

# ***Introduction to Cybersecurity, CyberLaw, and CyberForensics Information***

**William Favre Slater, III, M.S. in Cybersecurity, MBA, PMP, CISSP, CISA  
CISO / Sr. Cybersecurity Consultant / Project Manager / Program Manager  
Chicago, Illinois  
United States of America  
September 30, 2022**



**ACFTI**

**Slater Technologies**

# *Agenda*

- The Internet in 2022
- Cybersecurity
- CyberLaw and Examples of Lawbreakers
- CyberThreats & Cyber Vulnerabilities
- A Cyber Litigator's Advice – For Defendants
- CyberForensics and Forensics Principles
- How to Be Anonymous Online
- Summary & Conclusion
- Questions and Answers



ACFTI

Slater Technologies

# *THE INTERNET IN 2022*



ACFTI

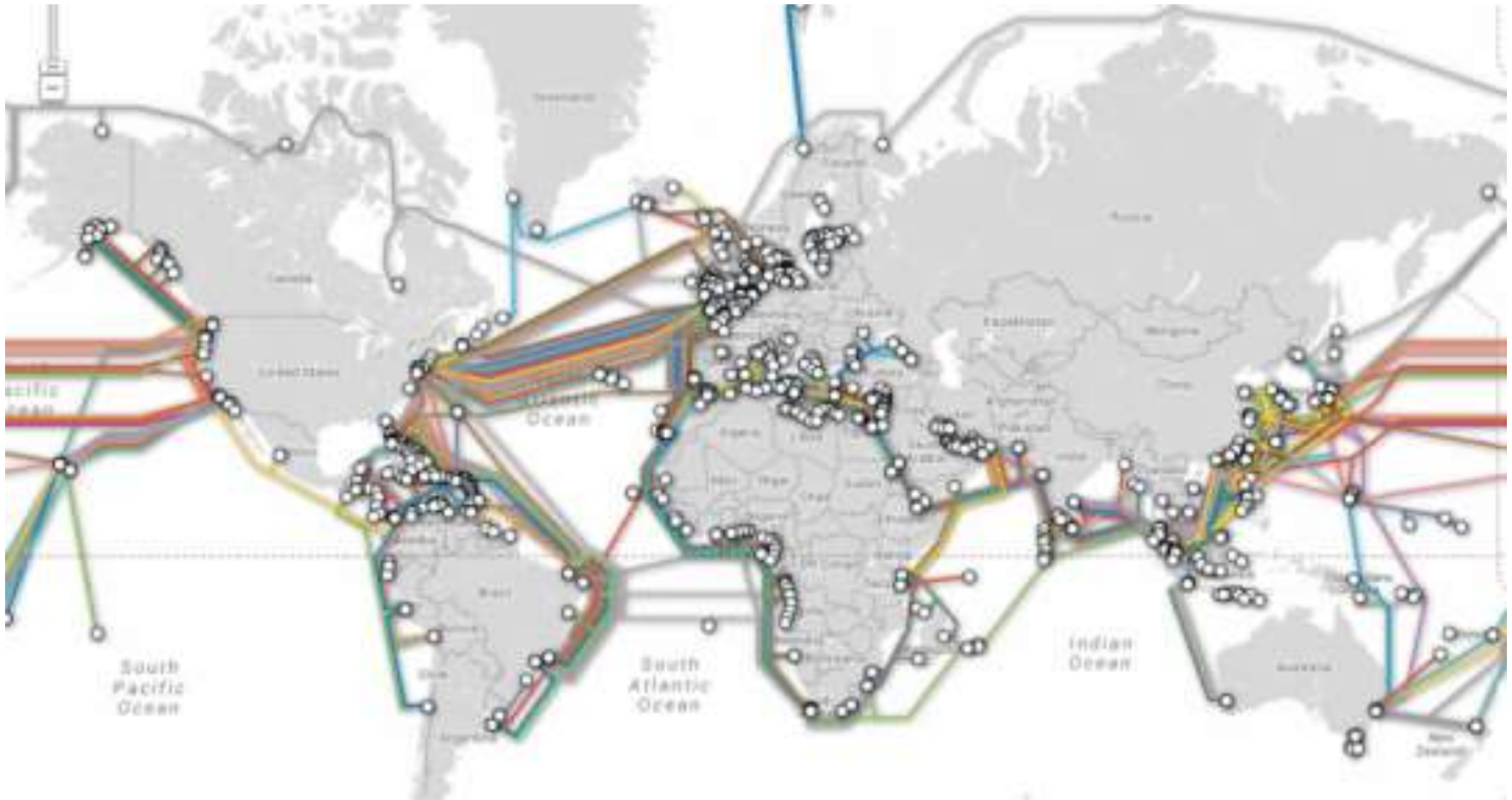
*Slater Technologies*



# The Internet is a Huge and Global Place

# Every Continent and Country Is Connected

## 24 x 7

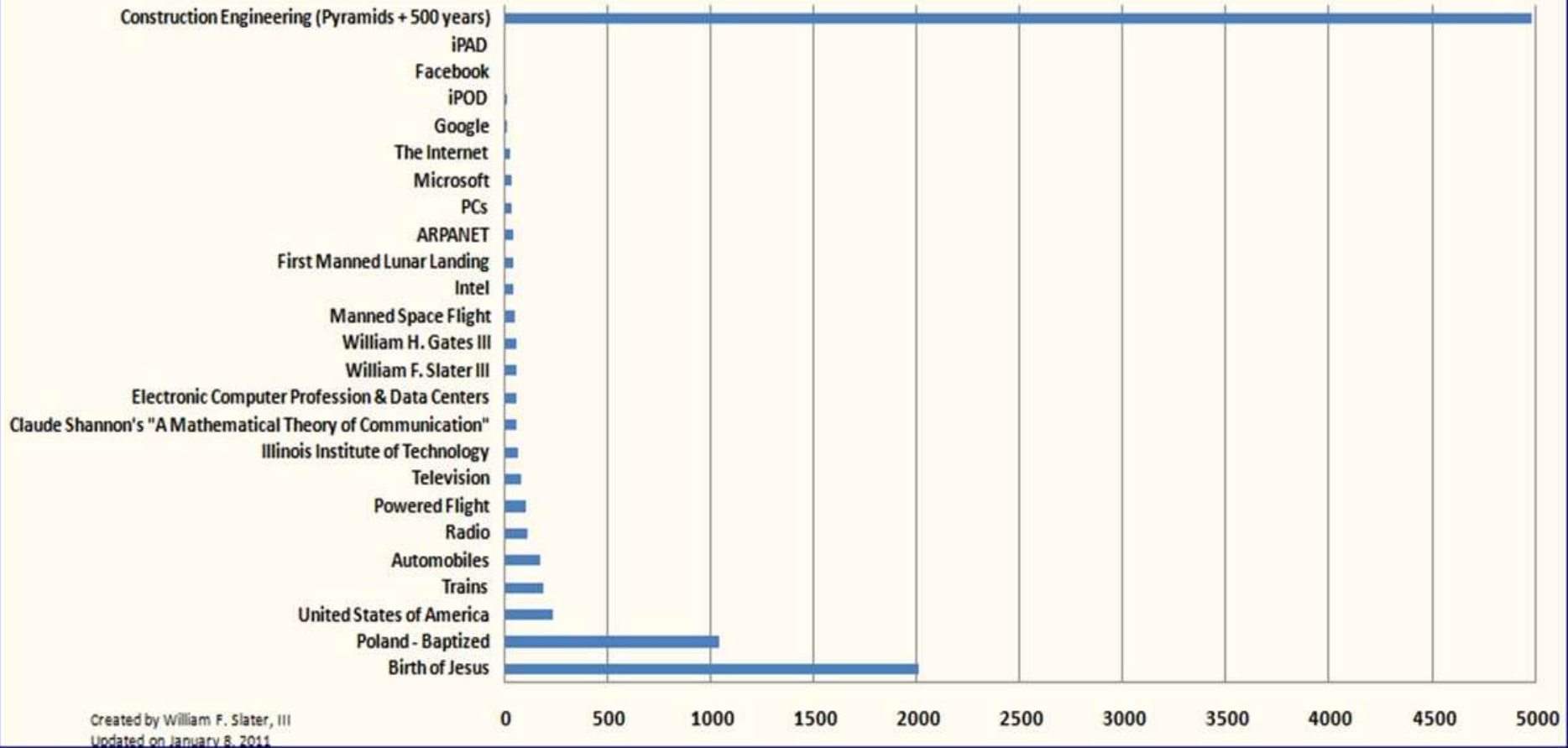


Notes: 1) Satellite connections are omitted here. 2) Due to totalitarian policies, the governments of 23 countries did temporarily shut down the Internet for their Citizens this year.

Slater Technologies

# Relatively Speaking

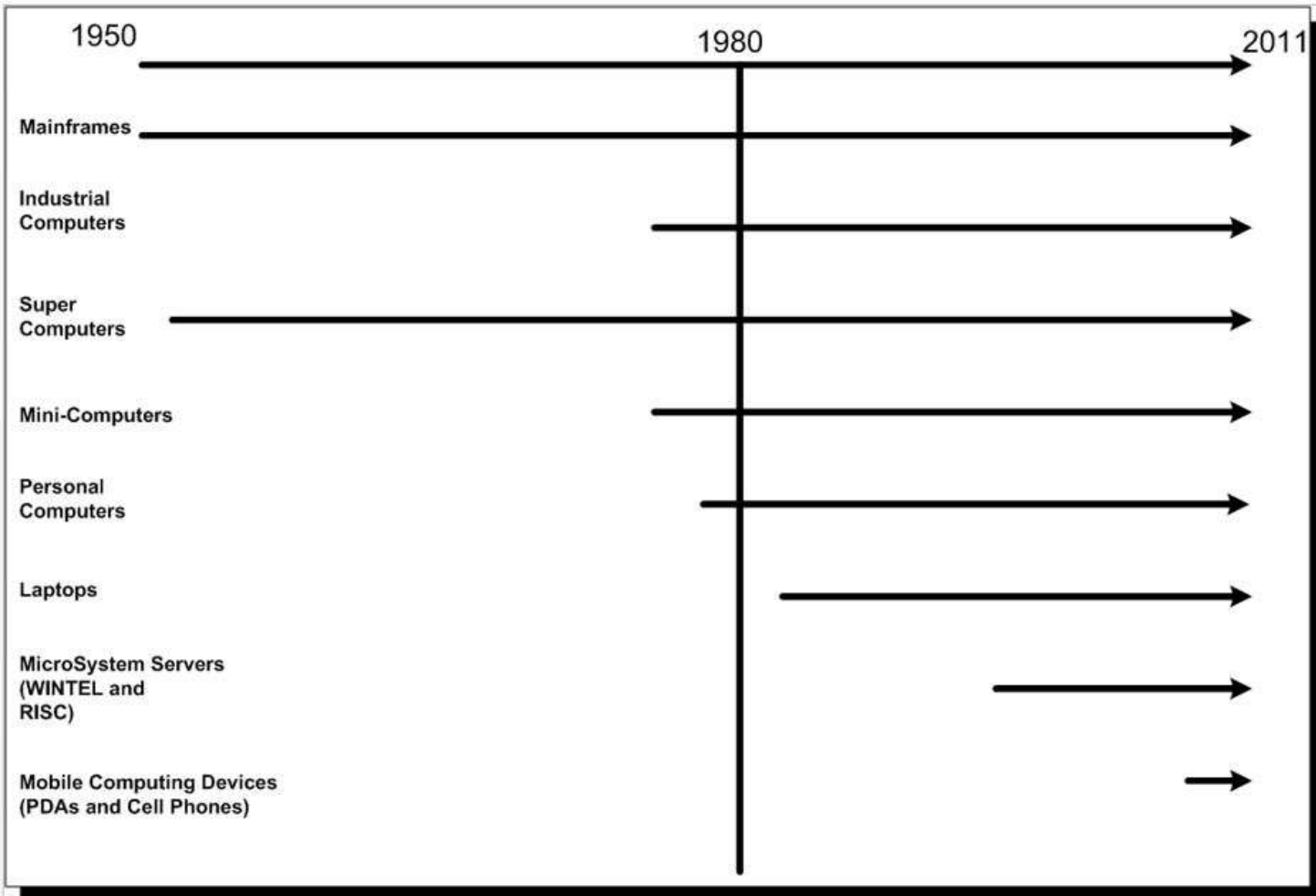
Putting Things into Even Larger Perspective - Important Milestones in Technology



Created by William F. Slater, III  
Updated on January 8, 2011



# Relatively Speaking

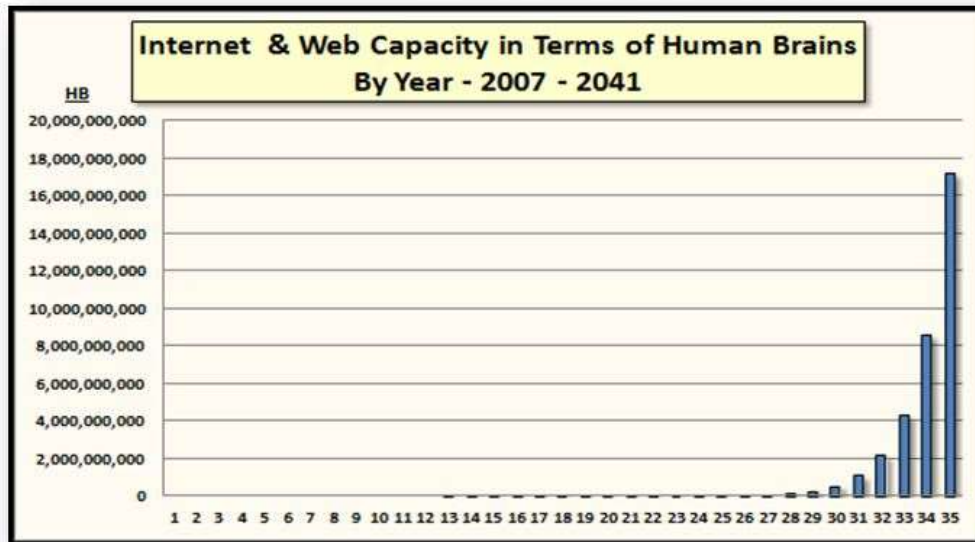


**Evolution of Modern Computing Platforms**



# Relatively Speaking

## Capacity of the Internet and the Web



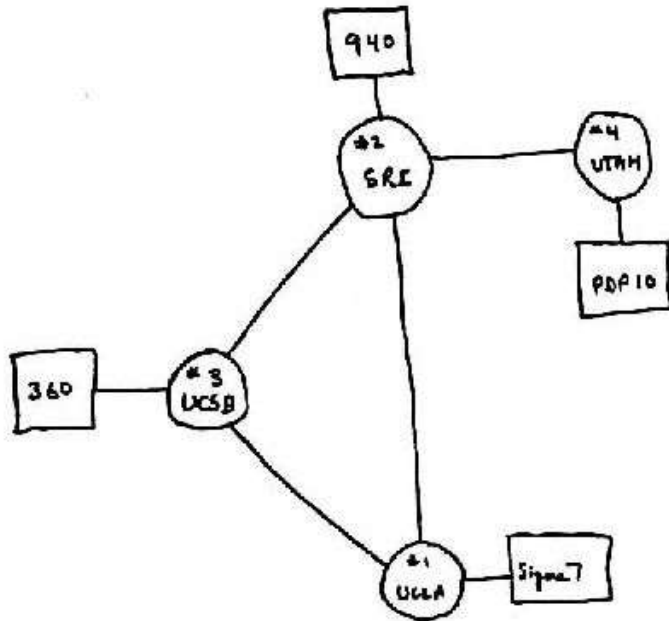
Count	Year	HB
1	2007	1
2	2008	2
3	2009	4
4	2010	8
5	2011	16
6	2012	32
7	2013	64
8	2014	128
9	2015	256
10	2016	512
11	2017	1,024
12	2018	2,048
13	2019	4,096
14	2020	8,192
15	2021	16,384
16	2022	32,768
17	2023	65,536
18	2024	131,072
19	2025	262,144
20	2026	524,288
21	2027	1,048,576
22	2028	2,097,152
23	2029	4,194,304
24	2030	8,388,608
25	2031	16,777,216
26	2032	33,554,432
27	2033	67,108,864
28	2034	134,217,728
29	2035	268,435,456
30	2036	536,870,912
31	2037	1,073,741,824
32	2038	2,147,483,648
33	2039	4,294,967,296
34	2040	8,589,934,592
35	2041	17,179,869,184



# In the Beginning...

## ARPANET September 1969

From Computer Desktop Encyclopedia  
Reproduced with permission.  
© 2000 The Computer Museum History Center



### Humble Beginnings

Scrawled on this paper in 1969 were the first four nodes of the ARPANET. Little did they realize these four nodes would grow to millions. (Image courtesy of The Computer History Museum, [www.computerhistory.org](http://www.computerhistory.org))



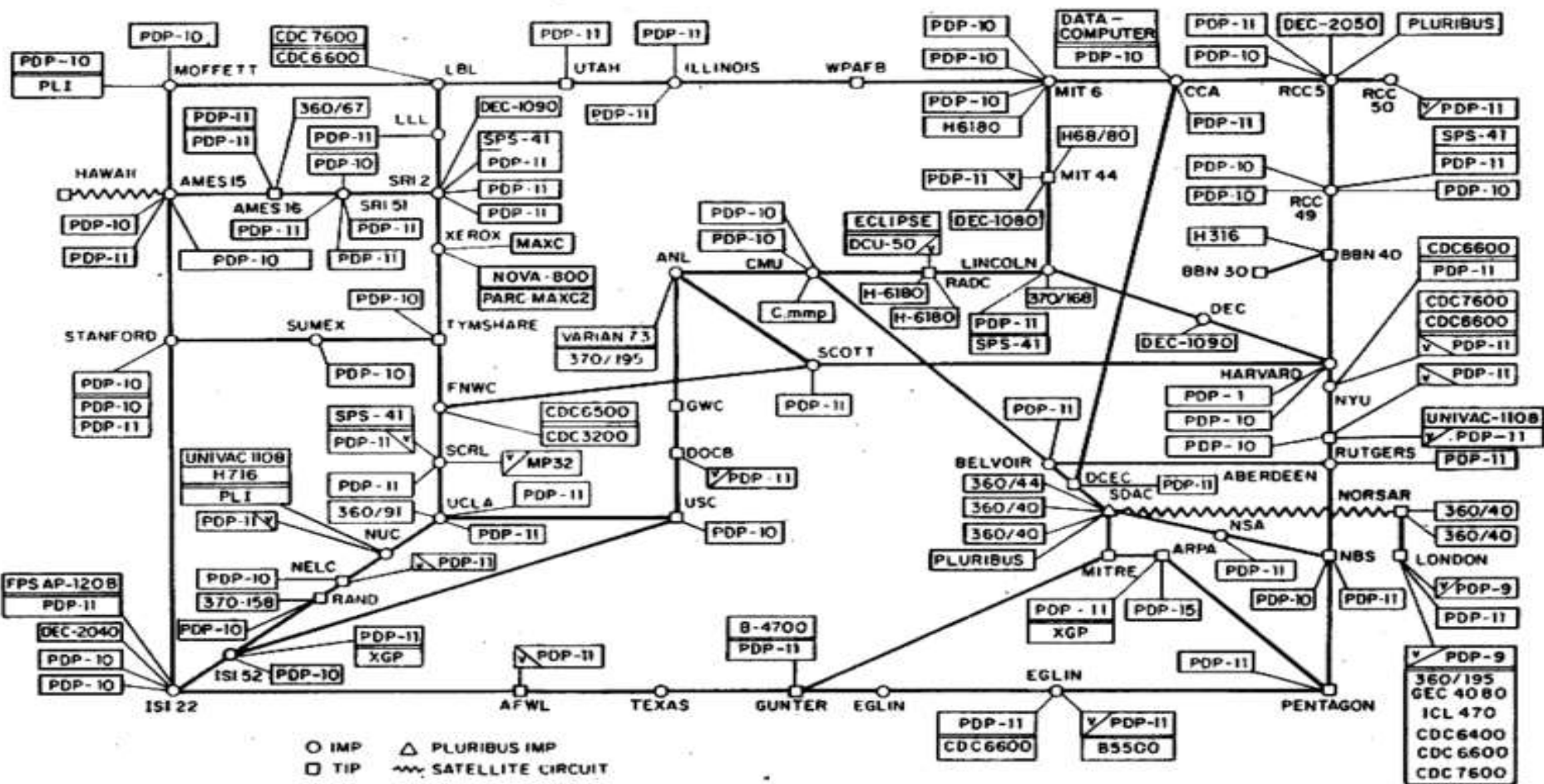
**The Founding Fathers: Leonard Kleinrock, Paul Baran, and Larry Roberts**

They were present at the creation. Baran, at the Rand Corporation in the late 1950s, conjured the idea of "packet switching." Roberts, chief computer scientist at the Pentagon's Advanced Research Projects Agency, oversaw the creation of the Arpanet in the late 1960s. In Kleinrock's laboratory at U.C.L.A., in 1969, this new digital way of transmitting data—precursor of today's Internet—came to life.

Slater Technologies

# ARPANET, March 1977

ARPANET LOGICAL MAP, MARCH 1977

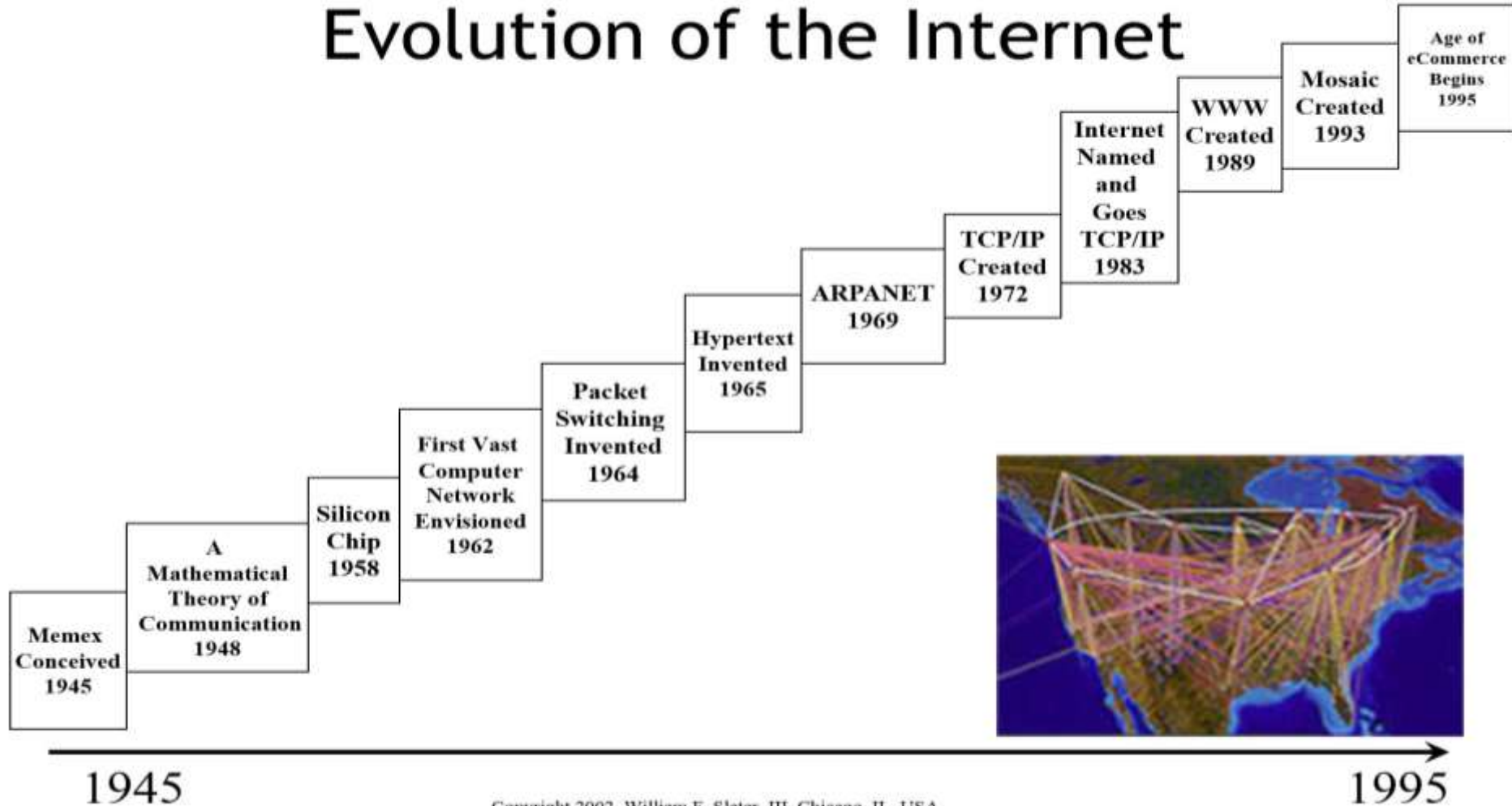


(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

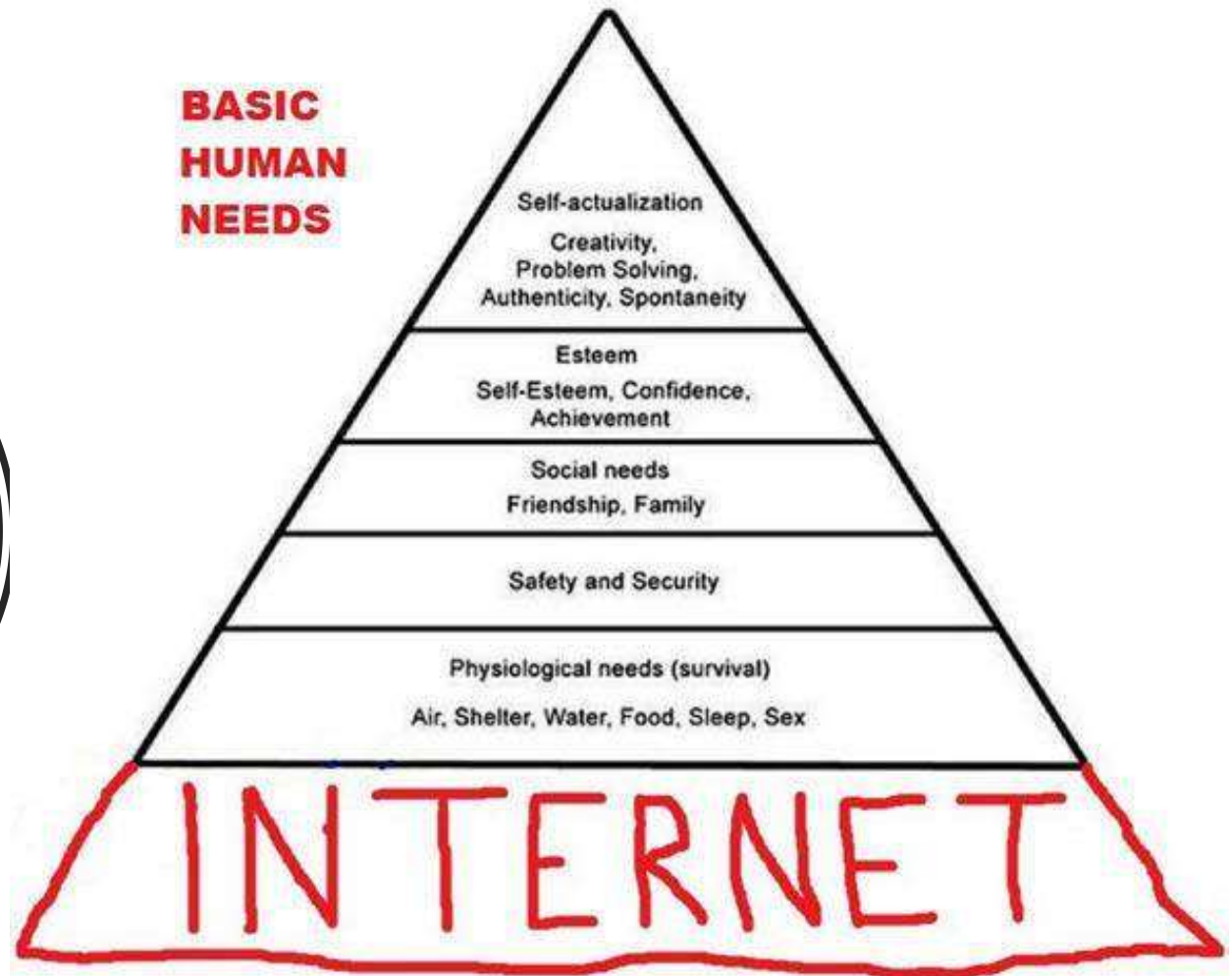
# Innovations that led to the Modern Internet

## A Brief Summary of the Evolution of the Internet

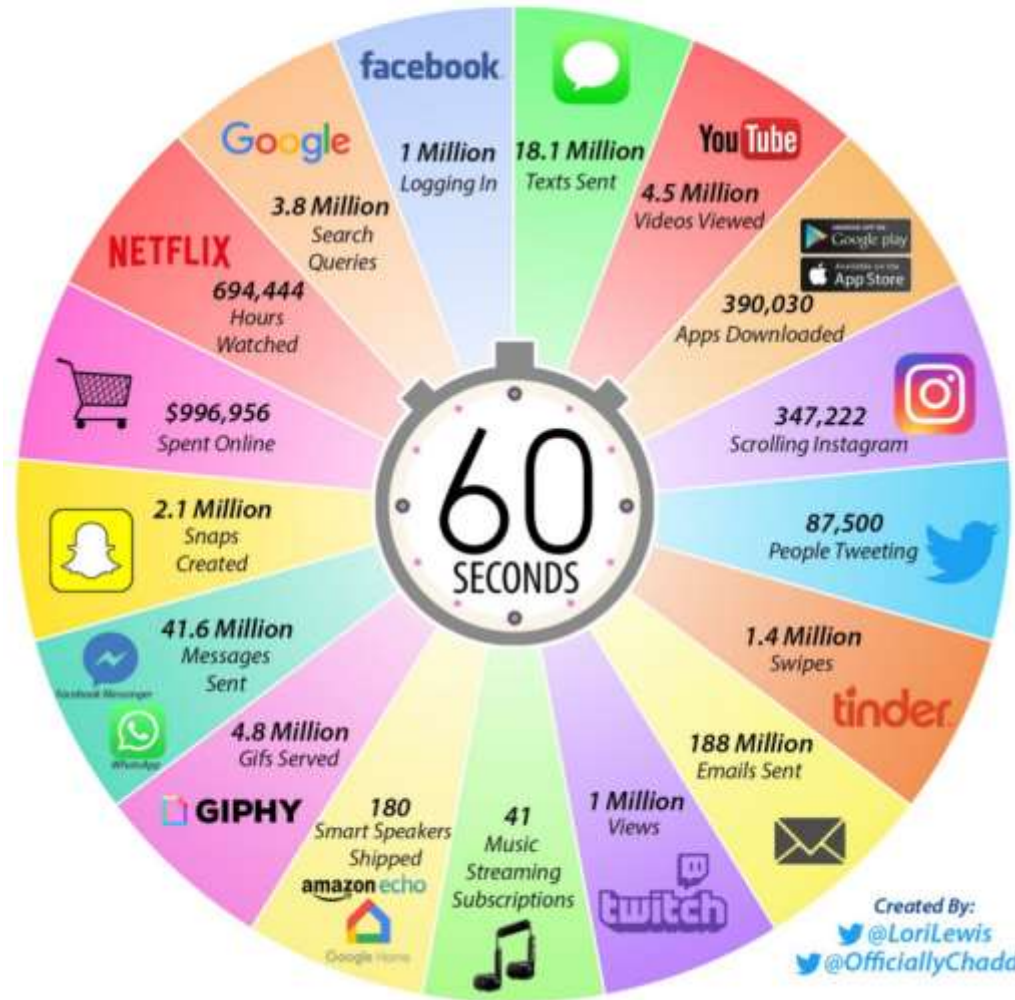


Copyright 2002, William F. Slater, III, Chicago, IL, USA

Modern  
Version of  
Maslow's  
Hierarchy of  
Needs



# 2019 *This Is What Happens In An Internet Minute*



2019 - What Happens on The Internet in 60 Seconds?



# 2020 *This Is What Happens In An* Internet Minute



2020 - What Happens on The Internet in 60 Seconds?

