FEDERAL BUREAU OF INVESTIGATION

“Fidelity, Bravery, and Integrity”

Combating the Insider Threat at the FBI: Real World Lessons Learned

Patrick Reidy

Disclaimer and Introduction

The views expressed in this presentation are those of the presenter and **do not** reflect the official policy or position of the Department of Justice, the Federal Bureau of Investigation, or the U.S. Government, nor does it represent an endorsement of any kind.

The 5 Lessons

1 Insider threats are not hackers

2 Insider threat is not a technical or “cyber security” issue alone

3 A good insider threat program should focus on deterrence, not detection

4 Avoid the data overload problem

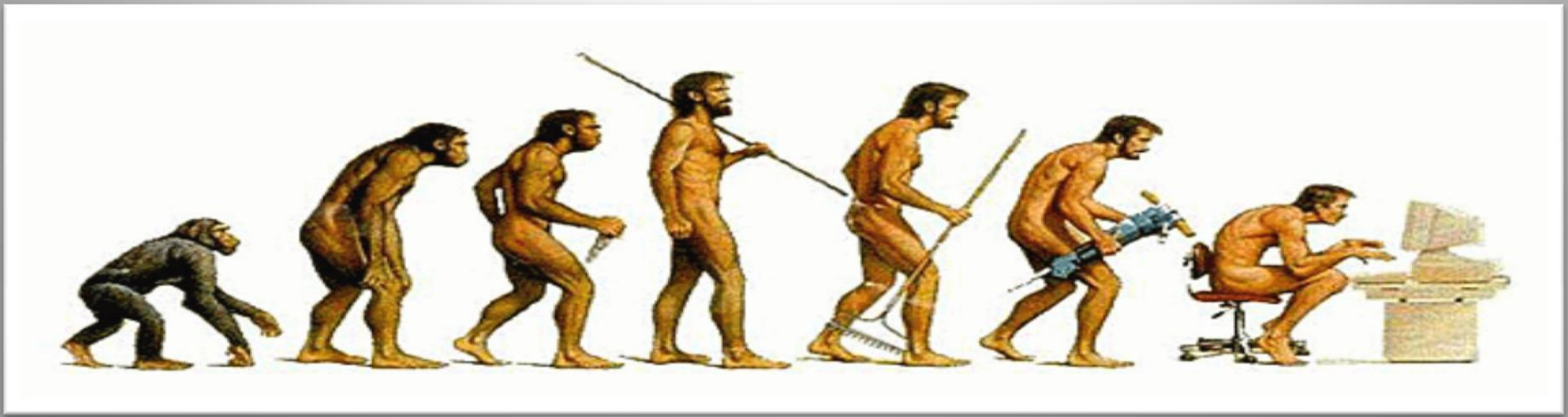
1 Use behavioral analytics

Our IA Program & Evolution

Threat focus: Computer intrusion
Protection: N/W perimeter, firewalls, IDS, proxies, A/V, DHCP, DNS
Detection technique: signature based

Threat focus: APT
Protection: + Internal N/W, host A/V, OS, application logs, email, net flow
Detection technique: + N/W anomaly

Threat focus: Insider
Protection: + DLP, DRM, Personnel data, data object interaction, non-N/W data
Detection technique: + data mining, behavioral



The Approach

Known Bad

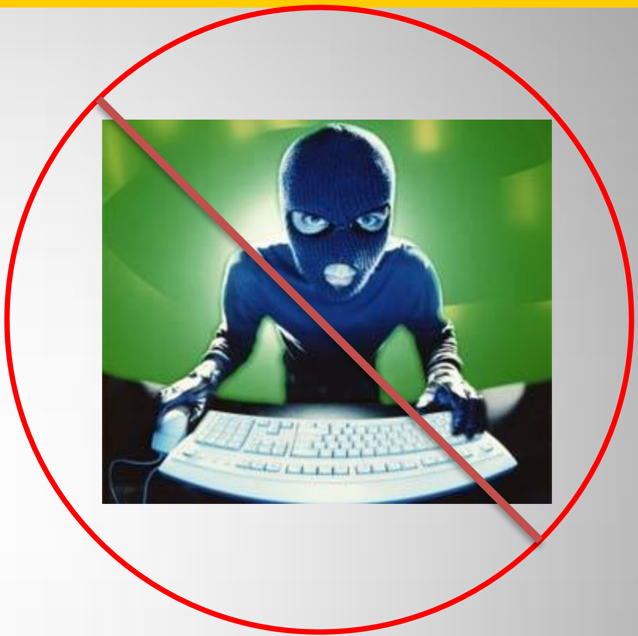
vs.

Assumed Good

- Test: 65 espionage cases and the activities of over 200 non-model employees
- Control: The rest of the user population

***Lesson #1*:**
The Misunderstood Threat

- NOT hackers
- People who joined organizations with no malicious intent
- Most tools and techniques are designed with the hacker in mind



VS.

+

Not The “Knuckle Head” Problem

- We lose most battles 2 feet from the computer screen
- 24% of incidents, 35% of our time
- The “knuckle head” problem
- Policy violations, data loss, lost equipment, etc.
- Address with user training campaigns & positive social engineering
- 7% drop incidents since last year

The Most Common Threat of Them All!?!?
Not So Fast..

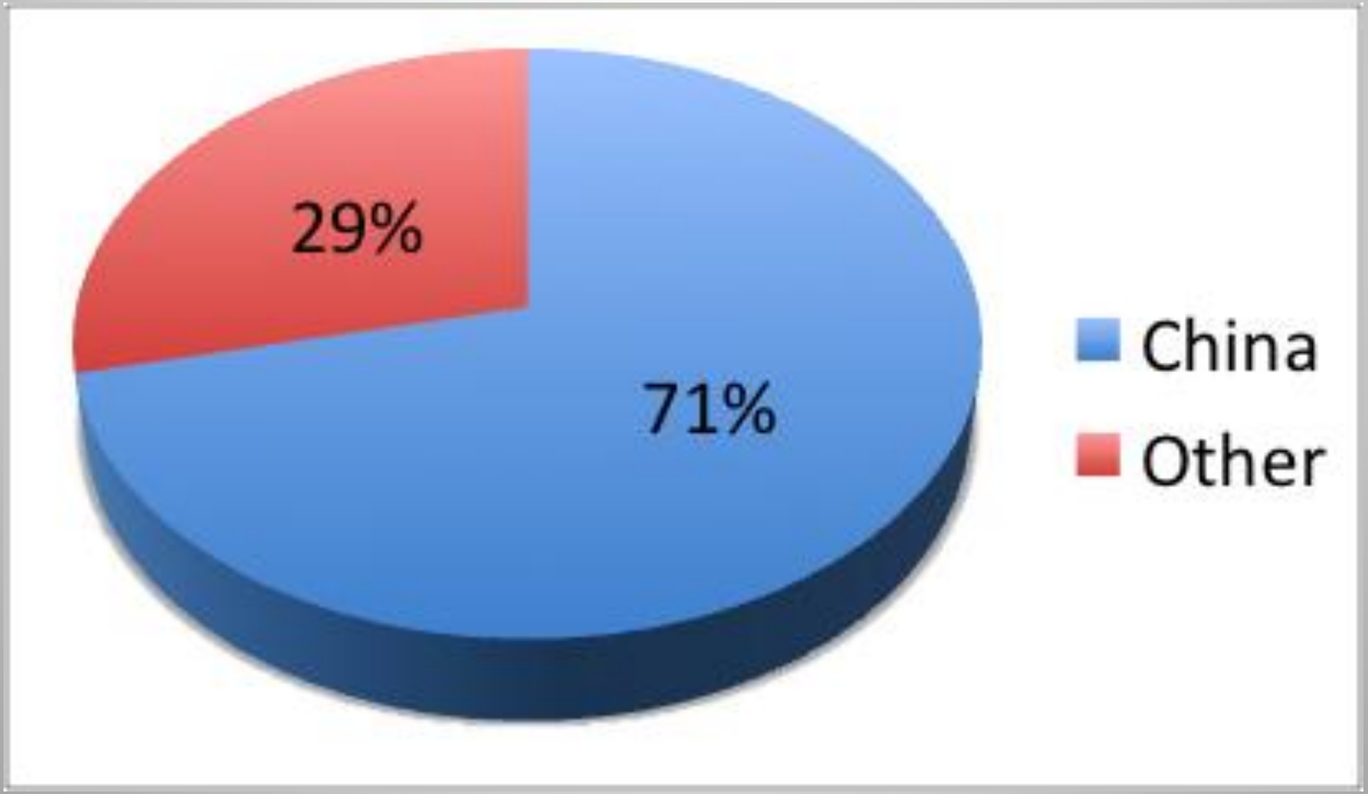
Joe Says...

