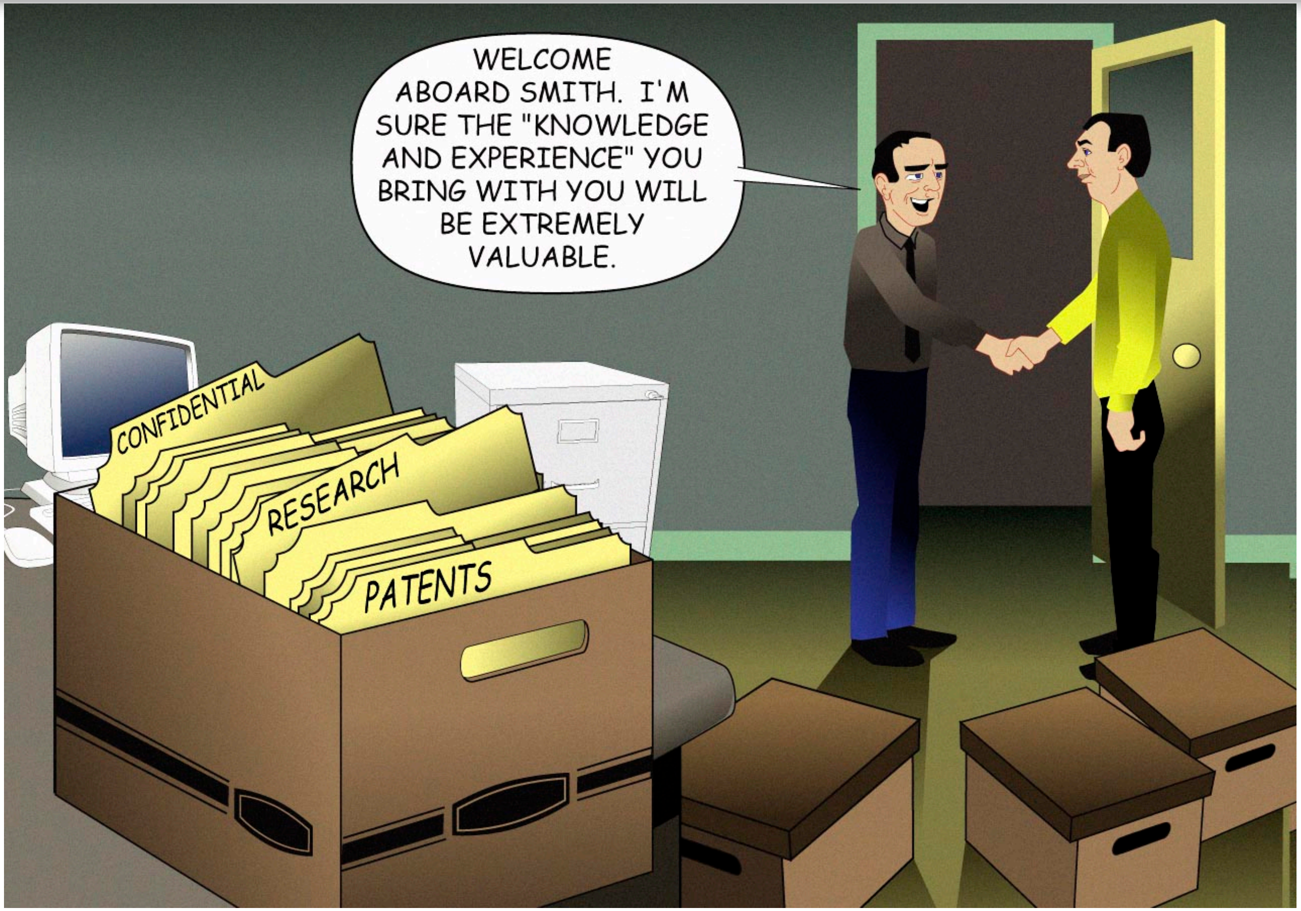
	IT Sabotage
% of crimes in case database**	35%
Current or former employee?	Former
Type of position	Technical (e.g. sys admins or DBAs)
Gender	Male

*** Does not include national security espionage*

Summary of Findings

	IT Sabotage
Target	Network, systems, or data
Access used	Unauthorized
When	Outside normal working hours
Where	Remote access
Recruited by outsiders	None
Collusion	None

Theft of Intellectual Property


WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
CONFIDENTIAL
RESEARCH
PATENTS

TRUE STORY:

Research scientist downloads 38,000 documents containing his company’s trade secrets before going to work for a competitor…

Information was valued at

$400 Million

Other Cases of Theft of IP

A technical operations associate at a pharmaceutical company downloads 65 GB of information, including 1300 confidential and proprietary documents, intending to start a competing company, in a foreign country…

- Organization spent over $500M in development costs

Simulation software for the reactor control room in a nuclear power plant was being run from a different country…

- A former software engineer born in that country took it with him when he left the company.