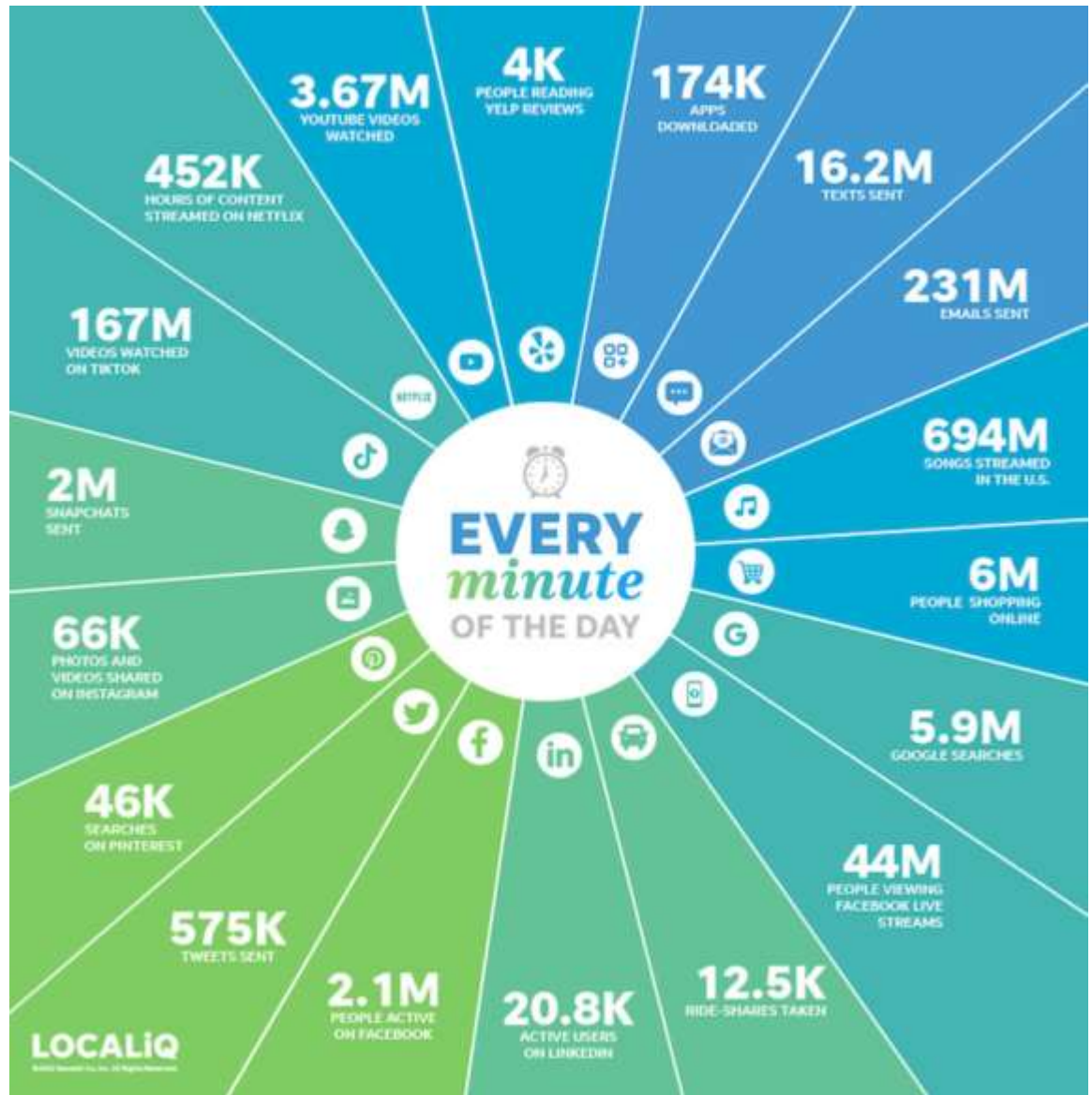
Created By:  
@LoriLewis  
@OfficiallyChadd



# 2021 - What Happens on The Internet in 60 Seconds?

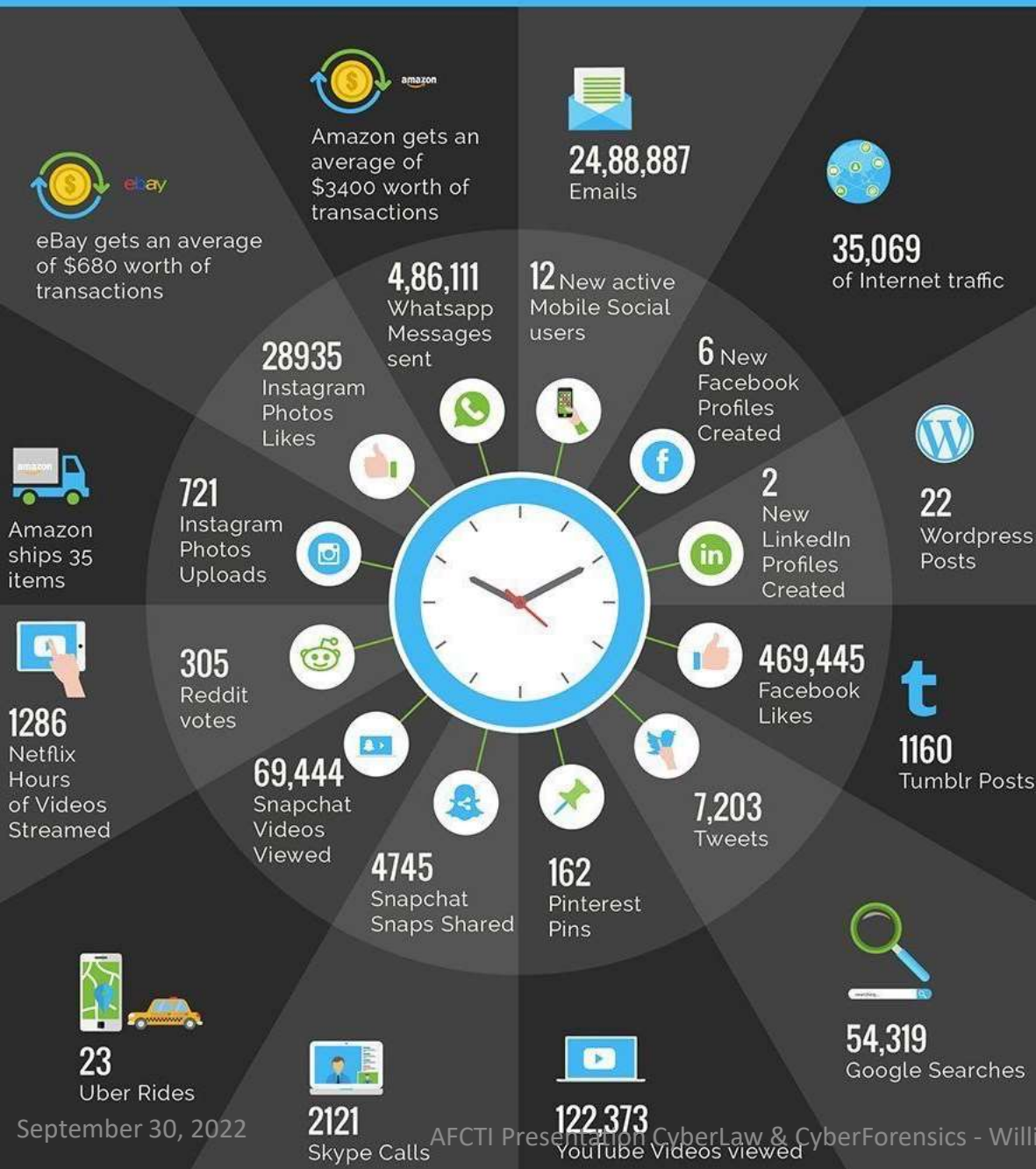


2022 - What Happens on The Internet in 60 Seconds?





# WHAT HAPPENS IN 1 SECOND OF THE INTERNET



# What Happens on The Internet in One Second?



# Digital Around the World - 2020

JUL  
2020

## OVERVIEW OF GLOBAL INTERNET USE

A SNAPSHOT OF INTERNET USE AROUND THE WORLD

TOTAL NUMBER  
OF GLOBAL  
INTERNET USERS



we  
are  
social

**4.57**  
BILLION

INTERNET USERS AS A  
PERCENTAGE OF TOTAL  
GLOBAL POPULATION



8

**59%**

ANNUAL GROWTH  
IN THE NUMBER OF  
GLOBAL INTERNET USERS



8

**+8.2%**  
**+346 MILLION**

AVERAGE AMOUNT OF TIME PER  
DAY SPENT USING THE INTERNET  
BY EACH INTERNET USER



**6H 42M**

20

SOURCES: ITC, GLOBALWEBINDEX, GSMA INTELLIGENCE, EUROSTAT, SOCIAL MEDIA PLATFORMS, SELF-SERVICE ADVERTISING TOOLS, APRI, CNNIC, UNITED NATIONS (ALL LATEST AVAILABLE DATA IN JULY 2020). TIME SPENT DATA FROM GLOBALWEBINDEX (Q1 2020), BASED ON A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE [GLOBALWEBINDEX.COM](https://www.globalwebindex.com) FOR MORE DETAILS.

COMPARABILITY ADVISORY: SOURCE CHANGES

we  
are  
social

Hootsuite

Slater Technologies

# Digital Around the World - 2021

APR  
2021

## OVERVIEW OF GLOBAL INTERNET USE

A SNAPSHOT OF INTERNET USE AROUND THE WORLD

⚠️ INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS

TOTAL NUMBER  
OF GLOBAL  
INTERNET USERS



**4.72**  
BILLION

INTERNET USERS AS A  
PERCENTAGE OF TOTAL  
GLOBAL POPULATION



**60.1%**

ANNUAL CHANGE  
IN THE NUMBER OF  
GLOBAL INTERNET USERS



**+7.6%**  
**+332 MILLION**

AVERAGE DAILY TIME SPENT  
USING THE INTERNET BY  
EACH INTERNET USER



**6H 56M**

PERCENTAGE OF USERS  
ACCESSING THE INTERNET  
VIA MOBILE DEVICES



**92.8%**

12

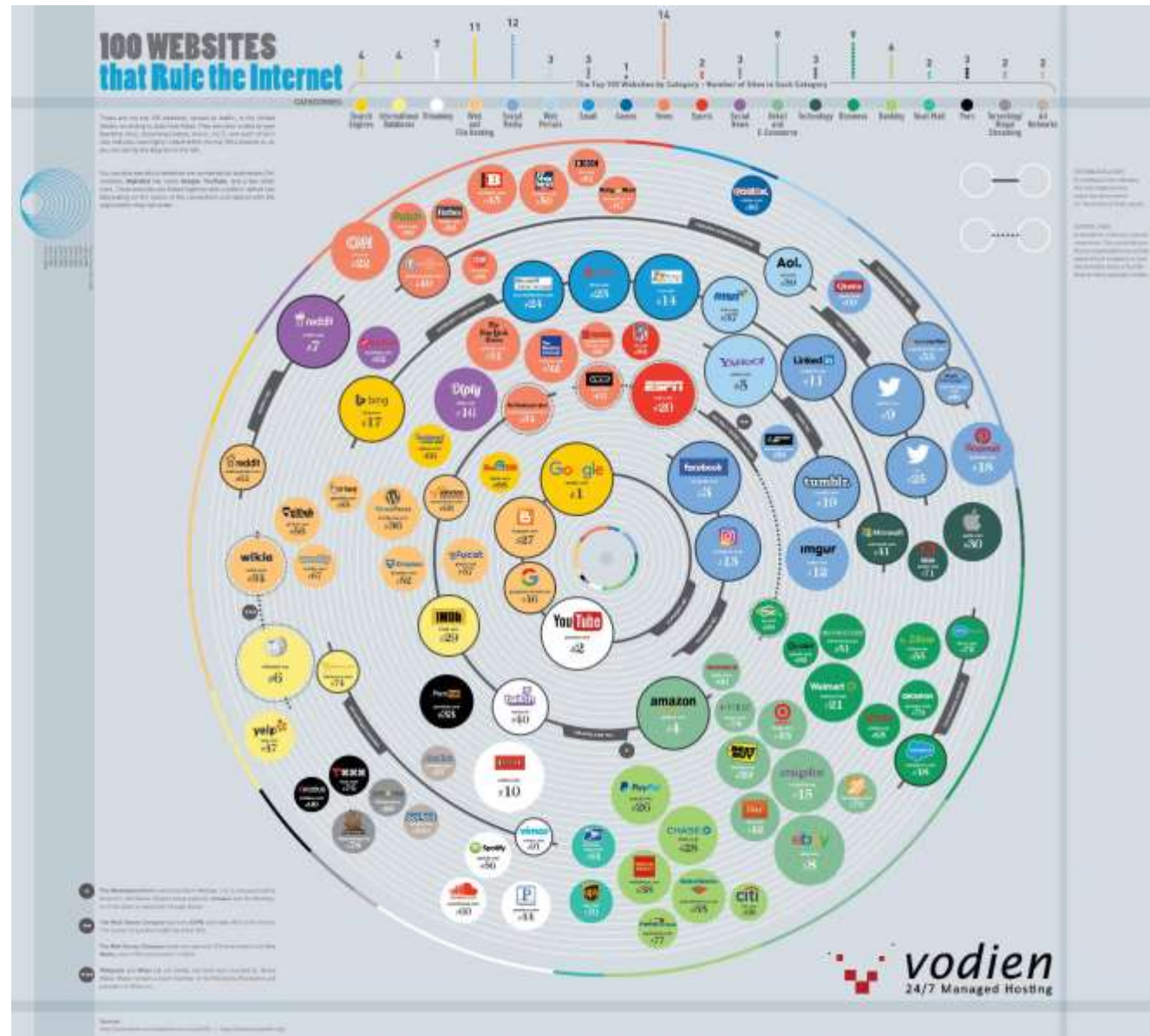
**SOURCES:** KEPCOS (APR 2021) BASED ON EXTRAPOLATIONS OF DATA PUBLISHED BY: THE ITC, LOCAL GOVERNMENT BODIES; GWI, GSMA INTELLIGENCE; EUROSTAT, APJIL, CNNIC; THE UNITED NATIONS. DATA FOR TIME SPENT AND MOBILE INTERNET SHARE FROM: GWI (Q4 2020). SEE [GLOBALWEBINDEX.COM](https://www.globalwebindex.com) FOR MORE DETAILS. **COMPARABILITY ADVISORY:** SOURCE AND BASE CHANGES. INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS. FIGURES ARE **NOT COMPARABLE** WITH DATA PUBLISHED IN PREVIOUS REPORTS.

we  
are  
social

Hootsuite

Slater Technologies

# The 100 Biggest Websites on the Internet



**vodien**  
24/7 Managed Hosting

**Slater Technologies**

# How People Use the Internet

Internet users say they spend about 6.5 hours a day online. What do they do there?

## They have fun:

Netflix has **125m** subscribers, **NETFLIX** about 55% of whom are international.

2018 data

About **1m** people **twitch** are always watching Twitch.



## They send information and updates to friends and colleagues:



**269bn** emails are sent and received each day.

## They run errands:



According to one survey **42%** of global respondents say they paid a bill using their mobile device.

## They pursue education:



Online education is worth **\$165bn** and is projected to reach **\$275bn** by 2022.

## They keep in touch with old friends and make new ones:



**2.2bn** people are monthly active users on Facebook.

Source: Business Insider; Global Web Index; Nielsen; Recode; Reuters; Statista

World101

Slater Technologies

# ***CYBERSECURITY***



**ACFTI**

*Slater Technologies*

# SECURITY – WHAT IS IT EXACTLY?

# What Is Security?

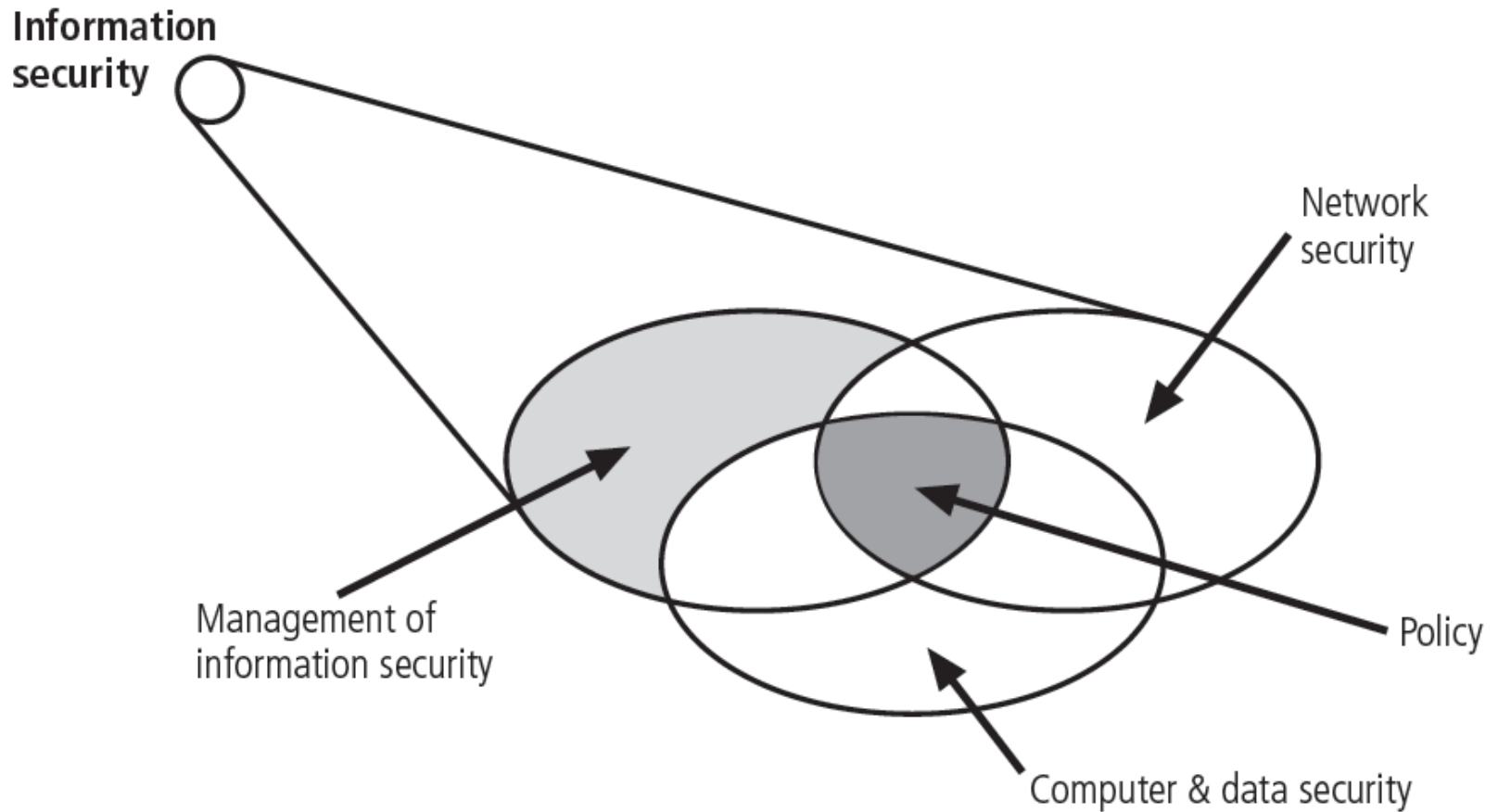
- Definitions
  - Security is defined as “the quality or state of being secure—to be free from danger”
  - Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another
- Specialized areas of security
  - Physical security, operations security, communications security, and network security



# What Is Security? (cont'd.)

- Information security
  - The protection of information and its critical elements (confidentiality, integrity and availability), including the systems and hardware that use, store, and transmit that information
    - Through the application of policy, technology, and training and awareness programs
- Policy, training and awareness programs and technology are vital concepts

# CNSS Security Model



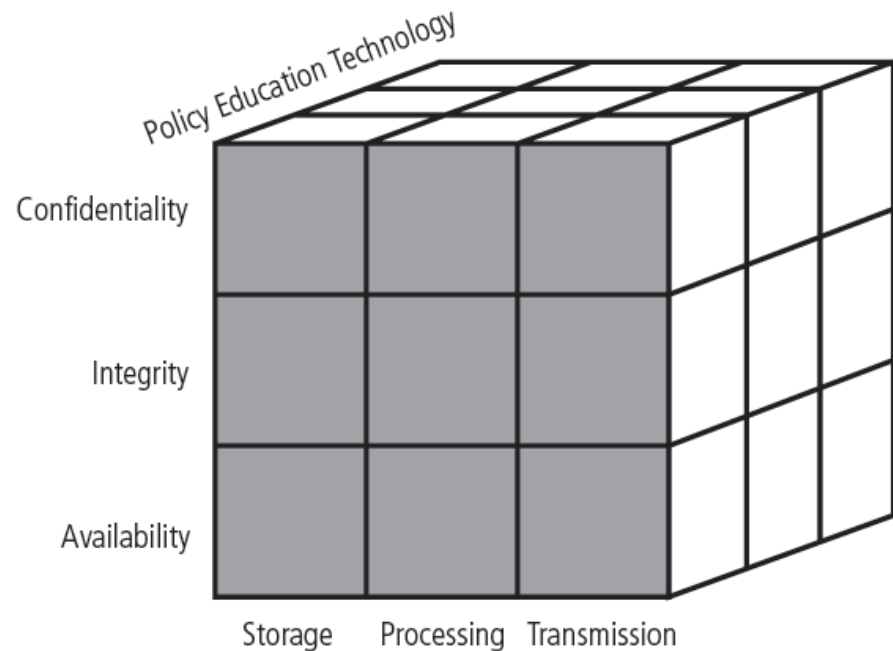
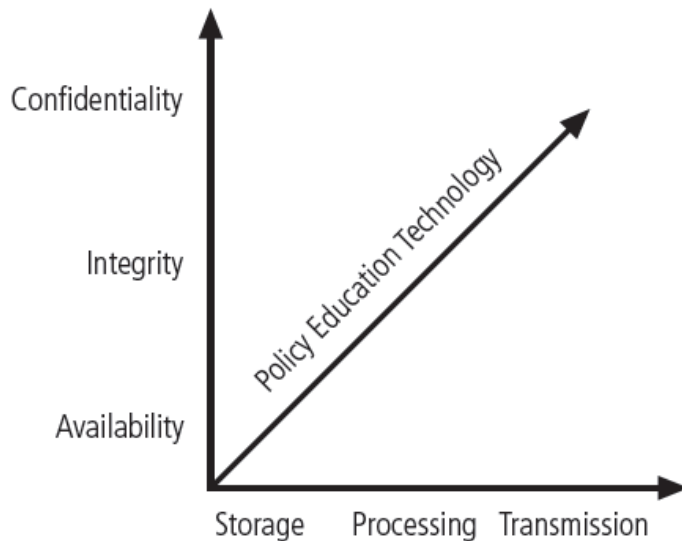
# CNSS Security Model (cont'd.)

- C.I.A. triangle
  - Confidentiality, integrity, and availability
  - Has expanded into a more comprehensive list of critical characteristics of information
- NSTISSC (CNSS) Security Model
  - Also known as the McCumber Cube
  - Provides a more detailed perspective on security
  - Covers the three dimensions of information security

# CNSS Security Model (cont'd.)

- NSTISSC Security Model (cont'd.)
  - Omits discussion of detailed guidelines and policies that direct the implementation of controls
  - Weakness of this model emerges if viewed from a single perspective
    - Need to include all three communities of interest

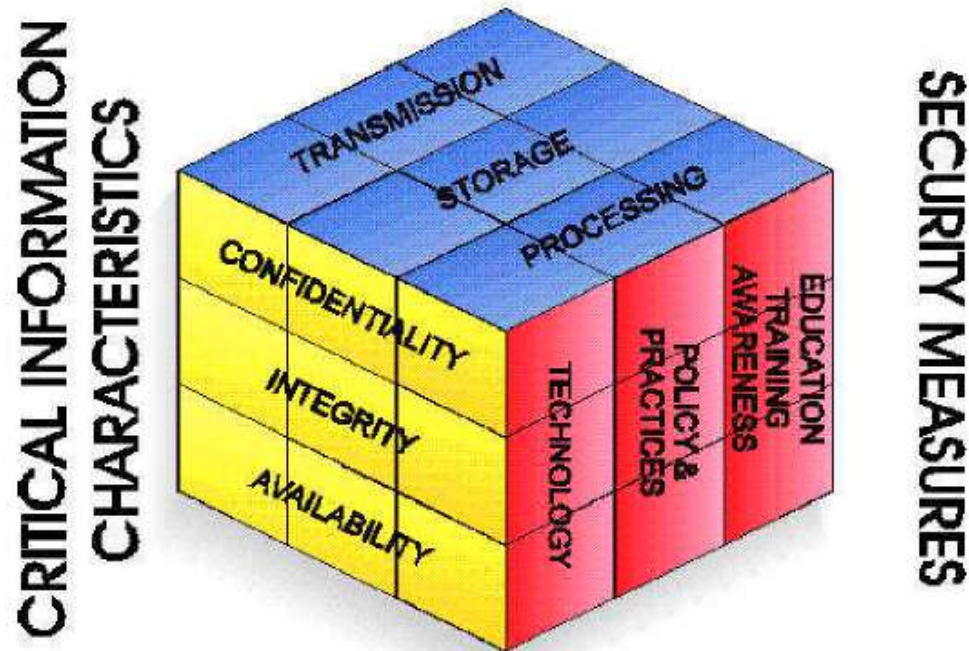
# CNSS Security Model (cont'd.)



# McCumber Cube Security Model

## McCumber Cube Model

Information States



# Key Concepts of Information Security

- Confidentiality
  - The characteristic of information whereby only those with sufficient privileges may access certain information
- Measures used to protect confidentiality
  - Information classification
  - Secure document storage
  - Application of general security policies
  - Education of information custodians and end users

# Key Concepts of Information Security (cont'd.)

- Integrity
  - The quality or state of being whole, complete, and uncorrupted
- Information integrity is threatened
  - If exposed to corruption, damage, destruction, or other disruption of its authentic state
- Corruption can occur while information is being compiled, stored, or transmitted



# Key Concepts of Information Security (cont'd.)

- Availability
  - The characteristic of information that enables user access to information in a required format, without interference or obstruction
  - A user in this definition may be either a person or another computer system
  - Availability does not imply that the information is accessible to any user
    - Implies availability to authorized users

# Key Concepts of Information Security (cont'd.)

- Privacy
  - Information collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected
  - Privacy as a characteristic of information does not signify freedom from observation
    - Means that information will be used only in ways known to the person providing it

# Key Concepts of Information Security (cont'd.)

- Identification
  - An information system possesses the characteristic of identification when it is able to recognize individual users
  - Identification and authentication are essential to establishing the level of access or authorization that an individual is granted
- Authentication
  - Occurs when a control proves that a user possesses the identity that he or she claims

# Key Concepts of Information Security (cont'd.)

- Authorization
  - Assures that the user has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset
  - User may be a person or a computer
  - Authorization occurs after authentication

# Key Concepts of Information Security (cont'd.)

- **Accountability**
  - Exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process

# Parkerian Hexad

- Confidentiality
- Integrity
- Availability
- Control
- Authenticity
- Utility



Elements of Information Security Management  
© simplicable.com



**Donn B. Parker**  
1929 - 2021

# What's Wrong with Information Security and How to Fix It

- Video Lecture by Donn B. Parker
  - <http://www.youtube.com/watch?v=RW9hOBCSy0g>



**Donn B. Parker**  
1929 - 2021

# *CYBERLAW AND EXAMPLES OF LAWBREAKERS*



ACFTI

Slater Technologies



# ***CYBERCRIME***



What's in an internet minute? According to data from RiskIQ and threat researchers around the world, a lot of evil.

## 2018 COST OF CYBER CRIME

### TOTAL COST

📌 **\$600 BILLION**<sup>1</sup>

🕒 **\$1,138,888/minute**

📌 **\$171,233/minute** spend by business on information security<sup>2</sup>

🌐 Globally, for large businesses affected, the average cost was **\$11.7 MILLION/year**<sup>3</sup>

📌 Ranging from **\$222/minute**

### CYBERCRIME VICTIMS

📌 **2.7 MILLION/day**<sup>4</sup>

🕒 **1,861/minute**



### RANSOMWARE

costs to organizations

📌 **\$8 BILLION/year**<sup>5</sup>

🕒 **\$15,221/minute**<sup>5</sup>

🕒 **1.5 organizations/minute** fall victim to ransomware attacks<sup>6</sup>

### MALWARE

🕒 **1,274 new malware variants/minute**<sup>7</sup>

### PHISHING EMAILS

🕒 **22.9 attacks/minute**<sup>8</sup>

### RECORDS LEAKED

from publicly disclosed incidents

📌 **2.9 BILLION/year**<sup>9</sup>

🕒 **5,518/minute**

## 2018 RISKIQ RESEARCH NUMBERS:

### NUMBER OF NEW BLACKLISTED MOBILE APPS

🕒 **.17/minute**<sup>10</sup>



### NUMBER OF NEW PHISHING DOMAINS STOOD UP

🕒 **.21/minute**<sup>11</sup>



### NUMBER OF MALVERTISING INCIDENTS

🕒 **9.2/minute**<sup>12</sup> (Q4 2017)

### INCIDENTS OF MAGECART

🕒 **.07/minute**<sup>13</sup>



### NUMBER OF NEW HOSTS RUNNING CRYPTO MINING MALWARE

🕒 **.05/minute**<sup>14</sup>



### NUMBER OF NEW SITES RUNNING COINHIVE

🕒 **.1/minute**<sup>15</sup> (crypto mining report)



### NUMBER OF POTENTIALLY VULNERABLE WEB COMPONENTS DISCOVERED

🕒 **4/minute**<sup>16</sup> (anatomy of an attack surface report)



Slater Technologies

# In 2021, Cybercrime Exceeded \$6 Trillion in Damages

## Global Cybercrime Damage Costs:

- **\$6 Trillion USD a Year.** \*
- **\$500 Billion a Month.**
- **\$115.4 Billion a Week.**
- **\$16.4 Billion a Day.**
- **\$684.9 Million an Hour.**
- **\$11.4 Million a Minute.**
- **\$190,000 a Second.**



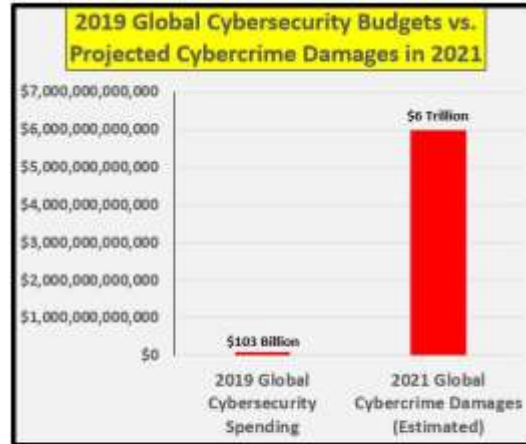
ALL FIGURES ARE  
PREDICTED BY 2021

\* SOURCE: CYBERSECURITY VENTURES



*Slater Technologies*

# 2019 Global Cybersecurity Budget vs. Projected Cybercrime in 2021



Sources:  
2017 Cybercrime Report by the Herjave Group - <https://www.herjavegroup.com/resources/the-2017-cybercrime-report/>  
ZDNet - <https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-ids/>

Graphics:  
William Favre Slater, III  
slater@billslater.com  
Copyright 2019



# 2019 Annual GDPs By Country

## Country GDPs, by Size

Today's visualization comes to us from HowMuch.net, and it charts the most recent composition of the global economic landscape.

