Unintended Consequences of the Information Age:

The Fate of Privacy

CIAC Center for Information Assurance
and Cybersecurity

Agenda

- Context
- Threat Landscape
- Threat Spectrum Evolution
- Strategies
  - Academia
  - Organizations and Industries
  - Local Governments
  - Individuals
 - Educators
- Capacity Building

How did we get here?

CONTEXT

Context Evolution

	Agricultural Age	**Industrial Age**	**Information Age**
Wealth	Land	Capital	Knowledge
Advancement	Conquest	Invention	Paradigm Shifts
Time	Sun/Seasons	Factory Whistle	Time Zones
Workplace	Farm	Capital equipment	Networks
Organization Structure	Family	Corporation	Collaborations
Tools	Plow	Machines	Computers
Problem-solving	Self	Delegation	Integration
Knowledge	Generalized	Specialized	Interdisciplinary
Learning	Self-taught	Classroom	Online

Smashing Industrial Age Infrastructure!

UNINTENDED CONSEQUENCES !!!

The Sorcerer's Apprentice

http://www.youtube.com/watch?v=4ryFOztZrrc

# Jez-do-it Approach to IT:
Would you organize heart surgery this way?

Vulnerabilities
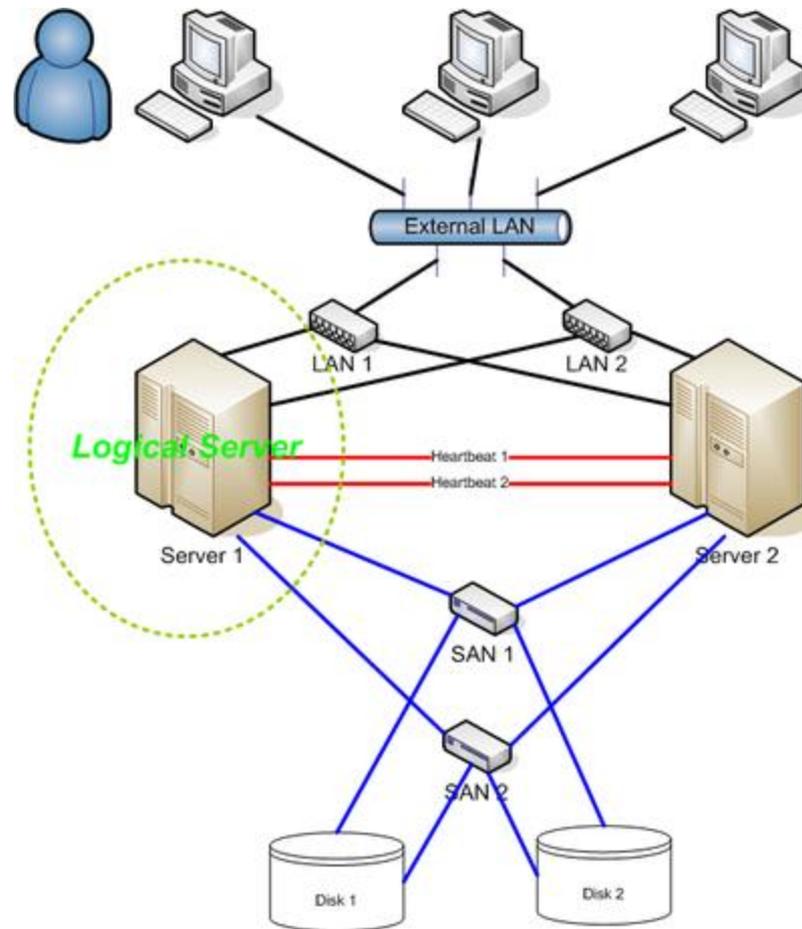
# Vulnerabilities

Evil Lurks!!
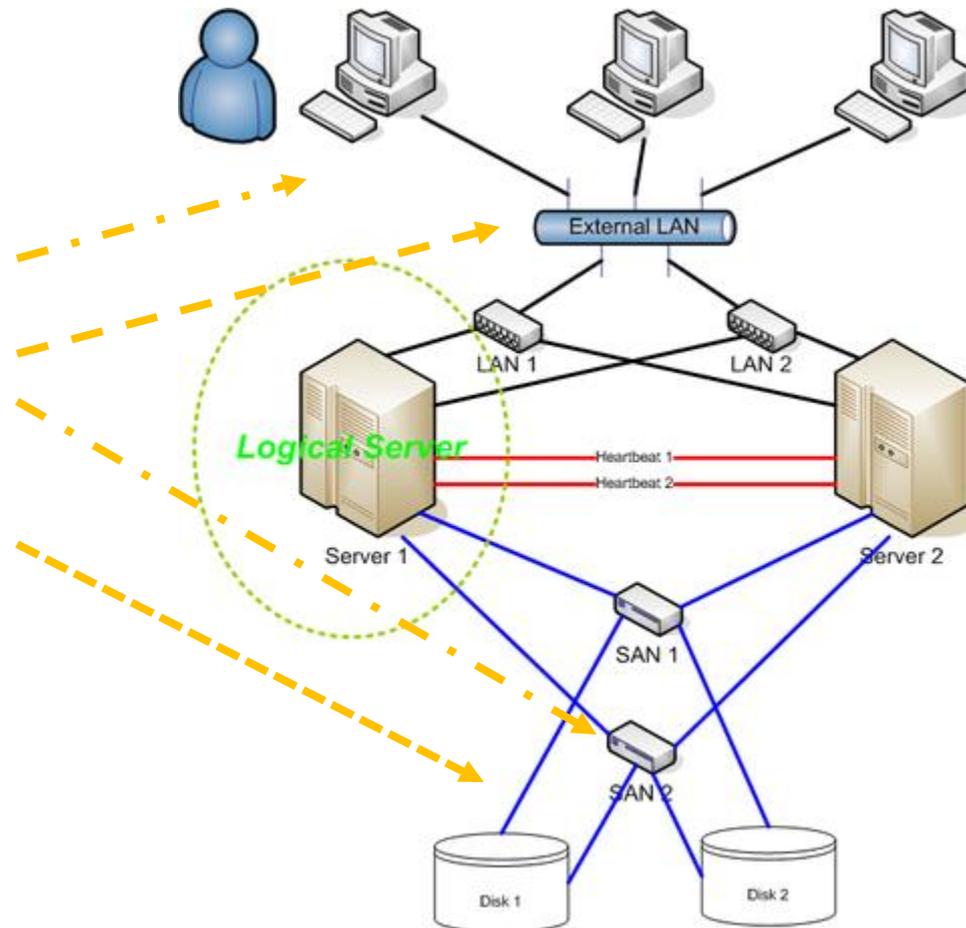
Threats

"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems…relies entirely on computer networks."—**Foreign Government Newspaper**

Information Age Threat Spectrum

National Security Threats	**Info Warrior**	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	**Terrorist**	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	**Institutional Hacker**	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

Making an Organization Secure

(Threats + Vulnerabilities = Controls)
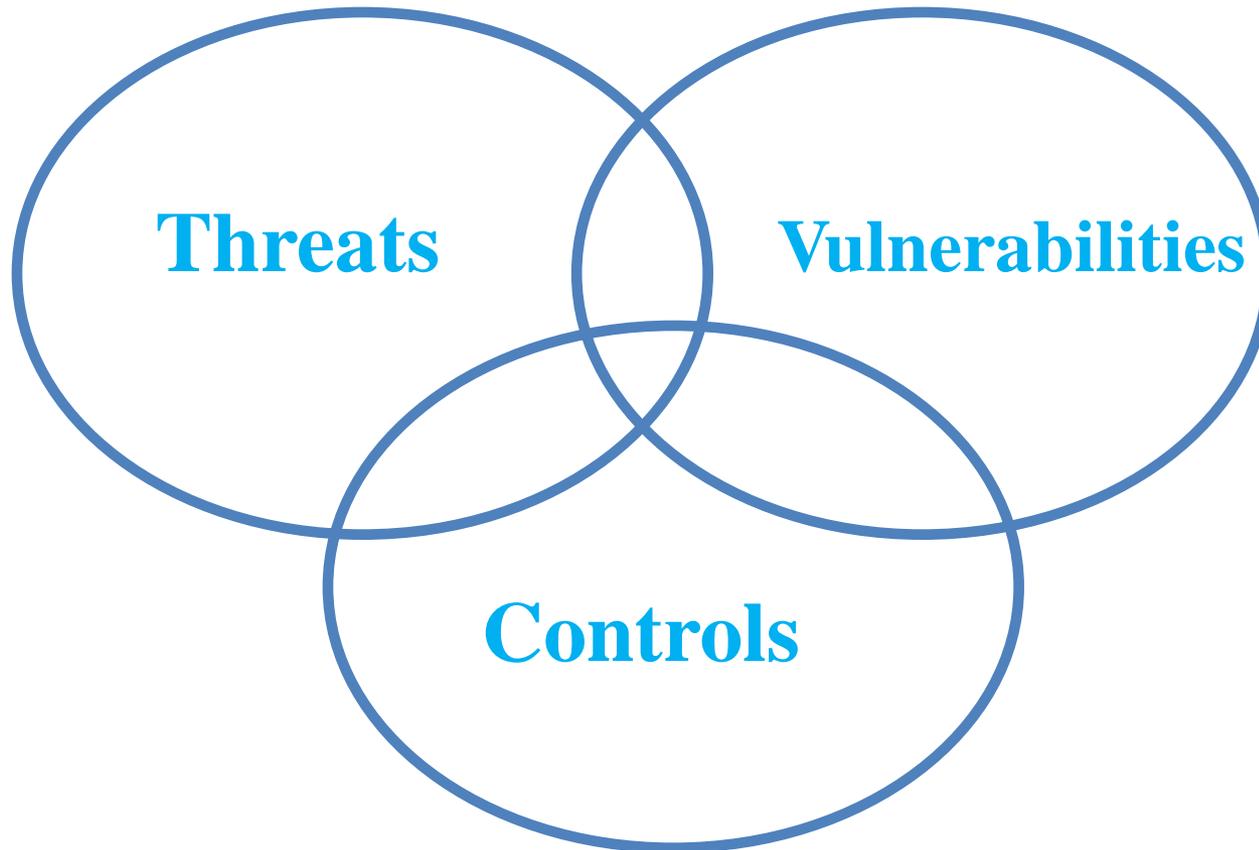
IT Security Evolution