- Insider threat *is not* the most numerous type of threat
  - 1900+ reported incidents in the last 10 years
  - ~ 19% of incidents involve malicious insider threat actors
- Insider threats are the *most costly and damaging*
  - Average cost $412K per incident
  - Average victim loss: ~$15M / year
  - Multiple incidents exceed $1 Billion

Sources: Ponemon Data Breach Reports: ‘08, ‘09, ‘10, ’11; IDC 2008; FBI / CSI Reports: ‘06, ‘07, ’08’, ‘09, ‘10/’11; Verizon Business Data Breach Reports: ‘09, ‘10, ‘11, ’12, ’13; CSO Magazine / CERT Survey: ‘10, ’11; Carnegie Mellon CERT 2011 IP Loss Report; Cisco Risk Report ‘08

FBI Case Statistics IEA 1996 - Present

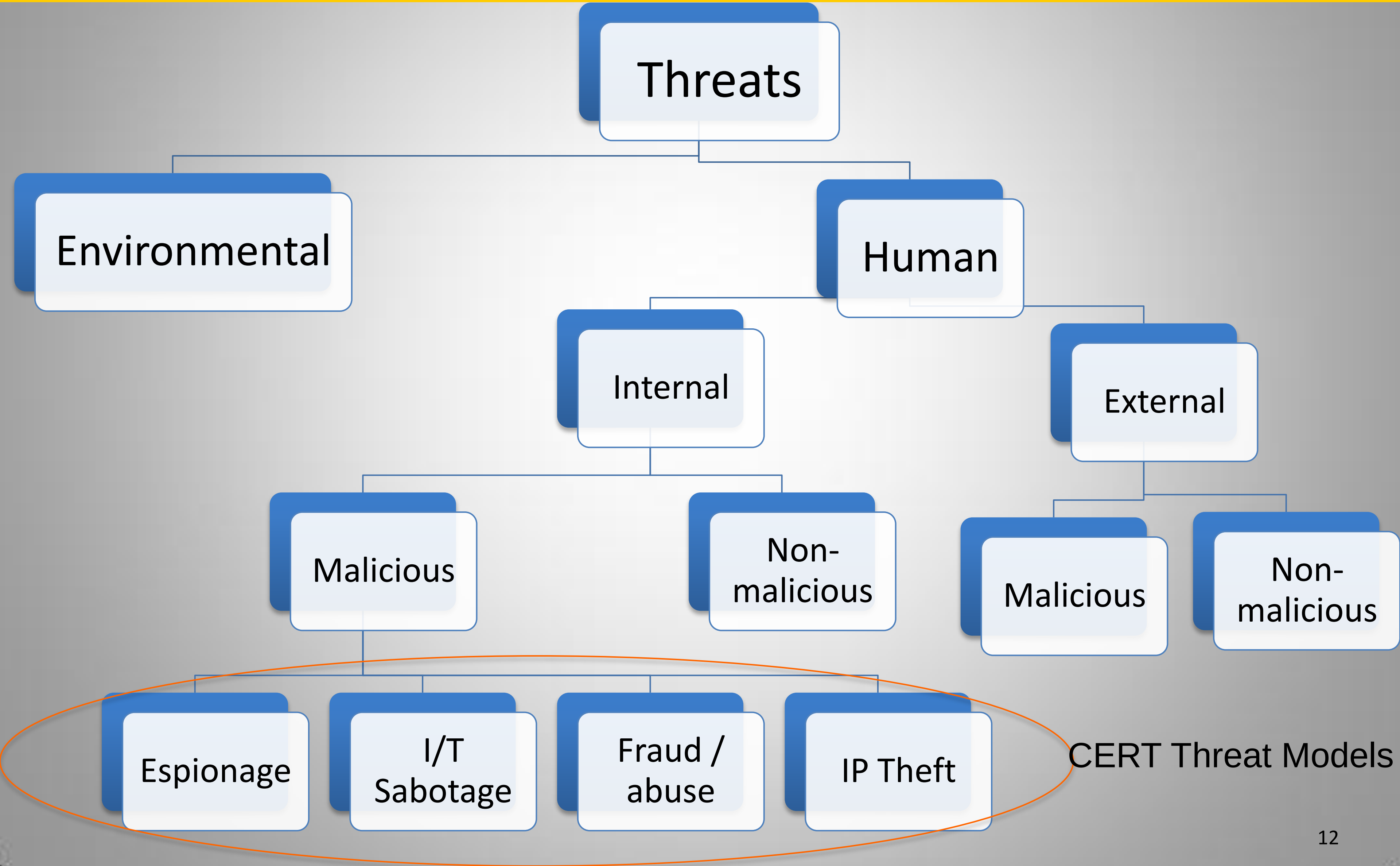
- Data from convictions under the Industrial Espionage Act (IEA) Title18 U.S.C., Section 1831
- Average loss per case: $472M



Solution: Define the Insider

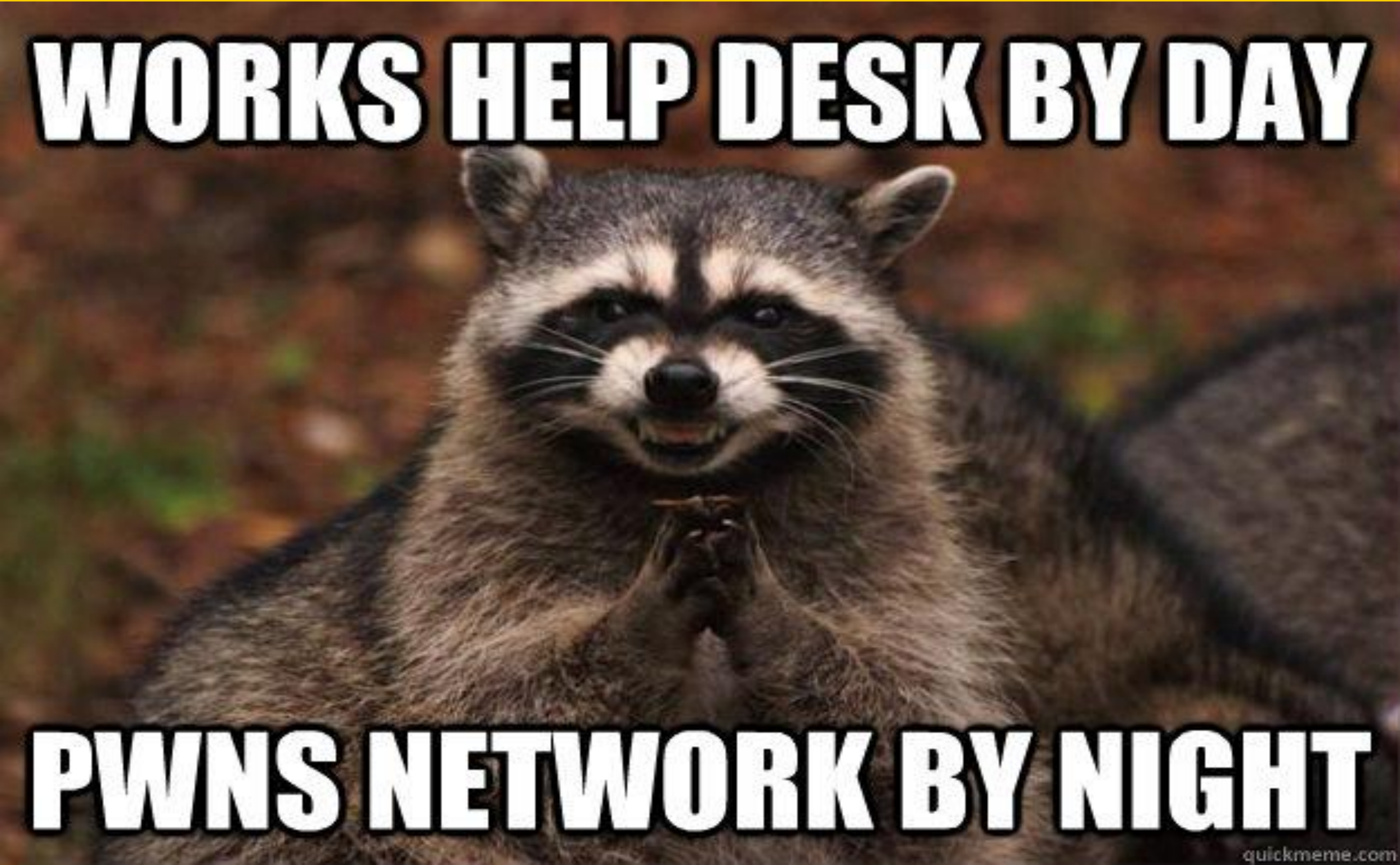
- Authorized people using their trusted access to do unauthorized things
- Boils down to *actors* with some level of *legitimate access*, and with some level of organizational *trust*
- Misunderstanding example: The APT **is not** an insider threat because they steal credentials.