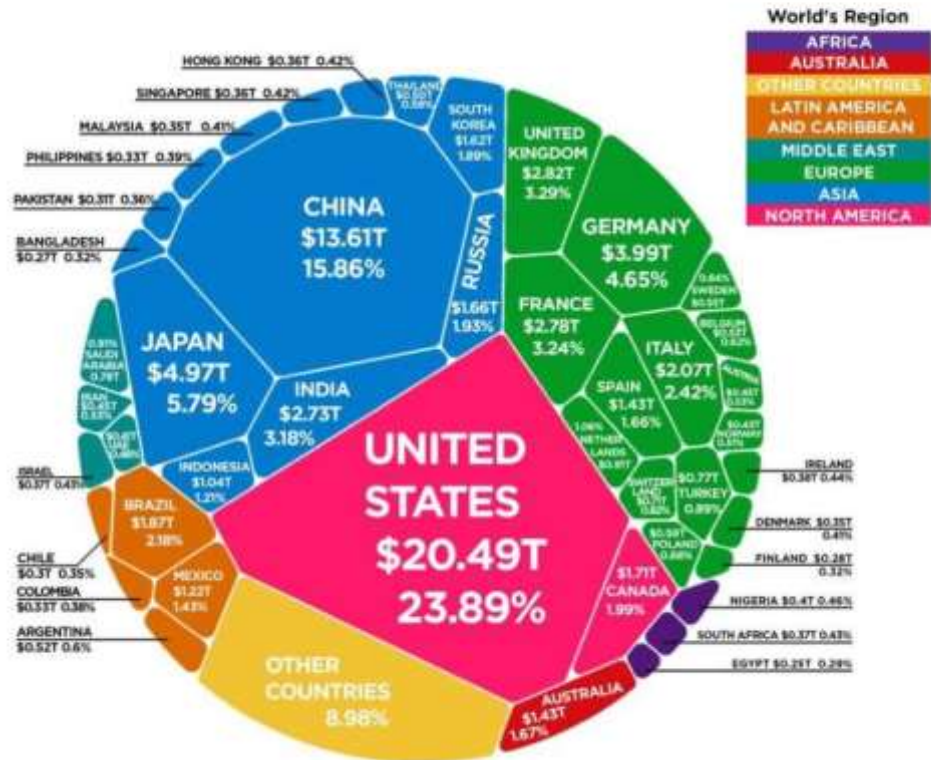
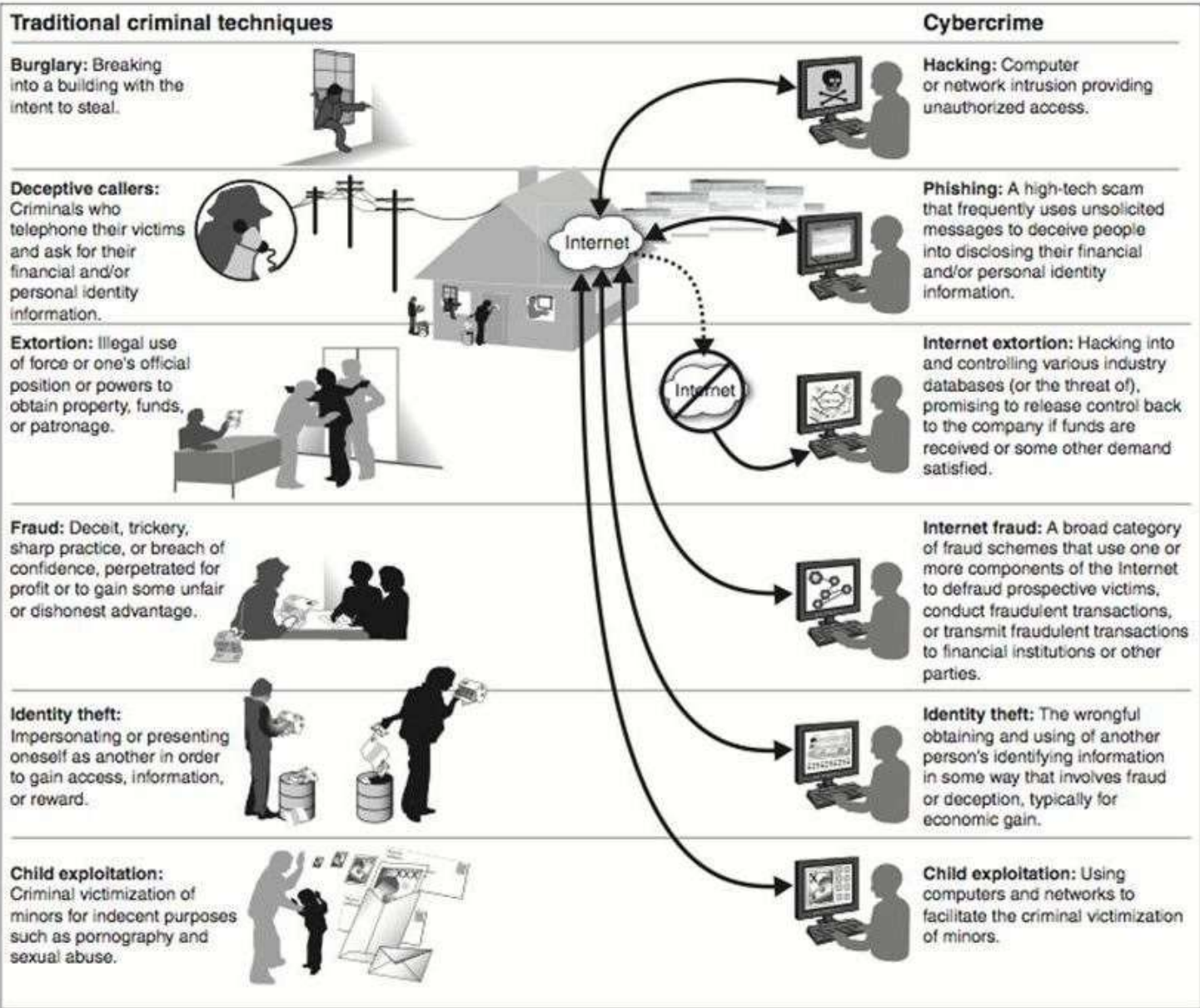


Figure 1: Comparison between Traditional Criminal Techniques and Cybercrime

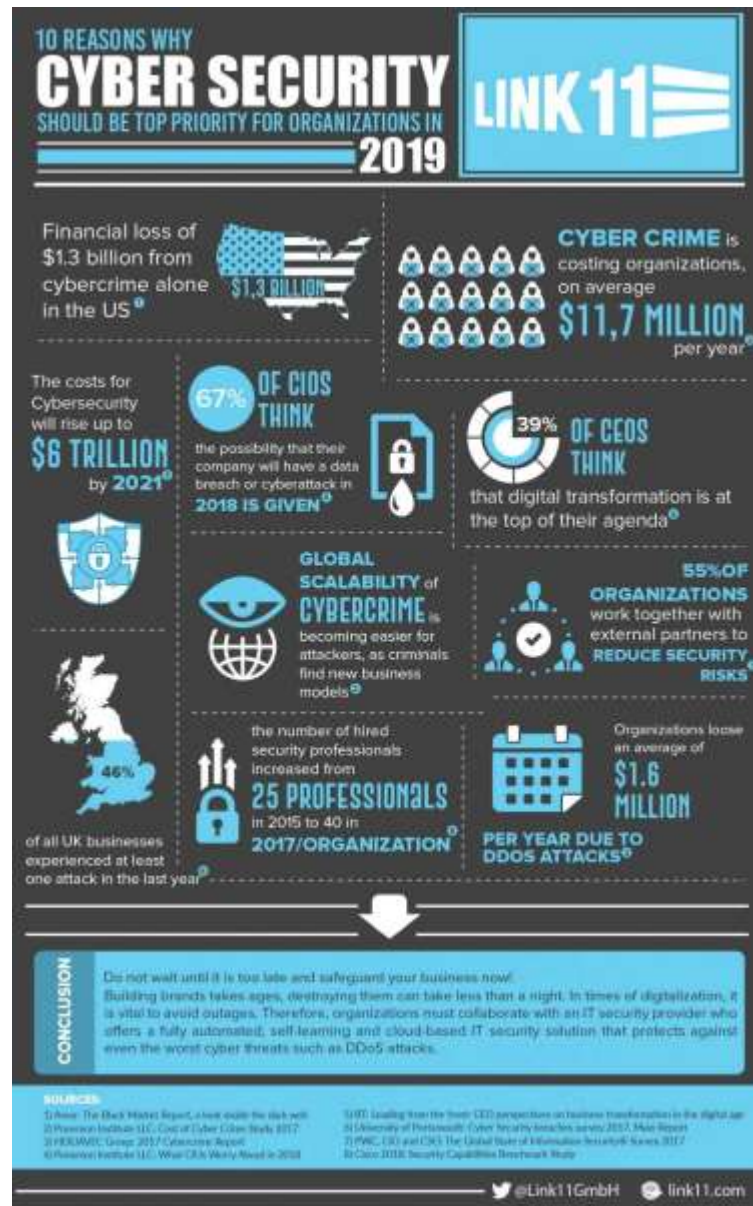


Source: GAO.

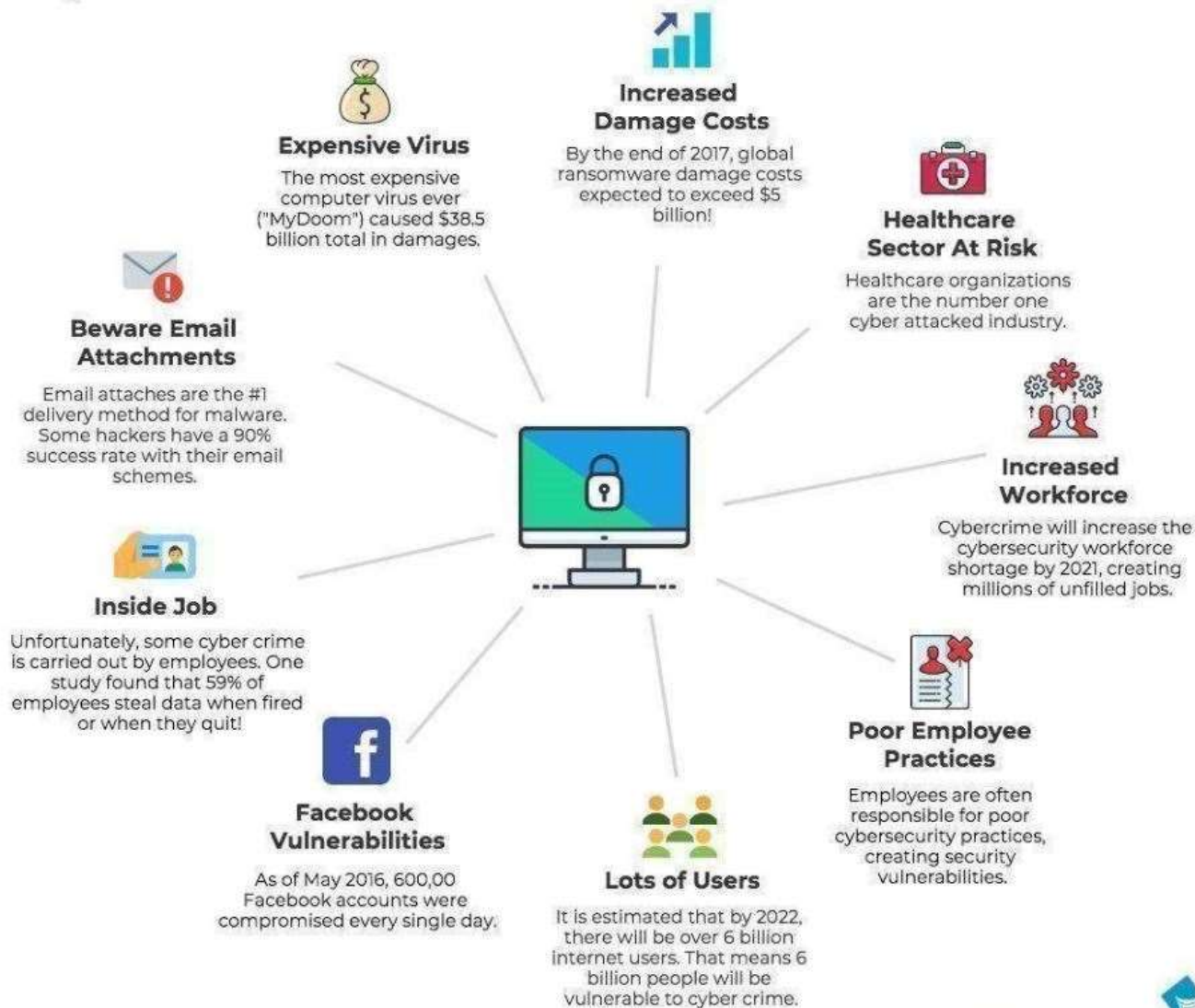
# Comparing Traditional Crime and Cybercrime



# 10 Reasons Why Cybersecurity Should Be Your Top Priority in 2019



# Cybercrime Facts & Stats



**Sources:**  
<http://www.blue-pencil.ca/top-12-cyber-crime-facts-and-statistics/>  
<https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html>  
<https://www.darkreading.com/endpoint/5-reasons-cybercriminals-target-healthcare/d/d-id/1325210?>  
<https://www.optus.com.au/enterprise/accelerate/security/10-sobering-facts-and-stats-about-cyber-crime>  
<https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/>



# Cybercrime Facts & Statistics





# 2018 Cybercriminal Shopping List



## 2018 CYBERCRIMINAL SHOPPING LIST

Recent mass data breaches have created an abundance of verified credentials for sale across the dark market.

What is your identity worth? See what cybercriminals are willing to pay for access to a variety of consumer accounts.



# 6 Ways Cybercriminal Get Your Information

United States  
**{CYBERSECURITY}**  
Magazine  
A Multi-Platform Publishing Portal

## 6 WAYS CYBER-CRIMINALS GET YOUR INFORMATION

### BACKDOOR

Any secret method of bypassing normal authentication or security controls. Backdoors are common, often added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons;

### DENIAL-OF-SERVICE ATTACKS

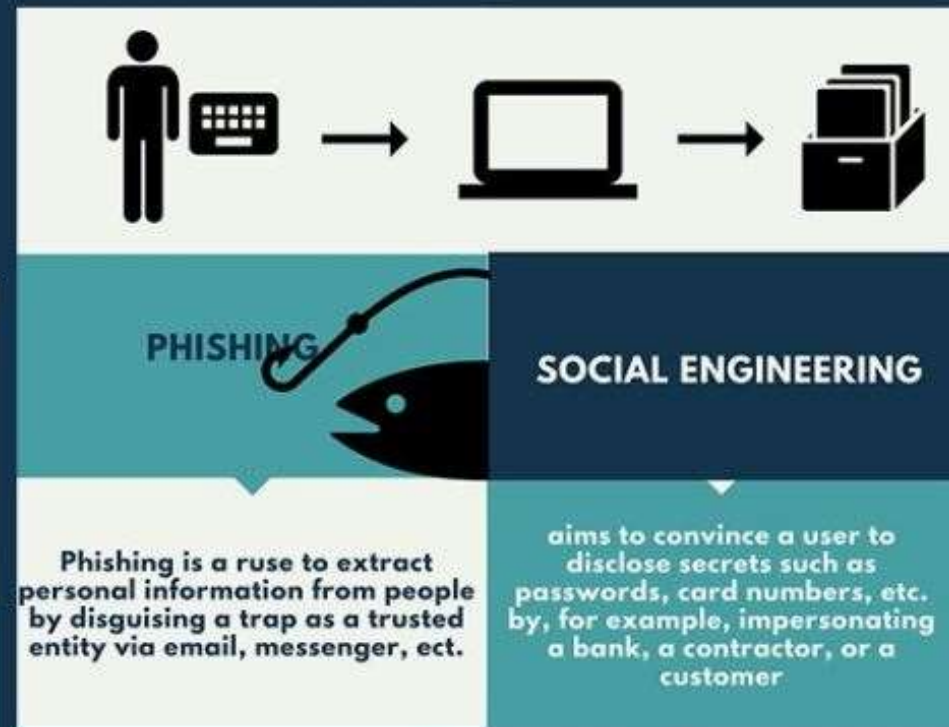
make a machine or network resource unavailable to its intended users

### DIRECT-ACCESS ATTACKS

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice

### SPOOFING

An attempt to use false data to pose as someone else, with the goal of gaining access to restricted information and data



Phishing is a ruse to extract personal information from people by disguising a trap as a trusted entity via email, messenger, ect.

aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer

[www.uscybersecurity.net](http://www.uscybersecurity.net)

Slater Technologies

Most small business owners  
have been cyber victims

HELP



Computer virus

**44%**



Phishing

**30%**



Trojan horses

**22%**



Hacking

**16%**



Data breach

**11%**



Issues due to  
unpatched software

**10%**



Unauthorized access  
to customer info

**9%**



Unauthorized access  
to company info

**8%**

Most Small  
Businesses Have  
Been Cybercrime  
Victims

Source: The 2015 Small Business Owner Study commissioned  
by Nationwide and conducted by Harris Poll Online.



Slater Technologies

# Numbers of Cybercrime Victims

2

THEME 1: SHOCKING SCALE: NUMBER OF VICTIMS



SHOCKING SCALE: NUMBER OF VICTIMS

## 1 MILLION+ VICTIMS A DAY

EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES



50,000

VICTIMS EVERY HOUR



820

VICTIMS EVERY MINUTE



14

VICTIMS EVERY SECOND



7/10

69%

69% of adults have experienced cybercrime in their lifetime. Compared to the 2010 survey, there has been a 3% rise in overall cybercrime



65%

Among all cybercrime victims surveyed, nearly two thirds have fallen prey in the past 12 months alone - a total of 431m adults in 24 countries

589 MILLION

Cybercrime has affected 589m people in just 24 countries - equivalent to 9% of the entire population of the world



## 431 MILLION

The total number of cybercrime victims in the past 12 months is greater than the entire populations of USA & Canada (347m) or Western Europe (400m)

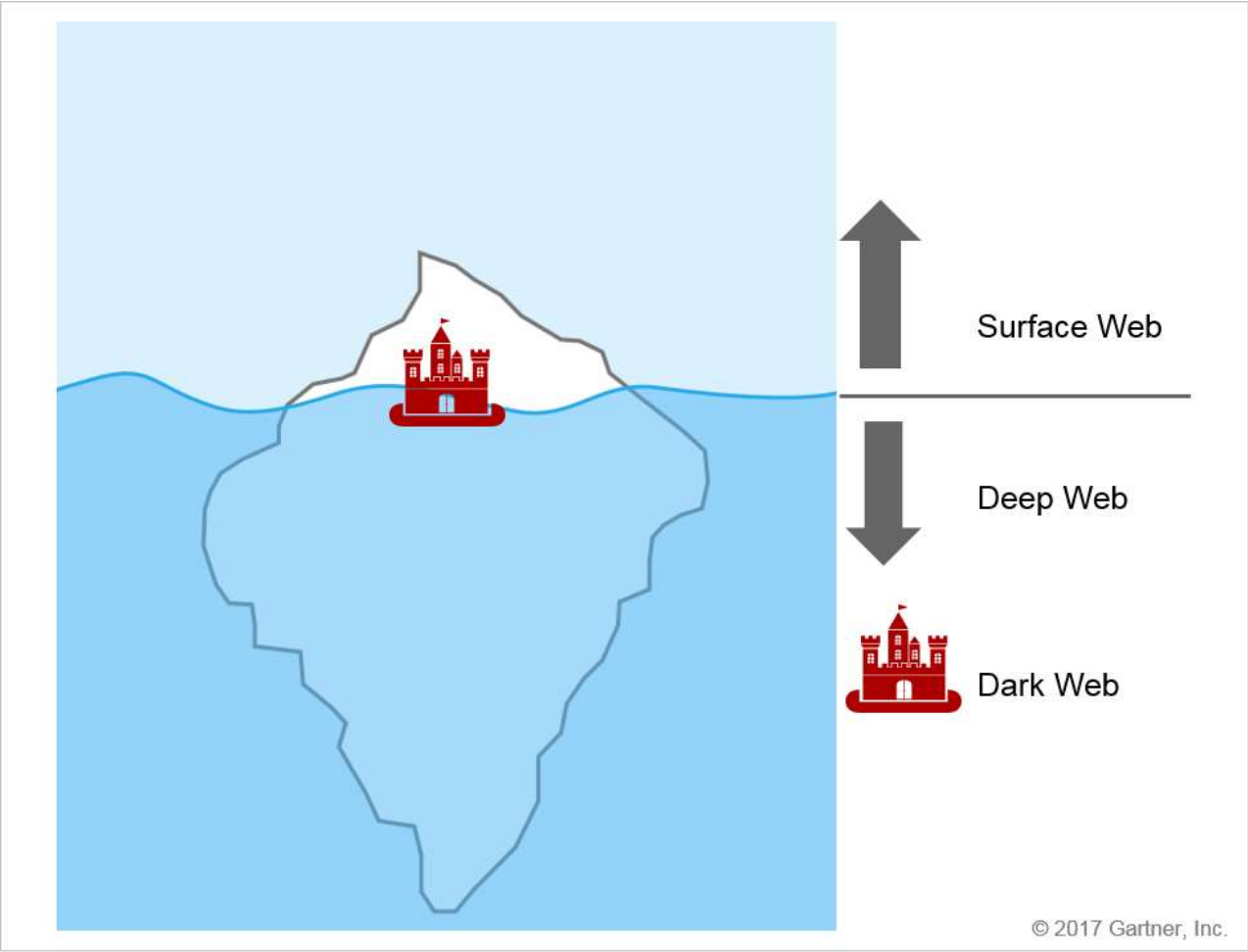
Slater Technologies

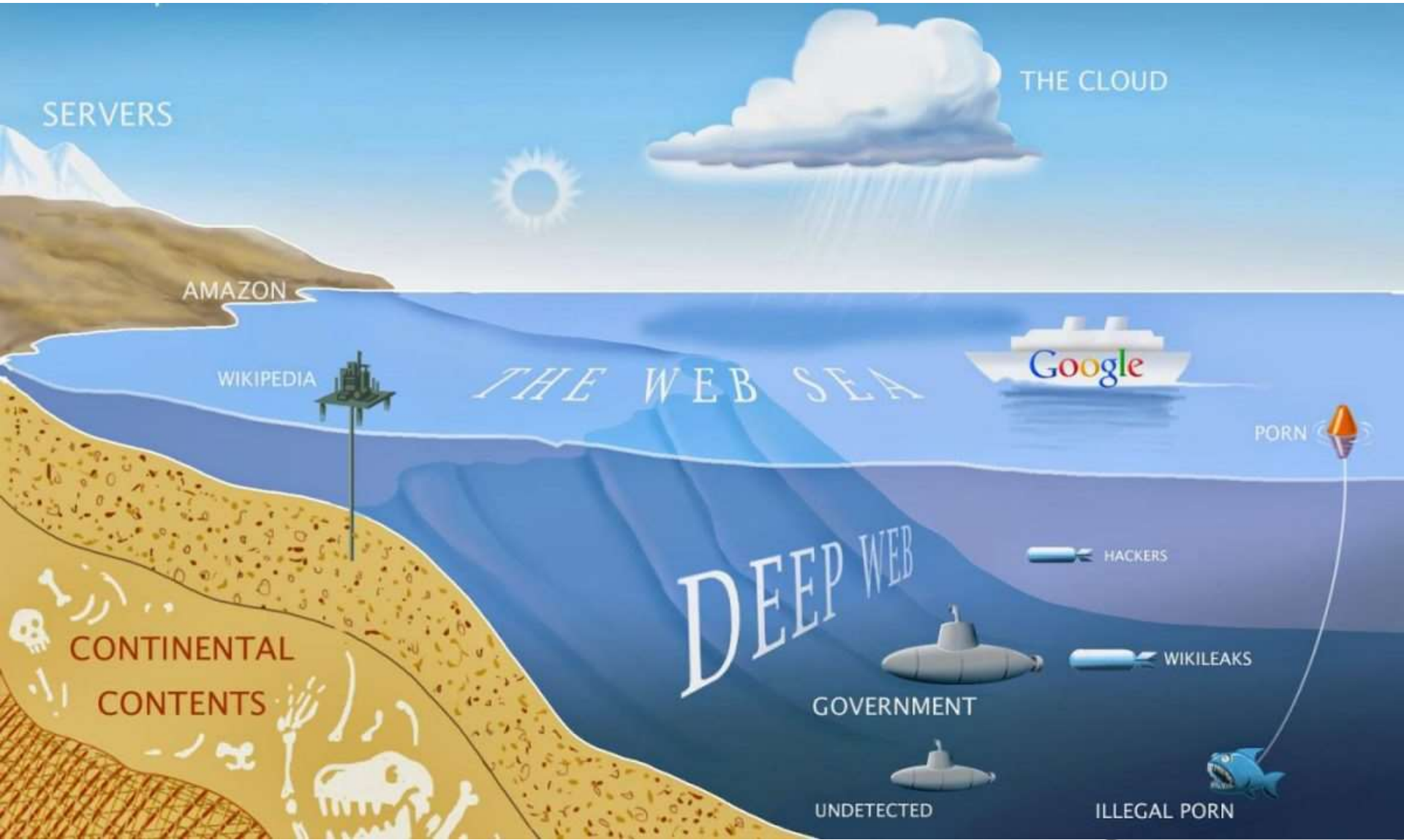


# The Dark Web

Slater Technologies

# The Deep Web Vs. The Dark Web





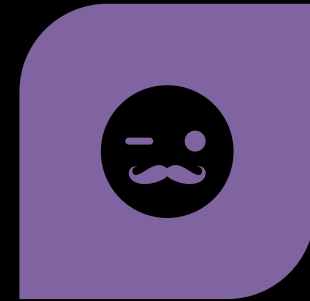
# The Deep Web Vs. The Dark Web



THE DEEP WEB AND THE DARK WEB ARE NOT THE SAME THING.



THE DEEP WEB HAS HARD-TO-FIND DATA AND INFORMATION THAT IS EITHER NOT NORMALLY INDEXED BY THE SEARCH ENGINES LIKE GOOGLE, BING, AND YAHOO, OR IT IS JUST VERY DIFFICULT TO FIND.



THE DARK WEB IS USUALLY FOR CYBERCRIMINALS AND SICK PEOPLE WANT TO DO BAD THINGS.



# THE DARKNET: The Underground for the Underground

## ACTORS

Those who lurk beyond the shadows of the Darknet



## CRYPTOCURRENCY

Greasing the wheels of the Darknet



## HOW TO ACCESS THE DARKNET

- Anonymity** — Download Tor for your operating system: <https://www.torproject.org/projects/torbrowser.html>
- Enhanced Anonymity** — Some systems can give away bits of information that can impact the effectiveness of Tor. To address this use The Anonymizer Incognito Live System (SALS) available here: <https://tails.boum.org/>
- Contribute back to Tor project by becoming a Relay** <https://www.torproject.org/docs/tor-doc-relay.html.en>
- Choose "Directory Site" or access point:**
  - Bat Blue Site (<http://batblue45678901.com/>)
  - Hidden Wiki (<http://www.hidden.wiki/>)
  - DuckDuckGo (<http://3g2upl4qq6k8c2o1m.com/>)

## ANONYMITY RULE OF THUMB

- Use Tor browser:
  - Use a seed/cyber browser exclusively for Tor to avoid unwanted identity leaks.
- Do NOT install browser plugins for Tor Browser
- Disable all ability to run scripts on Tor Browser
- Use HTTPS-where it exists
- Do NOT run executables or open documents while online
  - Most Open files in a separate virtual machine with networking disabled
- Disable your application downloaded by Tor (i.e. BitTorrent)
- Use Tor Bridge Relay: <https://www.torproject.org/docs/bridge.html>

Download the full report on the Darknet at [www.batblue.com/the-darknet](http://www.batblue.com/the-darknet)

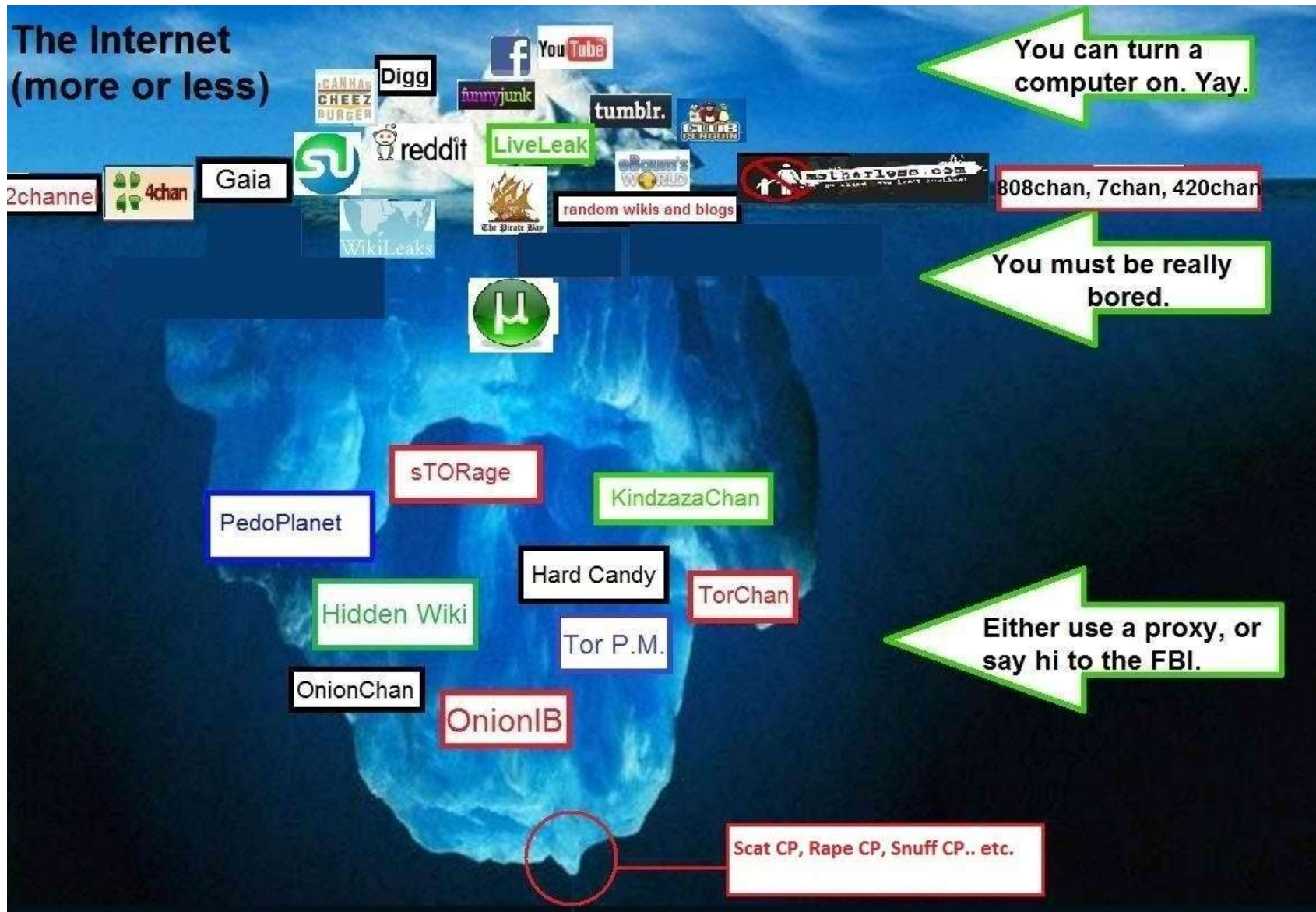


[www.batblue.com](http://www.batblue.com)

Technologies

The Dark Web

# The Internet (more or less)



# The Dark Web



It's an *evil place*



The domain of the *cybercriminal*



*Everything is for sale*, especially your sensitive data



*Software Exploit* kits are for sale for Cyber attacks



Appeals to people with *sick minds*



Requires a *Tor Browser*



*Cryptocurrency* is the coin of the realm

# The Dark Web Example – Silk Road

The screenshot shows the Silk Road anonymous market website. The browser address bar displays `silkroad-b5p3icr.onion.to/index.php/silkroad`. The page header includes the Silk Road logo (a camel), the text "Silk Road anonymous market", and navigation links for "messages 1", "orders 0", and "account \$0.00". A search bar is present with a "Go" button. The user is logged in as "the Dread Pirate Roberts" with a "logout" link. A "Shop by Category" sidebar lists various product categories with item counts. The main content area features a grid of product listings, each with an image, a name, and a price. A "News" sidebar on the right contains several article titles. A Walmart logo is visible at the bottom of the product grid.

**Silk Road**  
anonymous market

messages 1 | orders 0 | account \$0.00

Search  Go

Hi, **the Dread Pirate Roberts**

logout

Shop by Category

- Drugs 5,779
  - Cannabis 1,426
  - Dissociatives 122
  - Ecstasy 454
  - Opioids 379
  - Other 225
  - Precursors 22
  - Prescription 1,318
  - Psychedelics 875
  - Stimulants 653
- Apparel 114
- Art 9
- Books 998
- Collectibles 5
- Computer equipment 57
- Custom Orders 58
- Digital goods 414
- Drug paraphernalia 128
- Electronics 78
- Erotica 394
- Fireworks 12
- Food 5
- Forgeries 93
- Hardware 6
- Herbs & Supplements 4

 4-HO-MET 250mg \$3.58	 Valium - Diazepam from Cipla - 10mg - 10 tablets \$1.89	 10 x Amphetamine Salt 30MG TAB (Adderall) 30MG \$10.37	 Ps. Cubensis Cambodian Isolate 10cc Syringe \$2.76
 Sample Offer of 1gr labtested 84% MDMA \$3.54	 1/8oz (3.5g) Lemon Diesel \$5.68	 .5 Gram Meth - DCN Priority Shipping - FAST!! \$8.13	 Oxycontin 60MG X 5 \$15.42

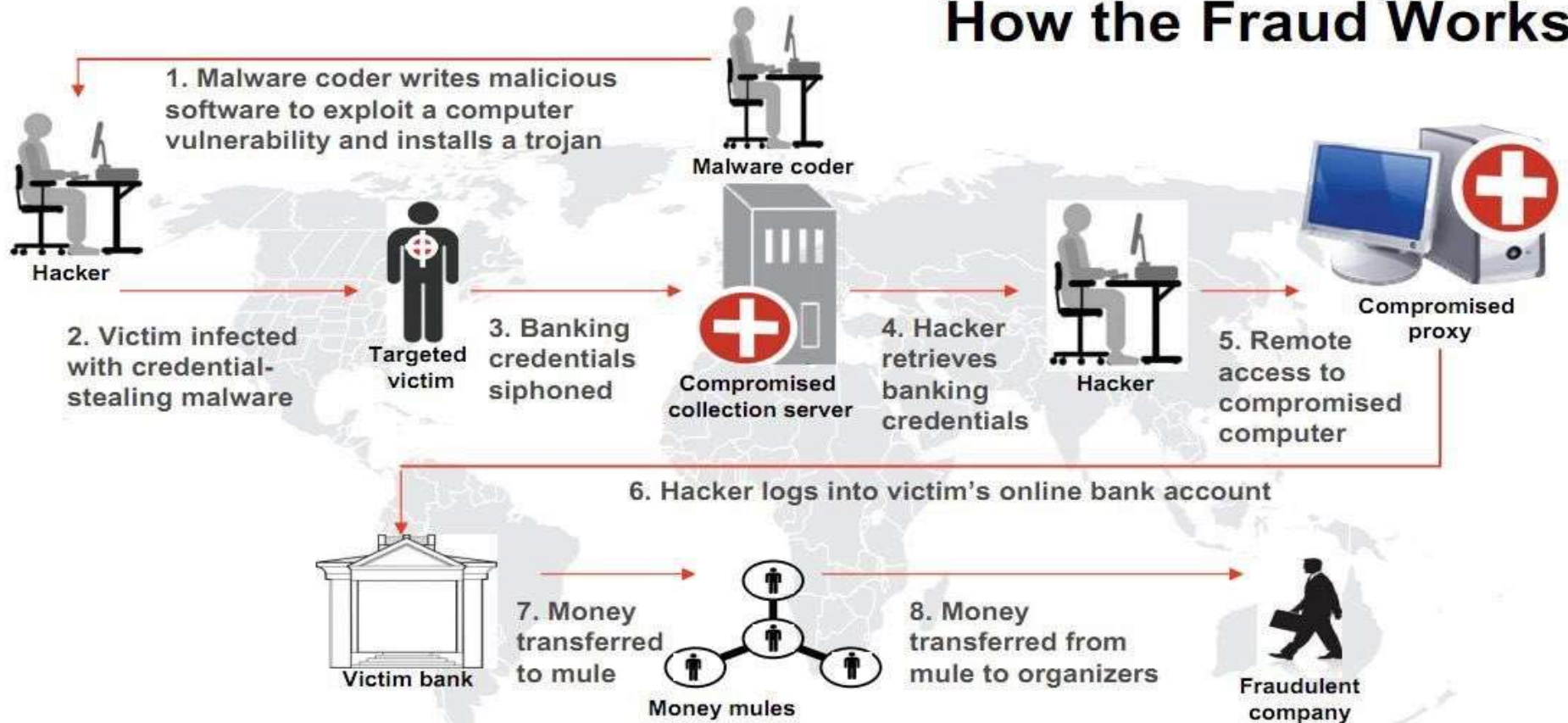
News

- Closing the Armory
- A brand new look for Silk Road!
- The gift that keeps on giving
- Who's your favorite?
- Acknowledging Heroes

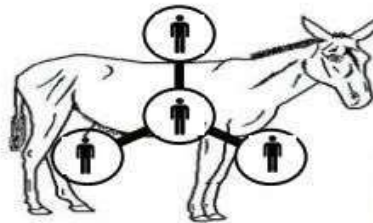
Walmart Save money. Live better.