1960-1980   **1985**   **1995 -**
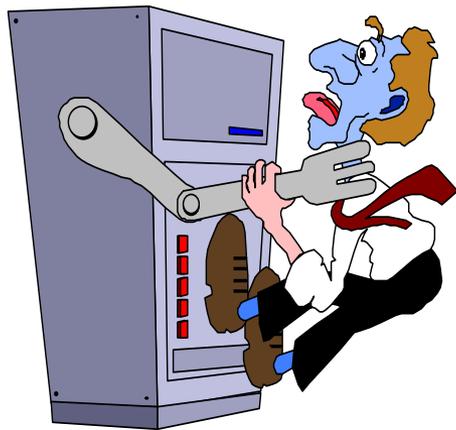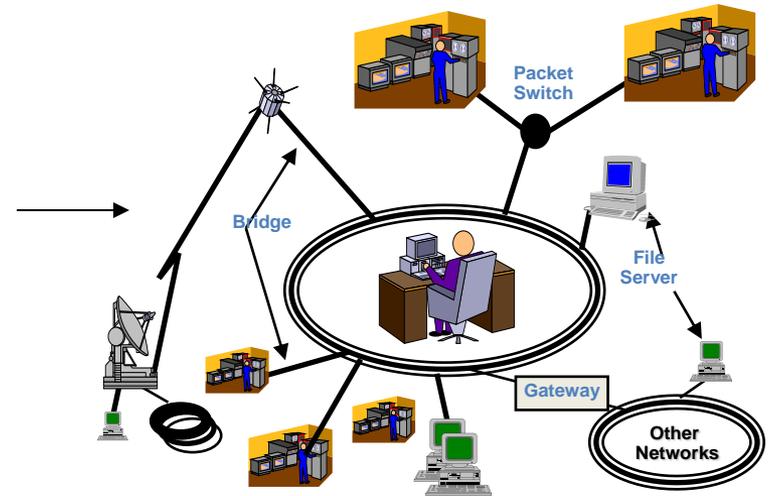
Computer Security ⟶ INFOSEC ⟶ Information Assurance
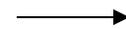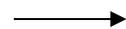
IT Management Evolution

- Mainframe
  - Access
    - Limited lists
    - Sign in logs
    - 7/24 attendants
  - Perimeter defense
    - Closed areas
    - Cypher locked doors
  - Disc forensics

- Distributed processing
  - Authentication
  - Firewalls
  - Network forensics

  - IDS
  - Forensic readiness
  - Drive security to physical layer
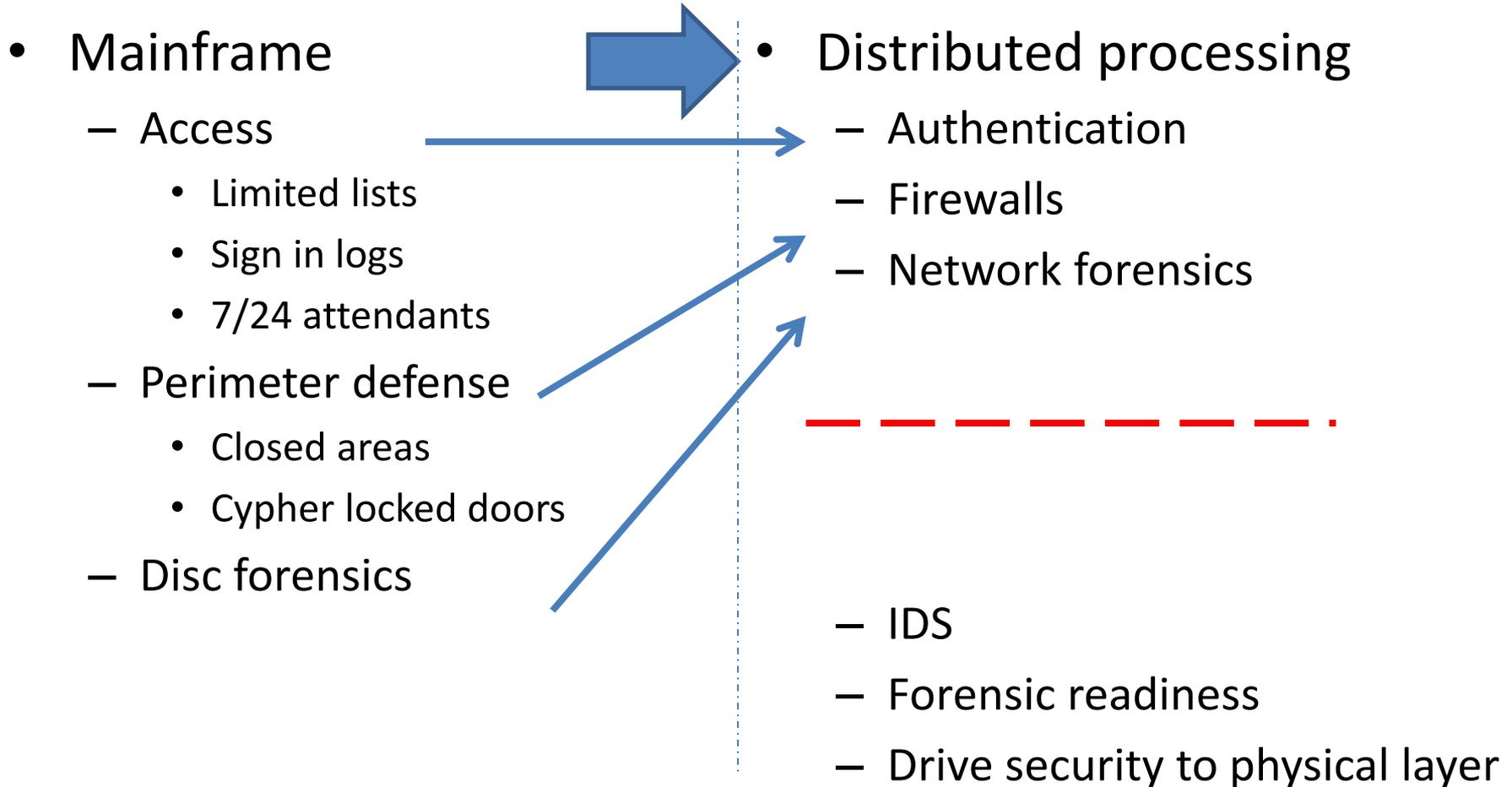
Trusting Controls Assumes

- Design implements policies

- Sum total of controls implement all policies

- Implementation is correct

- Installation/administration are correct

The common denominator?

People!!!

The Challenge

- People always the weakest link

- Design controls with people in mind

- Consider various dimensions
  - Organization
    - Create a culture of security
  - Psychology
    - Understand the Internet's nature
  - Social Engineering
    - Ward off people-focused attacks

Bottom line:

You Will Never Own a Perfectly Secure System!!!

You Will Never Own a Perfectly Secure System!!!

You Will Never Own a Perfectly Secure System!!!

Grim Reality

- If you have a luscious information object

- Probability of Attack = 1

- Function of:
 - Effort
  - Time

What's coming at us?

THREAT LANDSCAPE

WORLD INTERNET USAGE AND POPULATION STATISTICS
June 30, 2012

World Regions	Population (2012 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2012	Users % of Table
Africa	1,073,380,925	4,514,400	**167,335,676**	15.6 %	3,606.7 %	7.0 %
Asia	3,922,066,987	114,304,000	**1,076,681,059**	27.5 %	841.9 %	44.8 %
Europe	820,918,446	105,096,093	**518,512,109**	63.2 %	393.4 %	21.5 %
Middle East	223,608,203	3,284,800	**90,000,455**	40.2 %	2,639.9 %	3.7 %
North America	348,280,154	108,096,800	**273,785,413**	78.6 %	153.3 %	11.4 %
Latin America / Caribbean	593,688,638	18,068,919	**254,915,745**	42.9 %	1,310.8 %	10.6 %
Oceania / Australia	35,903,569	7,620,480	**24,287,919**	67.6 %	218.7 %	1.0 %
WORLD TOTAL	**7,017,846,922**	**360,985,492**	**2,405,518,376**	**34.3 %**	**566.4 %**	**100.0 %**

NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2012. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau and local census agencies. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local ICT Regulators and other reliable sources. (5) For definitions, disclaimers, navigation help and methodology, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2013, Miniwatts Marketing Group. All rights reserved worldwide.