Summary of Findings

	IT Sabotage	Theft of Intellectual Property
% of crimes in case database**	35%	18%
Current or former employee?	Former	Current
Type of position	Technical (e.g. sys admins or DBAs)	Technical (71%) - scientists, programmers, engineers Sales (29%)
Gender	Male	Male

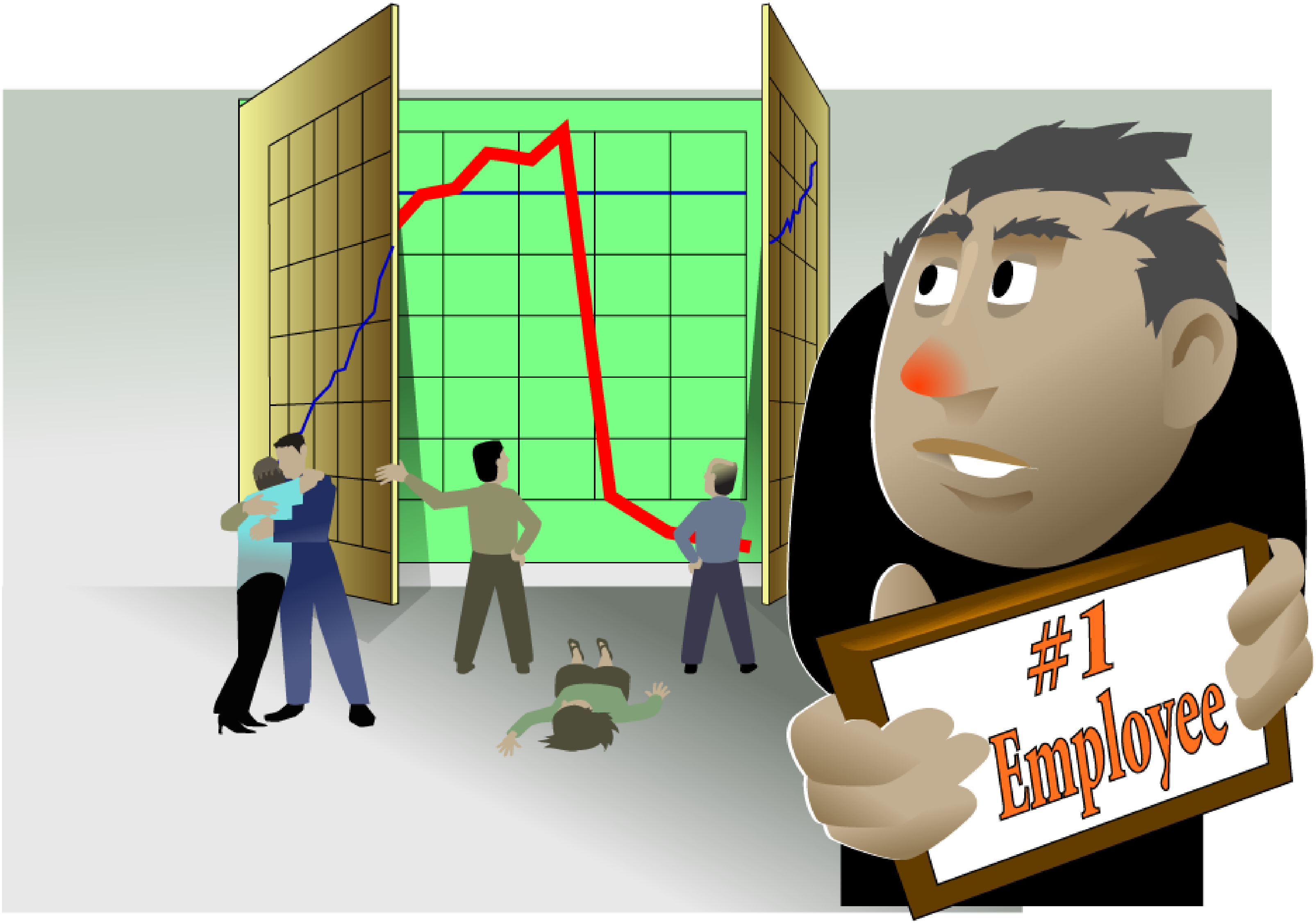
***** Does not include national security espionage***