# Cybercrime Pays Well

## How the Fraud Works



Victims are both financial institutions and owners of infected machines.



Money mules transfer stolen money for criminals, shaving a small percentage for themselves.



Criminals come in many forms:

- Malware coder
- Malware exploiters
- Mule organization

**"You have zero privacy anyway.. Get over it."**

**--Scott McNealy**

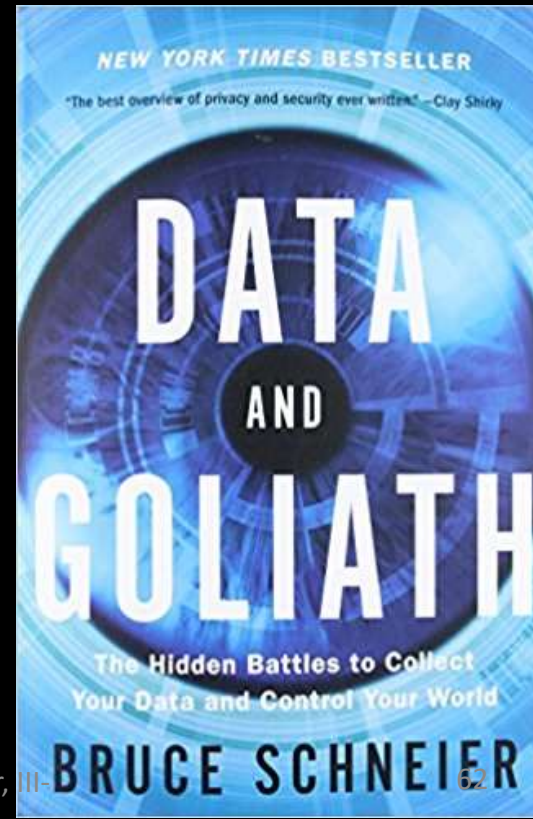
**Former chief executive officer of Sun Microsystems  
1999**

**"If something is free, you're  
not the customer; you're the  
product."**

**Bruce Schneier**

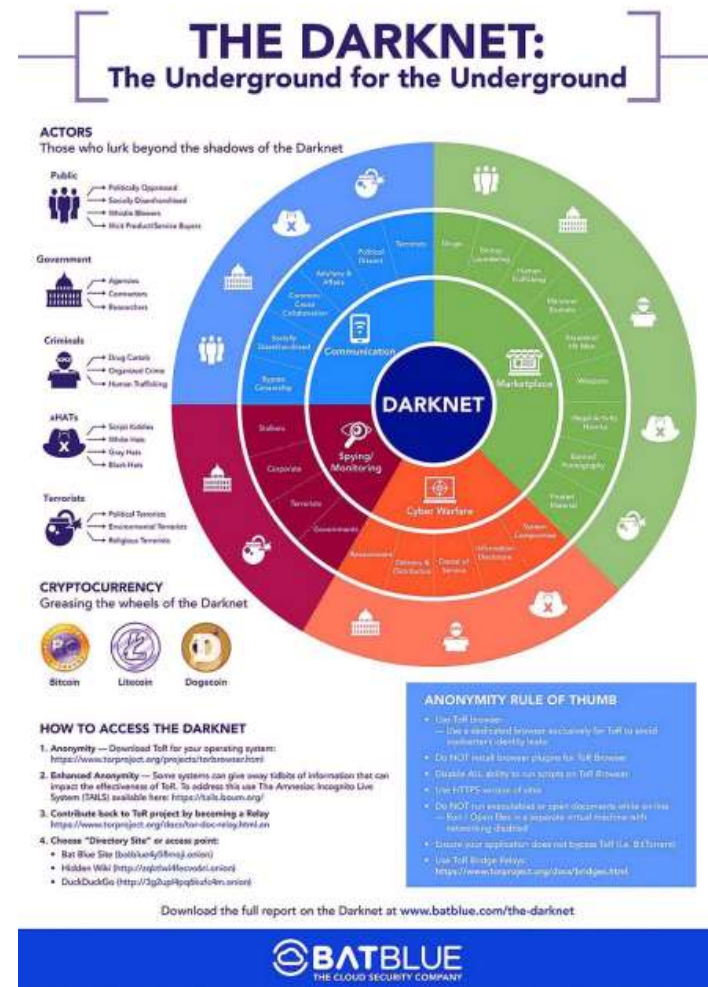
**Cybersecurity Researcher & Author  
2016**

**Data and Goliath: The Hidden Battles  
to Collect Your Data and Control Your  
World**



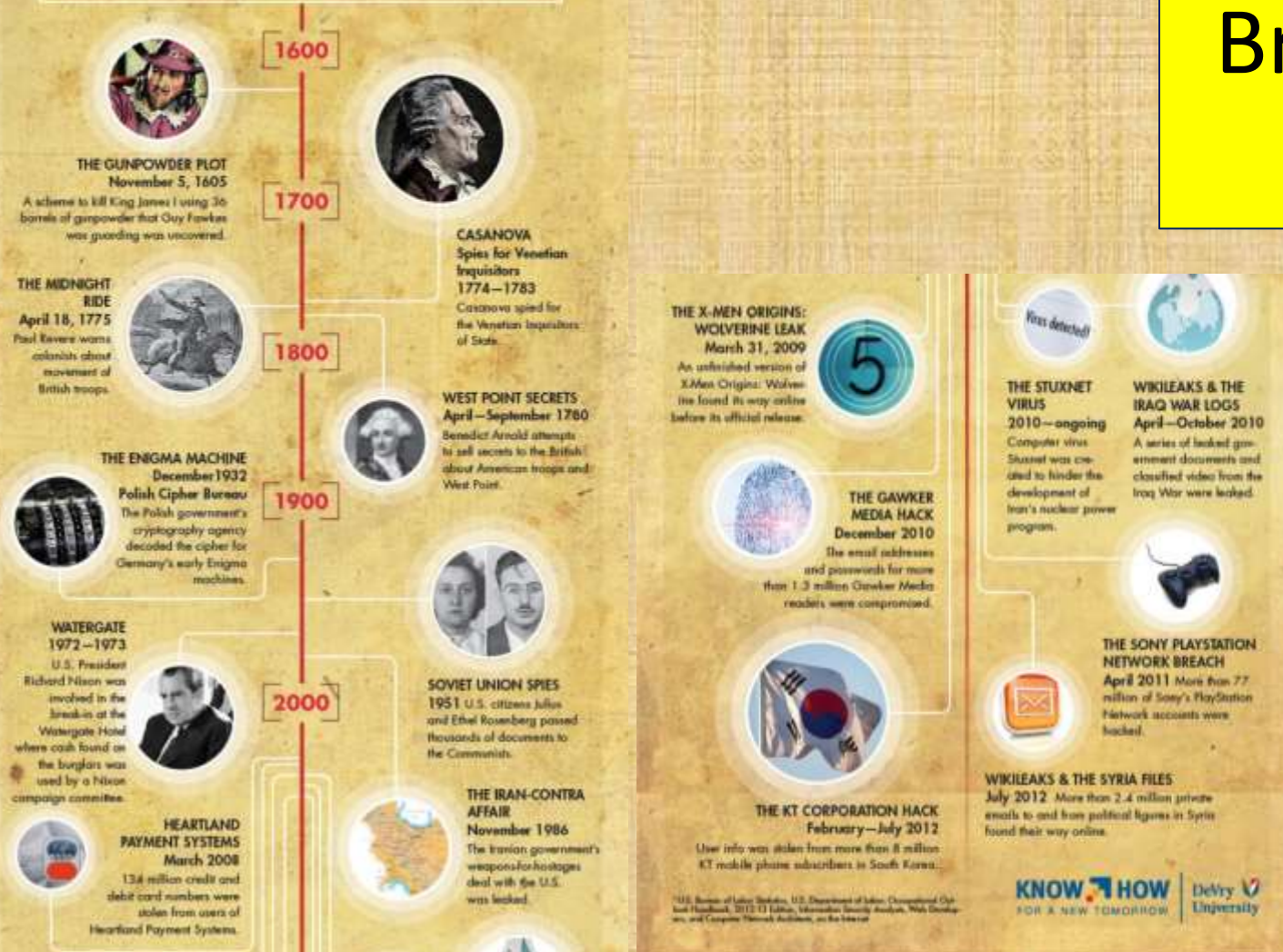
# The Problem

- **“Data Is The New Oil”**
  - In 2006, the top five companies were Oil Companies
  - Since 2015, the top five companies have been Digital Data Companies
- The Internet was not designed to be secure. Security came later.
- Privacy, especially digital privacy, has become increasingly difficult to achieve in the 21<sup>st</sup> Century.
- If we access and use the Internet and Smart Phones, we are unwittingly “leaking data”.
- Companies like Google, Facebook, Twitter, LinkedIn and thousands of others are harvesting (and selling) data about us when we use their services.
- Data brokerage firms such as Acxiom, Epsilon, Lotame, and Spokeo, etc., are buying, processing and categorizing our data and selling to other companies that in turn make decisions as important as hiring and firing of people.
- Thousands of Data Breaches in the last few years, especially with entities like Equifax, Target, Anthem, Home Depot, OPM have exposed our PII at an unprecedented rate.
- Bad actors misuse our data to hack accounts and steal identify, money, etc. and put it out for sale on the Dark Web, where people can buy it.



# A BRIEF HISTORY OF TOP SECURITY BREACHES

Data security has been a concern since the dawn of the spoken word, and breaches throughout history have led to both good and bad results for society. Today, with our information being mostly digital, hacks have become even more common. Employment of information security analysts, web developers and computer network architects is projected to grow 22% from 2010 to 2020<sup>1</sup> — faster than the average for all occupations. So, when did these data breaches begin? Here are some of history's top information breaches.



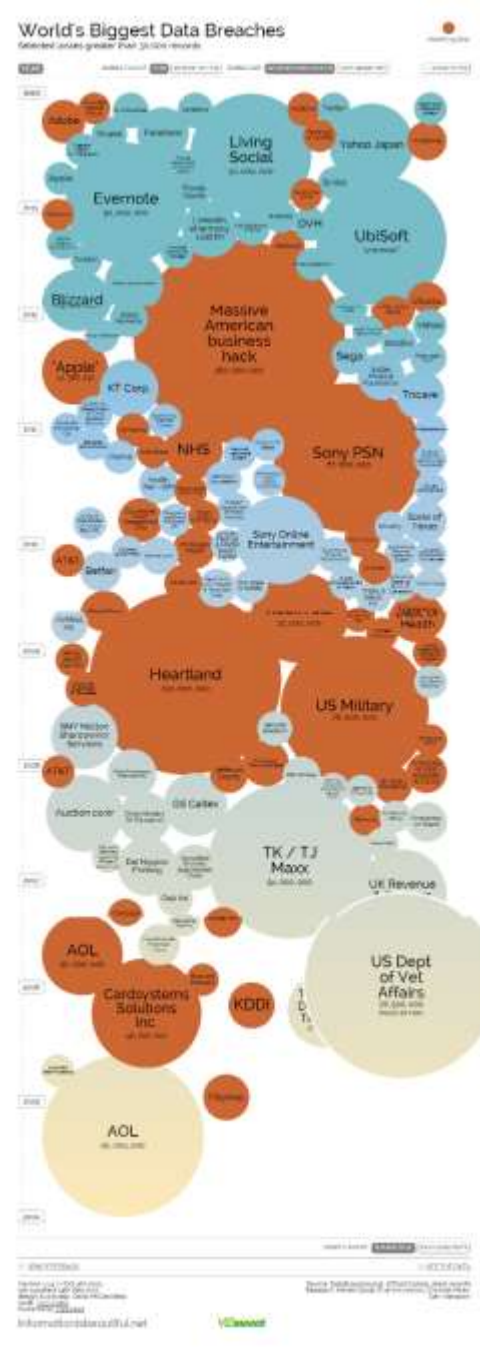
# Historic Security Breaches – Part 1

<sup>1</sup>U.S. Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, 2010 Edition, Information Security Analysts, Web Developers, and Computer Network Architects, at <http://www.bls.gov>

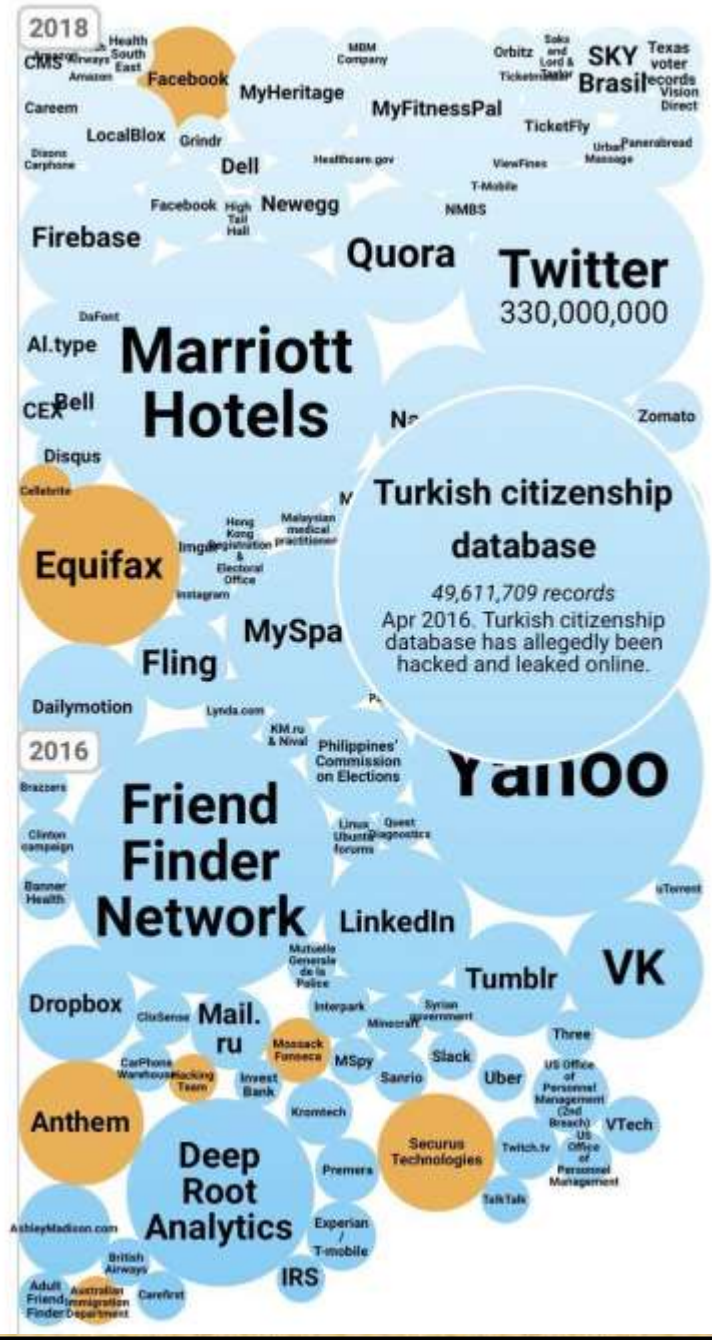




# Historic Security Breaches – Part 2



# Historic Security Breaches – Part 3





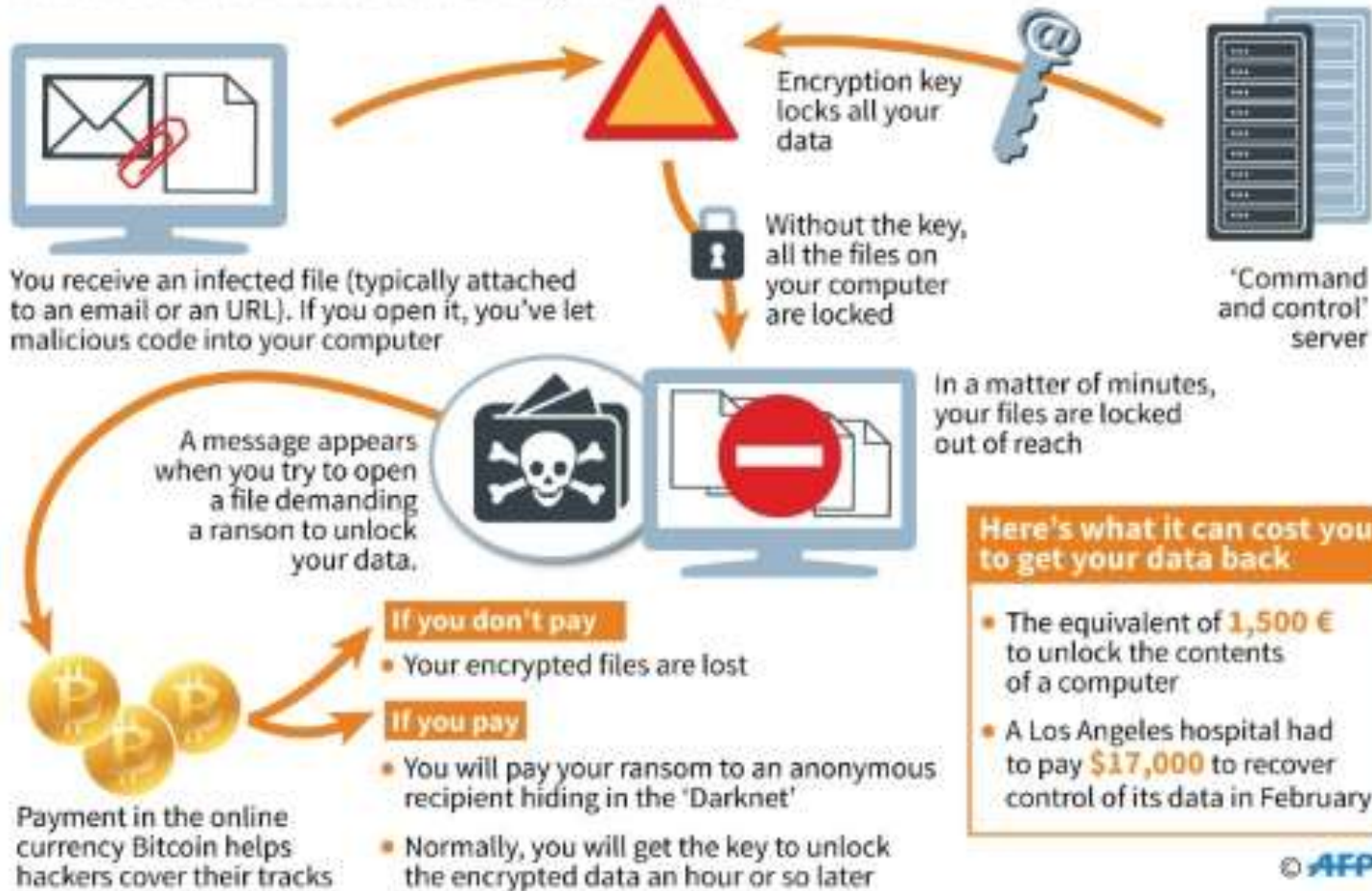
# According to the FBI in 2019

- The Biggest Internet-based Crimes Are:
  1. **Ransomware Attacks**
  2. Business E-Mail Compromise (BEC)
  3. Identity Theft

# According to the FBI in 2019

## Ransomware: how hackers take your data hostage

Malicious code blocks access to the data in your computer



# According to the FBI in 2019



# Business E-Mail Compromise – Most Common Subject Lines Used to Trick Victims

---

The top subject lines according to Barracuda analysis are based around the following key phrases:

1. Request
2. Follow up
3. Urgent/Important
4. Are you available?/Are you at your desk?
5. Payment Status
6. Hello
7. Purchase
8. Invoice Due
9. Re:
10. Direct Deposit
11. Expenses
12. Payroll

# 2018 IDENTITY FRAUD TRENDS

**1** IN 2017, 6.64 PERCENT of consumers became victims of **identity fraud**



An increase of over **one million victims** from the previous year, driven by growth in existing non-card fraud (ENCF) and account takeover (ATO).

**2** ACCOUNT TAKEOVER GREW SIGNIFICANTLY tripling over the past year, reaching a four-year high



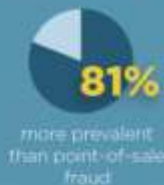
### ATO Victims

Paid an average of **\$290** out-of-pocket and spent **15 hours** on average in resolving fraud.

**3** ONLINE SHOPPING presents the greatest fraud risk



Card-not-present Fraud is now



As EMV restricts fraudsters' ability to commit fraud at physical locations, fraudsters are aggressively targeting online channels.

**4** FRAUDSTERS GETTING MORE SOPHISTICATED using stealthier and more complex monetization schemes



Fraudsters are blurring lines between fraud types, as 1.5 million victims of existing account fraud also had a fraudulent intermediary account opened in their name.

# 2018 Identity Fraud Trends

Slater Technologies

# Identity Theft

## IDENTITY THEFT AND PASSWORD SECURITY



WITH OUR LIVES NOW BECOMING MORE AND MORE INTERTWINED IN THE DIGITAL REALM OF THE INTERNET, HACKERS AND IDENTITY THIEVES ARE FINDING NEW WAYS TO STEAL PERSONAL INFORMATION AND MAKE PEOPLES LIVES A MISERY GET WISE TO THEIR TRICKS AND DON'T BECOME A VICTIM...

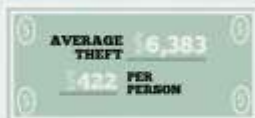
**1. EVERY YEAR IN AMERICA, 9 MILLION PEOPLE FALL VICTIM TO SOME FORM OF IDENTITY THEFT.**

This costs **\$52.6 billion** in damages.

The average theft per victim is **\$6383**.



**AVERAGE OUT OF POCKET EXPENSE FOR VICTIM IS \$422.**



**2. 47% OF IDENTITY THEFTS ARE PERPETRATED BY SOMEONE THE VICTIM KNEW.**



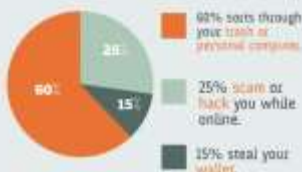
**RATES OF IDENTITY THEFT PER AGE**

People 65+ have the lowest rate at 2.3%.



People 25-34 have the highest rate of identity theft at 5.4%.

**3. THE BREAKDOWN OF HOW THIEVES GET YOUR INFORMATION:**



**A LOOK AT ONLINE IDENTITY THEFT:**

**57 million Americans receive scam emails a year**

19% click on the link inside.  
3% disclose bank and financial information by accident.  
1.7% are then scammed.

**4. RECEIVING BANK STATEMENTS TO YOUR HOME MAKES YOU 8 TIMES MORE LIKELY TO HAVE YOUR INFORMATION STOLEN THAN GOING PAPERLESS.**

**THEFT LIKELINESS 1:8 RATIO**



**THE MOST COMMON WAYS THIEVES USE YOUR INFORMATION:**



**5. A SHORT GUIDE TO PASSWORD SECURITY:**

The top 3 most commonly used passwords in America are...

12345  
123456  
123456789

**6. STATISTICS REVEAL THESE NAMES AND PASSWORDS COVER 26% OF THE POPULATION:**

20% Most Common

YOURSELF  
YOUR PARTNER  
PETS  
CITY YOU LIVE IN  
'GOD'  
'LETTERS'  
'MONEY'  
'LOVE'

**7. 1 IN 5 PEOPLE USE THE WORD 'PASSWORD' AS THEIR PASSWORD FOR ONLINE BANKING.**



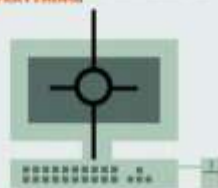
Hackers don't target banks online, but attack online forums and stores that hold your passwords.

**WHY? BECAUSE MOST PEOPLE USE THE SAME PASSWORD FOR EVERYTHING.**

**8. HACKERS CAN CRACK AN 8 CHARACTER PASSWORD IN ALL LOWERCASE WITHIN 2 HOURS.**

Adding one uppercase letter and a symbol makes it take 200 years.

**8 CHARACTER PASSWORD CRACK: 2 HRS**



www.OnlineMBA.com



"I just hacked a billion passwords by guessing 1-2-3-4-5."

Source: <https://brandongaille.com/22-incredible-internet-identity-theft-statistics/>





# Chinese Hacker Espionage Problem Disclosed by Mandiant Report – February 19, 2013

- A new report from Mandiant implicates a unit of the People's Liberation Army of China in the theft of terabytes of data from 141 organizations since 2006.
- URLs:  
[http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)
- <http://www.cyberwarzone.com/resources-mandiant-apt1-chinas-cyber-espionage-units-report>
- <http://www.economist.com/blogs/babbage/2013/02/chinese-cyber-attacks?fsrc=nlw|newe|2-20-2013|5066680|37961765>



The website of the Lanxiang vocational school in Jinan, China, says its 5,000-square-meter No. 5 computer training room has 2,000 personal computers. The computers have been replaced with the latest models.

### ATTACK ORIGINS

#	COUNTRY
2861	United States
2112	China
1045	Mil/Gov
746	Russia
339	France
349	Netherlands
301	Mexico
234	Germany
18	Israel
103	Ukraine

### ATTACK TARGETS

#	COUNTRY
8942	United States
181	Russia
44	Taiwan
20	Mil/Gov
15	Netherlands
4	Poland
2	France
1	Sweden
1	Canada

### LIVE ATTACKS

TIMESTAMP	ATTACKER ORGANIZATION	LOCATION	IP	TARGET LOCATION	TYPE SERVICE	PORT
2015-01-02 06:07:54.07	N/A	unknown, Mil/Gov	107.144.32.243	Saint Louis, United	http	80
2015-01-02 06:07:54.33	Iusace   PCS de Mexico, S.A.	Chihuahua, Mexico	187.188.203.75	Saint Louis, United	http-alt	8080
2015-01-02 06:07:54.69	CHINANET-HN Hengyang	Changsha, China	218.77.79.55	Saint Louis, United	unknown	49154
2015-01-02 06:07:54.96	CHINANET-HN Hengyang	Changsha, China	218.77.79.43	Saint Louis, United	ms-wbt-	3389
2015-01-02 06:07:55.36	N/A	unknown, Mil/Gov	107.144.32.243	Saint Louis, United	http	80
2015-01-02 06:07:55.68	CHINANET Zhejiang province	Hangzhou, China	115.230.124.174	unknown, Taiwan	unknown	9064
2015-01-02 06:07:55.95	N/A	unknown, Mil/Gov	190.113.89.154	Saint Louis, United	syslog	514
2015-01-02 06:07:56.37	Hotnet	unknown, Israel	213.57.113.12	Saint Louis, United	isakmp	500

Norse Cyber Attack Map  
 January 2, 2015, 0008 Central Time  
 Biggest Target: U.S. with 8942 attacks  
 Biggest Attacker: U.S. with 2861 attacks  
 Source: <http://map.ipviking.com/>

### ATTACK TYPES

#	SERVICE	PORT
1672	http-alt	8080
1208	http	80
699	telnet	23
409	ssh	22
358	isakmp	500
262	x11	6060
259	rfb	5900
251	wap-wsp	9200

Screenshot from the Norse Cyber Attack Map Showing Recent Cyberattacks December 2014



# Some Other Current and Future Cybersecurity Trends and Dangers to Keep Us Awake at Night



**Internet of Things:** which will add over 50 billion new devices by 2021. Yes – your TV and other home devices are watching and recording you.



**Massive proliferation & use of SmartPhones:** which now comprises well over 50 user connected Internet devices.



**DeepFakes:** which include **Artificial Intelligence (AI)** to use pictures, documents, and sound to deceive and commit cybercrimes.



**AI, Big Data, and Machine Learning:** which are now being used by Cybercriminals to perfect the speed, accuracy, and effectiveness of cyberattacks.



**Cyberattack Automation:** which is now being used by Cybercriminals to perfect the speed, accuracy, and effectiveness of cyberattacks.



**Botnets:** which are comprised of multiple programs running on computers that are controlled by one or a few command control programs. These can be from thousands to millions of programs, and can and have caused damage and/or disruption on a scale where they shut down the Internet in one or more countries.

# Compliance with Laws, Regulations and Policies

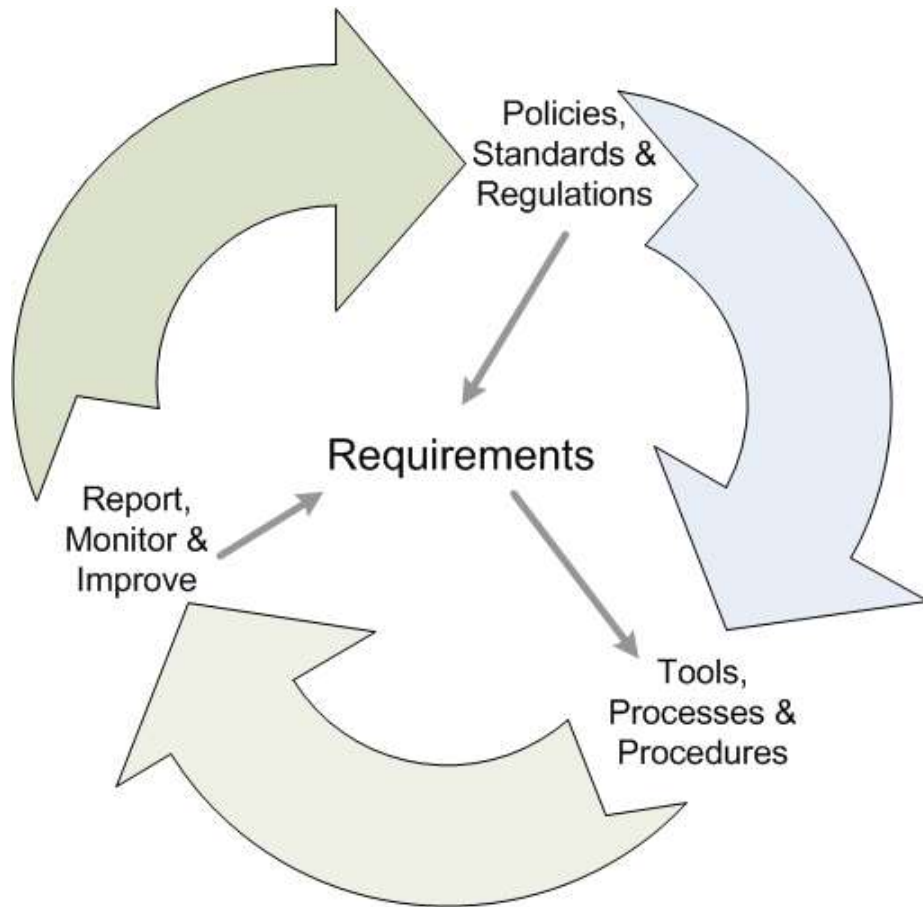
# Why Compliance Management, Safety and Security? And Why Now?

- Teaching people about hardware and software without emphasizing safety, security, and compliance with laws and regulations would be irresponsible and unethical.
- It would be like teaching you to drive a car and not mentioning things like Safety, State Driving Laws, and the Rules of the Road.



Image Source: <http://www.tellusdetroit.com/local/student-driver.html>

# The Cycle of Compliance Management



Jacobs, S. (2011). Engineering Information Security, New York, NY: IEEE Press.