Cyber Attack Sophistication Continues To Evolve

High

Intruder Knowledge

Tools

Attack Sophistication

Attackers Technical Skills

Low

1980 1985 1990 1995 2000+

Source: CERT

Equation 1: Mathematical model of hacker behavior

$$M = f\,[\,P\,(v) - (c_1 + c_2)\,]$$

where:

M = Hacker motivation
P = the probability of not failing to intrude
v = the value of success to the hacker
c_1 = the cost to the hacker
c_2 = the consequences to the hacker

WORLD INTERNET USAGE AND POPULATION STATISTICS
June 30, 2012

World Regions	Population (2012 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2012	Users % of Table
Africa	1,073,380,925	4,514,400	167,335,676	15.6 %	3,606.7 %	7.0 %
Asia	3,922,066,987	114,304,000	1,076,681,059	27.5 %	841.9 %	44.8 %
Europe	820,918,446	105,096,093	518,512,109	63.2 %	393.4 %	21.5 %
Middle East	223,608,203	3,284,800	90,000,455	40.2 %	2,639.9 %	3.7 %
North America	348,280,154	108,096,800	273,785,413	78.6 %	153.3 %	11.4 %
Latin America / Caribbean	593,688,638	18,068,919	254,915,745	42.9 %	1,310.8 %	10.6 %
Oceania / Australia	35,903,569	7,620,480	24,287,919	67.6 %	218.7 %	1.0 %
WORLD TOTAL	7,017,846,922	360,985,492	2,405,518,376	34.3 %	566.4 %	100.0 %

NOTES: (1) Internet Usage and World Population Statistics are for June 30, 2012. (2) CLICK on each world region name for detailed regional usage information. (3) Demographic (Population) numbers are based on data from the US Census Bureau and local census agencies. (4) Internet usage information comes from data published by Nielsen Online, by the International Telecommunications Union, by GfK, local ICT Regulators and other reliable sources. (5) For definitions, disclaimers, navigation help and methodology, please refer to the Site Surfing Guide. (6) Information in this site may be cited, giving the due credit to www.internetworldstats.com. Copyright © 2001 - 2013, Miniwatts Marketing Group. All rights reserved worldwide.

Dan Geer
Chief Scientist
Incutel

"In the world of networked computers every sociopath is you neighbor."

Courtesy: K. Bailey/E. Hayden, CISOs

Critical Infrastructure:
An Irresistible Target

Vulnerabilities…
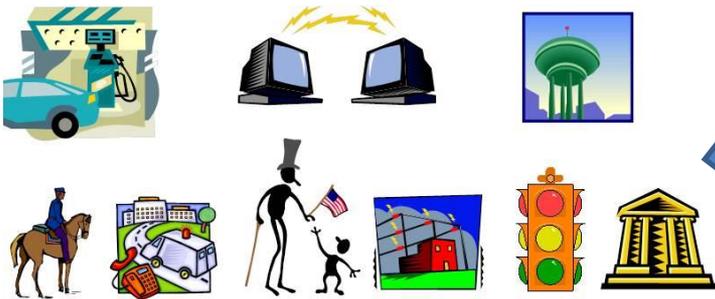
… gas and oil, telecommunications, water supply systems, emergency services, government services, electrical power systems, transportation, banking and finance.

Increasingly Interdependent Vulnerabilities

Profile of Electric Power System

Control Center
Generating Plant
Public Networks
Private Microwave Network
Transmission Substation
Distribution Substation

Key:
Leased Lines
Private Fiber Network
Microwave
Electric Power

Residential Loads 35%
Commercial Loads 31%
Industrial Loads 34%
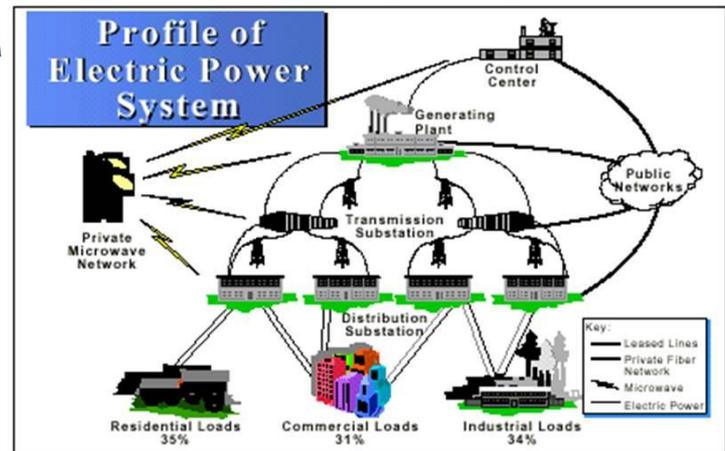
Why now is so urgent:

THREAT SPECTRUM EVOLUTION

Today's Criminals Come in Many Forms...all of which can do great harm

- **Script kiddies**

- **Hacktivists**

- **Cyber Criminals**

- **APTs / Nation States**

IMAGE SOURCE: http://upload.wikimedia.org/wikipedia/commons/4/48/Anonymus_logo.png

Source: GBA

Different Faces, Same Basic Process

Source: GBA
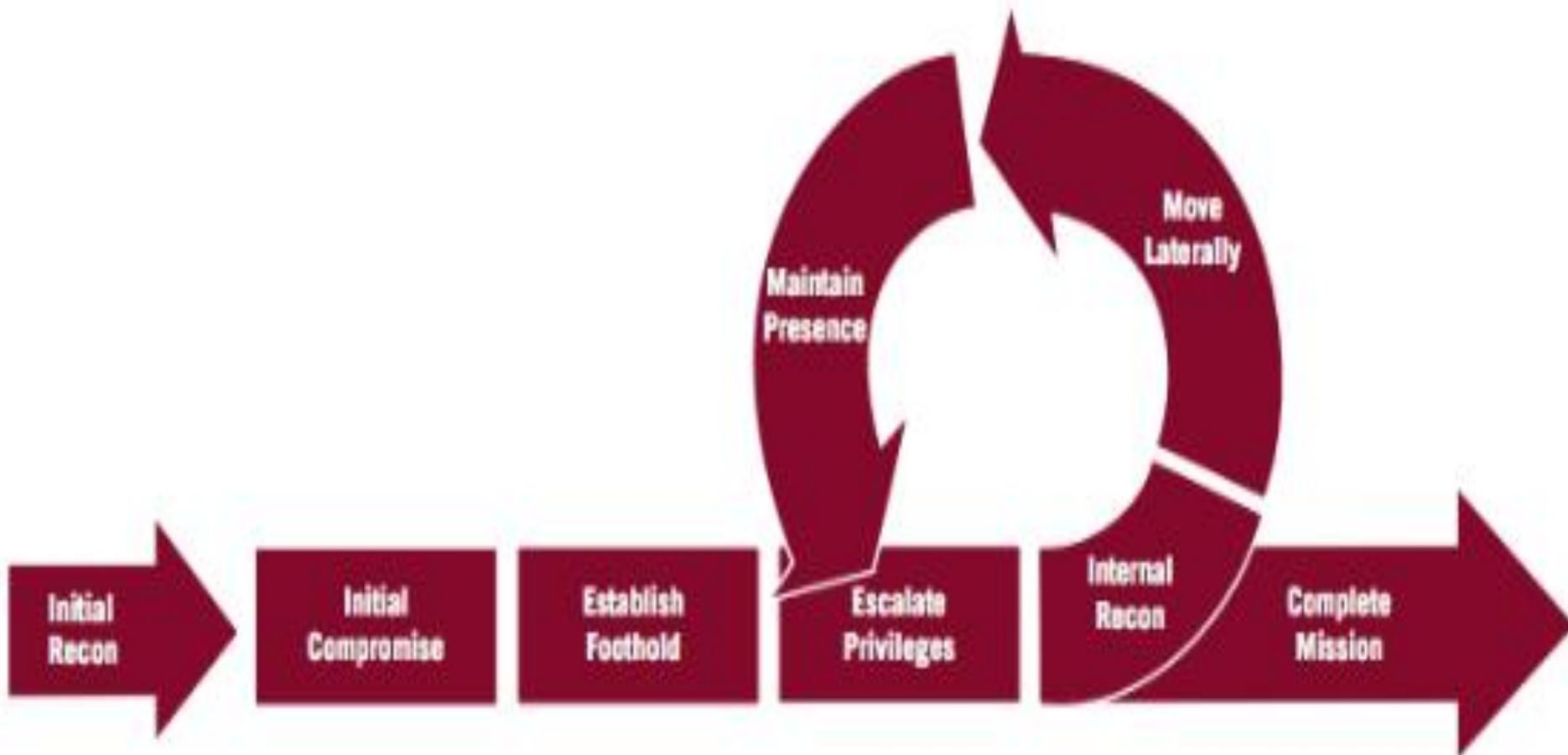
Common Script Kiddie Attack Progression

```
┌─────────────────────┐     ┌─────────────────┐     ┌─────────────────┐
│  Script Kiddie enjoys│     │ Identifies Target│     │    Scans for     │
│ hacking and wants to │ ──> │   Website(s)     │ ──> │ Vulnerabilities  │
│   build reputation   │     │                  │     │                  │
└─────────────────────┘     └─────────────────┘     └─────────────────┘

┌─────────────────────┐     ┌─────────────────┐
│ Defaces Website or  │ <── │    Exploits      │ <──
│ Steals Data from    │     │ Vulnerabilities  │
│     Database        │     │                  │
└─────────────────────┘     └─────────────────┘

        ┌──────────────────────────┐
        │ Publicly Posts Data Breach│
   ──>  │ Information and/or boasts  │
        │   about what they did      │
        └──────────────────────────┘
```