Summary of Findings

	IT Sabotage	Theft of Intellectual Property
Target	Network, systems, or data	IP (trade secrets) – 71% Customer Info – 33%
Access used	Unauthorized	Authorized
When	Outside normal working hours	During normal working hours
Where	Remote access	At work
Recruited by outsiders	None	Less than 1/4
Collusion	None	Almost ½ colluded with at least one insider; ½ acted alone

Fraud

An Incident of Insider Fraud



Fake drivers license sold to undercover agent claiming to be on the "No Fly list"

Other Cases of Fraud

An accounts payable clerk, over a period of 3 years, issues 127 unauthorized checks to herself an others...

- Checks totaled over $875,000

A front desk office coordinator stole PII from hospital...

- Over 1100 victims and over $2.8 M in fraudulent claims

A database administrator at major US Insurance Co. downloaded 60,000 employee records onto removable and solicited bids for sale over the Internet

An office manager for a trucking firm fraudulently puts her husband on the payroll for weekly payouts, and erases records of payments…

- Over almost a year loss of over $100K

Summary of Findings

	IT Sabotage	Theft of Intellectual Property	Fraud
% of crimes in case database**	35%	18%	40%
Current or former employee?	Former	Current	Current
Type of position	Technical (e.g. sys admins or DBAs)	Technical (71%) - scientists, programmers, engineers Sales (29%)	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)
Gender	Male	Male	Fairly equally split between male and female

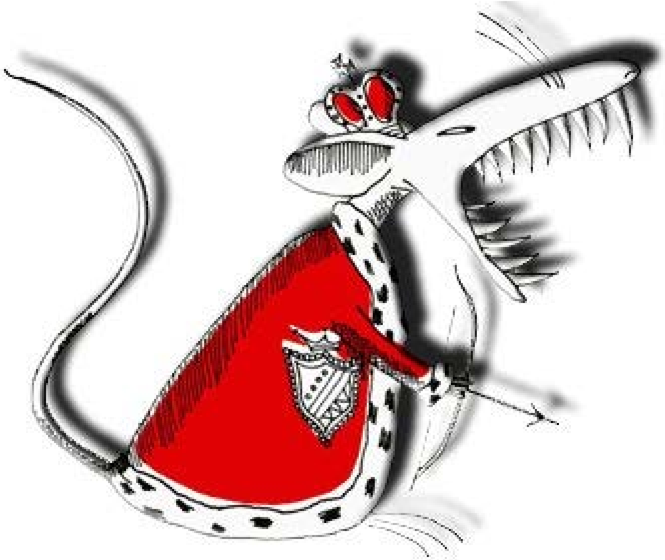
***** Does not include national security espionage***