Slater Technologies

# Three Key Principles

- We live in a Nation of Laws with which the citizens and visitors must comply.
- **Ignorance of the Law is no excuse** for breaking the Law.
- Dura Lex, Sed Lex
  - (Latin for “The Law is Harsh, but it is the Law.”)

# Two Kinds of Laws

- **Criminal Laws**
  - Federal
  - State (and also City Ordinances)
- **Civil Laws (Tort Law)**
  - Federal
  - State
  - Local (i.e. City Ordinances)



# Criminal and Civil Legal Actions Compared

<b>Factor</b>	<b><i>Criminal</i></b>	<b><i>Civil</i></b>
Plaintiff	The State (Public Sector)	Private and nonprofit interests
Prosecutor	The People	The Victim
Main Purpose	Punishment of the guilty	Redress of injury
Investigation	By or on behalf of the State	By the victim, or agents of the victim
Sanctions	Jail, prison Fines Specific corrective activity	Corrective action or behavior
Conviction	Beyond a reasonable doubt	Preponderance of evidence
Appeals	Possible by a defendant	Possible by either party

Source: McCrie, R. D. (2007). Security Operations Management, second edition. Burlington, MA: Elsevier.

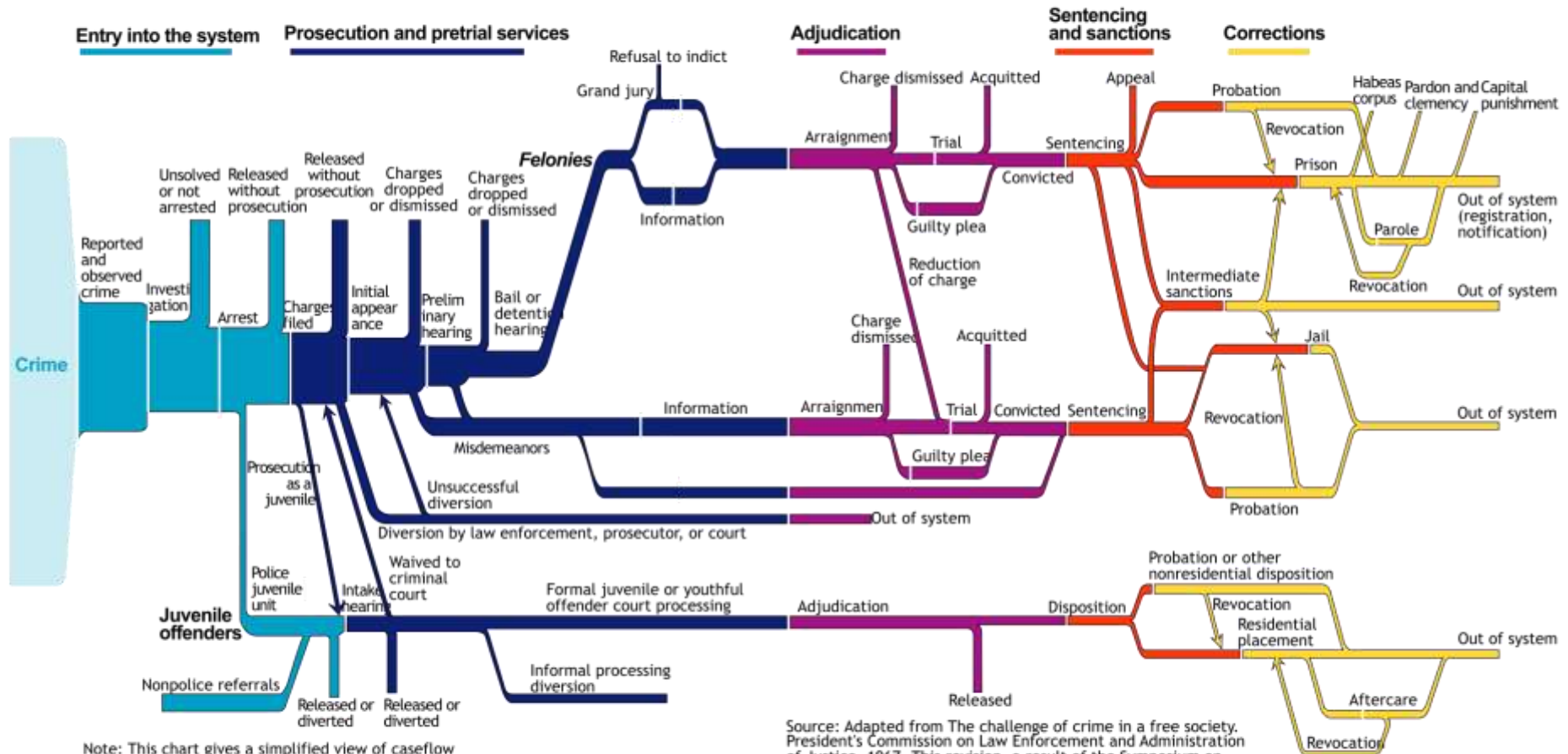
# Criminal and Civil Legal Actions Compared

- “Fundamental differences exist between criminal and civil litigation. A defendant may be sued criminally, civilly, or both, in which case different plaintiffs will bring charges. Private sector investigations normally serve the interests of plaintiffs and defendants in civil litigation. However, private investigators may be hired by the government, when indicated, to collect evidence on behalf of the public sector in criminal cases and administrative issues (McCrie, 2007).”

Source: McCrie, R. D. (2007). *Security Operations Management*, second edition. Burlington, MA: Elsevier.

# US. Criminal Justice System

What is the sequence of events in the criminal justice system?



Note: This chart gives a simplified view of caseload through the criminal justice system. Procedures vary among jurisdictions. The weights of the lines are not intended to show actual size of caseloads.

Source: Adapted from The challenge of crime in a free society. President's Commission on Law Enforcement and Administration of Justice, 1967. This revision, a result of the Symposium on the 30th Anniversary of the President's Commission, was prepared by the Bureau of Justice Statistics in 1997.



# INFORMATION SECURITY AND THE LAW

# Computer Fraud Abuse Act of 1987

- Still the Number 1 Legal Statute Used by the FBI to Investigate and Charge Cybercrime

Conspiracies and attempts to commit these acts are also criminalized under the CFAA. Federal law provides for potential imprisonment of up to 10 years for a violation of the CFAA and up to twenty years for a second offense. The chart below summarizes the various subsections of Section 1030 (CFAA) and the corresponding sentences:

## CFAA Offenses

Offense	Section	Sentence
Obtaining National Security Information	(a)(1)	10 yrs (20)
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 yrs (10)
Trespassing in a Government Computer	(a)(3)	1 yr (10)
Accessing a Computer to Defraud and Obtain Value	(a)(4)	5 yrs (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 yrs (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 yrs (20)
Negligently Causing Damage and Loss by Intentional Access	(a)(5)(C)	1 yr (10)
Trafficking in Passwords	(a)(6)	1 yr (10)
Extortion Involving Computers	(a)(7)	5 yrs (10)
Attempt and Conspiracy to Commit such an Offense	(b)	10 yrs for attempt but no penalty specified for conspiracy in section (c)

# Computer Fraud Abuse Act of 1987

In some circumstances, the CFAA also provides for a civil cause of action if a plaintiff can demonstrate the following:

- loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;
- the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
- physical injury to any person;
- a threat to public health or safety;
- damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or
- damage affecting 10 or more protected computers during any 1-year period.

# Computer Fraud Abuse Act of 1987

## Sudhish Ramesh

justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging-cisco-s-network

FOR IMMEDIATE RELEASE

Wednesday, December 9, 2020

### San Jose Man Sentenced To Two Years Imprisonment For Damaging Cisco's Network

#### Intrusion Resulted in Deletion of 16,000 WebEx Teams Accounts in Fall 2018

SAN JOSE – Sudhish Kasaba Ramesh was sentenced today to 24 months in prison and ordered to pay a \$15,000 fine for intentionally accessing a protected computer without authorization and recklessly causing damage, announced United States Attorney David L. Anderson and Federal Bureau of Investigation Special Agent in Charge Craig D. Fair. The sentence was handed down by the Honorable Lucy H. Koh, U.S. District Judge.

Ramesh, 31, of San Jose, pleaded guilty on August 26, 2020, to one count of intentionally accessing a protected computer without authorization and recklessly causing damage to Cisco. Ramesh worked for Cisco but resigned in approximately April 2018. According to the plea agreement, Ramesh admitted to intentionally accessing the Cisco Systems cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018. Ramesh further admitted that during his unauthorized access he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provides video meetings, video messaging, file sharing, and other collaboration tools. He admitted that he acted recklessly in deploying the code and consciously disregarded the substantial risk that his conduct would harm Cisco. As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks and caused Cisco to spend approximately \$1,400,000 in employee time to restore the damage to the application and refund over \$1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct.

Ramesh was charged by an information on July 13, 2020, with one count of Intentionally Accessing a Protected Computer Without Authorization and Recklessly Causing Damage, in violation of 18 U.S.C. §§ 1030(a)(5)(B) and (c)(4)(A)(i)(I).

U.S. District Judge Koh sentenced Ramesh today, following his guilty plea on August 26, 2020, to one count of Intentionally Accessing a Protected Computer Without Authorization and Recklessly Causing Damage, in violation of 18 U.S.C. §§ 1030(a)(5)(B) and (c)(4)(A)(i)(I). The defendant was further sentenced to serve a one year period of supervised release following the 24 months in prison and to pay a \$15,000 fine. The defendant is out of custody and will begin serving the sentence on February 10, 2021.

Susan Knight is the Assistant U.S. Attorney who is prosecuting the case with the assistance of Elise Etter. The prosecution is the result of an investigation by the Federal Bureau of Investigation. Cisco Systems, Inc. fully cooperated with the U.S. Attorney's Office and Federal Bureau of Investigation.

#### Component(s):

USAO - California, Northern

Updated December 9, 2020

Sudhish Ramesh, who was convicted in December 2020, is scheduled to complete his Federal Prison Sentence in February 2023 and will likely be deported back to his Home country.

Slater Technologies

# Computer Fraud Abuse Act of 1987

## Sudhish Ramesh

### ADDITIONAL INFO

- Ramesh has a Master of Science in Electrical and Computer Engineering from the University of California at Santa Barbara, a Bachelor of Technology in Electronics and Communication Engineering from Vellore Institute of Technology in India, and has several computer-related certifications.
- Ramesh's job history connects him to numerous technology companies, including Qualcomm, Oracle, and WePay.
- Though it cost them 2.4 million in restoration and refunds, Cisco did not request any restitution for the damages caused by Ramesh.
- Ramesh's motivation for his actions remains unknown.
- No customer data was compromised as a result of the defendant's conduct.

#### Resources for further exploration:

- Insider Threat Indicators Job Aid:  
[https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf?ver=\\_HedcDtQk9sSEZItNMLQzA==](https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf?ver=_HedcDtQk9sSEZItNMLQzA==)
- Privileged User Cybersecurity Responsibilities, DS-IA112.06:  
<https://public.cyber.mil/training/privileged-user-cybersecurity-responsibilities/>
- DHS - U.S. CERT "Combating the Insider Threat":  
<https://www.us-cert.gov/security-publications/Combating-Insider-Threat>

**IF YOU SEE SOMETHING, SAY SOMETHING!**

**Slater Technologies**



# Let's Think for a Minute...

- Name some ways that a person could break the law using a computer:



# Let's Think for a Minute...

- Name some ways that a person could break the law using a computer:
  - Stalking
  - Harassment
  - Defamation
  - Child pornography
  - Planning a crime or terrorism
  - Software piracy
  - Breaking into another computer
  - Destruction of data and/or software
  - Theft of data and/or software
  - Disruption of service(s)
  - SPAM
  - Identity Theft
  - Attempt to defraud
  - Hate e-mail
  - Creation and/or distribution of Malware
  - Involvement with foreign entities for cyber warfare attacks
  - Attempts to gain access to and/or distribute passwords or Personally Identifiable Information (PII)
  - Document Theft
  - Distributed Denial of Service Attacks



# Example of a Local Federal Computer Crime from 2011



U. S. Department of Justice

United States Attorney  
Northern District of Illinois

Patrick J. Fitzgerald  
United States Attorney

Federal Building  
219 South Dearborn Street, Fifth Floor  
Chicago, Illinois 60604  
(312) 353-5300

FOR IMMEDIATE RELEASE  
WEDNESDAY SEPTEMBER 28, 2011  
[www.justice.gov/usao/ih](http://www.justice.gov/usao/ih)

PRESS CONTACTS:  
AUSA Barry Jonas 312-886-8027  
AUSA Paul Tzar 312-697-4032  
Randall Samborn 312-353-5318

## **FORMER CME GROUP SOFTWARE ENGINEER INDICTED FOR THEFT OF GLOBEX COMPUTER TRADE SECRETS WHILE ALLEGEDLY PLANNING BUSINESS TO IMPROVE ELECTRONIC TRADING EXCHANGE IN CHINA**

CHICAGO — A former senior software engineer for Chicago-based CME Group, Inc., was indicted today for allegedly downloading and removing computer source code and other proprietary information while at the same time pursuing business plans to improve an electronic trading exchange in China. The defendant, **Chunlai Yang**, who was arrested in July, was charged with two counts of theft of trade secrets in an indictment returned by a federal grand jury, announced Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois, and Robert D. Grant, Special Agent-in-Charge of the Chicago Office of the Federal Bureau of Investigation.

Yang, 48, of Libertyville, was released on a \$500,000 secured bond following his arrest on July 1 after being charged in a criminal complaint. He will be arraigned on a date to be determined in U.S. District Court. The indictment seeks forfeiture of computers and related equipment that were seized from Yang.

## 旅美侨领因涉窃取商业机密被FBI逮捕

最新法律案例及资讯 · 热点追踪

2011年7月20日

### 法佑网 Staff Legal Reporter 报道

2011年7月2日消息,美国联邦调查局(FBI)已于1日逮捕了前芝加哥商业交易所集团(CME)高级程序员杨春来(音, Chunlai Yang),他被控从该公司窃取商业机密,以借此在中国筹建交易所。

### 涉嫌窃取证券交易情报

杨春来现年49岁,拥有美国公民身份,被捕后已在初审法院出庭。FBI在证词中称他盗取了“A公司”的大量专有源代码。后经证实,此“A公司”正是杨春来在2000年便加入的CME集团。该集团亦确认杨春来因“某些不当行为”,已经被公司解雇。



CME集团是美国证券交易业界的重要公司,其名下除拥有芝加哥商业交易所(Chicago Mercantile Exchange)之外,还经营着芝加哥期货交易所(Chicago Board of Trade)等多家美国大型金融衍生品交易所。

该公司发言人称,在此案中尚未发现客户信息、交易记录和需监管信息遭到泄露。

FBI提到,杨春来利用进入CME专有电子交易系统的权限,非法下载了他本来无权占有的文件至办公电脑上。

CME的安保人员向FBI提供了杨电脑上的截屏图像,以说明其盗窃行为。部分被盗的文件还被杨转存至外部闪存中。

Source: [http://www.81law.com/news/sa\\_news\\_aid\\_1649/](http://www.81law.com/news/sa_news_aid_1649/)

Slater Technologies

Source: <http://www.cybercrime.gov/yangIndict.pdf>

# Example of a Local Federal Computer Crime

According to the indictment, Yang began working for CME Group in 2000 and was a senior software engineer at the time of his arrest. His responsibilities included writing computer code and, because of his position, he had access to the software programs that supported CME Group's Globex electronic trading platform. Globex allowed market participants to buy and sell exchange products from any place at any time. The source code and algorithms that made up the supporting programs were proprietary and confidential business property of CME Group, which instituted internal measures to safeguard and protect its trade secrets.

Between Dec. 8, 2010, and June 30, 2011, Yang allegedly downloaded more than 1,000 computer files containing CME computer source code from CME's secure internal computer system to his CME-issued work computer; he then transferred many of these files from his work computer to his personal USB flash drives; and then transferred many of these computer files from his USB flash drives to his personal computer located at his home. During the same time, Yang also downloaded and printed numerous CME internal manuals and guidelines describing how many of the computer files that comprise Globex operate and how these computer files interact with each other, the indictment alleges.

Source: <http://www.cybercrime.gov/yangIndict.pdf>



Chunlai Yang  
Sr. Financial Applications Developer

# Example of a Local Federal Computer Crime

To help the Chinese exchange attract more customers and generate higher profits, Gateway proposed to expand the capabilities of Zhangjiagang's software by providing customers with more ways of placing orders; connecting the exchange's database storage system and matching systems; rewriting the trading system software in the JAVA computer programming language; raising the system's capacity and speed by modifying communication lines and structures; and developing trading software based on the FIX computer coding language, the indictment alleges.

CME Group has fully cooperated with the investigation.

Each count of theft of trade secrets carries maximum penalty of 10 years in prison and a \$250,000 fine. If convicted, the Court must impose a reasonable sentence under the advisory United States Sentencing Guidelines.

The government is being represented by Assistant United States Attorneys Barry Jonas and Paul Tzur.

The public is reminded that an indictment contains only charges and is not evidence of guilt. The defendant is presumed innocent and is entitled to a fair trial at which the government has the burden of proving guilt beyond a reasonable doubt.

###

Source: <http://www.cybercrime.gov/yangIndict.pdf>



Chunlai Yang  
Sr. Financial Applications Developer

Slater Technologies

# Some Federal Laws

<b>1974</b>	Privacy Act of 1974 (Public Law 93-579, 5 U.S. Code 552a). - sets limits on the collection and transfer of personal data by government agencies and lets citizens sue agencies that violate the act (Lane, 1997).
<b>1984</b>	Computer Fraud and Abuse Act - originally enacted as part of the Crime Control Act and was the first statute to specifically address computer crime. In 1990, this was amended it “to cover all computers used in interstate commerce or communications” and to prohibit forms of computer abuse which arise in connection with, and have a significant effect upon, interstate or foreign commerce.
<b>1986</b>	Electronic Communications Privacy Act of 1986 - the most comprehensive piece of federal legislation dealing with the interception of and access to electronic communications such as e-mail and voice mail.
<b>1987</b>	The Computer Security Act of 1987
<b>1996</b>	Health Insurance Portability and Accountability Act (HIPAA) of 1996 - required the Department of Health and Human Services to promulgate regulations governing the disclosure of health information.
<b>1999</b>	Gramm-Leach-Bliley Act - for the purpose of implementing the congressional policy that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers to protect the security and confidentiality of those customers’ nonpublic personal information...
<b>2001</b>	USA PATRIOT Act, H.R. 3162
<b>2005</b>	H.R. 4127 - Data Accountability and Trust Act (DATA)
<b>2009</b>	HITECH Act (part of the ARRA 2009 legislation)

# Other Federal Laws

- USA PATRIOT Act Expired on May 31, 2015
- USA FREEDOM Act Signed into Law on June 2, 2015
  - Cooperation and Data Exchange Between Federal Agencies
  - Telecommunications Providers will retain User Metadata related to communications
  - <https://www.congress.gov/bill/113th-congress/house-bill/3361>
  - [https://en.wikipedia.org/wiki/USA\\_Freedom\\_Act](https://en.wikipedia.org/wiki/USA_Freedom_Act)

## USA FREEDOM Act



<b>Long title</b>	To reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes.
<b>Acronyms (colloquial)</b>	USA FREEDOM Act, a backronym for " <i>Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act</i> "
<b>Nicknames</b>	Freedom Act

# NSA CELEBRATES PASSAGE OF USA 'FREEDOM' ACT, WHILE SKYPE KEEPS ITS SPYING EYES ON YOU

The NSA is coming out of this unscathed



by COIN TELEGRAPH | JUNE 16, 2015



29



33



0



Both privacy advocates and the NSA are celebrating the **USA Freedom Act** that passed the Senate on June 2. The act legalized and simplified the collecting of phone metadata for the NSA. Meanwhile Skype continues to collect voice, chat, video and other data, and deliver it to the **Five Eyes** international spy coalition.

Source:

<http://www.infowars.com/nsa-celebrates-passage-of-usa-freedom-act-while-skype-keeps-its-spying-eyes-on-you/>

Slater Technologies



# Learn About the Edward Snowden and the NSA Data Breach

- Visit <http://billslater.com/snowden>
- Search on these words together:
  - Edward Snowden NSA Data Breach Presentation
- Former NSA Contractor Edward Snowden is now a new Citizen of Russia, effective September 26, 2022



Slater Technologies

# U.S. Department of Justice Computer Crime Website



<http://www.cybercrime.gov/>



## Computer Crime & Intellectual Property Section United States Department of Justice

Home Computer Crime Intellectual Property Electronic Evidence Other High Tech Legal issues About CCIPS

News Site Index  Search

### Computer Crime & Intellectual Property Section

#### Latest Press Releases

- [Cybersecurity: Protecting America's New Frontier](#) (November 15, 2011)
- [Administrator of VisionTech Components, LLC Sentenced To 38 Months In Prison For Her Role In Sales of Counterfeit Integrated Circuits Destined to U.S. Military and Other Industries To 38 Months In Prison For Her Role In Sales of Counterfeit Integrated Circuits Destined to U.S. Military and Other Industries: Counterfeit Devices Were Sold to U.S. Navy and Defense Contractors](#) (October 25, 2011)
- [Two Top Administrators of Ninjavidéo Website Plead Guilty to Criminal Copyright Conspiracy](#) (October 25, 2011)
- [Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets: First Prosecution In Indiana for Foreign Economic Espionage](#) (October 18, 2011)
- [Three Sentenced to Federal Prison for Forcing Labor and Distributing Pirated/Counterfeit CDs and DVDs](#) (October 14, 2011)
- [Former Citadel Employee Arrested for Theft of Financial Firm's Trade Secrets: Hard drives recovered from canal allegedly contained effort to construct currency futures trading platform based on Citadel's proprietary model](#) (October 13, 2011)
- [La Plata Man Pleads Guilty in Scheme to Sell Counterfeit Viagra](#) (September 30, 2011)
- [Ninjavidéo Founder Pleads Guilty in Virginia to Criminal Copyright Conspiracy](#) (September 29, 2011)
- [Former CME Group Software Engineer Indicted For Theft Of Globex Computer Trade Secrets](#) (September 28, 2011)
- [Founder of Ninjavidéo Pleads Guilty to Criminal Copyright Conspiracy](#) (September 23, 2011)
- [Virginia Store Owner Arrested for Selling Counterfeit Goods](#) (September 21, 2011)
- [Chinese National indicted with Trafficking in Counterfeit Merchandise of over 1000 Items](#) (September 16, 2011)
- [Southern California Man Sentenced to 30 Months In Prison for Importing Counterfeit Exercise Equipment](#) (September 12, 2011)
- [Ninjavidéo Website Operators Charged with Criminal Copyright Conspiracy](#) (September 9, 2011)
- [Online Identity Thief Sentenced in Virginia to 14 Years in Prison for Selling Counterfeit Credit Cards Leading to More Than \\$3 Million in Losses](#) (September 9, 2011)
- [Two Texas Men Guilty of Trafficking Counterfeit Goods at Mall Kiosks](#) (September 9, 2011)
- [Virginia Woman Sentenced to 60 Months In Prison for Importing and Selling Counterfeit Cisco Computer Networking Equipment](#) (September 9, 2011)
- [Seven Indicted For Extensive Counterfeit Media Operation](#) (September 8, 2011)

#### Hot Documents

- [How to Report Cyber and IP Crime](#)
  - [How to Report Computer- and Internet-Related Crime](#)
  - [How to Report Intellectual Property Crime](#)
- [IP Enforcement Coordinator's 2010 Annual Report](#) (February 2011)
- [PRO IP Act Annual Report 2010 \(PDF\)](#) (December 2010)
- [FBI PRO IP Act Annual Report 2010 \(PDF\)](#) (December 2010)
- [2010 Joint Strategic Plan on Intellectual Property Enforcement\(PDF\)](#) (June 2010)
- [Testimony of Deputy Assistant Attorney General Jason M. Weinstein on Combating IP Crime \(PDF\)](#) (December 2009)
- [USA Bulletin on Economic Espionage and Trade Secrets \(PDF\)](#) (November 2009)
- [CCIPS Manual on Electronic Search and Seizure - Updated 2009 \(August 24, 2009\)](#)
- [New Law Review Article, "Data Breaches: What the Underground World of 'Carding' Reveals"\(PDF\)](#) (May 2008)
- [NPR interview with CCIPS and FBI: Cyber Sleuths Zero In as Web Fraud Takes Toll \(January 20, 2008\)](#)
- [Digital Forensic Analysis Methodology Flowchart \(PDF\)](#) (August 22, 2007)
- [CCIPS "Prosecuting Computer Crimes" Manual \(March 2007\)](#)
- [CCIPS "Prosecuting Intellectual Property Crimes" Manual \(October 2006\)](#)
- [United States Joins Council of Europe Convention on Cybercrime \(September 29, 2006\)](#)
  - [More Information on the Cybercrime Convention](#)
- [Cyberethics](#)

# U.S. Department of Justice Computer Crime Website



<http://www.cybercrime.gov/>

## Reporting Computer, Internet-Related, or Intellectual Property Crime

Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement.

- Reporting Computer Crime
- Reporting Intellectual Property Crime

## Reporting Computer Hacking, Fraud and Other Internet-Related Crime

The primary federal law enforcement agencies that investigate domestic crime on the Internet include: the Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF). Each of these agencies has offices conveniently located in every state to which crimes may be reported. Contact information regarding these local offices may be found in local telephone directories. In general, federal crime may be reported to the local office of an appropriate law enforcement agency by a telephone call and by requesting the "Duty Complaint Agent."

Each law enforcement agency also has a headquarters (HQ) in Washington, D.C., which has agents who specialize in particular areas. For example, the FBI and the U.S. Secret Service both have headquarters-based specialists in computer intrusion (i.e., computer hacker) cases.

To determine some of the federal investigative law enforcement agencies that may be appropriate for reporting certain kinds of crime, please refer to the following table:

Type of Crime	Appropriate federal investigative law enforcement agencies
Computer intrusion (i.e. hacking)	<ul style="list-style-type: none"> <li>• FBI local office</li> <li>• U.S. Secret Service</li> <li>• Internet Crime Complaint Center</li> </ul>
Password trafficking	<ul style="list-style-type: none"> <li>• FBI local office</li> <li>• U.S. Secret Service</li> <li>• Internet Crime Complaint Center</li> </ul>
Counterfeiting of currency	<ul style="list-style-type: none"> <li>• U.S. Secret Service</li> </ul>
Child Pornography or Exploitation	<ul style="list-style-type: none"> <li>• FBI local office</li> <li>• if imported, U.S. Immigration and Customs Enforcement</li> <li>• Internet Crime Complaint Center</li> </ul>
Child Exploitation and Internet Fraud matters that have a mail nexus	<ul style="list-style-type: none"> <li>• U.S. Postal Inspection Service</li> <li>• Internet Crime Complaint Center</li> </ul>
Internet fraud and SPAM	<ul style="list-style-type: none"> <li>• FBI local office</li> <li>• U.S. Secret Service (Financial Crimes Division)</li> <li>• Federal Trade Commission (online complaint)</li> <li>• if securities fraud or investment-related SPAM e-mails, Securities and Exchange Commission (online complaint)</li> <li>• The Internet Crime Complaint Center</li> </ul>
Internet harassment	<ul style="list-style-type: none"> <li>• FBI local office</li> </ul>
Internet bomb threats	<ul style="list-style-type: none"> <li>• FBI local office</li> <li>• ATF local office</li> </ul>
Trafficking in explosive or incendiary devices or firearms over the Internet	<ul style="list-style-type: none"> <li>• FBI local office</li> <li>• ATF local office</li> </ul>

# U.S. Department of Justice Computer Crime Website



<http://www.cybercrime.gov/>

## Other Cybercrime Reporting Resources

- The Internet Crime Complaint Center (IC3)

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving internet related crimes.

- The Internet Crime Complaint Center
- Department of Homeland Security's National Infrastructure Coordinating Center: (202) 282-9201 (report incidents relating to national security and infrastructure issues)
- U.S. Computer Emergency Readiness Team (U.S. CERT) (online reporting for technicians)
- National Association of Attorney General's Computer Crime Point of Contact List (all state-related cyber questions)

## Reporting Intellectual Property Crime

Type of Crime	Appropriate federal investigative law enforcement agencies
Copyright piracy (e.g., software, movie, sound recordings)	<ul style="list-style-type: none"><li>• FBI local field office</li><li>• U.S. Immigration and Customs Enforcement (ICE)</li><li>• Internet Crime Complaint Center</li></ul>
Trademark counterfeiting	<ul style="list-style-type: none"><li>• FBI local field office</li><li>• U.S. Immigration and Customs Enforcement</li><li>• Internet Crime Complaint Center</li></ul>
Theft of trade secrets	<ul style="list-style-type: none"><li>• FBI local field office</li></ul>

- "Reporting Intellectual Property Crime: A Guide for Victims of Counterfeiting, Copyright Infringement, and Theft of Trade Secrets" (PDF)

This guide is contained in Appendix C of the Report of the Department of Justice's Intellectual Property Task Force (October 2004) (PDF). The guide also contains the following checklists for reporting intellectual property crime to law enforcement:

- Checklist for Reporting a Copyright Infringement or Counterfeit Trademark Offense (PDF)
- Checklist for Reporting a Theft of Trade Secrets Offense (PDF)
- Other Government Initiatives to Combat Cybercrime
  - The STOP Initiative ([www.stopfakes.gov](http://www.stopfakes.gov))

The [stopfakes.gov](http://stopfakes.gov) website provides information to consumers and businesses on intellectual property, including information on how to report trade in fake goods.
  - National Intellectual Property Rights Coordination Center

The IPR Coordination Center's responsibilities include:

    - Coordinating U.S. government domestic and international law enforcement activities involving IPR issues.
    - Serving as a collection point for intelligence provided by private industry, as well as a channel for law enforcement to obtain cooperation from private industry (in specific law enforcement situations).
    - Integrating domestic and international law enforcement intelligence with private industry information relating to IPR crime, and disseminating IPR intelligence for appropriate investigative and tactical use.
    - Developing enhanced investigative, intelligence and interdiction capabilities.
    - Serving as a point of contact regarding IPR law enforcement related issues.

Those with specific information regarding intellectual property crime can submit an IPR Coordination Center Complaint Referral Form.



# Federal Laws

## PROSECUTING COMPUTER CRIMES

Computer Crime and  
Intellectual Property Section  
Criminal Division



Published by  
Office of Legal Education  
Executive Office for  
United States Attorneys

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes, and makes no public release of it. Individuals receiving the book in training are reminded to treat it confidentially.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. See *United States v. Carey*, 440 U.S. 741 (1979).

H. Marshall Jarrett  
Director, EOUSA

Michael W. Bailie  
Director, OLE

OLE  
Litigation  
Series

Ed Hagen  
Assistant Director,  
OLE

Scott Eltringham  
Computer Crime  
and Intellectual  
Property Section  
Editor in Chief

## Table of Contents

Preface and Acknowledgements.....	v	Chapter 5. Sentencing.....	131
Chapter 1. Computer Fraud and Abuse Act.....	1	A. Base Offense Levels.....	131
A. Key Definitions.....	4	B. Adjustments Under Section 2B1.1.....	132
B. Obtaining National Security Information..... § 1030(a)(1).....	12	C. CAN-SPAM Act.....	142
C. Accessing a Computer and Obtaining Information..... § 1030(a)(2).....	16	D. Wiretap Act.....	143
D. Trespassing in a Government Computer..... § 1030(a)(3).....	23	E. Generally-Applicable Adjustments.....	144
E. Accessing to Defraud and Obtain Value..... § 1030(a)(4).....	26	F. Conditions of Supervised Release.....	146
F. Damaging a Computer or Information..... § 1030(a)(5).....	35	Appendices	
G. Trafficking in Passwords..... § 1030(a)(6).....	49	A. Unlawful Online Conduct and Applicable Federal Laws.....	149
H. Threatening to Damage a Computer..... § 1030(a)(7).....	52	B. Jury Instructions.....	157
I. Attempt and Conspiracy..... § 1030(b).....	55	C. Best Practices for Working with Companies.....	173
J. Forfeiture..... § 1030(i) & (j).....	56	D. Best Practices for Victim Response and Reporting.....	177
Chapter 2. Wiretap Act.....	59	E. Network Crime Resources.....	185
A. Intercepting a Communication..... § 2511(1)(a).....	60	Table of Authorities.....	189
B. Disclosing an Intercepted Communication..... § 2511(1)(c).....	73	Index.....	201
C. Using an Intercepted Communication..... § 2511(1)(d).....	77		
D. Statutory Exceptions and Defenses.....	78		
E. Statutory Penalties.....	87		
Chapter 3. Other Network Crime Statutes.....	89		
A. Unlawful Access to Stored Communications..... § 2701.....	89		
B. Identity Theft..... § 1028(a)(7).....	96		
C. Aggravated Identity Theft..... § 1028A.....	100		
D. Access Device Fraud..... § 1029.....	102		
E. CAN-SPAM Act..... § 1037.....	105		
F. Wire Fraud..... § 1343.....	109		
G. Communication Interference..... § 1362.....	110		
Chapter 4. Special Considerations.....	113		
A. Jurisdiction.....	113		
B. Venue.....	115		
C. Statute of Limitations.....	120		
D. Juveniles.....	121		

Slater Technologies

# Commonwealth of Massachusetts

## Data Privacy Law

- Enacted in September 2008
- People and companies that handle personal data are legally obligated to protect it and encrypt it
- Companies must have a comprehensive Information Security program
- Requires risk-based approach
- Requires written evidence of
  - An active information security program
  - Internal and external audits
  - Annual review of security or whenever organizational changes that could affect security will occur
- Penalties include: **\$5000 for each violation**
- Additional exposures include legal costs and civil litigation

Section:

- [17.01: Purpose and Scope](#)
- [17.02: Definitions](#)
- [17.03: Duty to Protect and Standards for Protecting Personal Information](#)
- [17.04: Computer System Security Requirements](#)
- [17.05: Compliance Deadline](#)

**17.01 Purpose and Scope**

**(1) Purpose**

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation are to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

**(2) Scope**

The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

**17.02: Definitions**

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

**Breach of security**, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

**Electronic**, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

# Commonwealth of Massachusetts Data Privacy Law

(Excerpt)

## 17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- (a) Designating one or more employees to maintain the comprehensive information security program;
- (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:
  1. ongoing employee (including temporary and contract employee) training;
  2. employee compliance with policies and procedures; and
  3. means for detecting and preventing security system failures.
- (c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.
- (d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
- (e) Preventing terminated employees from accessing records containing personal information.
- (f) Oversee service providers, by:
  1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and
  2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 17.03 (2)(f)(2) even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as

# Commonwealth of Massachusetts Data Privacy Law

(Excerpt)

Slater Technologies



## 17.04: Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

1. Secure user authentication protocols including:
  - (a) control of user IDs and other identifiers;
  - (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
  - (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
  - (d) restricting access to active users and active user accounts only; and
  - (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
2. Secure access control measures that:
  - (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
  - (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
3. Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.
4. Reasonable monitoring of systems, for unauthorized use of or access to personal information;
5. Encryption of all personal information stored on laptops or other portable devices;
6. For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
8. Education and training of employees on the proper use of the computer security system and the importance of personal information security.