Source: GBA
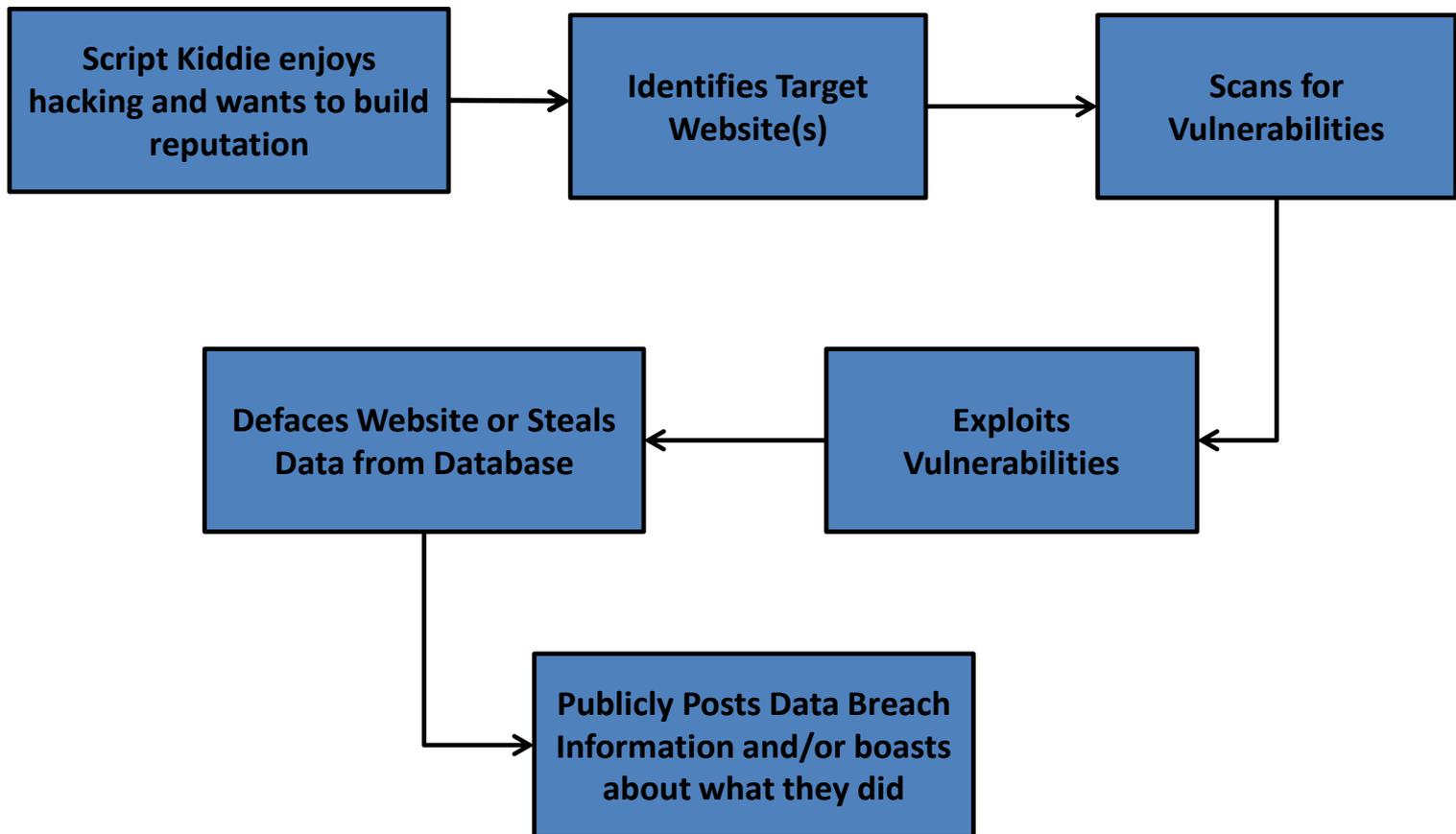
Script Kiddie Damage

"ACK!3STX" (age 15) - Austria

Threat Type – External / Script Kiddie / Hacker
Capability – Moderately Skilled

http://simple.wikipedia.org/wiki/File:Braeden_hacking.jpg

- **Hacked 259 websites in 90 days**

- **Stole and leaked information**

- **Defaced corporate websites**

Screenshot of Defacement by 15 Year Old

Source: GBA

What is an Advanced Persistent Threat?

ADVANCED
PERSISTENT
THREAT

APT

- **Highly Skilled**

- **Nation State Sponsored**

- **They have more time, and more resources than you**
- **If you are targeted, they WILL get into your system**

http://wp.latussolutions.com/wp-content/uploads/2012/01/APT2-Smaller.png

Source: GBA

Methodology / APT Attack Progression

The details change, but the process is generally the same

Source: GBA
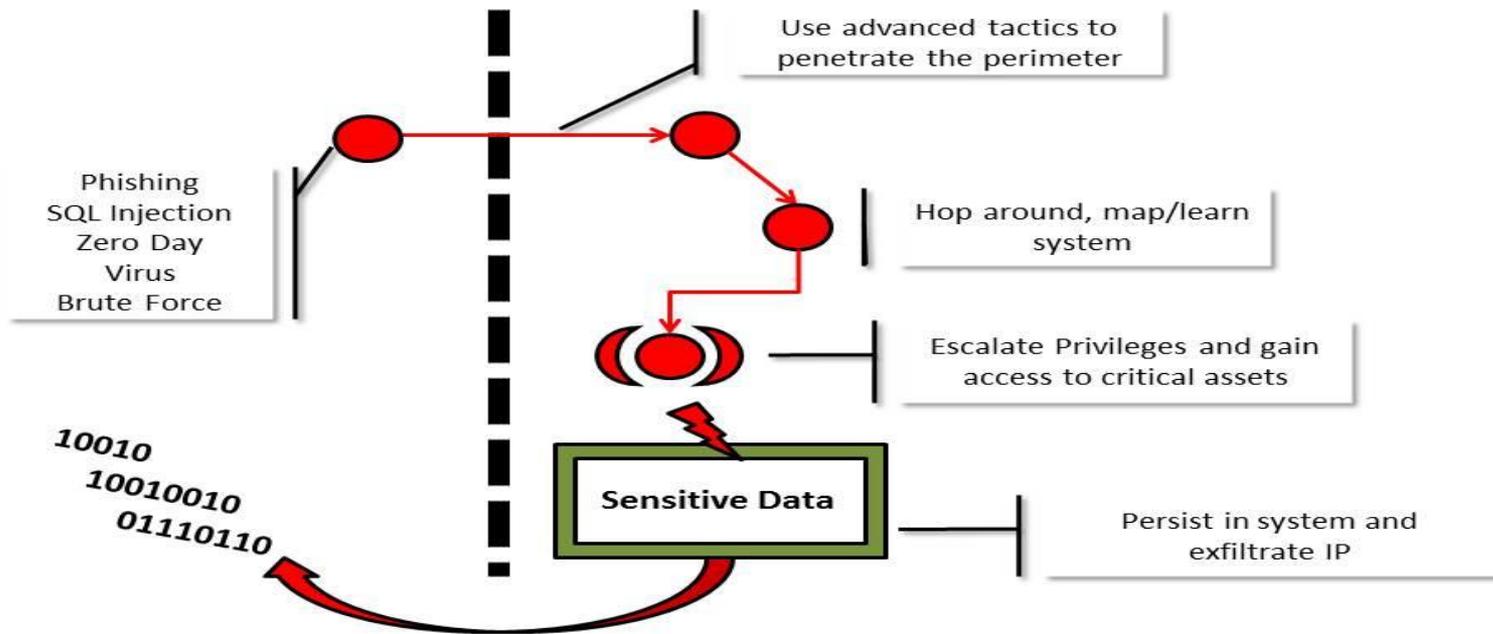
APT1 - China

- **Sponsorship by Chinese government (alleged)**

- **Infiltration of American businesses**
  - Coca-Cola, RSA Security, Televent

- **Only 1 of 20 suspected state-sponsored groups in China**
  - Dozens more in other countries

http://www.theregister.co.uk/2013/02/19/china_apt_report_mandiant/

Motivation

- **Geopolitical**
- **Economic**
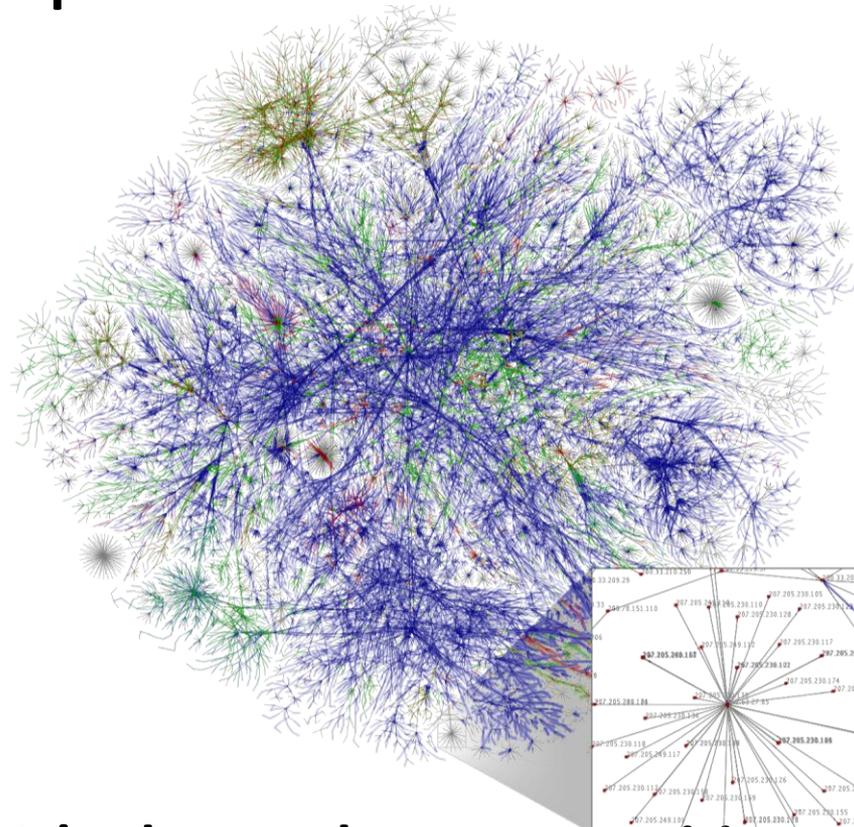
It's always about competition