Insider Threats in the Cloud

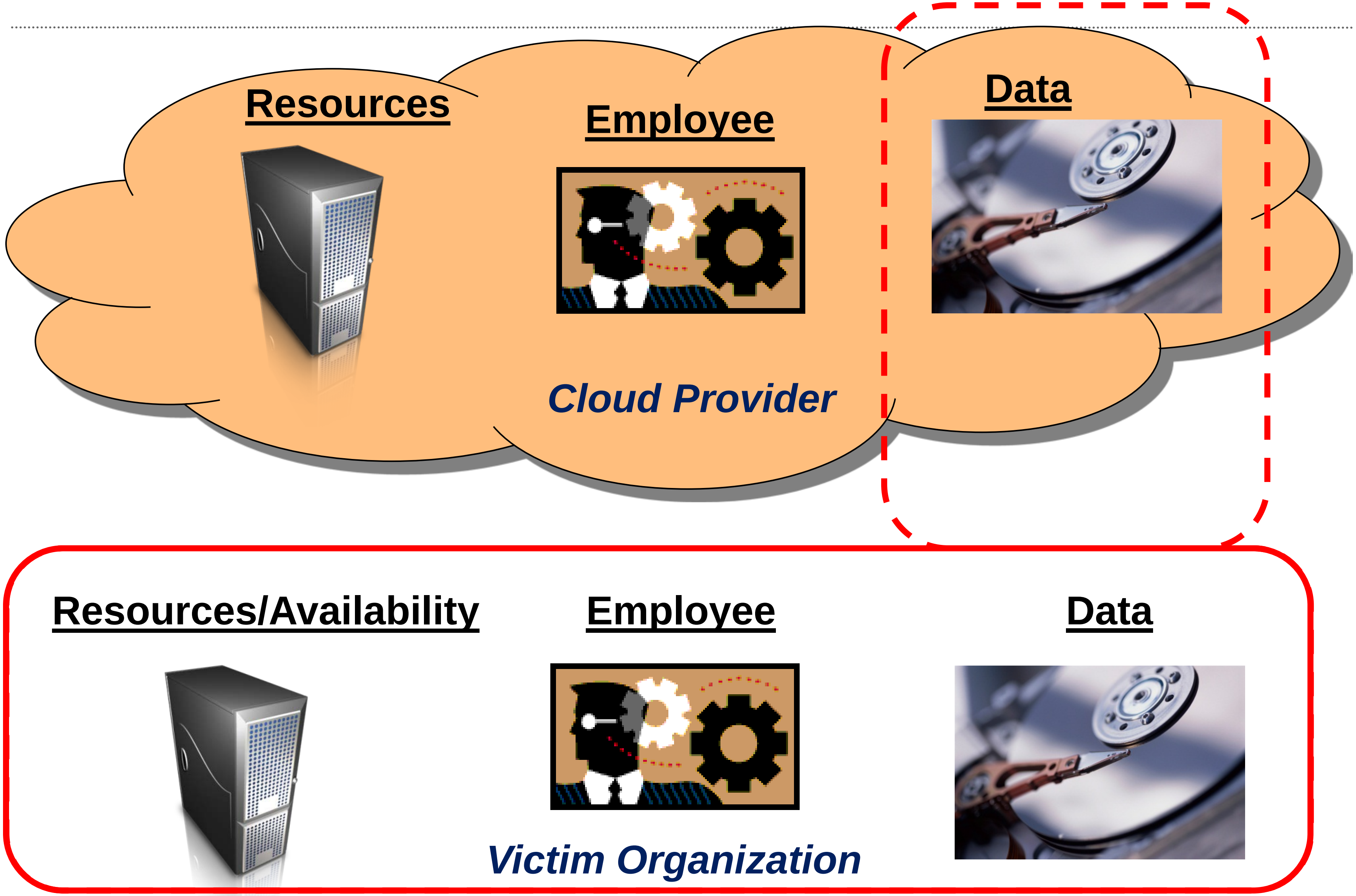
Identified by Cloud Security Alliance (CSA) “Top Threats to Cloud Computing, v 1.0”