# Commonwealth of Massachusetts Data Privacy Law

(Excerpt)

## Who needs Mass 201 CMR 17?

All persons, corporations, associations, partnerships or other legal entities with systems containing Massachusetts resident's personal information in transit or at rest are responsible for complying with the 201 CMR 17 regulations by **March 1, 2010**. However, the regulations also require businesses to complete internal and external security risk assessments prior to the effective date. The regulation applies regardless of whether the entities or the data is either inside or outside state borders, and applies equally to private and public sector organizations.

## Penalties for non-compliance

The penalties for non-compliance with 201 CMR 17 are enforced through Massachusetts General Law Title XV: Regulation of Trade, chapter 93A, section 4. Violators may be faced with a civil penalty of \$5,000 for each violation, are required to pay the reasonable costs of investigation and litigation of such violation (including reasonable attorney's fees), and are subject to additional civil action since 201 CMR 17 creates a baseline standard that allows plaintiffs in civil suits to argue that a business that lost data was negligent. Title XV also requires any data breach be reported to both the Office of Consumer Affairs and Business Regulation (OCABR) and the Attorney General.

## What you need to be Mass 201 CMR 17 compliant

The new Massachusetts Privacy Law requires the following criteria be met:

- ▶ an internal and external risk assessment of the human, physical, technical environment based on the criteria outlined in 201 CMR 17
- ▶ the computer security provisions in the regulation use a risk-based approach that comply to the extent that it is technically feasible, meaning that reasonable means must be used to accomplish a required result if there is a reasonable technology is available
- ▶ the results of the internal and external risk assessments must be documented in a Written Comprehensive Information Security Program (WISP)
- ▶ the scope of the WISP must be reviewed at least on an annual basis or whenever there is a change in business practices that may impact security controls

The OCABR published [the 201 CMR 17 Compliance Checklist](#) as an aid to be used by either organizations themselves or their auditors when conducting their risk assessment. However, additional guidance on how and where to submit risk assessment results is expected from the state prior to the March 2010 deadline

# Commonwealth of Massachusetts Data Privacy Law

## Non-Compliance / Compliance Facts

(Excerpt)

Slater Technologies

# State of Illinois Personal Information Protection Act (PIPA)

- Enacted in June 2005
- People and companies that handle personal data are legally obligated to protect it
- Penalties are covered under the Consumer Fraud and Protection Act
- Additional exposures include legal costs and civil litigation

AN ACT concerning business.

Be it enacted by the People of the State of Illinois,  
represented in the General Assembly:

Section 1. Short title. This Act may be cited as the  
Personal Information Protection Act.

Section 5. Definitions. In this Act:

"Data Collector" may include, but is not limited to,  
government agencies, public and private universities,  
privately and publicly held corporations, financial  
institutions, retail operators, and any other entity that, for  
any purpose, handles, collects, disseminates, or otherwise  
deals with nonpublic personal information.

"Breach of the security of the system data" means  
unauthorized acquisition of computerized data that compromises  
the security, confidentiality, or integrity of personal  
information maintained by the data collector. "Breach of the  
security of the system data" does not include good faith  
acquisition of personal information by an employee or agent of  
the data collector for a legitimate purpose of the data  
collector, provided that the personal information is not used  
for a purpose unrelated to the data collector's business or  
subject to further unauthorized disclosure.

"Personal information" means an individual's first name or  
first initial and last name in combination with any one or more  
of the following data elements, when either the name or the  
data elements are not encrypted or redacted:

(1) Social Security number.

(2) Driver's license number or State identification  
card number.

(3) Account number or credit or debit card number, or  
an account number or credit card number in combination with  
any required security code, access code, or password that  
would permit access to an individual's financial account.

"Personal information" does not include publicly available  
information that is lawfully made available to the general  
public from federal, State, or local government records.

# State of Illinois Personal Information Protection Act (PIPA)

(Excerpt)

Slater Technologies

Section 10. Notice of Breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

(b) Any data collector that maintains computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed \$250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.

(d) Notwithstanding subsection (c), a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

Section 15. Waiver. Any waiver of the provisions of this Act is contrary to public policy and is void and unenforceable.

Section 20. Violation. A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

# State of Illinois Personal Information Protection Act (PIPA)

(Excerpt)

Slater Technologies

# White House Cyberspace Policy Review - July 2009

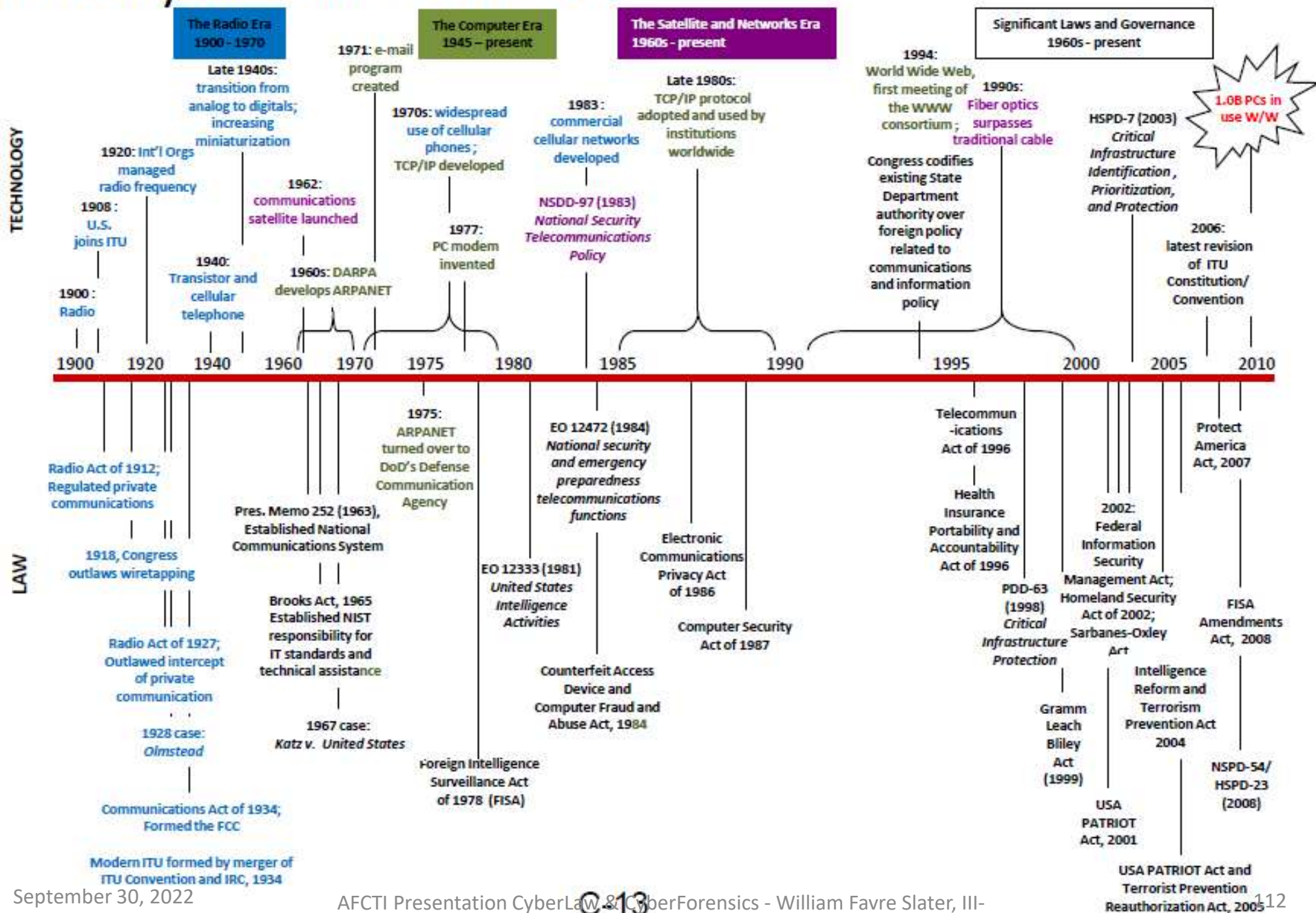
TABLE 1: NEAR-TERM ACTION PLAN

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.
6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. Prepare a cybersecurity incident response plan; initiate a dialog to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize their contribution and engagement.
9. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
10. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

# Cyberspace Policy Review

## The Near-Term Action Plan

# History Informs our Future







## The White House Blog



### The Administration Unveils its Cybersecurity Legislative Proposal

Posted by Howard A. Schmidt on May 12, 2011 at 02:00 PM EDT

Today I am happy to announce that the Administration has transmitted a [cybersecurity legislative proposal](#) to Capitol Hill in response to Congress' call for assistance on how best to address the cybersecurity needs of our Nation. This is a milestone in our national effort to ensure secure and reliable networks for Americans, businesses, and government; fundamentally, [this proposal](#) strikes a critical balance between maintaining the government's role and providing industry with the capacity to innovatively tackle threats to national cybersecurity. Just as importantly, it does so while providing a robust framework to protect civil liberties and privacy.

When the President released his [Cyberspace Policy Review \(pdf\)](#) almost two years ago, he declared cyberspace as a key strategic asset for the United States and its security just as vital. This legislative proposal is the latest achievement in the steady stream of progress we are making in securing cyberspace and completes [another near-term action item \(pdf\)](#) identified in the Cyberspace Policy Review.

**The Administration proposal helps safeguard your personal data and enhances your right to know when it has been compromised.** In addition to educating you on how to protect yourself from cyber threats with the [Stop. Think. Connect.](#) campaign, we believe organizations should inform you when your sensitive personal information may have been compromised. This notice not only helps you to protect yourself against harms like identity theft, but also incentivizes organizations to have better data security in the first place. Today, our country has a patchwork of 47 state notification laws. Our proposal simplifies and strengthens this reporting requirement and reaches all Americans.

**It helps protect our national security by addressing threats to our power grids, water systems, and other critical infrastructure.** These systems are the backbone of our modern economy; many are privately owned, but all merit our support in protecting them. The Administration proposal advances the security of our increasingly "wired" critical infrastructure, strengthens the criminal penalties for hacking into the systems that control these vital resources, and clarifies the ability of companies and the government to voluntarily share information about cybersecurity threats and incidents in a privacy-protective manner. This is behavior we want and need to promote.

**It helps the U.S. government protect our federal networks, while creating stronger privacy and civil liberties protections that keep pace with technology.** Since our Federal systems are under constant pressure by hackers, criminals and other threats, the government needs better tools to detect and prevent those threats. Part of cybersecurity is about finding malicious programs, and stopping their spread before they have any impact.

On May 12, 2011, The White House submitted new legislative proposal to Congress – the Legislation will provide new federally mandated requirements for companies to report data breaches to their affected customers

May 2011

Slater Technologies

# Presidential Cybersecurity Executive Order

- February 12, 2013
- Defined Critical Infrastructure
- Encouraged information sharing

# ***CYBERTHREATS & CYBERVULNERABILITIES***

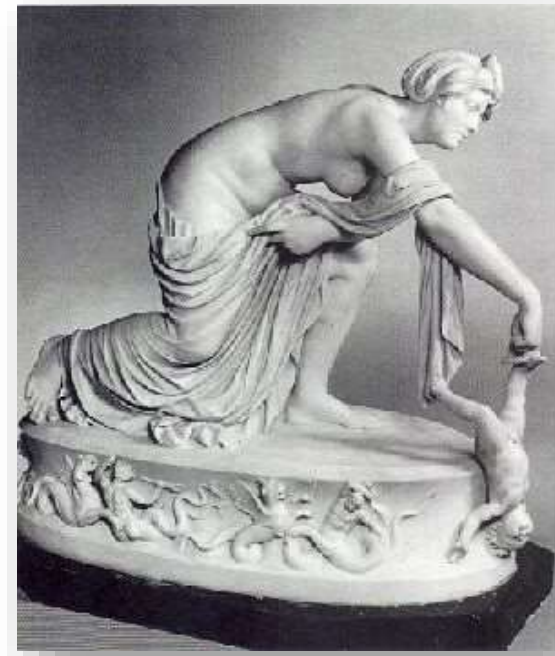


**ACFTI**

*Slater Technologies*

# Vulnerabilities

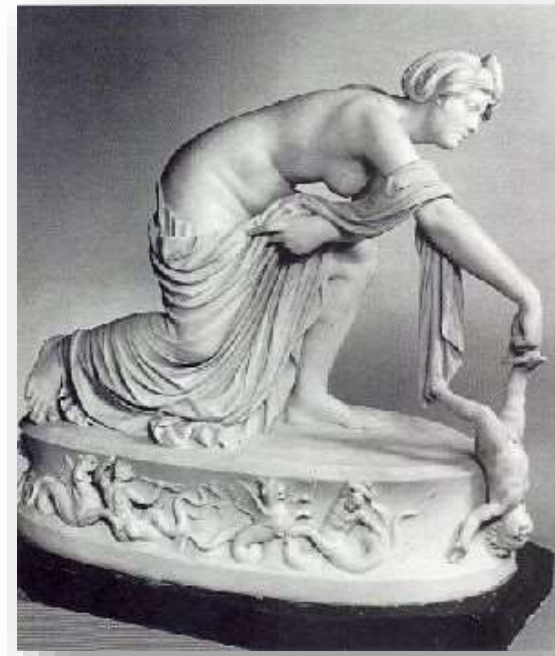
- Vulnerability – definition
- Vulnerability examples



Thetis dipping Achilles  
into the River Styx

# Vulnerabilities

- What is a “vulnerability”?
  - A situation or condition that represents an opportunity for a threat to damage or for information to be stolen from the organization, IT Systems or network.
  - Comes from the Latin word, “vulnus”, meaning “wound”
  - Sometimes called, “*The Achilles Heel.*”



Thetis dipping Achilles  
into the River Styx

# The Death of Achilles



Achilles was mortally wounded in the one place he was vulnerable: his heel.

# Some Sources of Vulnerabilities

- Complicated user interface
- Default passwords not changed
- Disposal of storage media without deleting data
- Equipment sensitivity to changes in voltage
- Equipment sensitivity to moisture and contaminants
- Equipment sensitivity to temperature
- Inadequate cabling security
- Inadequate capacity management
- Inadequate change management
- Inadequate classification of information
- Inadequate control of physical access
- Inadequate maintenance
- Inadequate network management
- Inadequate or irregular backup
- Inadequate password management
- Inadequate physical protection

# Some Sources of Vulnerabilities

- Inadequate protection of cryptographic keys
- Inadequate replacement of older equipment
- Inadequate security awareness
- Inadequate segregation of duties
- Inadequate segregation of operational and testing facilities
- Inadequate supervision of employees
- Inadequate supervision of vendors
- Inadequate training of employees
- Incomplete specification for software development
- Insufficient software testing
- Lack of access control policy
- Lack of clean desk and clear screen policy
- Lack of control over the input and output data
- Lack of internal documentation
- Lack of or poor implementation of internal audit
- Lack of policy for the use of cryptography



# Some Sources of Vulnerabilities

- Lack of procedure for removing access rights upon termination of employment
- Lack of protection for mobile equipment
- Lack of redundancy
- Lack of systems for identification and authentication
- Lack of validation of the processed data
- Location vulnerable to flooding
- Poor selection of test data
- Single copy
- Too much power in one person
- Uncontrolled copying of data
- Uncontrolled download from the Internet
- Uncontrolled use of information systems
- Undocumented software
- Unmotivated employees
- Unprotected public network connections
- User rights are not reviewed regularly

# WHAT ARE THREATS?

# Threats

- Threat – definition
- Some sources of threats
- More threat examples

# Threats

- What is a “threat”?
  - Something that can potentially cause damage or theft to the organization, IT Systems or network.

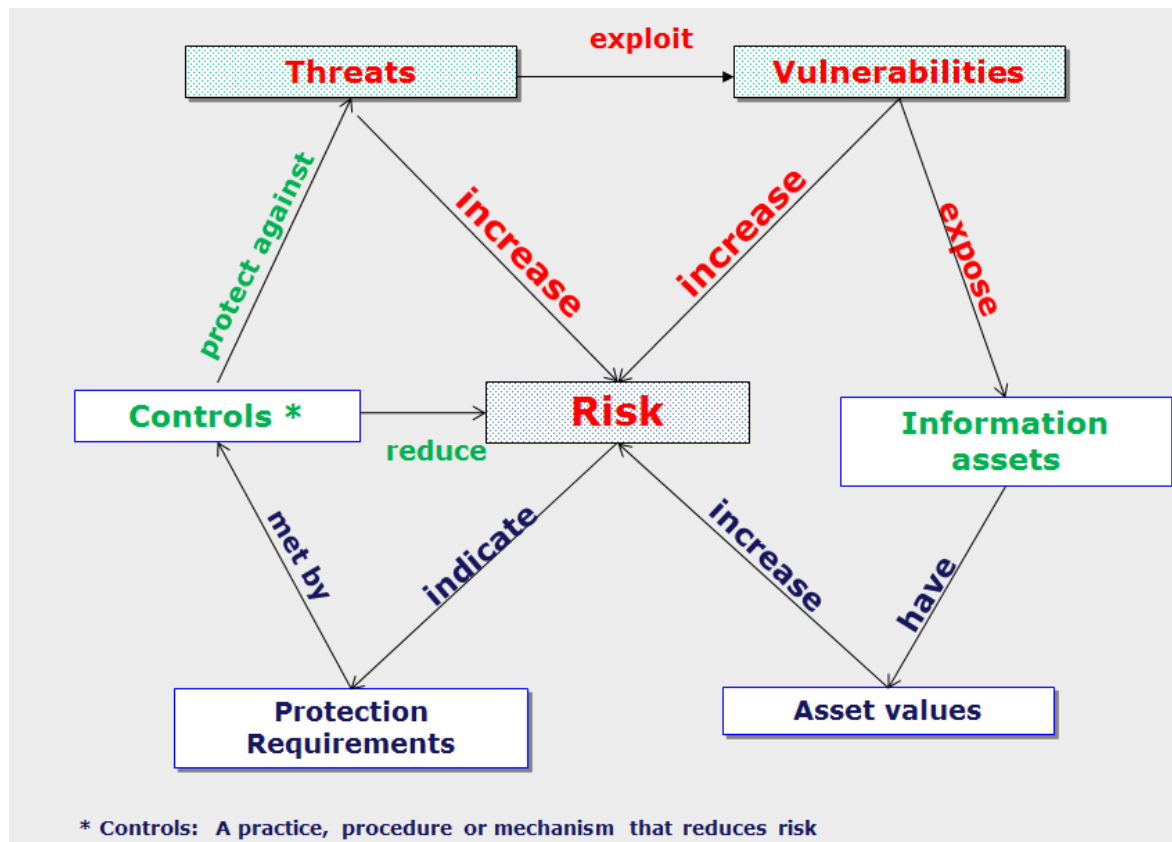
# Some Sources of Threats

- Misguided Employees
- Mistakes by careless Employees
- External Parties
- Low awareness of security issues
- Lack of or lapse in security policy compliance
- Growth in networking and distributed computing
- Growth in complexity and effectiveness of hacking tools and viruses
- Natural disasters e.g. fire, flood, earthquake, hurricanes, etc.

# Typical Threats that Represent Business Risks

Threat Category	Example
Human Errors or failures	Accidents, Employee mistakes
Compromise to Intellectual Property	Piracy, Copyright infringements
Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
Deliberate Acts of sabotage / vandalism	Destruction of systems / information
Deliberate Acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros Denial of service
Deviations in quality of service from service provider	Power and WAN issues
Forces of nature	Fire, flood, earthquake, lightening
Technical hardware failures or errors	Equipment failures / errors
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological Obsolescence	Antiquated or outdated technologies

# Risk Model Showing Relationships Between Threats, Vulnerabilities, and Controls



# **QUICK STORY ABOUT DAVID BREWER, MICHAEL NASH, AND THE "BREWER EVENTS".**



# So Let's Simplify This Stuff And Make it Easier, Achievable and More Manageable



**Dr. David Brewer, FBCS, CITP**

Note: with clients – he had to start using the Word, “EVENT”, because he learned Executive Management got upset About the connotation of Words like **THREATS** and **VULNERABILITIES**

Co-author of the ISO 27001 standard security framework, October 2005  
Co-author of ISO 27001 Annex A Insights, December 2010  
Director, Gamma Secure Systems Limited  
ISO/IEC 27001 and ISO 9001 Certified for the  
Provision of Information Security Consultancy  
[www.gammassl.co.uk](http://www.gammassl.co.uk)

# Brewer Event List

Event Code	Event Description
S1	Theft
S2	Acts of God, vandals and terrorism
S3	Fraud
S4	IT failure
S5	Hacking
S6	Denial of Service
S7	Disclosure
S8	Law
B1	Inappropriate deployment of people
B2	Failure to maintain proper records
B3	Issuance of wrong documents
NA	Not Applicable
P	Policy

# Risk Management Strategies

Code	Risk Management Strategy
1	Remediate
2	Transfer
3	Accept
4	Avoid
5	Not Applicable

# Applying the Brewer Events with Risk Management Strategies

Event Code	Event Description	Management Strategy
S1	Theft	1
S2	Acts of God, vandals and terrorism	3
S3	Fraud	1
S4	IT failure	1
S5	Hacking	1
S6	Denial of Service	1
S7	Disclosure	1
S8	Law	4
B1	Inappropriate deployment of people	1
B2	Failure to maintain proper records	1
B3	Issuance of wrong documents	4
NA	Not Applicable	3
P	Policy	1

Code	Risk Management Strategy
1	Remediate
2	Transfer
3	Accept
4	Avoid
5	Not Applicable



# ***A CYBER LITIGATOR'S ADVICE – FOR DEFENDANTS***

*Slater Technologies*

# Are You Reducing Your Cyber Legal Risks?

**Hillard M. Sterling**

**Clausen Miller P.C.**

**10 South LaSalle Street**

**Chicago, Illinois 60603**

**hsterling@clausen.com**

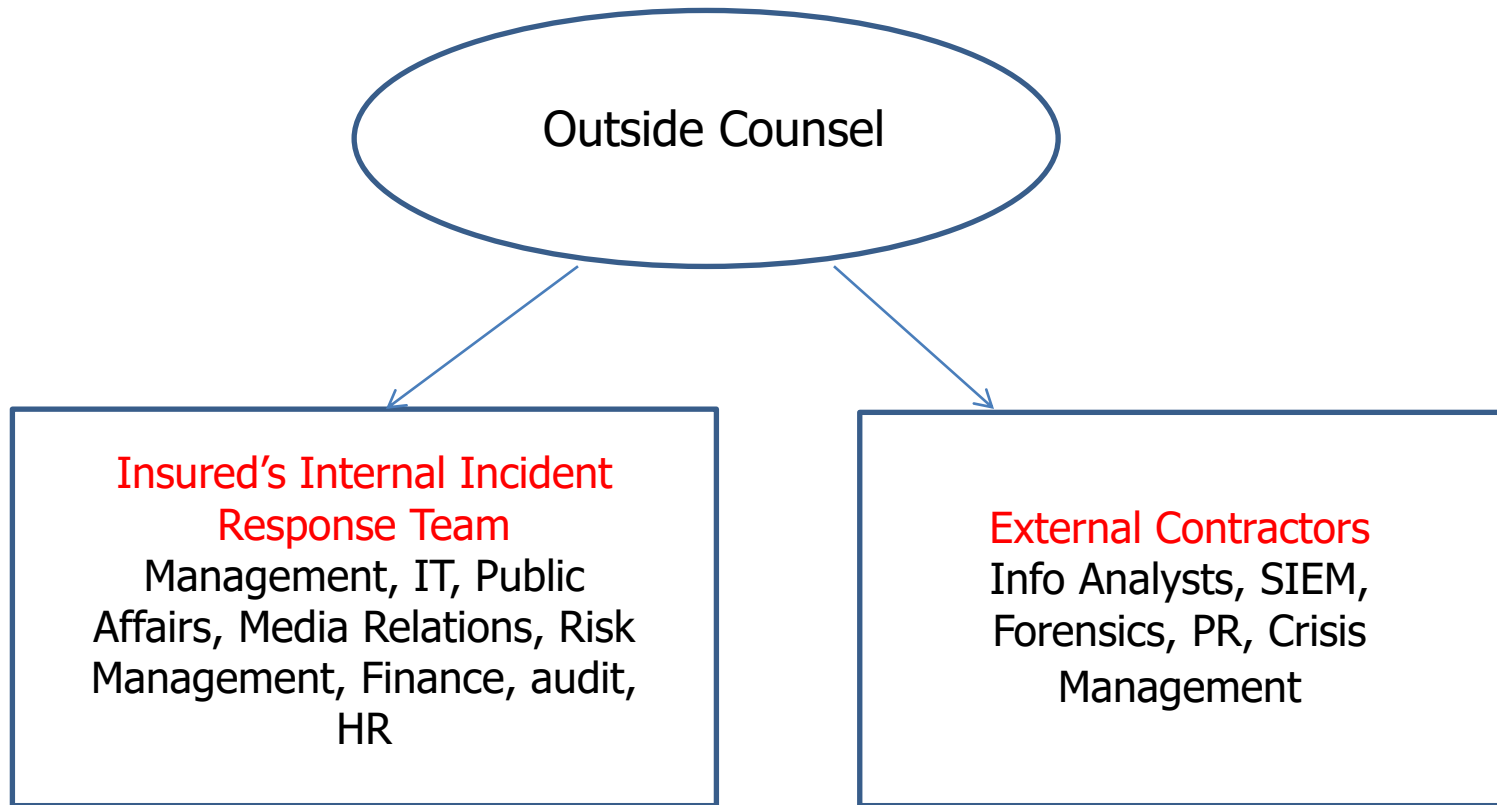
**312.606.7747**



# Typical Post-Data Breach Event Sequence

- **Breach**
- **Initial Investigation (Need Protection)**
- **Notification**
- **Additional Investigation/Litigation and/or Regulatory Action (Need Protection)**

# Model Data Breach Response Investigative Team





# When & Why to Engage Outside Counsel?

- **Early**
- **Why**
  - Increased Flexibility to uncover root cause of breach
  - Avoid careless creation of documents
  - Litigation hold notices /preserve existing documents
  - Restrict circulation of investigation materials



# Legal Standards to Which You are Held

- **Statutory – e.g., GLB, SOX**
- **State laws – Notification, Consumer Protection**
- **Regulations**
- **Guidelines**
- **Industry Standards**
- **Best Practices**
- **“Reasonableness”**
- **Whatever the FTC says, with hindsight**

# States Have Not Stood Idly By

- **State Trade Secret Statutes**
- **Baby FTC Acts combat IP theft using unfair competition law**
- **Generally provide for a private right of action**
- **Provide varying levels of specificity regarding the application of unfair competition as it related to misappropriated IT**

# Traditional Theories of Liability

- **Liability for breach of Personally Identifiable Information (“PII”) & Protected Health Info. (“PHI”)**
  - Violation of privacy laws and common law rights
  - Breach of contract
  - Negligence: 11/11/14, Connecticut Supreme Court held that HIPAA may provide applicable standard of care for negligence claim.
  - Fraud
  - Unfair trade practices
- **Recovery**
  - Compensatory damages
  - Treble damages
  - Attorneys’ fees
  - Punitive damages, Statutory Fines

# Playing Defense: Prepare Well!

- **Prioritize Data Based On Risks**
- **Comprehensive Data-Governance Plan**
- **Incident Response Plan**
- **Table-Top Exercises**
- **Policies**
  - Access, Use, Transmission
  - Email
  - Mobile, Laptops, Tablets
  - Social Media
- **Communication**
- **Implementation: Stewards**
- **Training**
- ***Metrics***
- ***Use Attorney-Client Privilege When Possible***

# Implement Compliant Corporate Policies

- **Access, Use, Transmission**

- User ID and Passwords
- Access Protocols
- Third-Party Access
- Employee Screening
- Dedicated Devices
- Device Management
- Laptop Restrictions
- Business Uses
- Non-Disclosure
- Software Restrictions
- Data Backups
- Encryption

# Implement Compliant Corporate Policies

- **Email**

- Primarily for Business and Permissible Content
- Confidential or Proprietary Data Secured and Encrypted
- No Clicking on Suspicious Emails, Docs, and/or Links
- No Expectation of Privacy
- Retained if Business Record
- Retained in Accordance With Record Retention Policies
- No ISPs for Company Business
- Compliance With Statutory or Regulatory Requirements
- No Expectation of Privacy

# Implement Compliant Corporate Policies

- **Mobile / BYOD**

- Acceptable Use Only
- No Access of Non-Work Websites
- Permitted and Prohibited Apps
- Permitted Operating Systems
- No Direct Connections to Network
- Proper and Authorized IT Support and Maintenance
- Strong Password Protected
- Automatic Locks
- Remotely Wiped if Lost, Employee Terminated, or Breach



# Data Management is Key: Reduce and Destroy Bad Data

- **Email**
  - **Must be part of document retention/destruction policy.**
  - **Stop preserving exhibits for your opponent.**
- **Avoid Creating Smoking Guns**
- **Routine Destruction Programs**
- **Attorney-Client Privilege**
- **Protect Self-Critical Analyses, Investigations**
- **Preemptive Data Security**
- **APTs**
- **Social Media – New and Leading Cause of Malware**

# Best Practices

- **How do you protect your customers and your firm?**
  - E-Mail Encryption
  - Password Protection – Change Frequently
  - Construct and Maintain an Appropriate Firewall
  - Back-up your Data
  - Avoid Public Wi-Fi
  - Understand how to wipe your smartphone
  - Educate your clients
  - Be Proactive - Constantly review and
    - update your systems

# Best Practices

## Are your vendors secure?

- Due diligence may be mandatory (GLB, HIPAA)
- Questionnaires are required at minimum
- May need to visit and verify if high risk

-Components to review and assess:

- Data leakage protection
- Monitoring, alerting, and enforcement

- Forensics/Investigation
- External device control
- Encryption
- Management and support
- Reporting and compliance
- Identity management
- Company profile

# Intensified Ransomware

- **Coverage: Extortion and/or Business Interruption**
- **Emerging Virulent Variants:**
  - Cryptolocker, Torrentlocker, CryptoFortress
  - Encryption of any file found through wildcard searches
  - Encryption of files in network shares
  - Volume shadow copies deleted to prevent restoration
  - "Freemium" offer to convince victims that they can recover files
- **Damages and Harm Expanded Exponentially**
  - More data at risk
  - Ransom paid in bitcoins
  - Amounts increasing - hundreds to thousands
  - Repeated ransom demands - "Thanks, but we want more."