Source: GBA

The Basic Attack Process, Recap

Where PRISEM fits

Recon → Exploitation, Infiltration → Escalation of Privileges → Exfiltration of Data

Persist (as Needed)

Remain Covert / Cover Tracks
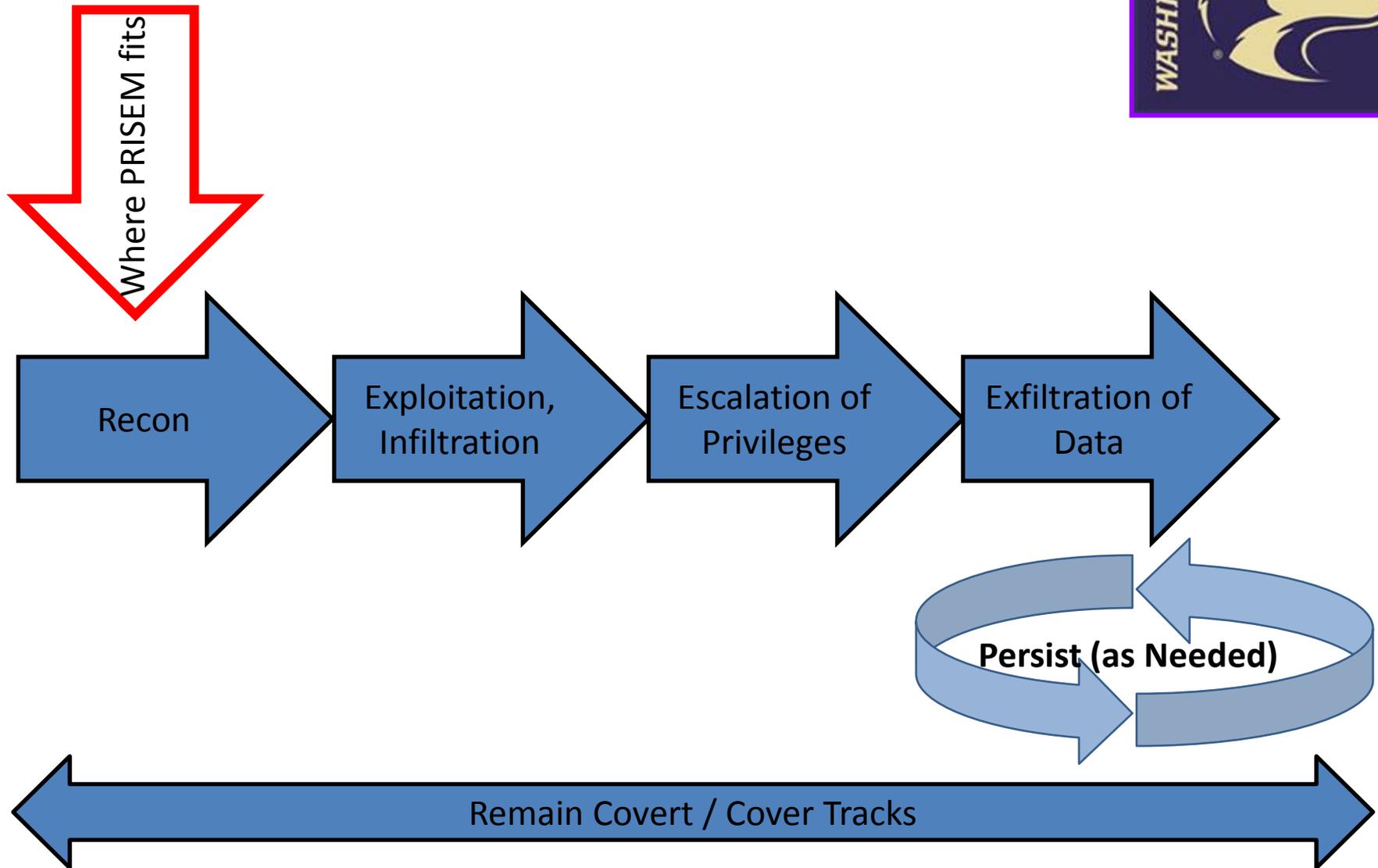
Source: GBA

Malicious Trends and Motives

Percentage of Attacks By Industry

Industry	Percentage of Total Victims
Retail	21.7%
Manufacturing	12.2%
Information	10.4%
Food Services	9.9%
Professional	9.9%
Unknown	8.4%
Finance	8.1%
Transportation	6.1%
Public	3.5%
Other Services	2.6%
Utilities	1.7%
Administrative	1.4%
Educational	1.2%
Healthcare	0.9%
Wholesale Trade	0.9%
Accomodation	0.6%
Construction	0.6%
Real Estate	0.3%

■ Percentage of Total Victims
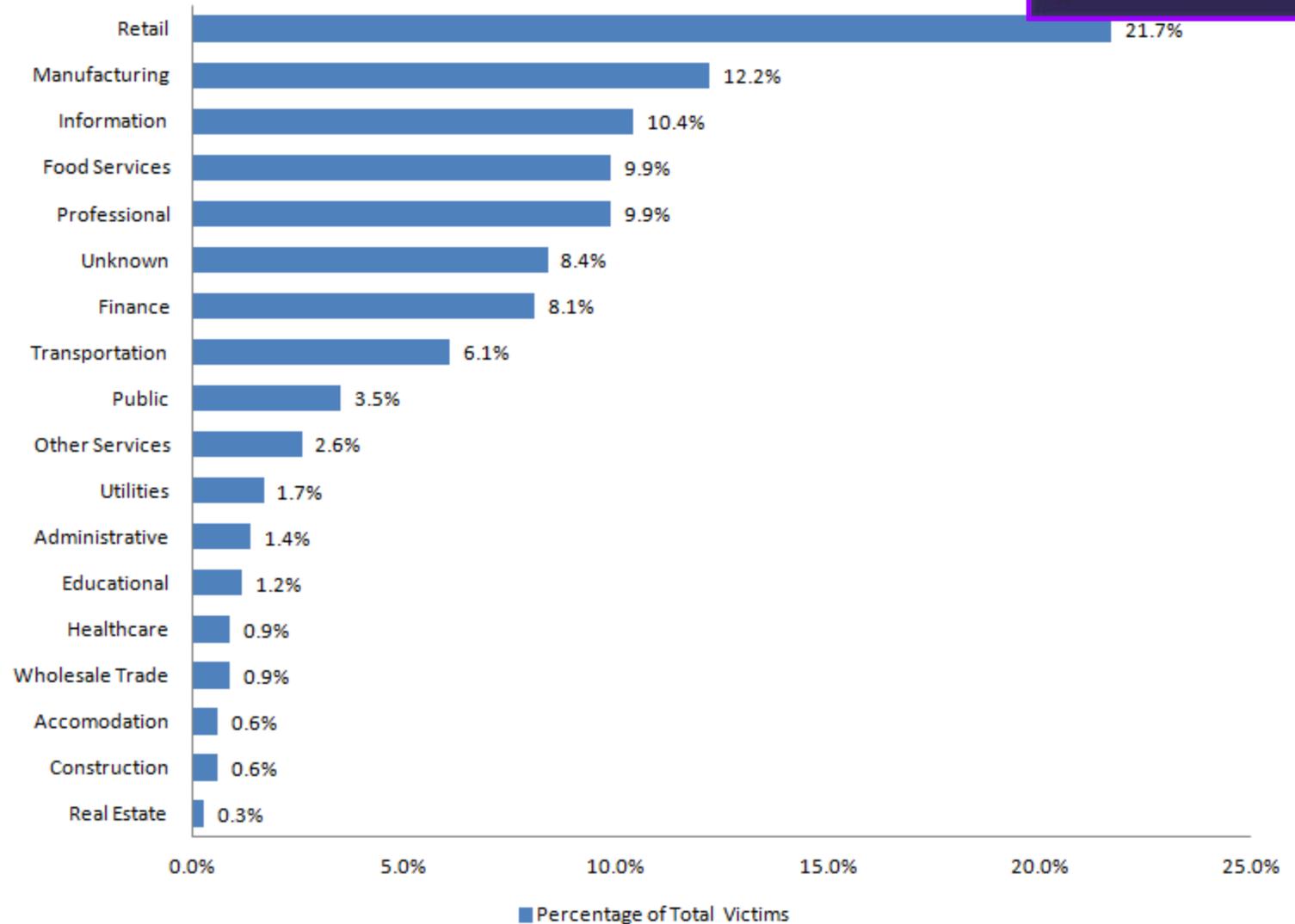
Source: GBA