The Threat Tree



CERT Threat Models

Sysadmins: Evil? Not So Fast…

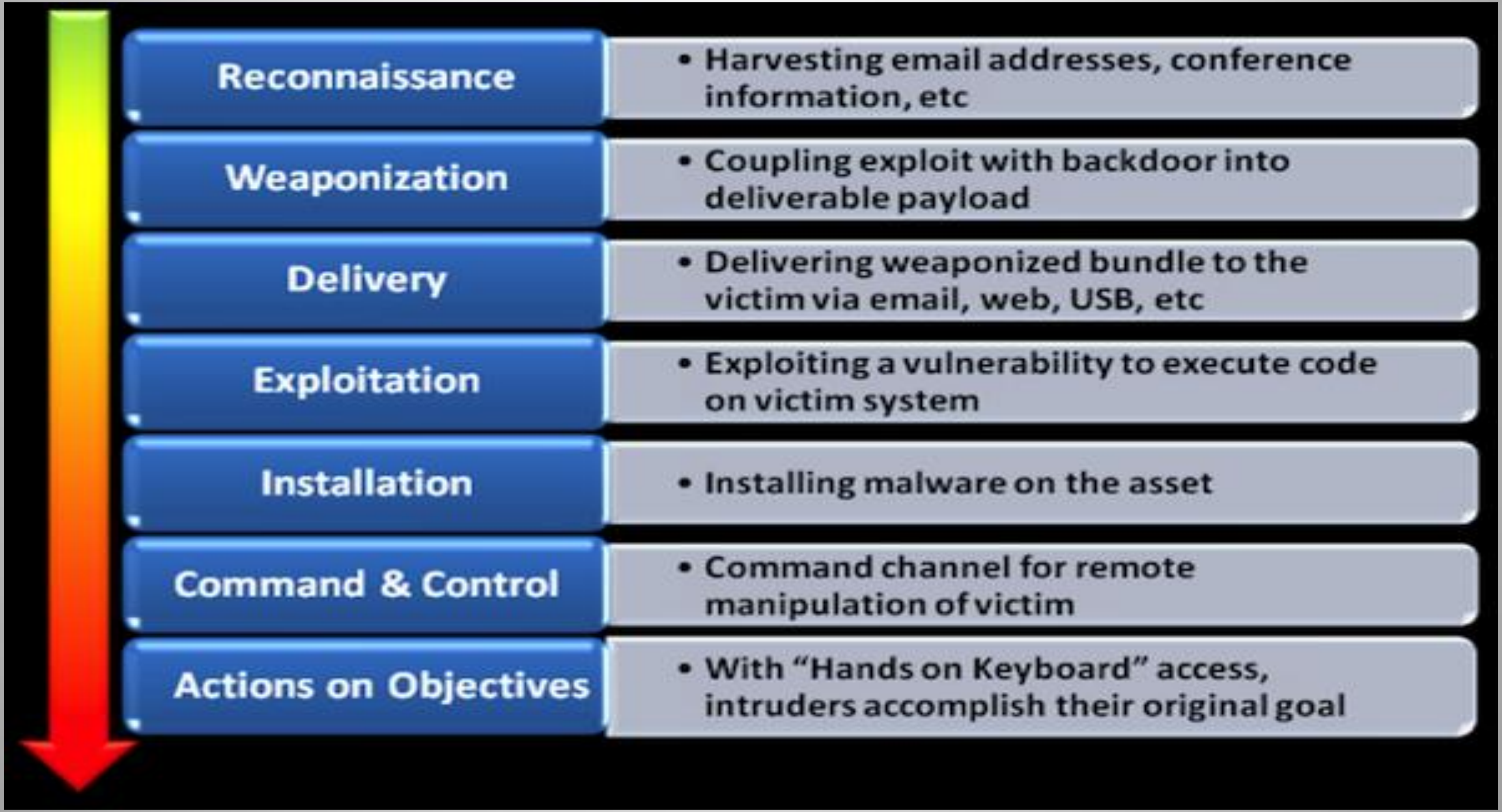


Joe Says…

- 1.5% of espionage cases reviewed involved the use of system admin privileges
- .8% of internal FBI incidents involved system admin cases
- CMU Cert show different statistics for IT sabotage:
  - 90% of IT saboteurs were system admins
  - http://www.cert.org/blogs/insider_threat/2010/09/insider_threat_deep_dive_it_sabotage.html

The Intrusion Kill Chain

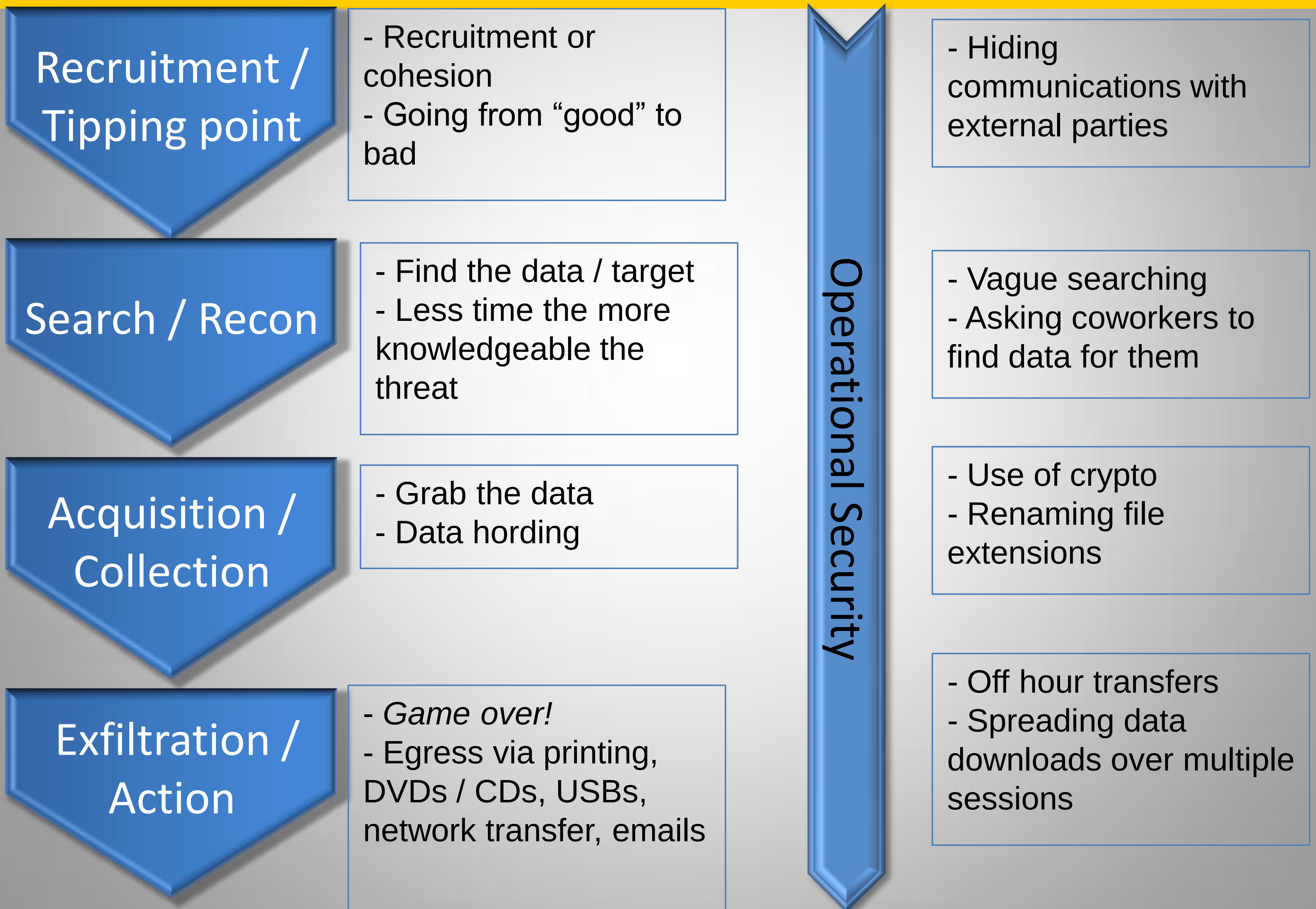
- The Intrusion Kill Chain is excellent for attacks, but doesn’t exactly work for insider threats



Reconnaissance	• Harvesting email addresses, conference information, etc
Weaponization	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponized bundle to the victim via email, web, USB, etc
Exploitation	• Exploiting a vulnerability to execute code on victim system
Installation	• Installing malware on the asset
Command & Control	• Command channel for remote manipulation of victim
Actions on Objectives	• With “Hands on Keyboard” access, intruders accomplish their original goal

Reference: *Intelligence-Driven Computer Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain.* E.M. Hutchings, M.J. Cloppert, et. al.

The Insider Threat Cyber “Kill Chain”



Recruitment / Tipping point

- Recruitment or cohesion
- Going from “good” to bad

- Hiding communications with external parties

Search / Recon

- Find the data / target
- Less time the more knowledgeable the threat

- Vague searching
- Asking coworkers to find data for them

Acquisition / Collection

- Grab the data
- Data hording

- Use of crypto
- Renaming file extensions

Exfiltration / Action

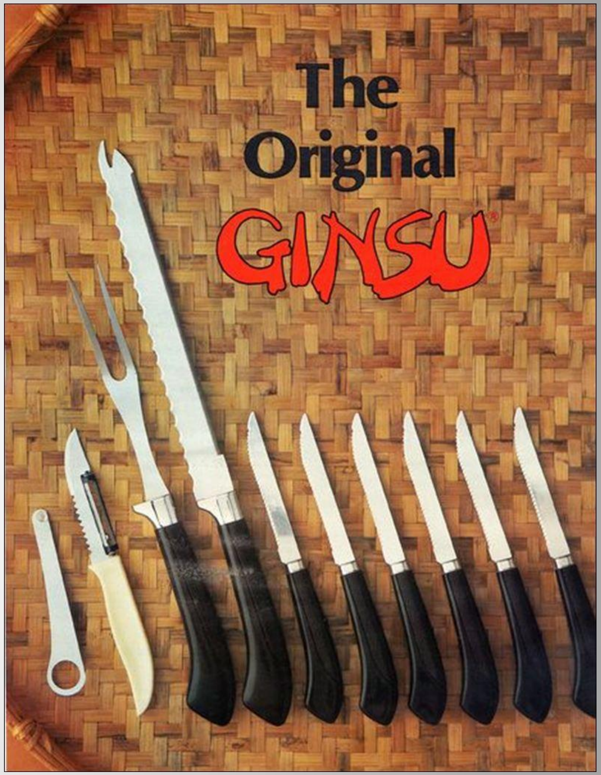
- *Game over!*
- Egress via printing, DVDs / CDs, USBs, network transfer, emails

- Off hour transfers
- Spreading data downloads over multiple sessions

Operational Security

Beware the Silver Bullet

- Many want you to believe insider threats are hackers in order to sell you things
- IDS, Firewalls, AV, etc. ***do not work***
  - No rules are being broken!
- Question vendor claims
  - Some great capabilities, but no “out of the box” solutions
  - Data loss prevention, digital rights management, and IP theft protection products are maturing