# Questions?

**Hillard M. Sterling  
Clausen Miller P.C.  
10 South LaSalle Street  
Chicago, Illinois 60603  
hsterling@clausen.com  
312.606.7747**

# ***CYBERFORENSICS & FORENSICS PRINCIPLES***

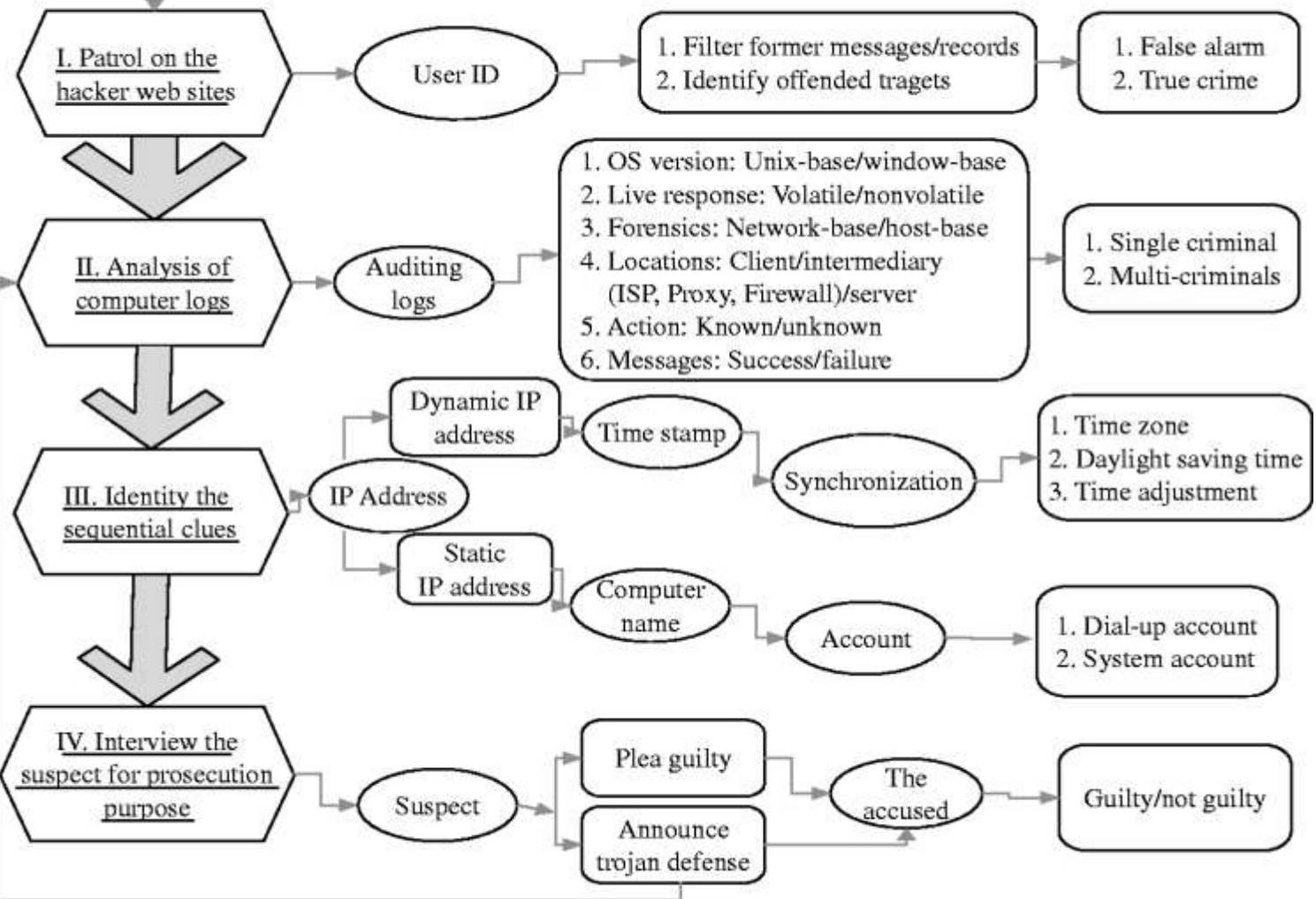
*Slater Technologies*

- 1. Information form arrested criminal
- 2. Trace back habitat on the internet

Procedures

Processes

Outputs



Phase:

Element:

Option:



# **Guide to Computer Forensics and Investigations Fourth Edition**

## *Chapter 1*

### *Computer Forensics and Investigations as a Profession*



# Objectives

- Define computer forensics
- Describe how to prepare for computer investigations and explain the difference between law enforcement agency and corporate investigations
- Explain the importance of maintaining professional conduct

# Understanding Computer Forensics

- **Computer forensics**
  - Involves obtaining and analyzing digital information
    - As evidence in civil, criminal, or administrative cases
- **FBI Computer Analysis and Response Team (CART)**
  - Formed in 1984 to handle the increasing number of cases involving digital evidence

# Understanding Computer Forensics (continued)

- **Fourth Amendment** to the U.S. Constitution
  - Protects everyone's rights to be secure in their person, residence, and property
    - From search and seizure
  - **Search warrants** are needed

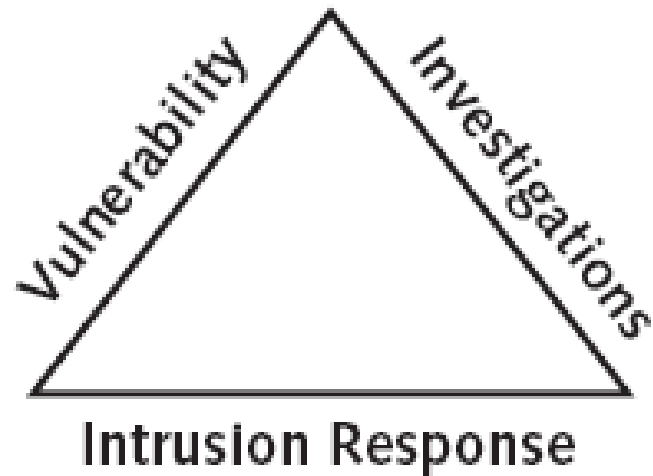
# Computer Forensics Versus Other Related Disciplines

- Computer forensics
  - Investigates data that can be retrieved from a computer's hard disk or other storage media
- Network forensics
  - Yields information about how a perpetrator or an attacker gained access to a network
- **Data recovery**
  - Recovering information that was deleted by mistake
    - Or lost during a power surge or server crash
  - Typically you know what you're looking for

# Computer Forensics Versus Other Related Disciplines (continued)

- Computer forensics
  - Task of recovering data that users have hidden or deleted and using it as evidence
  - Evidence can be **inculpatory** (“incriminating”) or **exculpatory**
- **Disaster recovery**
  - Uses computer forensics techniques to retrieve information their clients have lost
- Investigators often work as a team to make computers and networks secure in an organization

# Computer Forensics Versus Other Related Disciplines (continued)



**Figure 1-2** The investigations triad

# Computer Forensics Versus Other Related Disciplines (continued)

- **Enterprise network environment**
  - Large corporate computing systems that might include disparate or formerly independent systems
- **Vulnerability assessment and risk management group**
  - Tests and verifies the integrity of standalone workstations and network servers
  - Professionals in this group have skills in **network intrusion detection and incident response**

# Computer Forensics Versus Other Related Disciplines (continued)

- **Litigation**
  - Legal process of proving guilt or innocence in court
- **Computer investigations** group
  - Manages investigations and conducts forensic analysis of systems suspected of containing evidence related to an incident or a crime



# Understanding Case Law

- Technology is evolving at an exponential pace
  - Existing laws and statutes can't keep up change
- Case law used when statutes or regulations don't exist
- Case law allows legal counsel to use previous cases similar to the current one
  - Because the laws don't yet exist
- Each case is evaluated on its own merit and issues

# Developing Computer Forensics Resources

- You must know more than one computing platform
  - Such as DOS, Windows 10, Windows 11, Linux, Macintosh, and current Windows platforms
- Join as many computer user groups as you can
- **Computer Technology Investigators Network (CTIN)**
  - Meets monthly to discuss problems that law enforcement and corporations face

# Developing Computer Forensics Resources (continued)

- **High Technology Crime Investigation Association (HTCIA)**
  - Exchanges information about techniques related to computer investigations and security
- User groups can be helpful
- Build a network of computer forensics experts and other professionals
  - And keep in touch through e-mail
- Outside experts can provide detailed information you need to retrieve digital evidence

# Preparing for Computer Investigations

- Computer investigations and forensics falls into two distinct categories
  - Public investigations
  - Private or corporate investigations
- Public investigations
  - Involve government agencies responsible for criminal investigations and prosecution
  - Organizations must observe legal guidelines
- Law of **search and seizure**
  - Protects rights of all people, including suspects

# Preparing for Computer Investigations (continued)

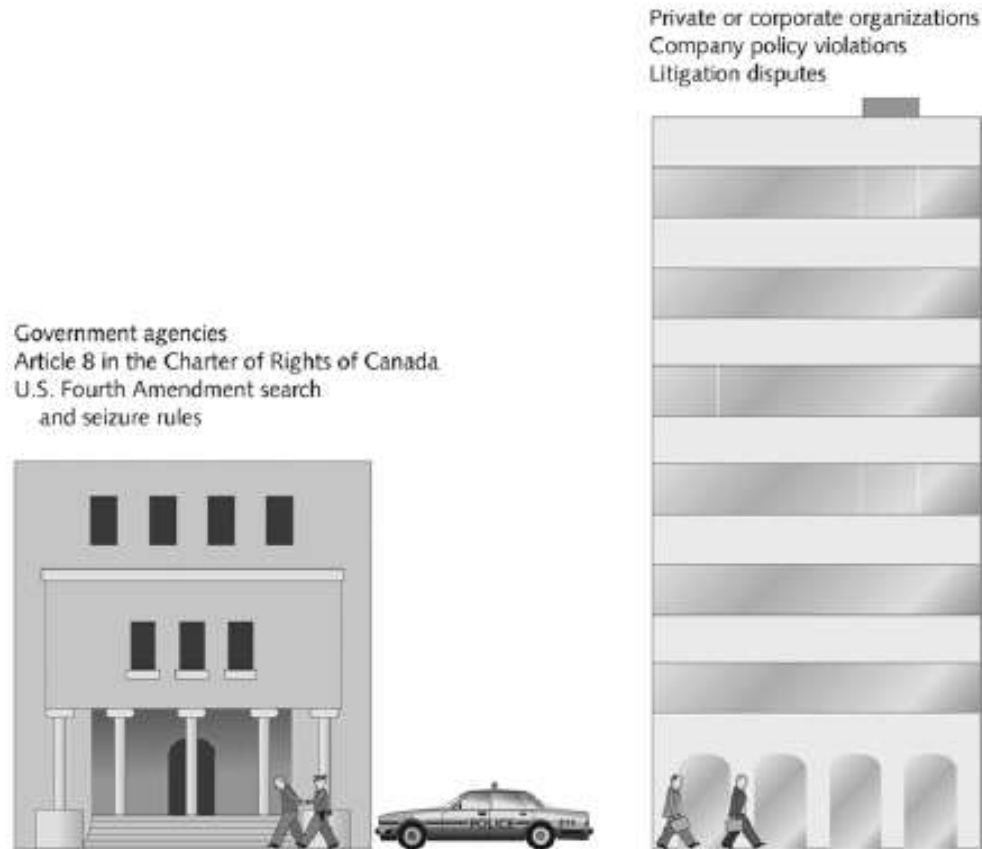


Figure 1-5 Public and private investigations

# Preparing for Computer Investigations (continued)

## The 4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

# Preparing for Computer Investigations (continued)

- Private or corporate investigations
  - Deal with private companies, non-law-enforcement government agencies, and lawyers
  - Aren't governed directly by **criminal law** or Fourth Amendment issues
  - Governed by internal policies that define expected employee behavior and conduct in the workplace
- Private corporate investigations also involve litigation disputes
- Investigations are usually conducted in civil cases

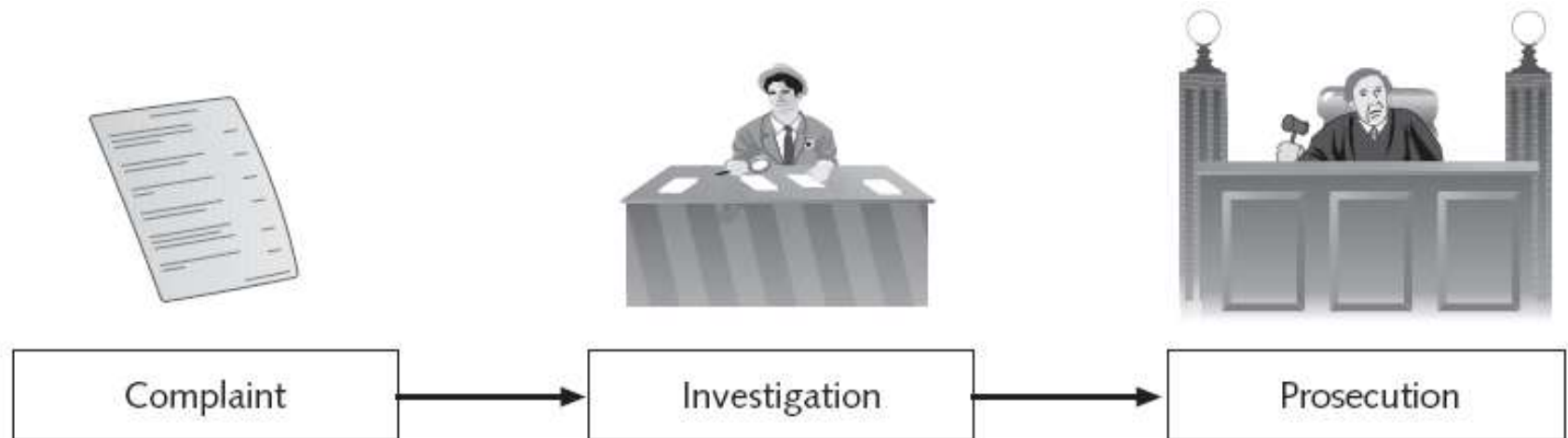
# Understanding Law Enforcements Agency Investigations

- In a **criminal case**, a suspect is tried for a criminal offense
  - Such as burglary, murder, or molestation
- Computers and networks are only tools that can be used to commit crimes
  - Many states have added specific language to criminal codes to define crimes involving computers
- Following the legal process
  - Legal processes depend on local custom, legislative standards, and rules of evidence



# Understanding Law Enforcements Agency Investigations (continued)

- Following the legal process (continued)
  - Criminal case follows three stages
    - The complaint, the investigation, and the prosecution



**Figure 1-7** The public-sector case flow

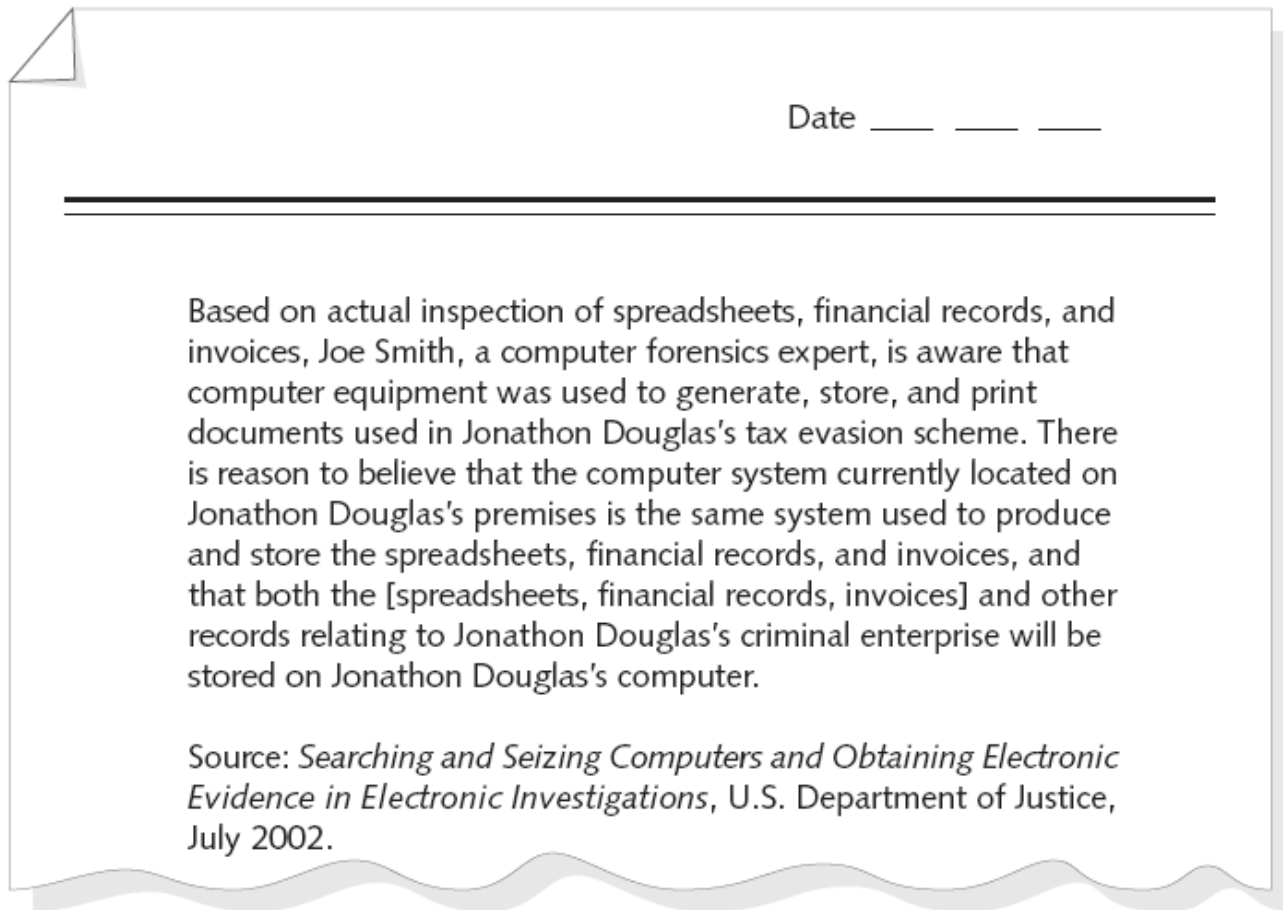
# Understanding Law Enforcements Agency Investigations (continued)

- Following the legal process (continued)
  - A criminal case begins when someone finds evidence of an illegal act
  - Complainant makes an **allegation**, an accusation or supposition of fact
  - A police officer interviews the complainant and writes a report about the crime
    - **Police blotter** provides a record of clues to crimes that have been committed previously
  - Investigators delegate, collect, and process the information related to the complaint

# Understanding Law Enforcements Agency Investigations (continued)

- Following the legal process (continued)
  - After you build a case, the information is turned over to the prosecutor
  - **Affidavit**
    - Sworn statement of support of facts about or evidence of a crime
      - Submitted to a judge to request a search warrant
    - Have the affidavit **notarized** under sworn oath
  - Judge must approve and sign a search warrant
    - Before you can use it to collect evidence

# Understanding Law Enforcements Agency Investigations (continued)



**Figure 1-8** Typical affidavit language

# Understanding Corporate Investigations

- Private or corporate investigations
  - Involve private companies and lawyers who address company policy violations and litigation disputes
- Corporate computer crimes can involve:
  - E-mail harassment
  - Falsification of data
  - Gender and age discrimination
  - Embezzlement
  - Sabotage
  - **Industrial espionage**

# Understanding Corporate Investigations (continued)

- Establishing company policies
  - One way to avoid litigation is to publish and maintain policies that employees find easy to read and follow
  - Published company policies provide a **line of authority**
    - For a business to conduct internal investigations
  - Well-defined policies
    - Give computer investigators and forensic examiners the authority to conduct an investigation
- Displaying Warning Banners
  - Another way to avoid litigation

# Understanding Corporate Investigations (continued)

- Displaying Warning Banners (continued)
  - **Warning banner**
    - Usually appears when a computer starts or connects to the company intranet, network, or virtual private network
    - Informs end users that the organization reserves the right to inspect computer systems and network traffic at will
    - Establishes the right to conduct an investigation
  - As a corporate computer investigator
    - Make sure company displays well-defined warning banner

# Understanding Corporate Investigations (continued)

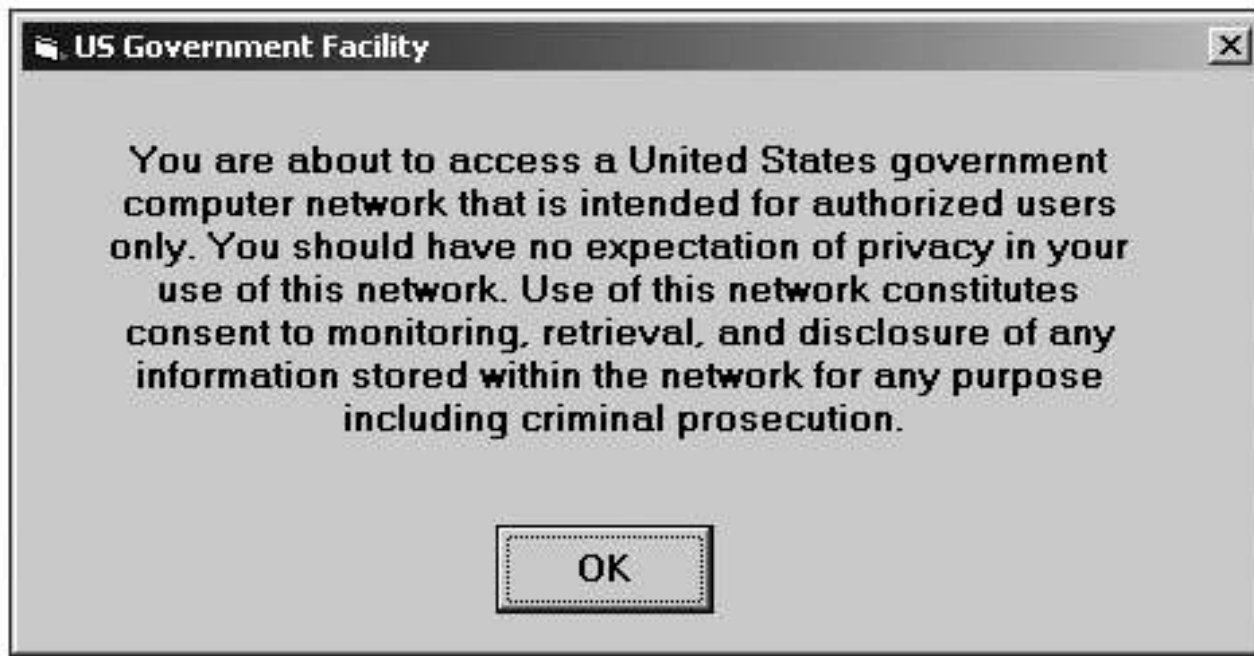


Figure 1-9 A sample warning banner



# Understanding Corporate Investigations (continued)

- Designating an authorized requester
  - **Authorized requester** has the power to conduct investigations
  - Policy should be defined by executive management
  - Groups that should have direct authority to request computer investigations
    - Corporate Security Investigations
    - Corporate Ethics Office
    - Corporate Equal Employment Opportunity Office
    - Internal Auditing
    - The general counsel or Legal Department

# Understanding Corporate Investigations (continued)

- Conducting security investigations
  - Types of situations
    - Abuse or misuse of corporate assets
    - E-mail abuse
    - Internet abuse
  - Be sure to distinguish between a company's abuse problems and potential criminal problems
  - Corporations often follow the **silver-platter doctrine**
    - What happens when a civilian or corporate investigative agent delivers evidence to a law enforcement officer

# Understanding Corporate Investigations (continued)

- Distinguishing personal and company property
  - Many company policies distinguish between personal and company computer property
  - One area that's difficult to distinguish involves PDAs, cell phones, and personal notebook computers
  - The safe policy is to not allow any personally owned devices to be connected to company-owned resources
    - Limiting the possibility of commingling personal and company data

# Maintaining Professional Conduct

- **Professional conduct**
  - Determines your credibility
  - Includes ethics, morals, and standards of behavior
- Maintaining objectivity means you must form and sustain unbiased opinions of your cases
- Maintain an investigation's credibility by keeping the case confidential
  - In the corporate environment, confidentiality is critical
- In rare instances, your corporate case might become a criminal case as serious as murder

# Maintaining Professional Conduct (continued)

- Enhance your professional conduct by continuing your training
- Record your fact-finding methods in a journal
- Attend workshops, conferences, and vendor courses
- Membership in professional organizations adds to your credentials
- Achieve a high public and private standing and maintain honesty and integrity

# Summary

- Computer forensics applies forensics procedures to digital evidence
- Laws about digital evidence established in the 1970s
- To be a successful computer forensics investigator, you must know more than one computing platform
- Public and private computer investigations are different

# Summary (continued)

- Use warning banners to remind employees and visitors of policy on computer and Internet use
- Companies should define and limit the number of authorized requesters who can start an investigation
- Silver-platter doctrine refers to handing the results of private investigations over to law enforcement because of indications of criminal activity
- Computer forensics investigators must maintain professional conduct to protect their credibility

# ***HOW TO BE ANONYMOUS ONLINE***

*Slater Technologies*



# Presentation Abstract

- In the day and age of big Data Breaches and loss of privacy, many people wonder how they can do a better job of guarding their privacy and their data, and possibly even attempting to be invisible or anonymous when they use the Internet. This presentation will cover the challenges of privacy, and the methods and tools that can be used to allow Internet users become anonymous and do a better job of guarding their digital privacy.

# How to Be Anonymous Online

## Agenda

- Introduction
- Legal Stuff
- The Problem
- Why Would You Want to Be Anonymous Online?
- 17 Steps to Being Completely Anonymous Online
- 17 Essential Tools to Protect Your Online Identity, Privacy
- Other Threats to Your Privacy and Identity – Life in The Surveillance Society
- Other Forms of Accomplishing Anonymity in Your Daily Life
- 10 Tips for Data Privacy in Businesses
- Advantages and Disadvantages
- Parting Thoughts
- Conclusion
- Questions
- References

# Introduction

- The creators of the ARPANET (1969) which evolved into the Internet (1983) created something that was designed to be simple, reliable, platform-independent, and perform well. The Internet population had 50 million users in less than four years, and today there are over 2.5 billion on the Internet. Since the Internet went “business critical” in 1997, lack of security and loss of privacy have been constant issues, and every year it has continued to get worse, leading to serious crimes involving hacking, identity theft, stalking, harassment, etc. It is no wonder then that many Internet users are pondering the idea of going online as anonymous users to protect their privacy. This presentation will address the problems related to lack of privacy, and how to plan and implement methods and tools to protect privacy. While many of these tools and techniques are free, it still requires regular efforts and knowledge to stay abreast of the threats, as well as the selecting the right tool at the right time to meet each threat. Suffice it to say that privacy protection must become a new way of operating on the Internet and using your smartphone, if it is to be done successfully.

# LEGAL STUFF

# 4<sup>th</sup> Amendment

## U.S. Constitution – Bill of Rights

### The 4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

# Data Privacy Laws by State

## Why Storing and Protecting Data Is Important: Evaluating State Data Breach Notification Laws

### Holding Out

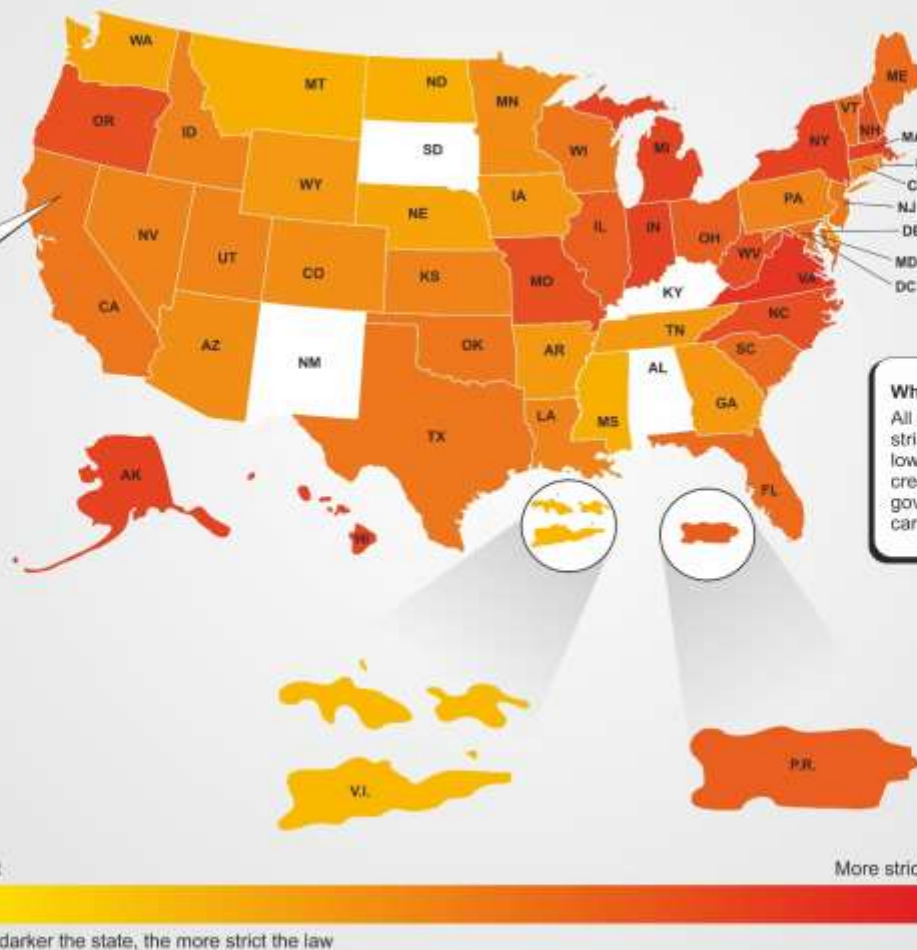
Four states have yet to enact a data breach notification law: Alabama, Kentucky, New Mexico and South Dakota.

### The Original Standard

California was the first state to enact data breach notification legislation. The law went into effect on July 1, 2003. Outside the scope used in this analysis, California's laws include provisions specifically for credit reporting agencies and for businesses owning or maintaining medical data. Other states carry these provisions as well.

### Why Certain States Stand Out

All of the laws are strict, but the stricter laws include a relatively low bar triggering notification to credit reporting agencies and government entities. They also carry higher maximum fines.



Note: A score of zero means a data breach notification law does not exist in that state.

State	Score
AL	0
KY	0
NM	0
SD	0
V.I.	5
ND	6
MS	7
MT	7
NE	7
WA	7
AR	8
DE	8
GA	8
IA	8
TN	8
WY	8
AZ	9
CO	9
MN	9
CT	10
ID	10
KS	10
LA	10
NV	10
PA	10
RI	10
UT	10
CA	11
NJ	11
OK	11
TX	11
WI	11
DC	12
FL	12
MD	12
ME	12
SC	12
VT	12
IL	13
OH	13
P.R.	13
MO	14
NC	14
NH	14
OR	14
WV	14
AK	15
HI	15
IN	15
MA	15
MI	15
NY	15
VA	16

Less strict

More strict

Key: The darker the state, the more strict the law

imation

SOURCE: Imation Corp., based on evaluation of individual state laws obtained via National Conference of State Legislatures website and evaluations available publicly online from various law firms.  
NOTE: This information should not be considered legal advice and is not based on a legal analysis of the laws. Check with your attorney regarding laws applicable to your business.  
As of July 2, 2012.

imation is a global scalable storage and data security company. For more information, visit: [www.imation.com/compliancemap](http://www.imation.com/compliancemap)

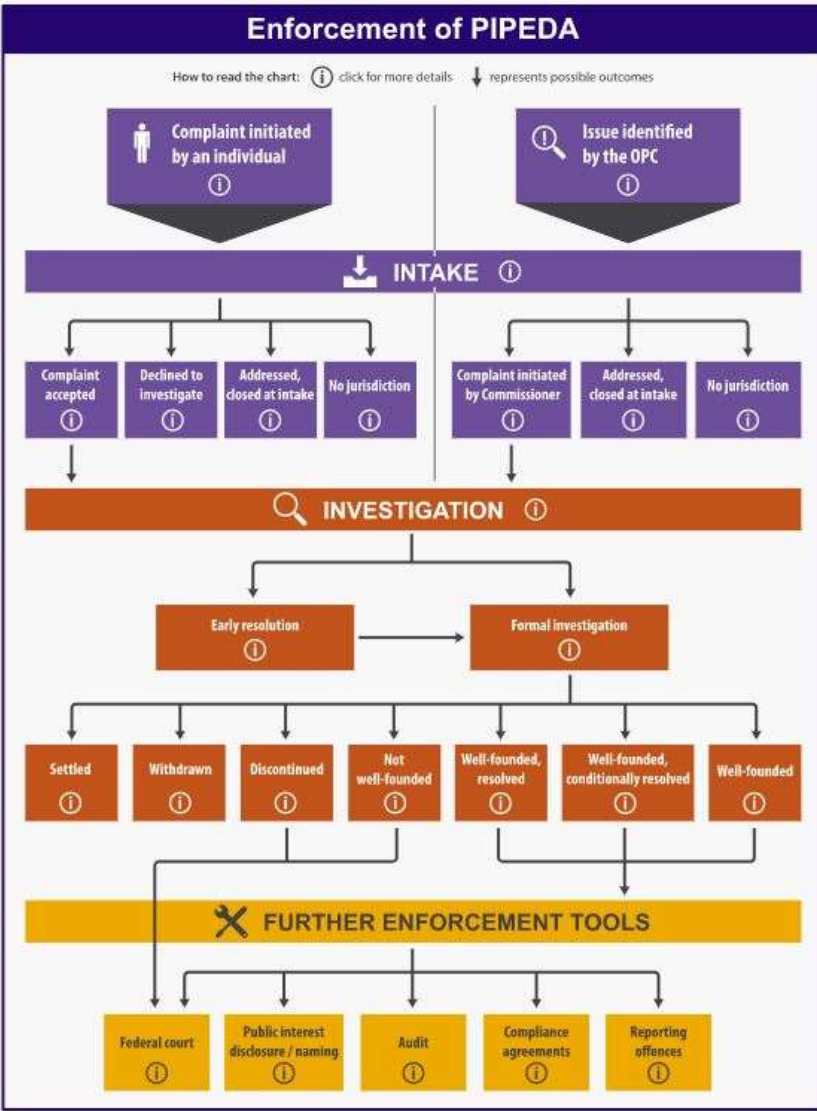
# Personal Information Protection and Electronic Documents Act (PIPEDA)

Canadian Federal  
Data Privacy  
Law Enforcement



PIPEDA has established 10 privacy principles for the collection, use, disclosure, and retention of personal information. These are good standards to follow in any province.