Malicious Trends and Motives

2013 Hacking Motivations

■ Hacktivism   □ Cyber Crime   ■ Cyber Espionage   ■ Cyber Warfare

4%
6%
44%
46%
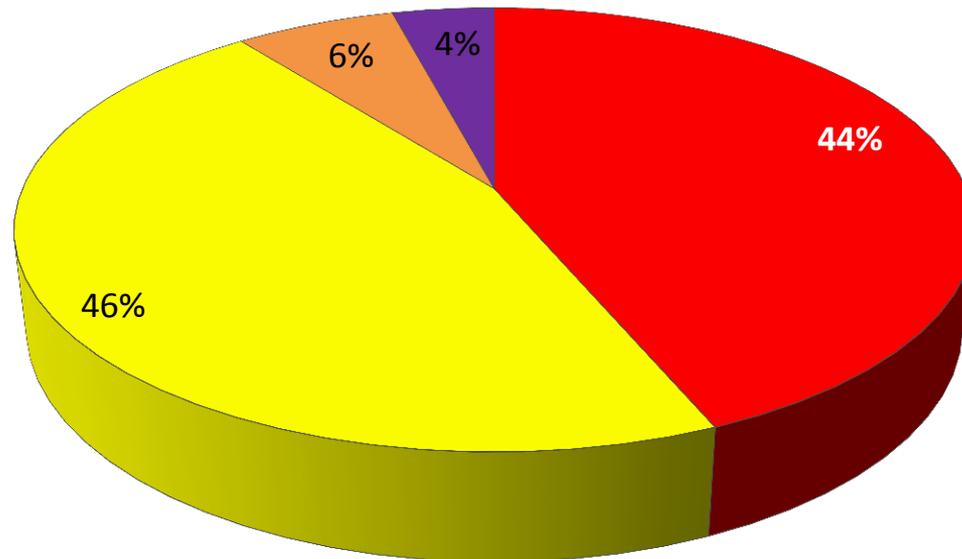
Hacktivism = Internet Protests by groups like Anonymous
Cyber Crime = Hackers committing electronic crimes
Cyber Espionage = Government hacking for intelligence
Cyber Warfare = Countries fighting electronically (Iran VS Israel)

Source: GBA

Malicious Trends and Motives
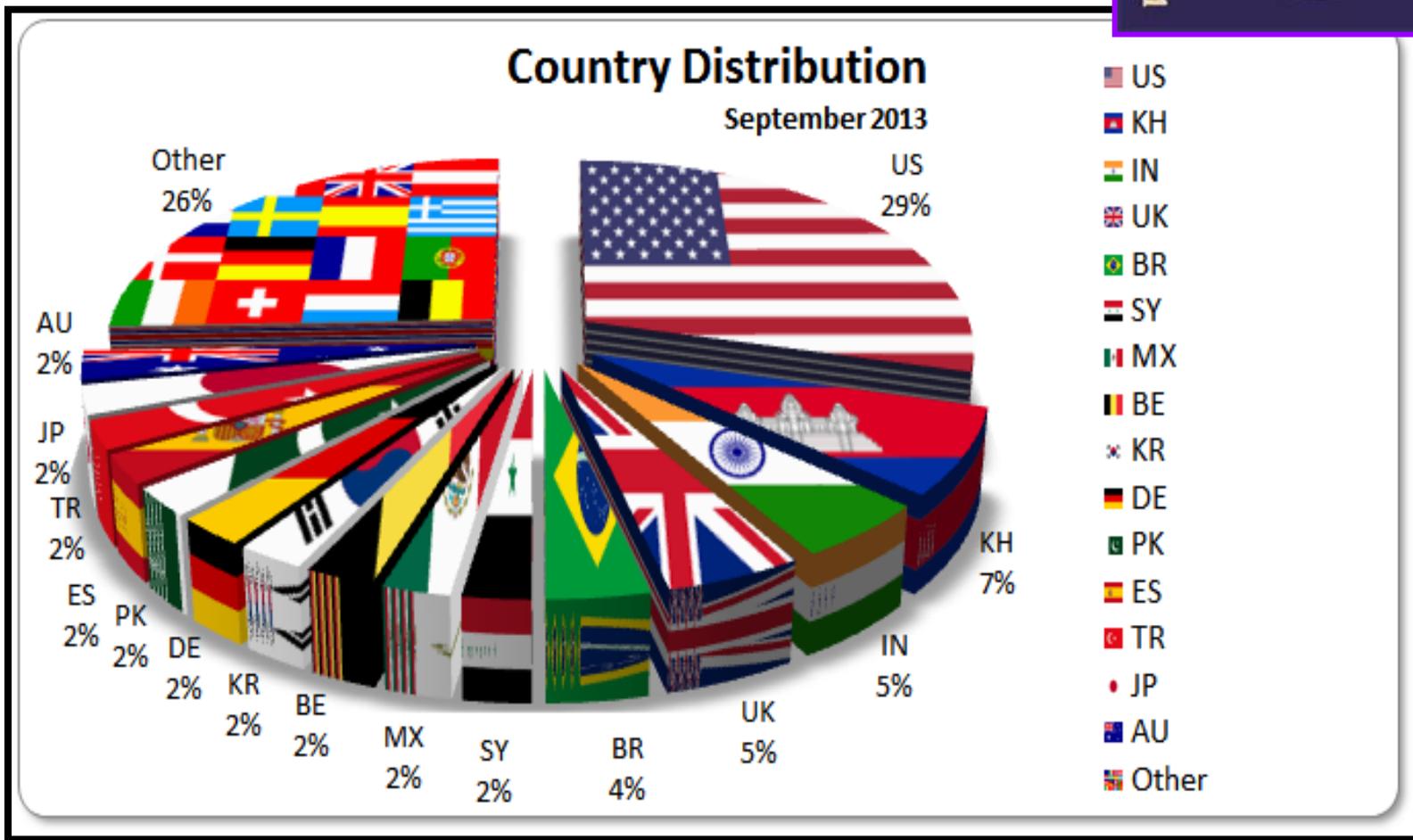
Which countries got attacked the most (Sep 2013)

http://hackmageddon.com/2013/10/20/september-2013-cyber-attacks-statistics/

Source: GBA

Malicious Trends and Motives

- Do you have an Android Smart phone??
    - Most frequently attacked phone on the market (79% of all phones)
    - Big problem if you use your phone for work

    http://www.bbc.co.uk/news/technology-23863495

- Danger lurks in plain site (websites)
  Have you ever visited CNN, AMAZON, Ebay, U of Phoenix or BBC websites?
  They've all been used to conduct cyber attacks against users like yourselves

- Cybercriminals love to use Facebook, Twitter Google, Bing, Youtube for their dirty work...

    http://www.youtube.com/watch?v=Fzyquo7Y2Vs

Source: GBA

A TYPICAL WEEK IN SEATTLE

- 30,000-60,000 password guesses
- Targeted attacks
- Websites attacked every 4 minutes
- 75 pieces of malware removed, 200 blocked
- 100M web pages viewed; 3M sites blocked
- 20% of e-mail has hostile intent; 1% slips through
- Outbound network traffic to all countries
- 10 desktops "phoning home" to C&C