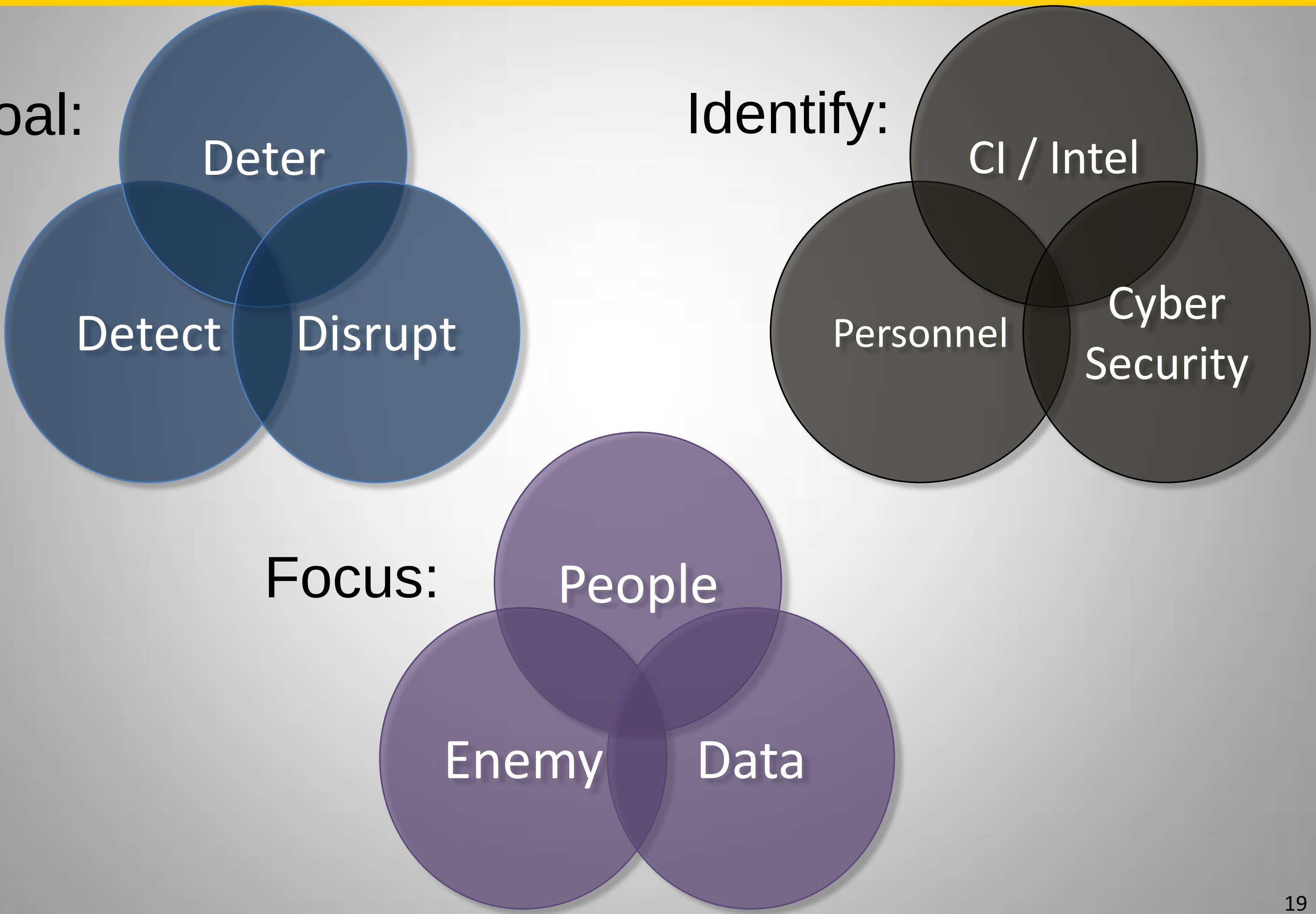


Click Here to Catch Spy

Lesson # 2:
This is Not a Simple Cyber Security Problem

- We trust the threat
- Insider threat programs are not just policy compliance shops
- 90% of problems are ***not*** technical
  - Programs do not just bolt into Security Operations Centers
  - Dedicated staff with clear objectives are a must

Solution:
The Multidisciplinary Approach



Goal:

Deter

Detect

Disrupt

Identify:

CI / Intel

Personnel

Cyber Security

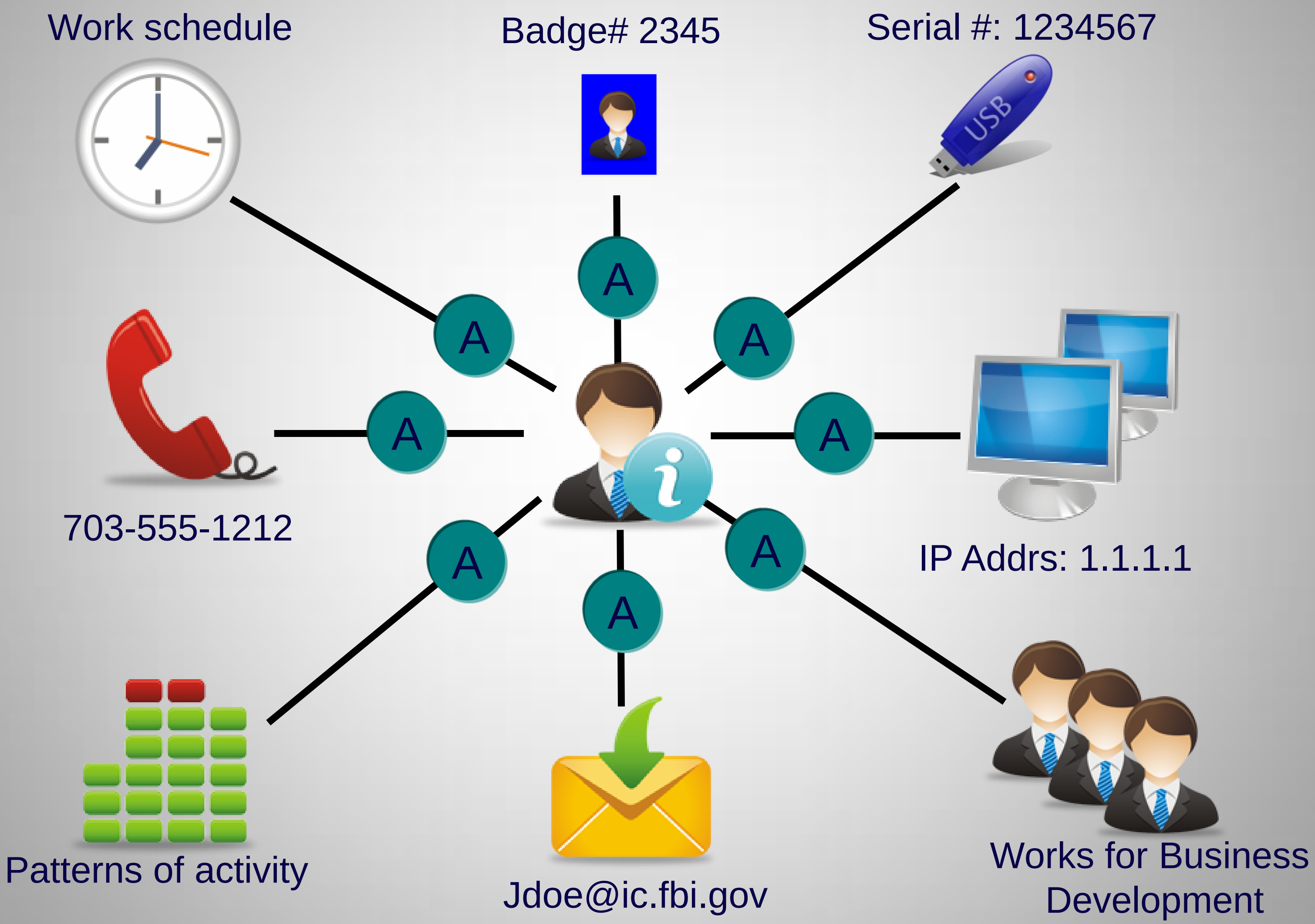
Focus:

People

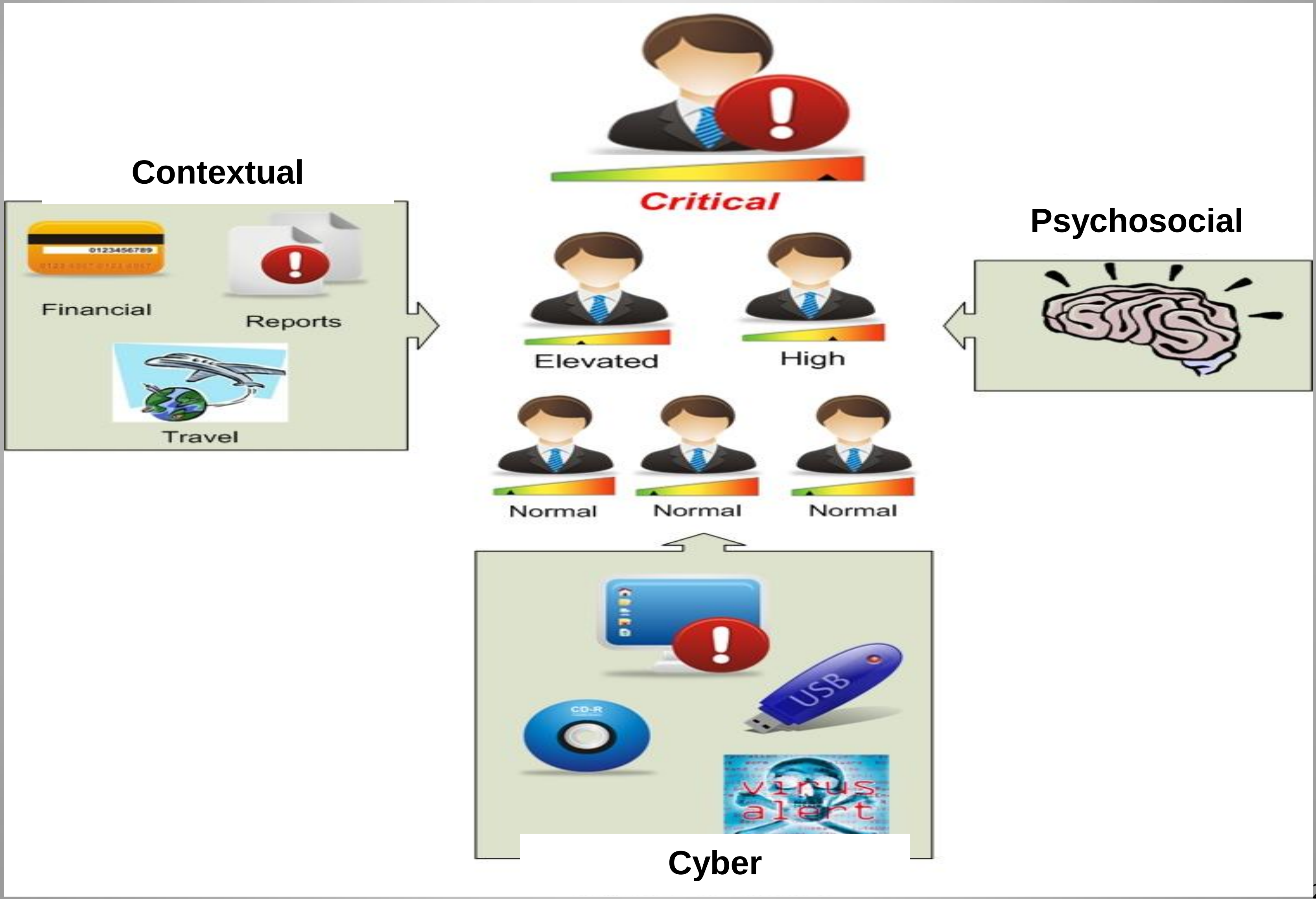
Enemy

Data

Do You Know Your People?