- Malicious insider working for cloud provider

But there are other insider threats related to cloud computing…



Provider / Organization Relationship



Resources

Employee

Data

Cloud Provider

Resources/Availability

Employee

Data

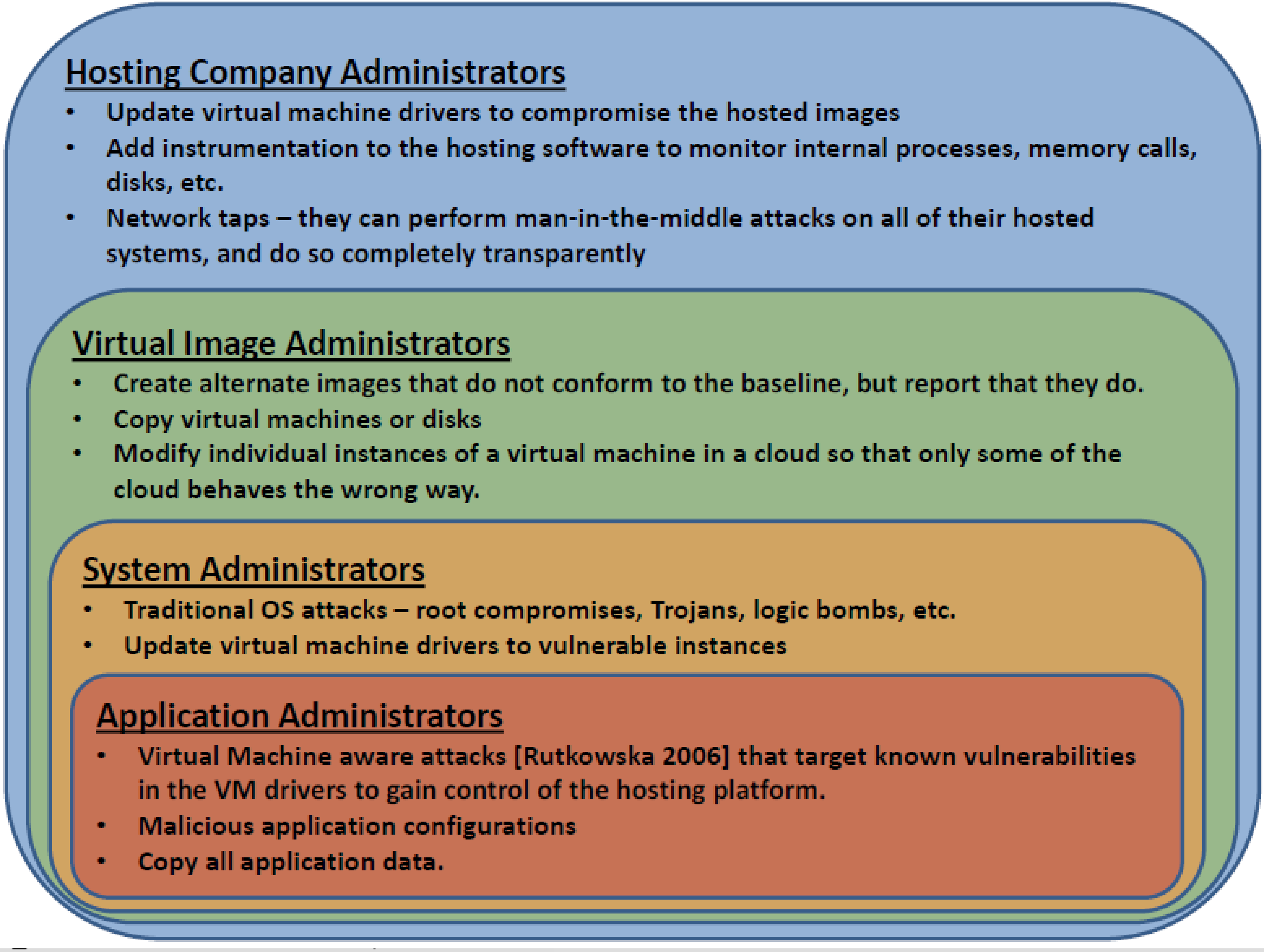
Victim Organization

Cloud-Related Malicious Insider Threats

Malicious Cloud Provider Employee

- *Rogue Administrator*
  - We’ve seen cases of insider threats from trusted business partners
  - True examples of cloud service providers are rare, but do exist
  - Important to weigh the risks carefully; the provider has much to lose as well

Rogue Administrators



Hosting Company Administrators

- Update virtual machine drivers to compromise the hosted images
- Add instrumentation to the hosting software to monitor internal processes, memory calls, disks, etc.
- Network taps – they can perform man-in-the-middle attacks on all of their hosted systems, and do so completely transparently

Virtual Image Administrators

- Create alternate images that do not conform to the baseline, but report that they do.
- Copy virtual machines or disks
- Modify individual instances of a virtual machine in a cloud so that only some of the cloud behaves the wrong way.

System Administrators

- Traditional OS attacks – root compromises, Trojans, logic bombs, etc.
- Update virtual machine drivers to vulnerable instances

Application Administrators

- Virtual Machine aware attacks [Rutkowska 2006] that target known vulnerabilities in the VM drivers to gain control of the hosting platform.
- Malicious application configurations
- Copy all application data.