City of Bellevue Location

Alerts for Last 24 Hours

1 Critical Alerts
0 High Alerts
6 Medium Alerts
22 Low Alerts
116 Informational Alerts
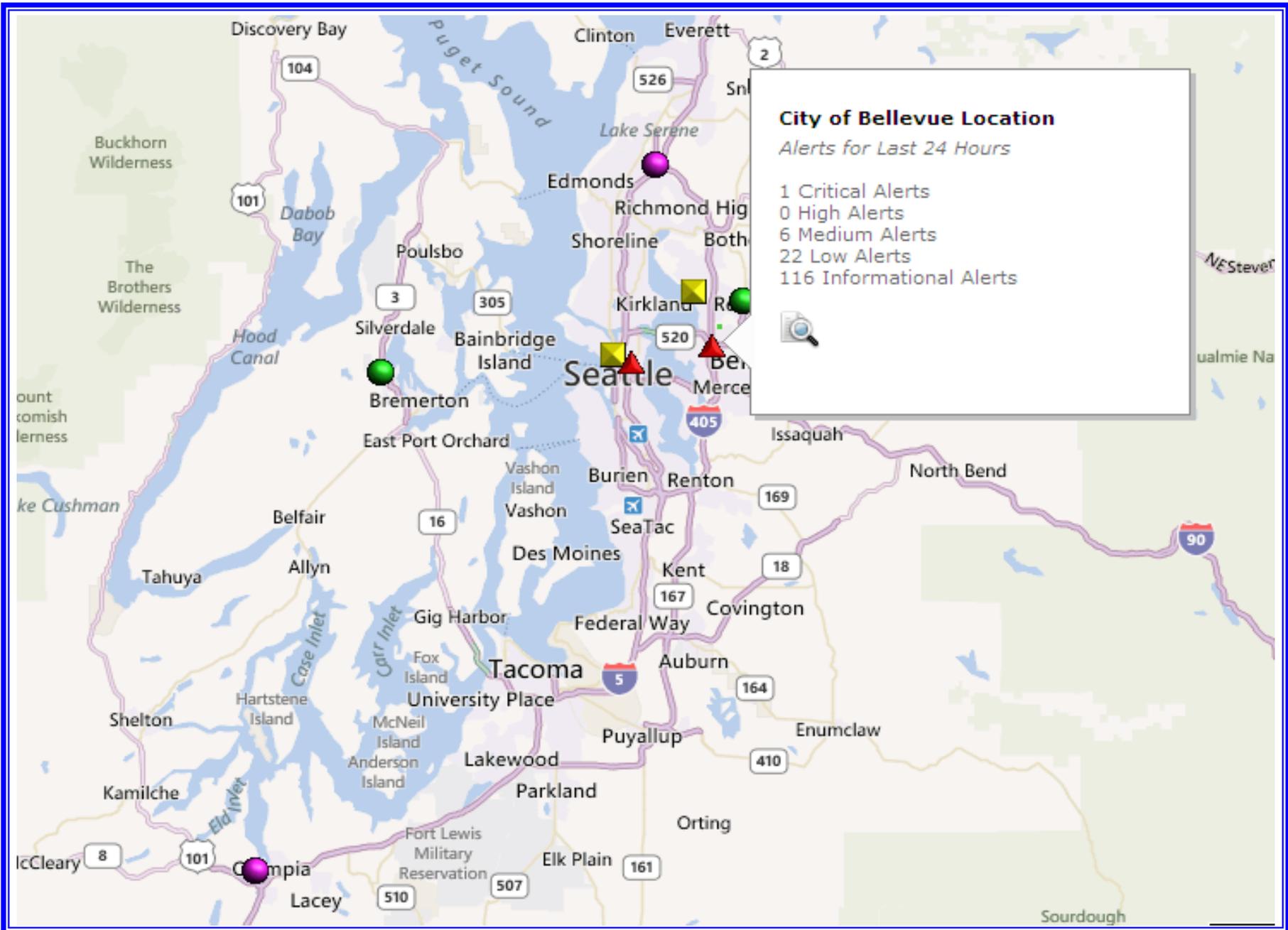
U.S. Essentials Breakdown

The number of attacks reported to a U.S. Department of Homeland Security cyber security response team grew by 52% in 2012, according to a recent report from the team
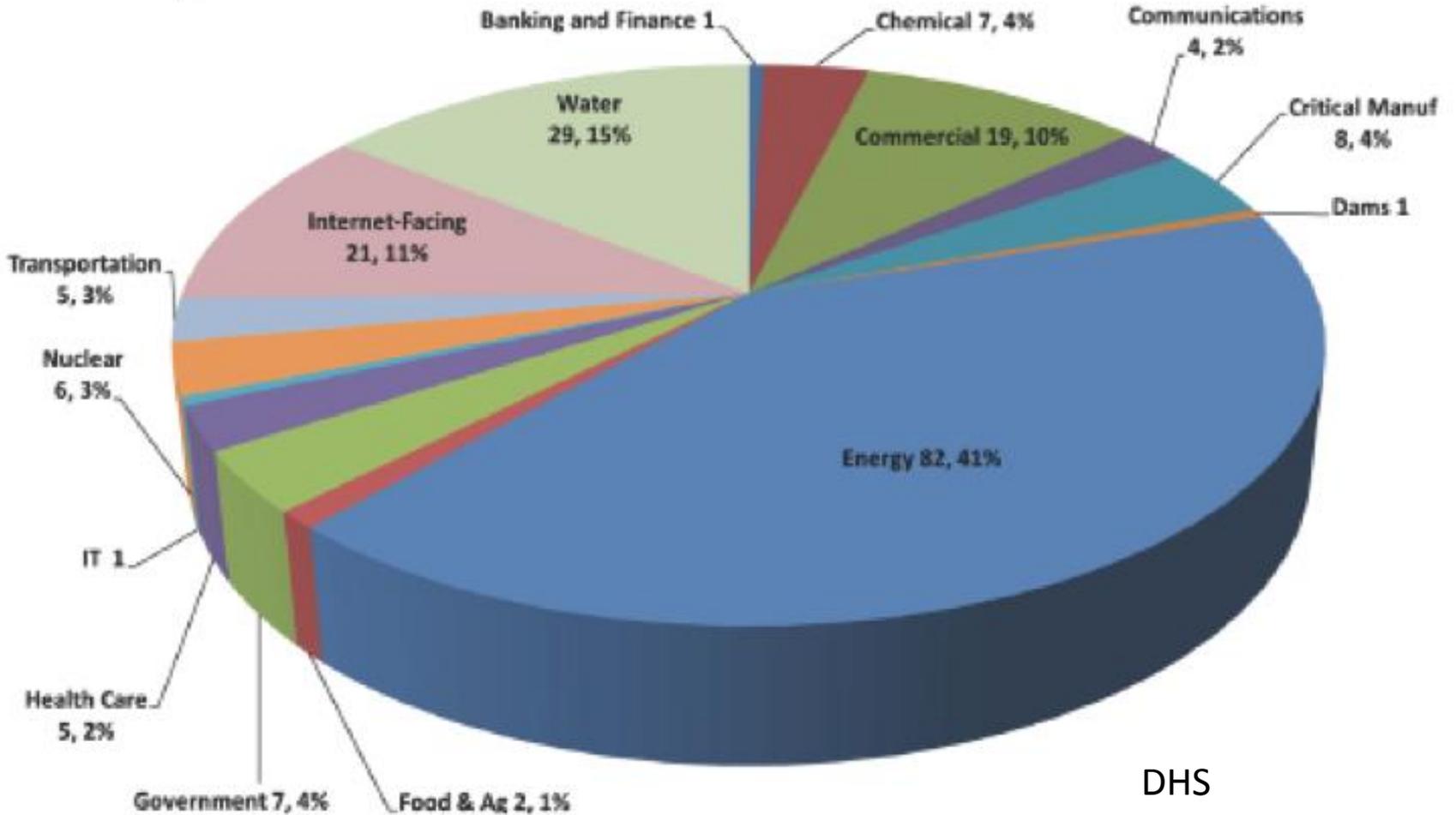
DHS

What can you do?

STRATEGIES FOR INDIVIDUALS

Back to FTC.gov   **Report ID Theft** | Order Publications | Privacy Policy | FTC Search

FIGHTING BACK AGAINST
IDENTITY THEFT
FEDERAL TRADE COMMISSION

DETER   DETECT   DEFEND

CONSUMERS | BUSINESSES | LAW ENFORCEMENT | MILITARY | MEDIA | REFERENCE DESK | EN ESPAÑOL

DETECT IDENTITY THEFT

Detect suspicious activity by routinely monitoring your financial accounts and billing statements. If you are unable to take these steps while you are deployed, consider placing an active duty alert on your credit report.

INSPECT:

Your credit report. Credit reports contain information about you, including what accounts you have and your bill-paying history.

Hot Links

Use Our Materials In Your Community

Address   http://www.identitytheft.gov/index.html

Google ▾ identity theft   G Search ▾   114 blocked   ABC Check ▾   AutoLink ▾   AutoFill   Options ▾

Y! ▾   Search Web   Upgrade your Toolbar Now ▾   Mail ▾   Help ▾

Identity theft is a crime.
Resources from the Government

About the Task Force ▸

Report Identity Theft ▸

Victims' Rights ▸

ID thieves steal **your good name**, bilk billions of dollars from **the economy**, and strain **law enforcement** resources.

▶ **Combating Identity Theft: A Strategic Plan**
Final recommendations released April 23, 2007.
Strategic Plan [PDF]
Volume II: Supplemental Information [PDF]

Webcast of Press Conference

▶ **Taking Action**

http://www.identitytheft.gov/index.html   Internet

Start   HOME - Comc...   Unintended C...   Identity_Theft...   Lecture 9 Priv...   Identity the...   10:57 AM

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media History Mail Print Edit Discuss

Address http://www.komando.com/ Go Links

Google ▾ Kim Komando |G| Search ▾ 114 blocked ABC Check ▾ AutoLink ▾ AutoFill Options »

Y! ▾ [   ] Search Web Upgrade your Toolbar Now ▾ Mail ▾ Help ▾

Newsletters Kim Shop Listen Columns Downloads Sites Tips Guide Kids Board

ON AIR

Kim's Club 🔑
Podcasts, Archives & More

Free Newsletters ✉
Join 4.9 million subscribers

Shop 🛒
Buy Online

Show Picks of the Week

News

- **LISTEN**: Tune in to my show and minutes
- **COOL**: Sign up for my Cool Site of the Day
- **LISTEN**: An add-on for Google Earth
- **COLUMNS**: Take control of your Bookmarks
- **GUIDES**: Portable video players
- **NETWORKING**: Secure a wireless repeater
- **SECURITY**: Avoid becoming a zombie
- **MYSPACE**: Test your kids on MySpace safety
- **SHOP**: All 7 best-selling books

Cool Site of the Day
No talking...

Tip of the Day
iTunes alternatives...

Trivia

GoToMyPC

Which key on a keyboard should you press if the words you are typing start overwriting each other?