The Whole Person Approach



Critical

Contextual

Financial

Reports

Travel

Psychosocial

Elevated

High

Normal

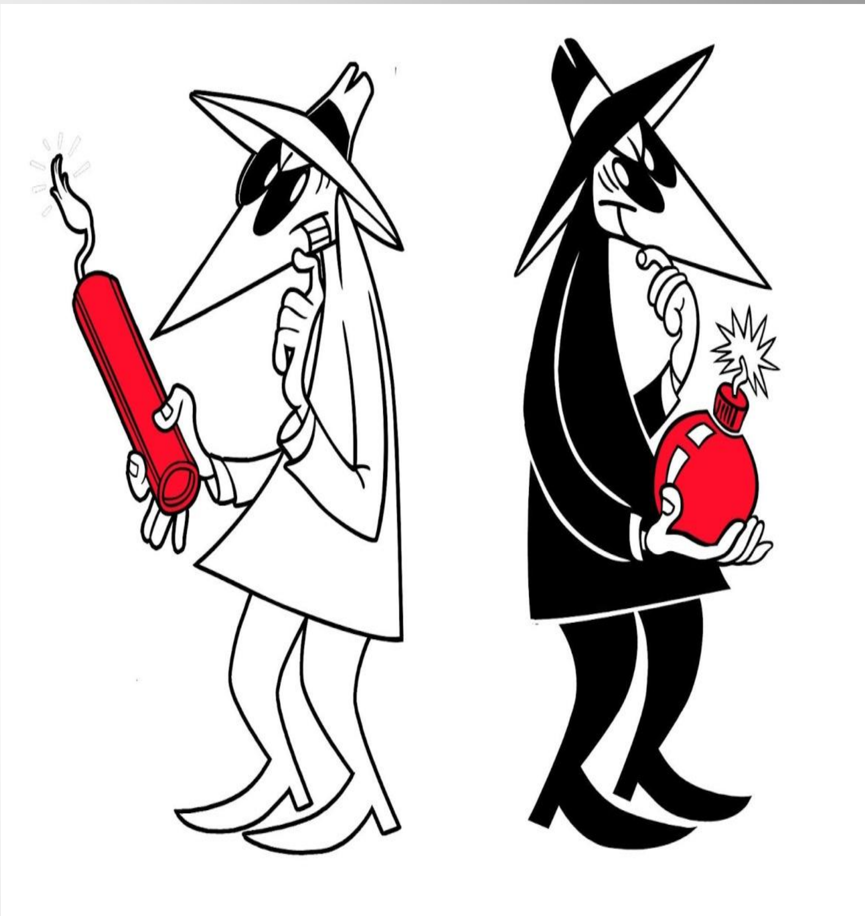
Normal

Normal

Cyber

Know Your Enemy

- Who would be targeting your organization?
- Who would they target inside your organization?
- Who are the high risk individuals in your organization?



Know Your Data

- What are the crown jewels of your organization?
- What data / people would the enemy want to target?
- Action:
  - Identify sensitive data
  - Rate top 5 most important systems in terms of sensitive data

The Value Proposition of Insider Threat and Data Protection Programs

It’s complex

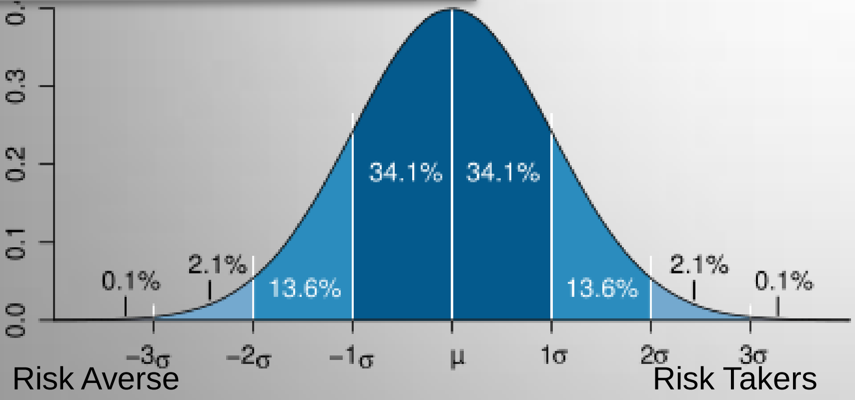
It’s expensive

It may take years to achieve tangible results

However…

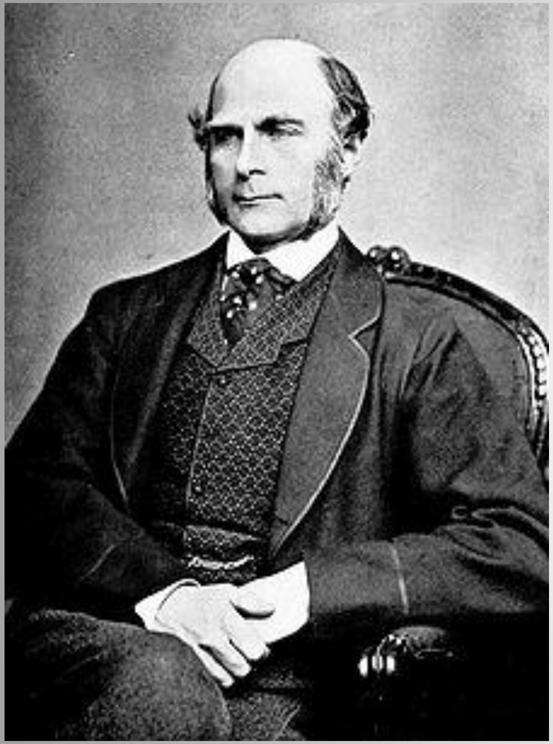
- This is about survival in a hostile market place
- If your data is secure you can penetrate risky markets
- Your enemy is your business partner, are you designed that way?

Lesson #3:
Focus on Deterrence Not Detection



- ► Make environment where being an insider is not easy
- ► Deploy data-centric, not system-centric security
- ► Crowd-source security
- ► Use positive social engineering

Solution:
Crowdsource Security!



Francis Galton (1822-1911)

- Aren’t security subject matter experts the best to make decisions?
  - Nope!
- British scientist who wanted to show empirically that educated people are superior
- Asked “commoners” to guess the weight of an ox at a fair
- Results:
  - No single villager correct, but average < 2 lbs. off
  - No single SME correct, average SME > 6 lbs off

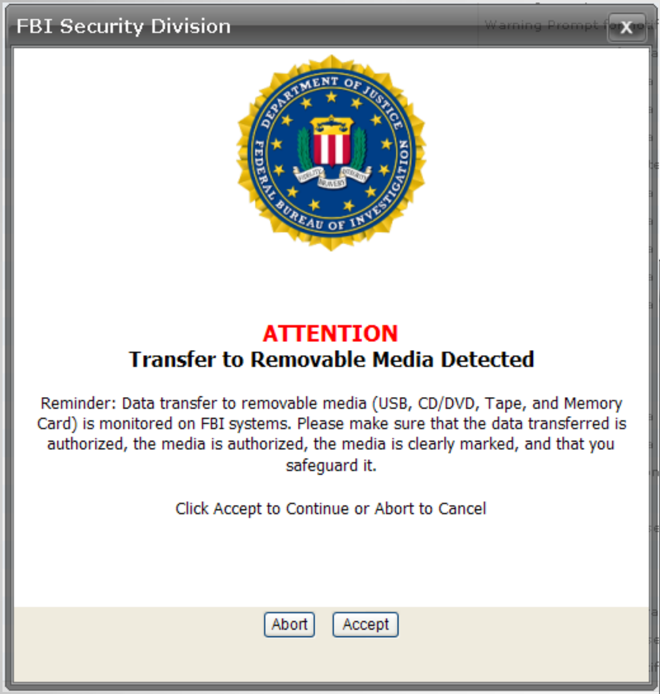
Crowdsourcing Security at the FBI

- 13,900 people come to work armed everyday
- Our people are trusted to enforce the law and keep the country safe

vs.

If we can train them to use guns, we can train them to use data

Solution:
Positive Social Engineering



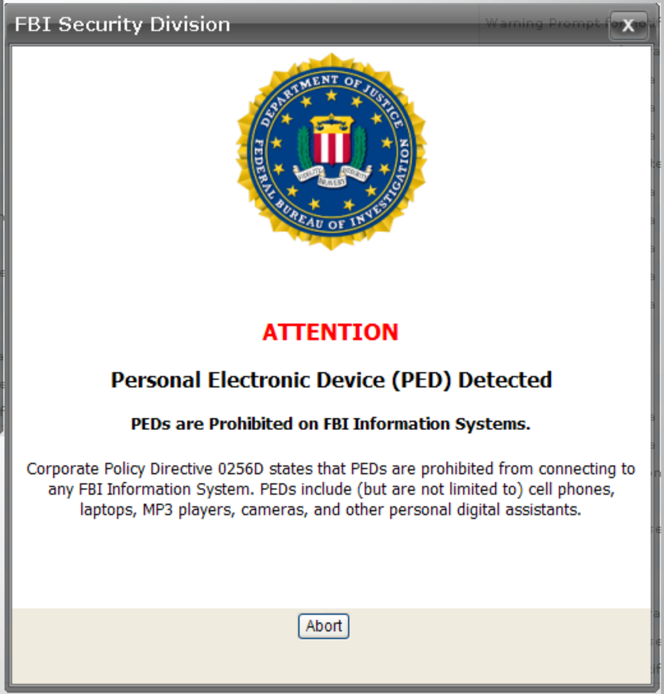
ATTENTION

Transfer to Removable Media Detected

Reminder: Data transfer to removable media (USB, CD/DVD, Tape, and Memory Card) is monitored on FBI systems. Please make sure that the data transferred is authorized, the media is authorized, the media is clearly marked, and that you safeguard it.