Cloud-Related Malicious Insider Threats

Malicious Local Employee

- Exploiting weaknesses of the Cloud
    - Example weakness – the organization may not have direct control of the resources providing data/services
    - Most likely Fraud or Theft of IP
    - Don’t count out sabotage, though
- Attacking organization data in the cloud
    - Access control models may be different
    - Effecting change quickly may be difficult
        - Example case: Email provider
    - Example exploit: Replication Lag
        - Similar to Byzantine Generals Problem

Cloud-Related Malicious Insider Threats

Malicious Local Employee

- Using the cloud to attack the organization
  - Example weakness – the Cloud is a very powerful tool; and a very powerful weapon, what if it is turned back on the org itself?
  - A financially troubled insider exploits the processing power of cloud services to crack password files, allowing unrestricted access to company bank accounts.
  - A disgruntled insider uses several relatively cheap, easily configured cloud systems to launch a distributed denial of service attack on his organization, hindering incident investigation and limiting forensic analysis.
  - A insider planning to leave the company leverages cloud storage to consolidate and exfiltrate sensitive information to take to a new job with a competitor.

Protecting Against Malicious Insiders

- Rogue Administrators
  - From CSA
    - Supply chain management
    - HR requirements as part of legal contracts
    - Require information security and management practices transparency
    - Determine security breach notification processes
  - Enforcement of SLAs
  - Encryption
    - Where do you keep the keys?
  - What is the cost to the host provider?

Protecting Against Malicious Insiders

- Those that exploit weaknesses in the Cloud
  - Diligence in planning during implementation, transition, migration, and maintenance of cloud services
  - Current research continues in authorization and access control
    - Directory Virtualization
    - RBAC
  - Clear plans for handling incidents
    - Including authentication and authorization between org and host provider

Protecting Against Malicious Insiders

- Those that use the Cloud against you
  - Data Loss Prevention (DLP)
  - Limit access to potential exfiltration resources
  - Create separate environments for external communication

Future Research – Cloud Insider Threats

- Socio-technical approach
- Predictive models
- Identifying cloud-based indicators
- Virtualization and hypervisors
- Awareness and reporting
- Normal user behavior analysis
- Policy integration

Predictive Models

- Centre for the Protection of National Infrastructure (CPNI)
  - Ongoing insider threat risk management program, beginning before hire
- Greitzer, et al.
  - Identifies and weighs indicators of insider risk
  - Develops a reasoning system to integrate multiple data sources

Identifying Cloud-based Indicators

- Many indicators from other domains also apply here
  - Unusual search activity
  - Acquiring unknown access paths
- What about Cloud-specific indicators?
  - SLA violation
  - Improper virtual machine management
  - Using suspicious software
  - Performing similar activities across different platforms and/or customer systems
  - Lack of concern for company policy or protection of others’ data
- Four types of indicators (Ilgun, et al.)
  - Threshold, anomaly, rule-based, model-based

Virtualization and Hypervisors

- Attacks practically require authorized access to carry out
  - Hard to accidentally leak information across the hypervisor
- New technologies to separate virtualization at the hardware level

Awareness and Reporting

- May 2012 FBI news story, “Economic Espionage: How to Spot a Possible Insider Threat.”
- Many insiders in CERT’s database were detected through co-worker reporting
  - Or should have been detected…

Normal User Behavior Analysis

- Necessary to detect the clever insider
- Very little research in the literature on insider threat research that compares indicators to normal data
- Also useful for benchmarking, etc.

Policy Integration

- Necessary to merge policies from the org and the cloud
- Takabi et al. propose a trust management framework for policy integration and an ontology to address semantic heterogeneity among policies.
- Researchers should be careful to note implementation and/or enforcement constraints real-world organizations face.

Agenda

- Background: Cloud Computing
- Threats to Cloud Security
- Insider Threats in the Cloud
- Present, Past, and Future Attacks
- Threats to Cloud Security 2.0
- Future Research

Past Threats

- Blue Pill, Red Pill
  - Joanna Rutkowska, Black Hat 2006
  - Blue Pill – Infect machine
  - Red Pill – Detect infection
- Cloudburst

Present Threats

US-CERT VU#649219 (CloudBurst)

SYSRET 64-bit operating system privilege escalation vulnerability on Intel CPU hardware

Future Threats

- Encryption
- Supply chain
- Targeted attacks – corporate espionage
    - Provider collusion

Future Research

- Measurement/metrics
- Forensics
- Incident Response
- SLA enforcement
- Isolation
- Attack vectors
- CSA Reference Architecture
- ???

Threats to Cloud Security 2.0

Web site

Opportunity to contribute

Thank You!

Contact Info:

William R. Claycomb

claycomb@cert.org

Lead Research Scientist

CERT Insider Threat Research Center

Carnegie Mellon University