○ Scroll Lock
○ Insert
○ F12

Internet

Start Unintende... Exploring -... Microsoft ... Komand... Lecture 9 ... csse591_I... 9:53 AM

STOP. THINK. CONNECT. The national campaign for cybersecurity education and awareness.

STOP | THINK | CONNECT

Identity-Theft is the fastest growing crime in America; 9.9 MILLION victims were reported last year, according to a Federal Trade Commission survey!

Mari J. Frank. Esq. is a survivor of identity-theft, and the author of the book From Victim to Victor; A Step-by-Step Guide For Ending The Nightmare Of Identity Theft.

http://www.identitytheft.org/

http://www.identitytheft.gov/

What can teachers and librarians do?

STRATEGIES FOR EDUCATORS

Caution!!
Online Disinhibition Effect

- Dissociative anonymity
  - You can't be identified- anonymizers
- Invisibility
  - You can be who you want to be- 2nd life
- Asynchronicity
  - You don't have to deal with others' reactions- flaming
- Solipsistic introjection
  - Make up the other you can't see- Internet romances
- Dissociative imagination
  - Online is a game- excuse for crime
- Minimization of status and authority
  - Everyone is equal- personalities change online

J. Suler, Cyber Psychology & Behavior

Kid Nation

- Kids know technology better than adults

- More prone to commit <u>cyber</u> crime
  - Plagiarism sites
  - Music downloads
  - Disrespect for IP

- Cyberbullying

- Blind trust online

- Need for cyberethics training

5 Things Educators Can Do:

- Initiate cyber ethics/safety curriculum
    - Research existing programs
    - http://www.isafe.org
- Teach cyberethics/safety in the classroom
- Use the Internet as mode of delivery
    - http://www.cybersmartcurriculum.org
- Create acceptable use policy
- Have students make a pledge

J.Baum, Cyberethics
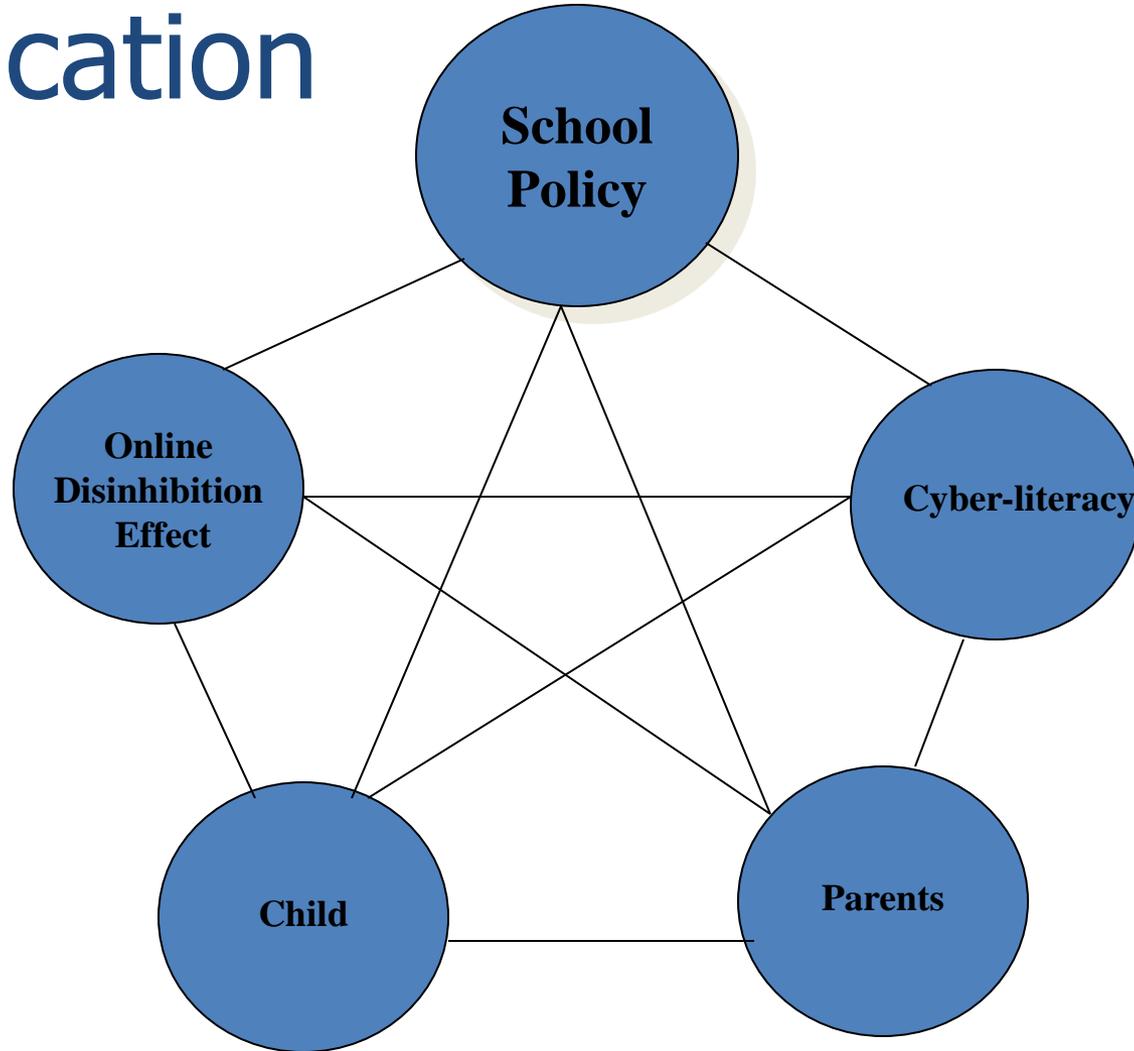
Education

Call to Action!

- Discuss needs at your school/organization
- Describe an action plan
- Discuss first steps
- Double check:
    - Is the plan doable?
    - Am I ready to take the first step?
    - Who do I need to get involved?
- Group discussion

WANTED BY THE FBI

FOR COMPUTER HACKING
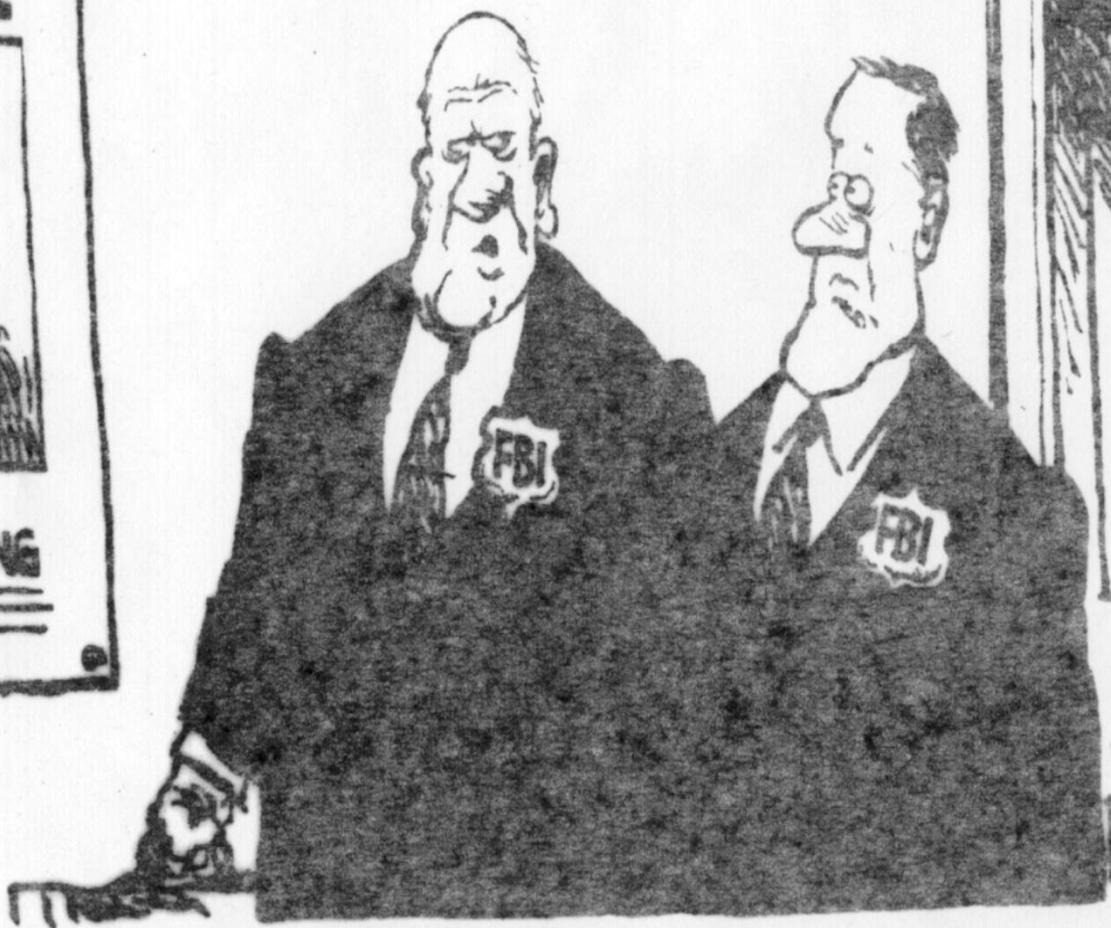
"FRANKLY, I MISS THE OLD DAYS OF JOHN DILLINGER AND AL CAPONE."