Click Accept to Continue or Abort to Cancel

Users will make good decisions given timely guidance



ATTENTION

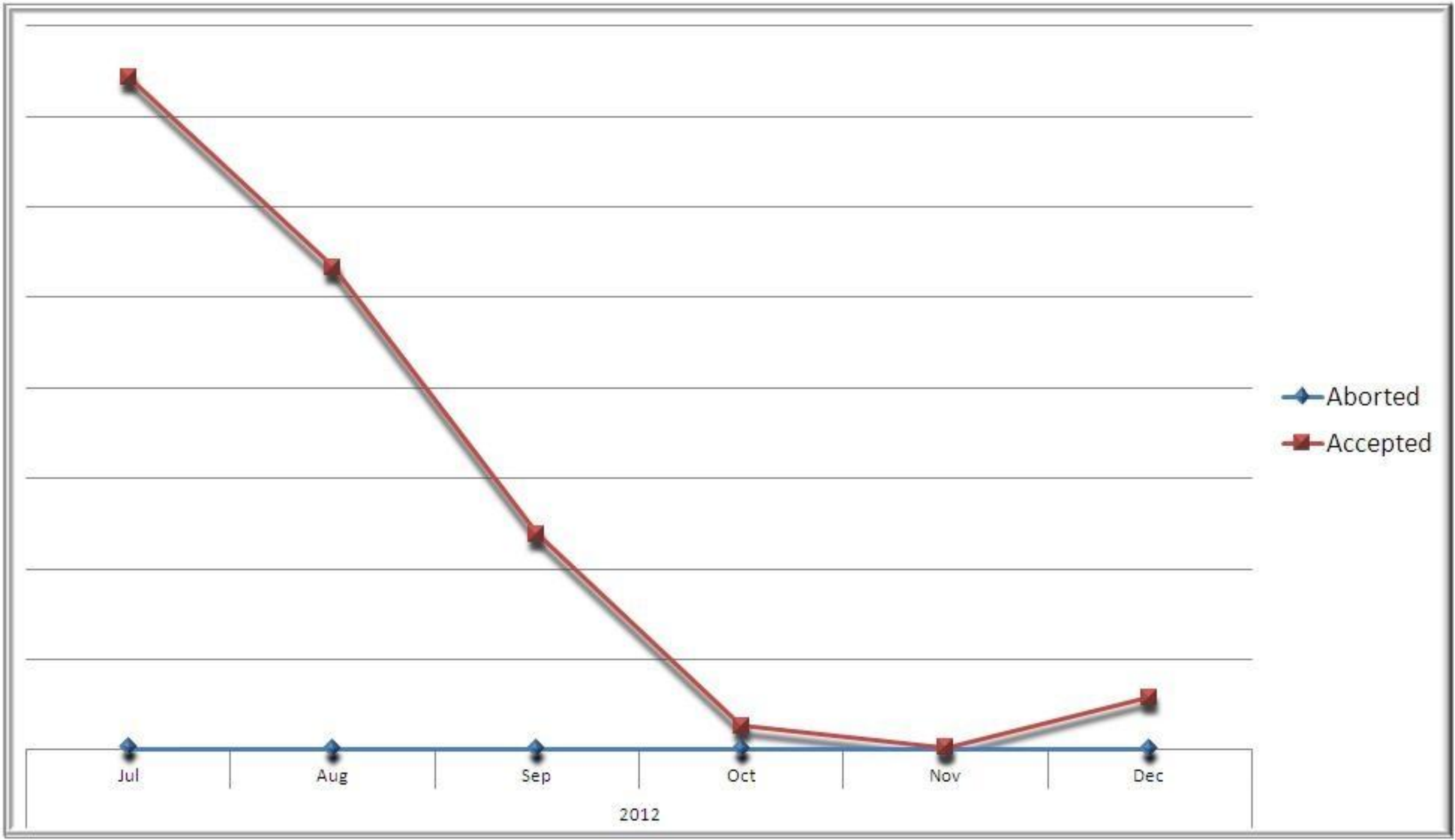
Personal Electronic Device (PED) Detected

PEDs are Prohibited on FBI Information Systems.

Corporate Policy Directive 0256D states that PEDs are prohibited from connecting to any FBI Information System. PEDs include (but are not limited to) cell phones, laptops, MP3 players, cameras, and other personal digital assistants.

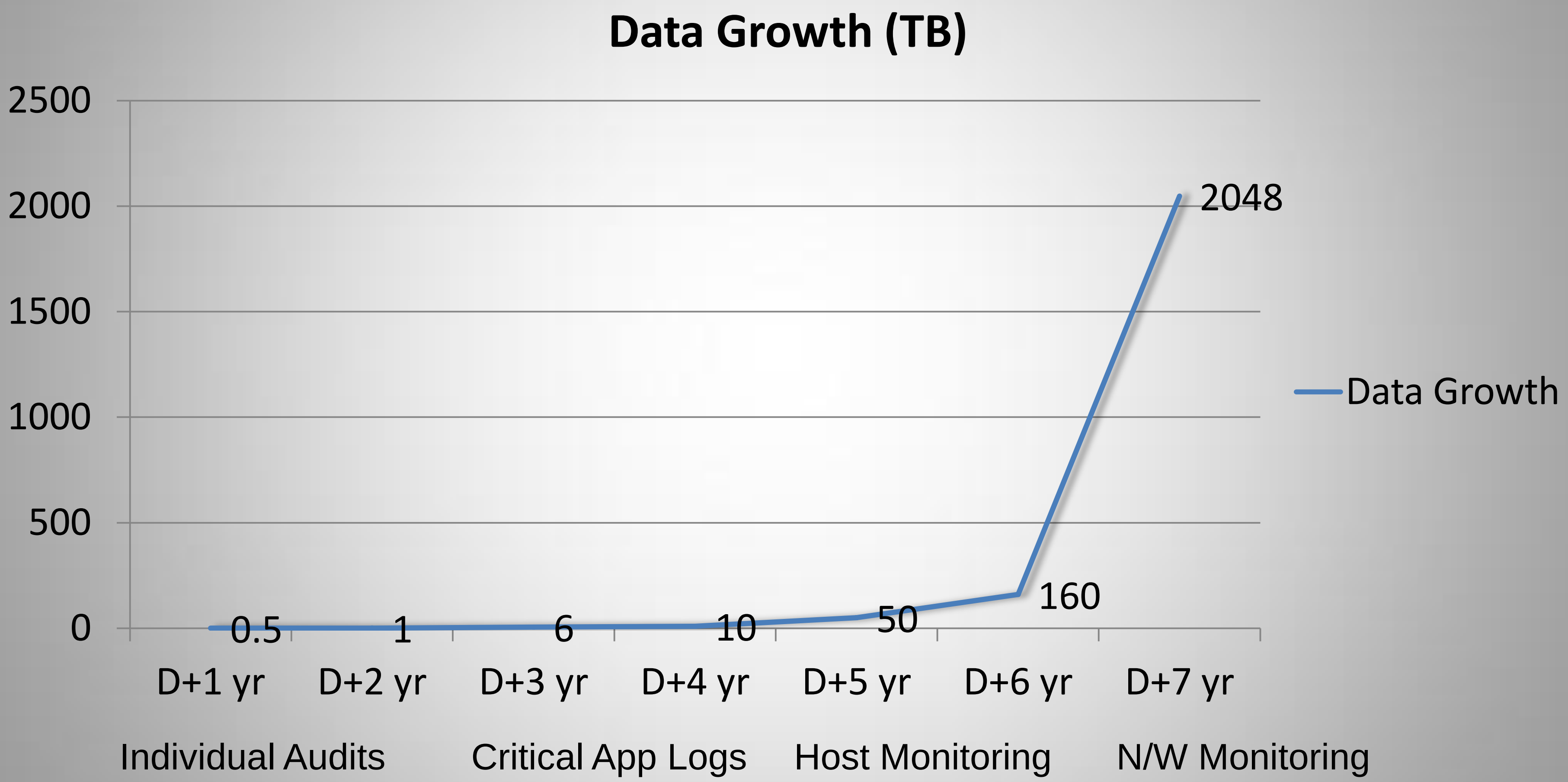
Risk reduction with no impact to workflow, etc.

Positive Social Engineering: RESULTS!



Source: Internal FBI Computer Security Logs

Lesson #4: The Data Overload Problem

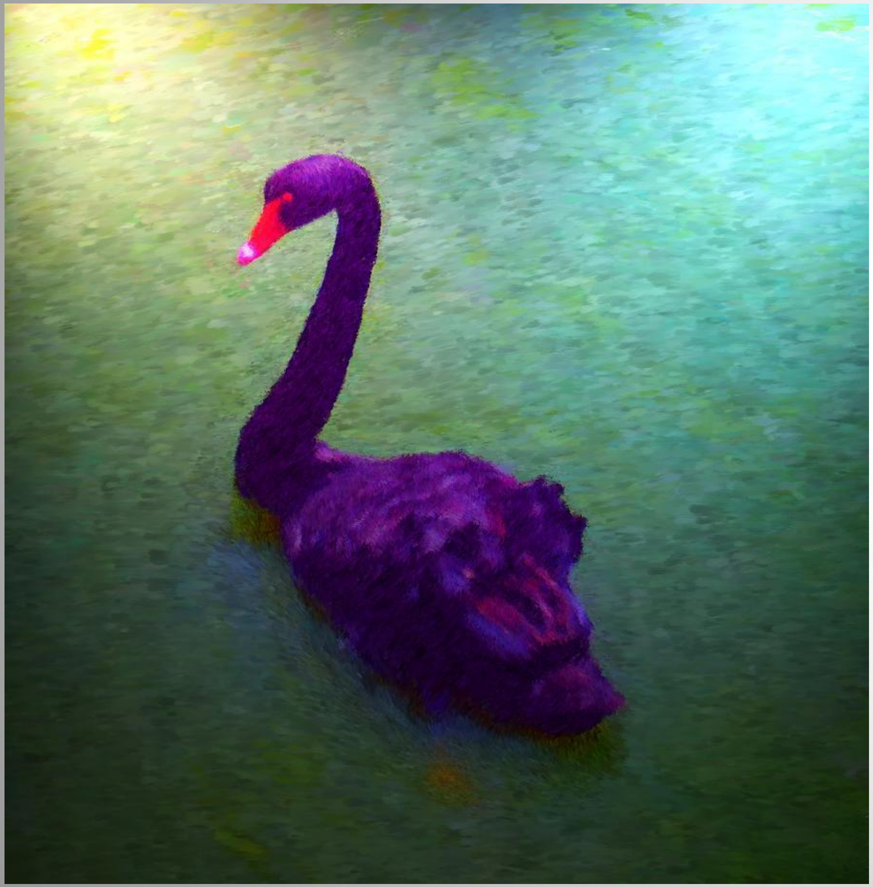


Every time Someone says "BYOD", god kills a kitten

Solution: Focus on Two Sources

- You don’t need everything
- HR data:
  - To “know your people”
  - Workplace/personnel issues
- System logs tracking data egress and ingress:
  - Printing, USB, CD/DVD, etc.

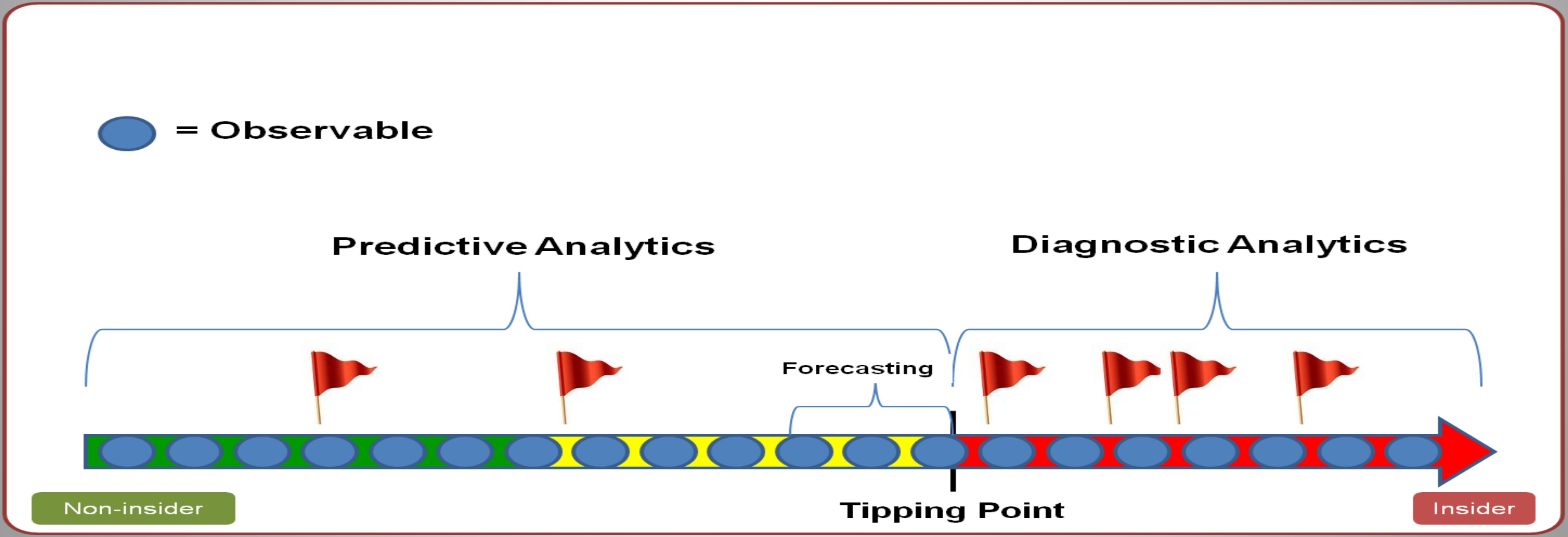
Lesson #5:
Detection of Insiders = Kinda Hard



- Prediction of rare events (i.e. insider threats) may not be possible
- Don’t waste time and money on the impossible
- ***Look for red flag indicators as they happen***

The Insider Threat Continuum

- Most people don’t evolve into true threats
- ~5% of the 65 espionage cases came in “bad”
- There are observable “red flags” we call *indicators*



Indicators must be ***observable*** and ***differentiating***

The Problem with Prediction

- ***A rodent out-predicted our first generation systems***

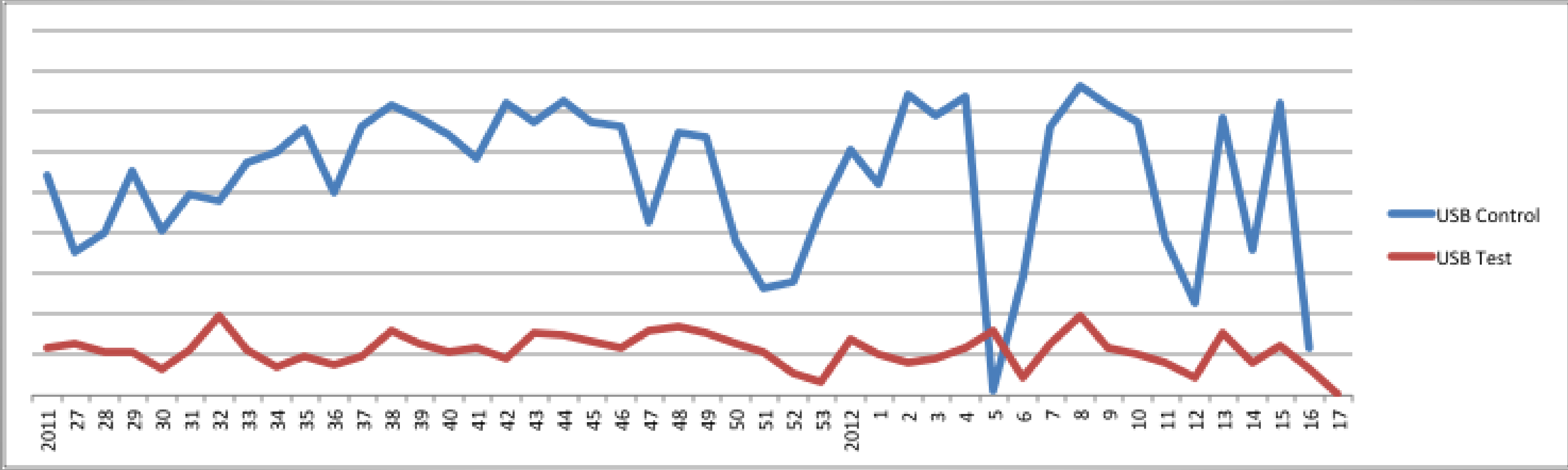
The Detection Problem:
A Needle in a Stack of Needles

Solution:
Use Behavioral Detection

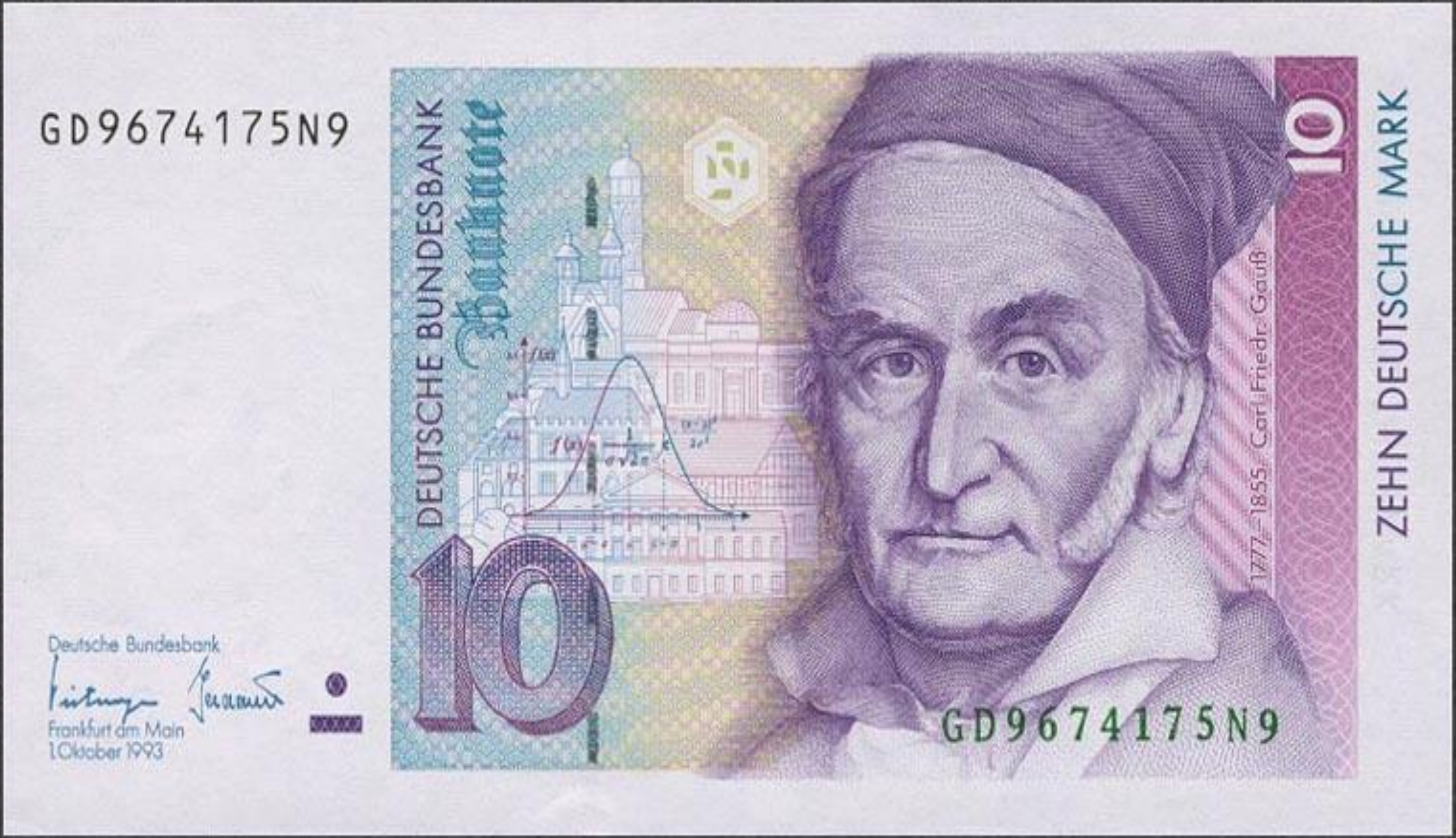
- Behavioral based detection
  - Think more like a marketer and less like an IDS analyst
  - Build a baseline based on users volume, velocity, frequency, and amount based on hourly, weekly, and monthly normal patterns
  - Cyber actions that differentiate possible insiders: data exfiltration volumetric anomalies

Looking at Averages

- All 5 egress points turned up nothing
- No statically relevant differences
- So what’s going on?

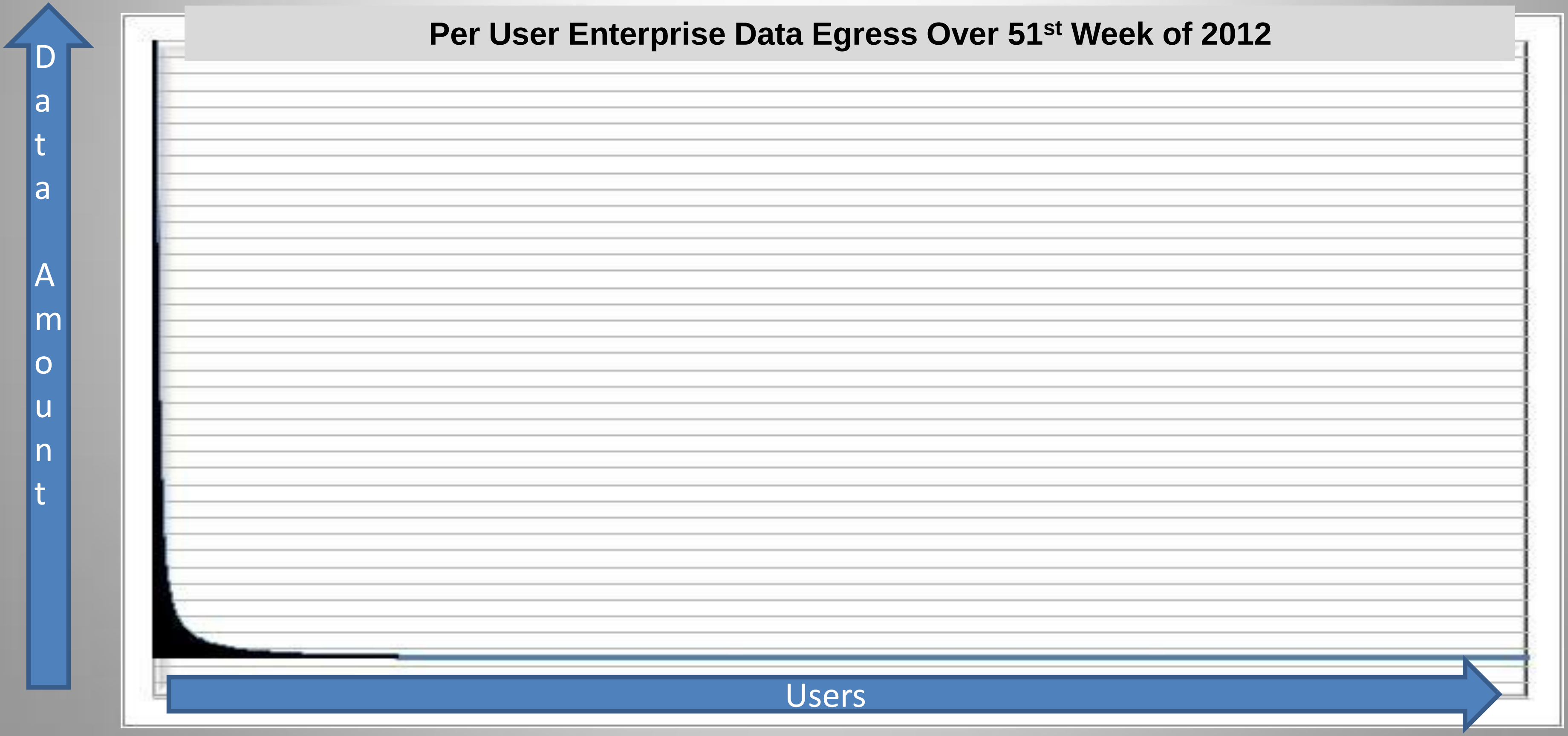


The Problem with Assumptions



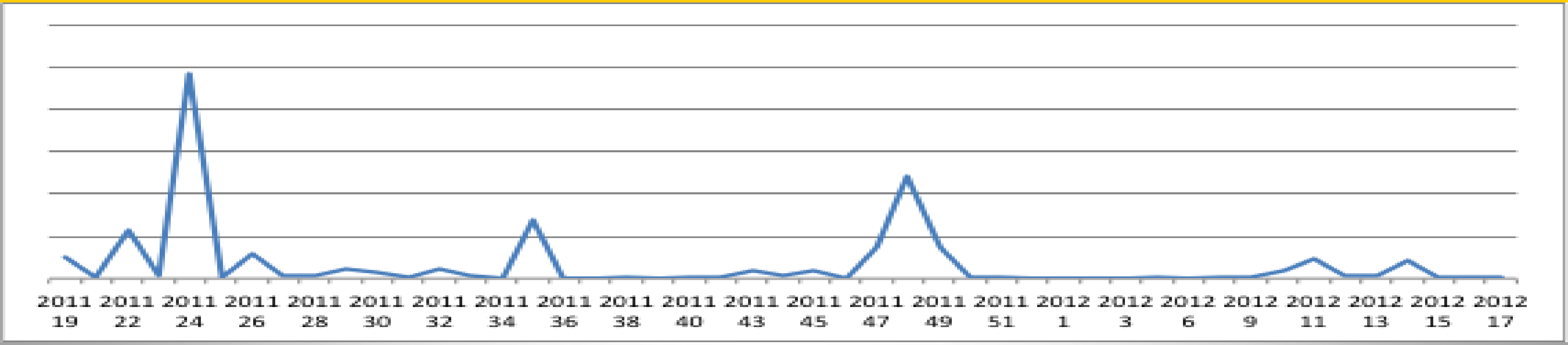
Findings in Data Movement

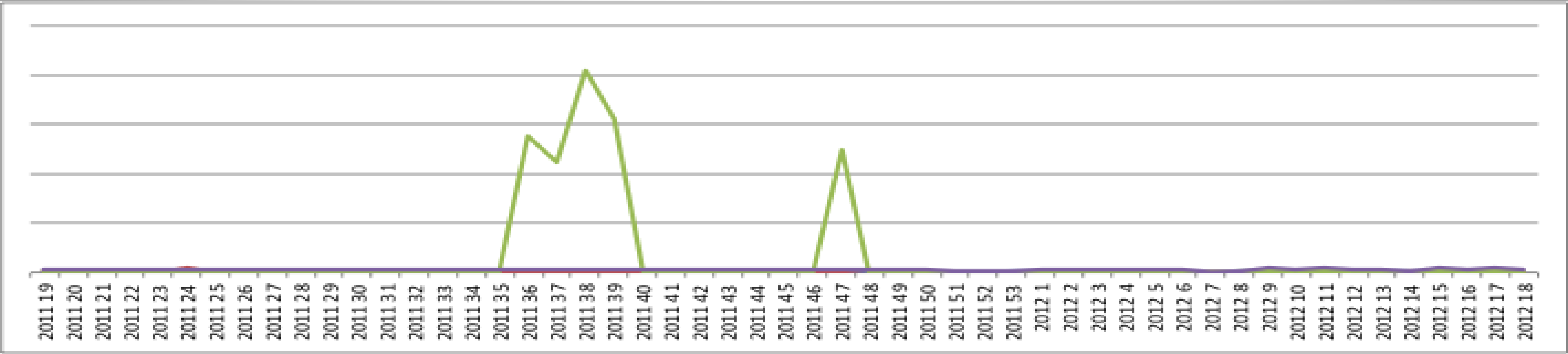
- Standard distributions (bell curves) are *very rare*
- >80% of data movement done by <2% of population
- *Hint:* Know your data or make huge analytic mistakes



Source: Internal FBI Computer Security Logs

Focus on the Individual





- 21% of test users showed a volumetric anomalies in a 90 day window more than once versus 12% of the control

The 5 Lessons & Solutions

1 Insider threats are not hackers.

- ✓ **Frame and define the threat correctly and focus on the insider threat kill chain**

2 Insider threat is not a technical or “cyber security” issue alone

- ✓ **Adopt a multidisciplinary “whole threat” approach**

3 A good insider threat program should focus on deterrence, not detection

- ✓ **Create an environment that discourages insiders by crowd sourcing security and interacting with users**

4 Avoid the data overload problem

- ✓ **Gather HR data and data egress/ingress logs**

5 Detection of insider threats has to use behavioral based techniques

- ✓ **Base detection on user’s *personal* cyber baselines**

Questions?

Or sit in uncomfortable silence.

Your choice.