- Accountability
- Identifying purpose
- Consent
- Limiting collection
- Limiting use, disclosure, retention
- Accuracy
- Safeguards
- Openness
- Individual access
- Challenging compliance



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada

# March 6, 2018

- State of Illinois Attorney General Lisa Madigan noted that the number one consumer crime that was reported in 2017 was Identity Theft, and this surge was largely due to data breaches like the Equifax Data Breach of 2017.

1. Identity Theft (credit cards, data breaches, utilities, government document fraud) -- 2,511 complaints
2. Education (student loan debt, loan counseling, for-profit schools) -- 2,399 complaints
3. Consumer Debt (collection agencies, mortgages, banks) -- 2,395 complaints
4. Construction/Home Improvement (remodeling, roofs and gutters, heating and cooling, plumbing) -- 2,113 complaints
5. Telecommunications (cable and satellite TV, telemarketing, cell phones, phone service and repairs) -- 2,031 complaints
6. Promotions/Schemes (phone scams, lottery scams, investment schemes, phishing) -- 2,004 complaints
7. Used Auto Sales (as-is used cars, financing, advertising, warranties) -- 1,728 complaints
8. Internet/Mail Order Products (internet and catalog purchases, TV and radio advertising) -- 1,071 complaints
9. Motor Vehicle/Non-Warranty Repair (collision, engines, oil changes and tune-ups) -- 656 complaints
10. New Auto Sales (financing, defects, advertising) -- 629 complaints



# Why Would You Want to Be Anonymous Online?

- Self-Preservation
- Reputation Protection
- You're a private person
- The massive amount of news on Data Breaches and Hack Attacks is sinking in
- You want to take back control of your online life
- Paranoia



# The Biggest Threats to Your Online Privacy



## GOVERNMENT INTELLIGENCE

Many governments can easily collect information on their citizens.



Encrypt your data and use a VPN to keep your personal information private.



## BROWSER AND WEBSITE DATA SHARING

Web browsers routinely collect and retain certain basic information about your internet connection and online activity.



Regularly clear your cache and cookies and configure your browser to protect you from tracking.



## SEARCH ENGINES

Google and other search engines collect information about you every day, sometimes passing it on to third parties.



Use an alternative search engine that doesn't collect user data, such as DuckDuckGo.



## NON-SECURE WEBSITES

Your ISP and other third parties can view any information you exchange with a non-secure website.



Be sure to check if the websites you visit have URLs beginning with https://.



## MALWARE

Malware can create a backdoor, giving cybercriminals access to your device and data.



Invest in reliable anti-malware and firewall software for your computer and mobile devices.



## CLOUD STORAGE

Most popular cloud storage services reserve the right to share your data with the authorities.



Manually encrypt your files before uploading them to the cloud.



## SOCIAL MEDIA AND EMAIL CORRESPONDENCE

Some social media platforms sell your information to advertisers, while email service providers can be compelled to hand over your information to the government.



Stay informed on social media privacy policies and settings. Encrypt your email or use a privacy-oriented service like ProtonMail.

# Biggest Threats to Your Online Privacy

# The NSA – The Only Branch Of Government That Really Listens to You

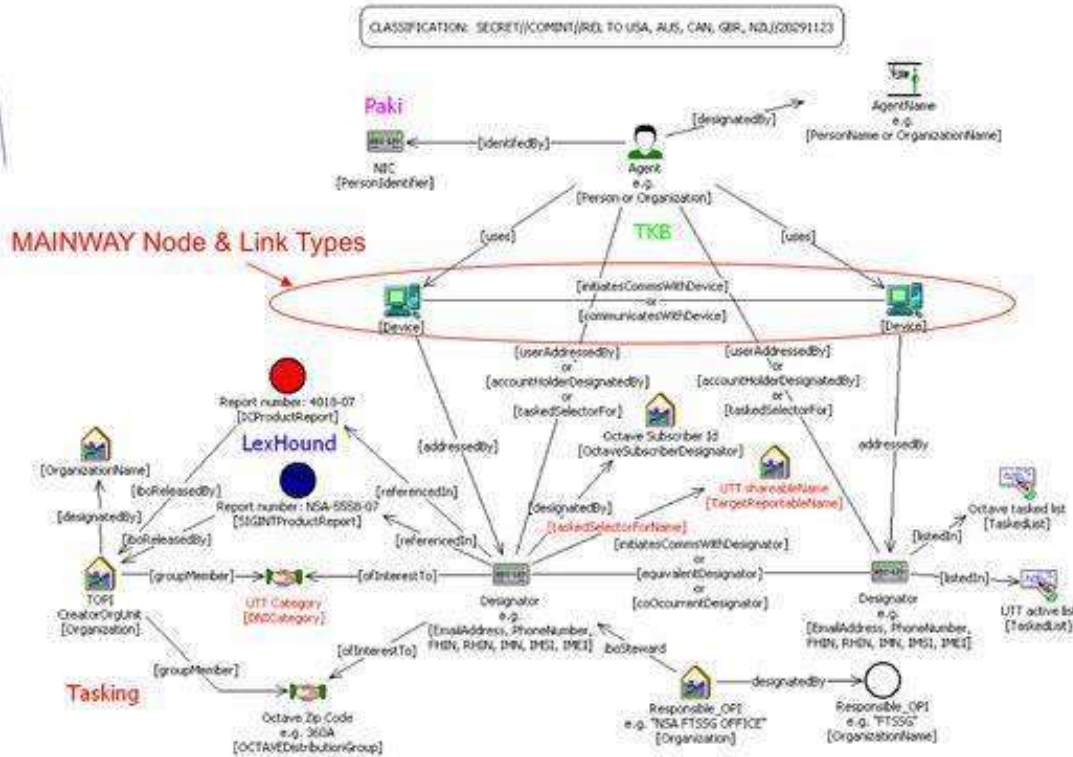
---



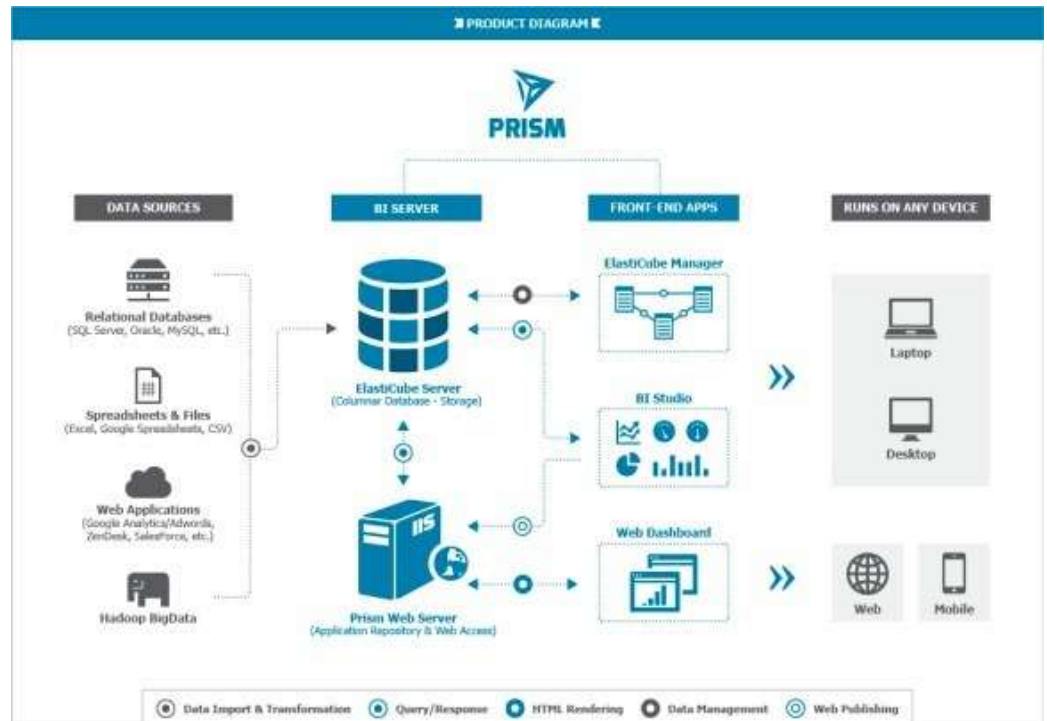
# NSA

SECRET//SI//REL TO USA, FVEY

## (S//SI//REL USA, FVEY) SYANPSE Data Model

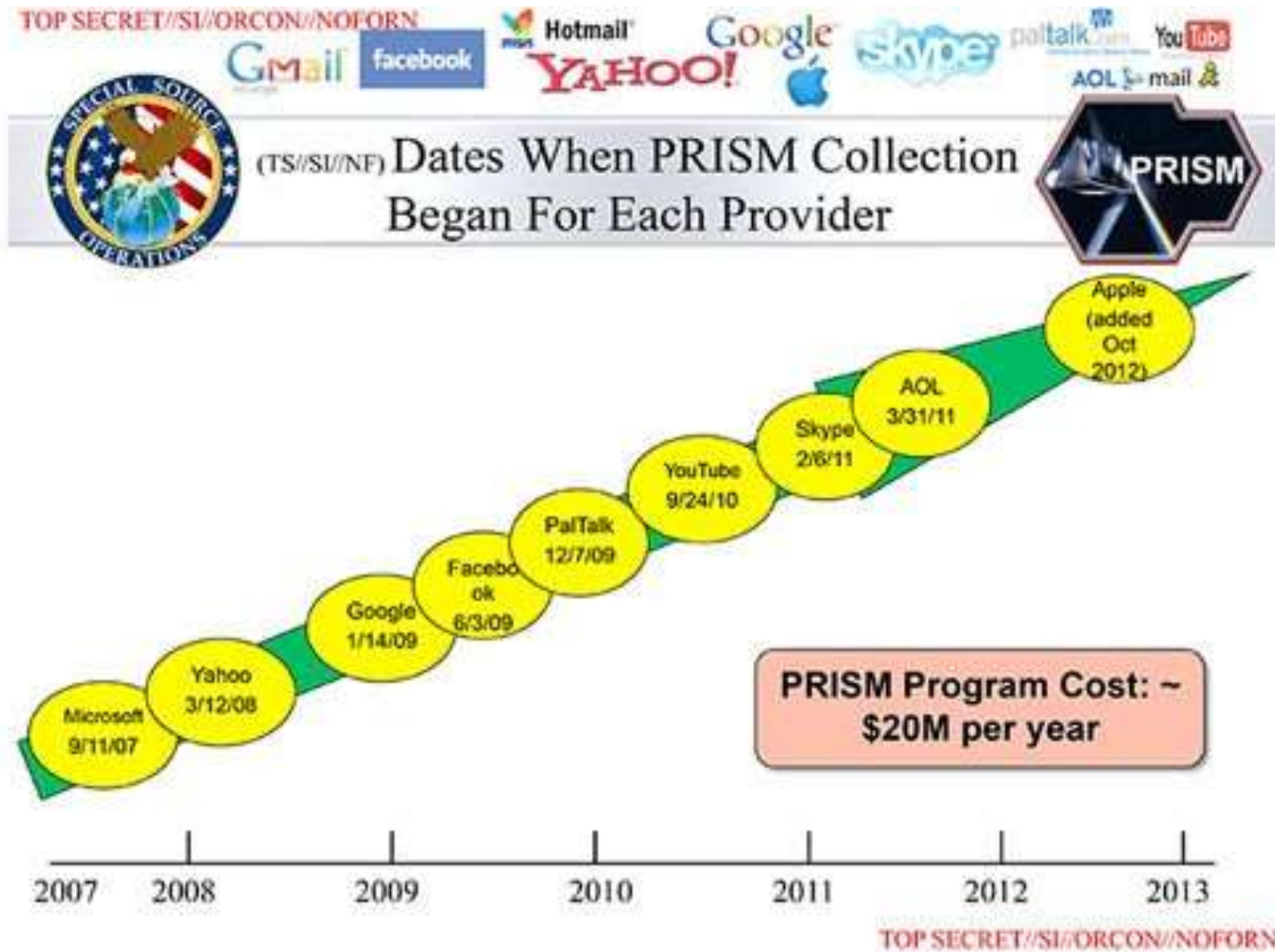


# NSA



Slater Technologies

# NSA and Large Internet Companies



NSA –  
*Always Be  
Careful  
What You  
Say or  
Enter  
Online*

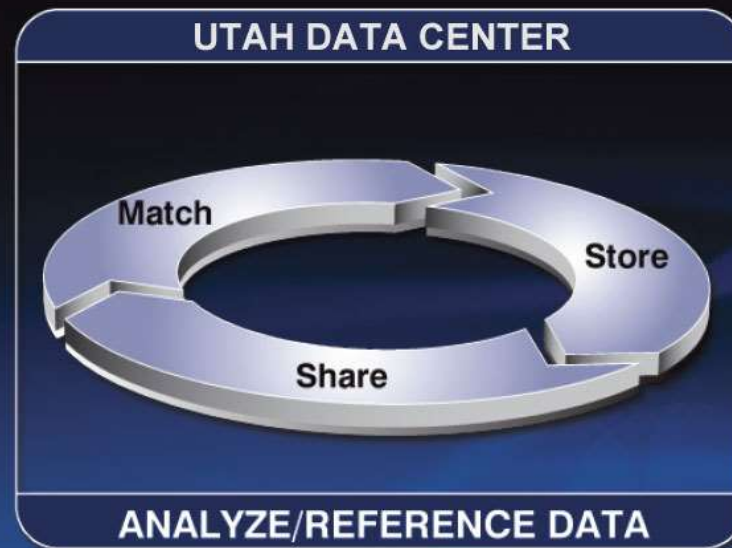


# What the NSA Collects

## Citizen Data

Website visits  
Internet searches  
Phone calls  
Skype calls  
Emails  
Text messages  
Credit card information  
Financial information  
Legal documents  
Travel documents  
Health records

Collect



Decide Act

## Operational Applications

Data Warehouse  
Surveillance and Monitoring  
Suspicious Activity Reporting (SAR)  
Terrorist Screening Center Alert

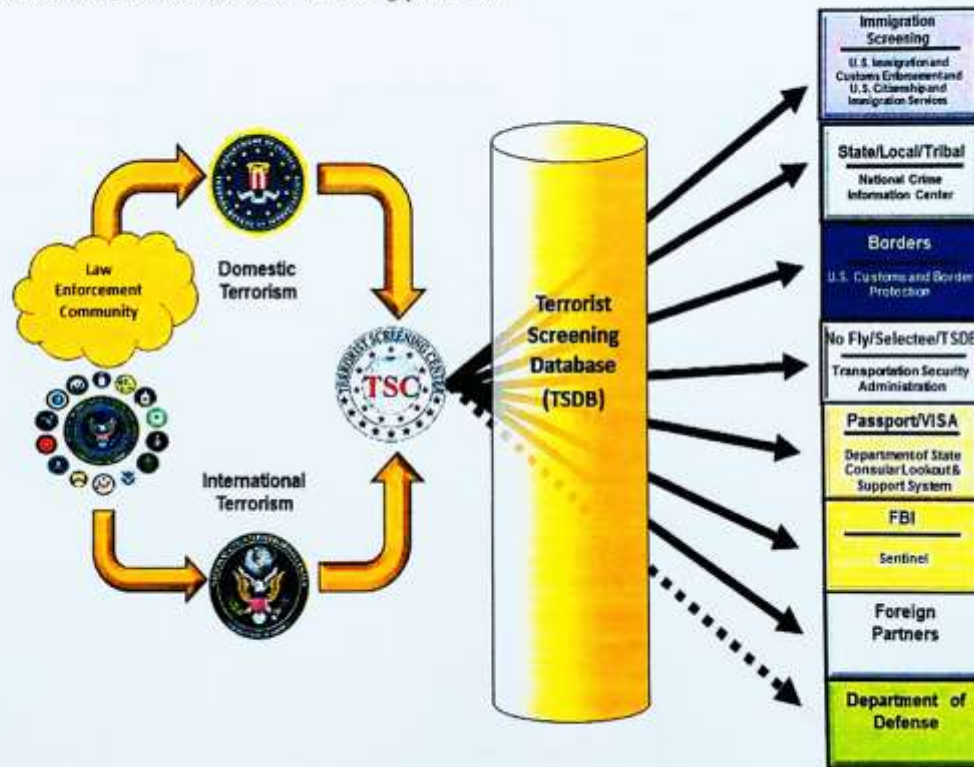
Source: nsa.gov/1.info

Slater Technologies



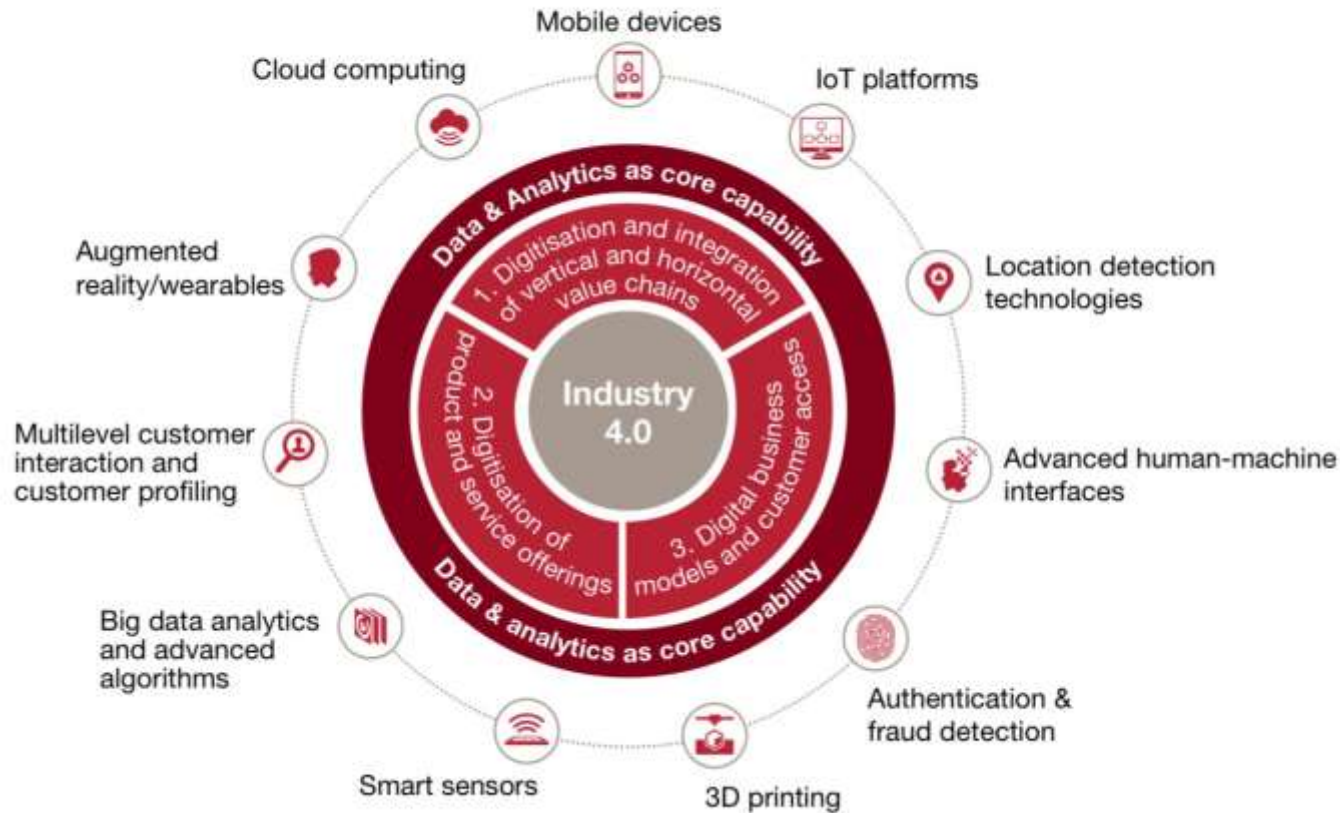
# NSA – Be Careful What You Say or Enter Online

1.32 **Collection, Nomination, Consolidation and the Use of the Terrorist Watchlist to Perform Screening Processes.** The following is a chart depicting the collection, TERRORIST nomination, consolidation and screening processes:



# Data Science and Data Analytics Is Driving Industry 4.0

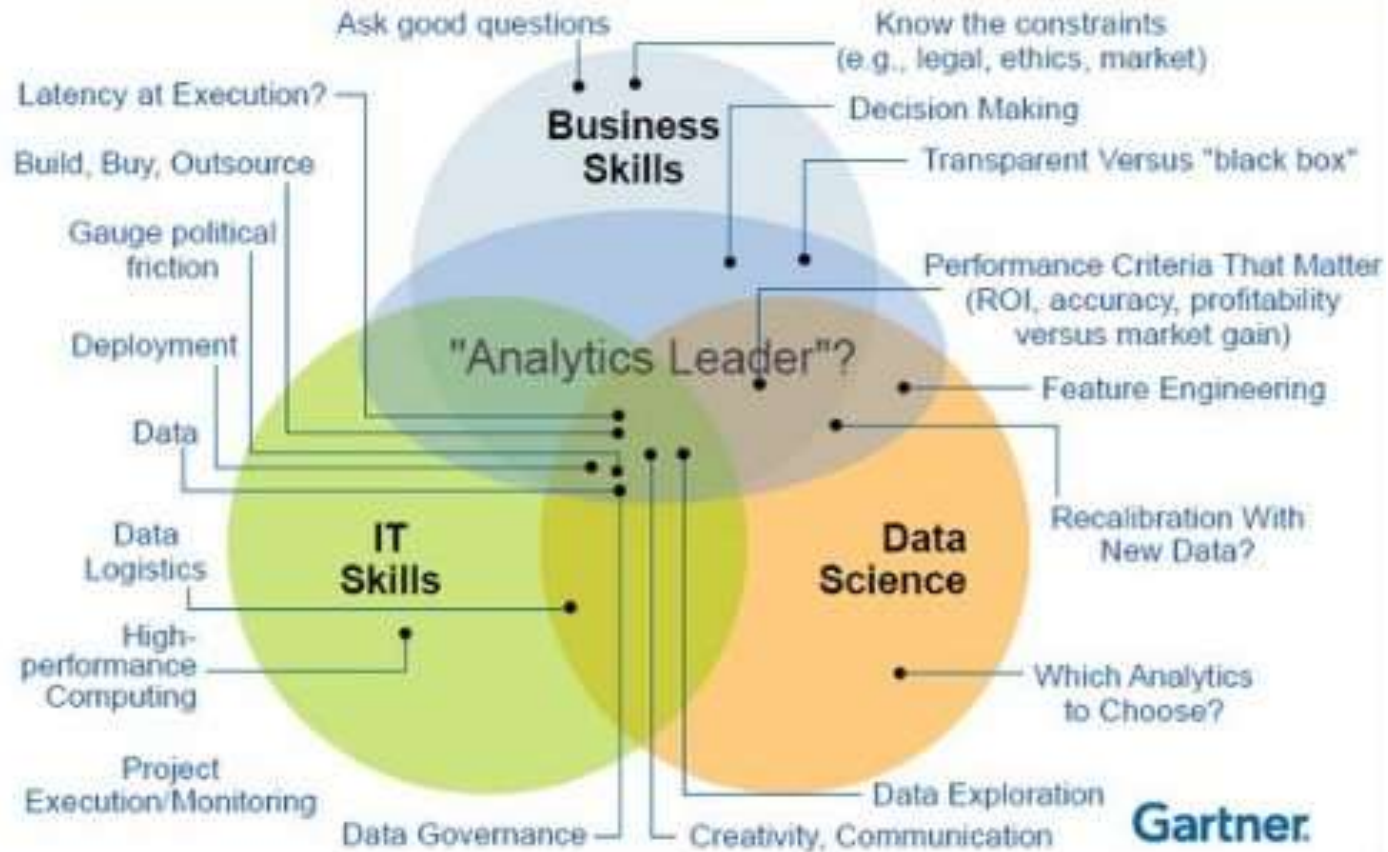
*Industry 4.0 framework and contributing digital technologies*



source pwc via @mikequindazzi

# Data Science Has Become a Huge Industry

## Driving the Success of Data Science Solutions: Skills, Roles and Responsibilities ...



# 17 Ways to Being Completely Anonymous Online

1. Find a safe country that values privacy
2. Get an anonymizing operating system
3. Use an anonymous VPN
4. Use Tor
5. Don't use plug-ins
6. Stick with HTTPS
7. Avoid the usual applications
8. Set up anonymous burner accounts
9. Never use credit cards
10. Test for DNS leaks and browser tracking
11. Test your overall privacy protection
12. Share files anonymously
13. Use a search engine that doesn't track your behavior
14. Turn off your location
15. Block Javascript
16. Keep your webmail private
17. Delete cookies and your browsing history

Source: 17 Ways to Being Completely Anonymous Online:

<https://www.csoonline.com/article/2975193/data-protection/9-steps-completely-anonymous-online.html>

Slater Technologies

# 17 Essential Tools to Protect Your Online Identity, Privacy

1. TPM
2. UEFI BIOS
3. Secure storage (encrypted)
4. Two-factor authentication
5. Logon account lockout
6. Remote find
7. Remote wipe
8. Secure VPN
9. Tor
10. Anonymity services
11. Anonymity hardware
12. Secure browsing
13. Secure e-mail
14. Secure chat
15. Secure payments
16. Secure file transfers
17. Anything Phil Zimmerman creates

Source: 17 Essential Tools to Protect Your Online Identity, Privacy:

<https://www.infoworld.com/article/3135324/security/17-essential-tools-to-protect-your-online-identity-and-privacy.html>

Slater Technologies

# THREE ADDITIONAL FREE TOOLS

# haveibeenpwned.com

The screenshot shows the homepage of haveibeenpwned.com. At the top, there is a navigation menu with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is a large white box containing the text ";--have i been pwned?". Below this is a sub-heading: "Check if you have an account that has been compromised in a data breach". A search bar is present with the placeholder text "email address" and a "pwned?" button. Below the search bar, four statistics are displayed: 270 pwned websites, 4,948,721,769 pwned accounts, 64,652 pastes, and 71,704,180 paste accounts. The "Top 10 breaches" section lists the following:

Icon	Count	Breach Name
Envelope	711,477,622	Online Spambot accounts
Envelope	593,427,119	Exploit.In accounts
Envelope	457,962,538	Anti Public Combo List accounts
Envelope	393,430,309	River City Media Spam List accounts
myspace	359,420,698	MySpace accounts
NetEase	234,842,089	NetEase accounts
LinkedIn	164,611,595	LinkedIn accounts

# panoptick.eff.org

Secure <https://panoptick.eff.org>

A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION [DONATE](#)

## PANOPTICK<sub>3.0</sub>

### Is your browser safe against tracking?

When you visit a website, online trackers and the site itself may be able to identify you – even if you’ve installed software to protect yourself. It’s possible to configure your browser to thwart tracking, but many people don’t know how.

Panoptick will analyze how well your browser and add-ons protect you against online tracking techniques. We’ll also see if your system is uniquely configured – and thus identifiable – even if you are using privacy-protective software.


[TEST ME](#)

Test with a real tracking company [whatatic](#)

Only [anonymous data](#) will be collected through this site.

Panoptick is a research project of the Electronic Frontier Foundation. [Learn more.](#)

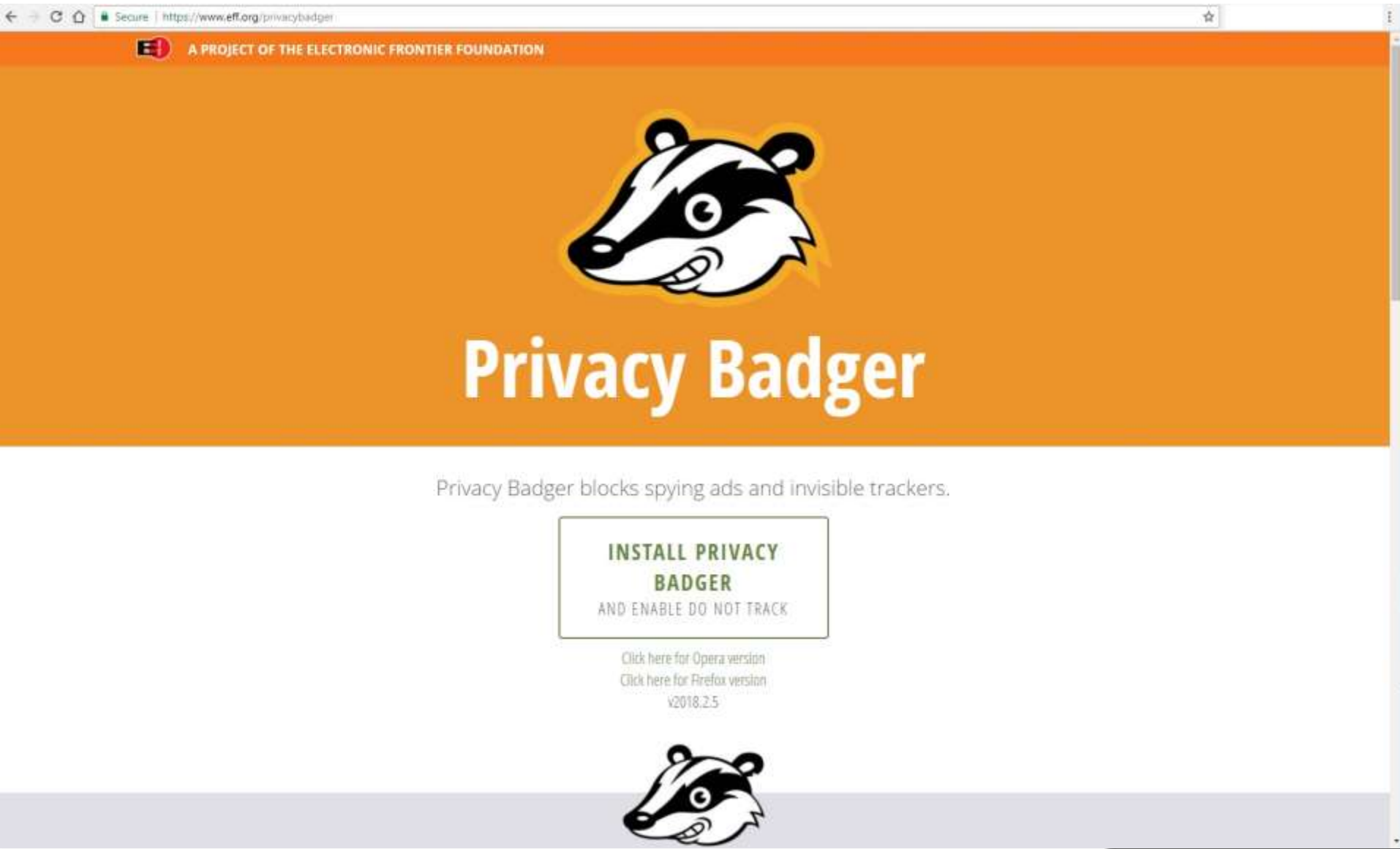
[SHARE ON FACEBOOK](#) [SHARE ON TWITTER](#) [SHARE ON GOOGLE+](#)

 A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION

[ABOUT PANOPTICK](#) [DONATE TO EFF](#) [CONTACT](#) [PRIVACY](#) [CC-LICENSE](#)




# www.eff.org/privacybadger



The screenshot shows a web browser window with the URL <https://www.eff.org/privacybadger>. The page features a large orange header with the Privacy Badger logo (a stylized badger head) and the text "Privacy Badger". Below the header, the text "A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION" is visible. The main content area is white and contains the text "Privacy Badger blocks spying ads and invisible trackers." followed by a call-to-action button that says "INSTALL PRIVACY BADGER AND ENABLE DO NOT TRACK". Below the button are two links: "Click here for Opera version" and "Click here for Firefox version v2018.2.5". At the bottom of the page, there is a smaller version of the Privacy Badger logo.

Secure | <https://www.eff.org/privacybadger>

**E** A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION




## Privacy Badger

Privacy Badger blocks spying ads and invisible trackers.

**INSTALL PRIVACY  
BADGER**  
AND ENABLE DO NOT TRACK

[Click here for Opera version](#)  
[Click here for Firefox version  
v2018.2.5](#)



# Other Threats to Your Privacy and Identity

## – Life in The Surveillance Society

- NSA
- FBI
- Local Police – Sting Ray
- Your Big Screen Digital TV
- Your Grocery Store
- Retail stores – everywhere you use a credit or debit card
- Your Cell Phone
- Internet of Things Devices (Think **Amazon Echo**)
- Surveillance Satellites
- Drones
- Private Eyes (Detectives)
- Nosey and Untrustworthy Neighbors
- Untrustworthy Family Members and Friends
- Bad Actors

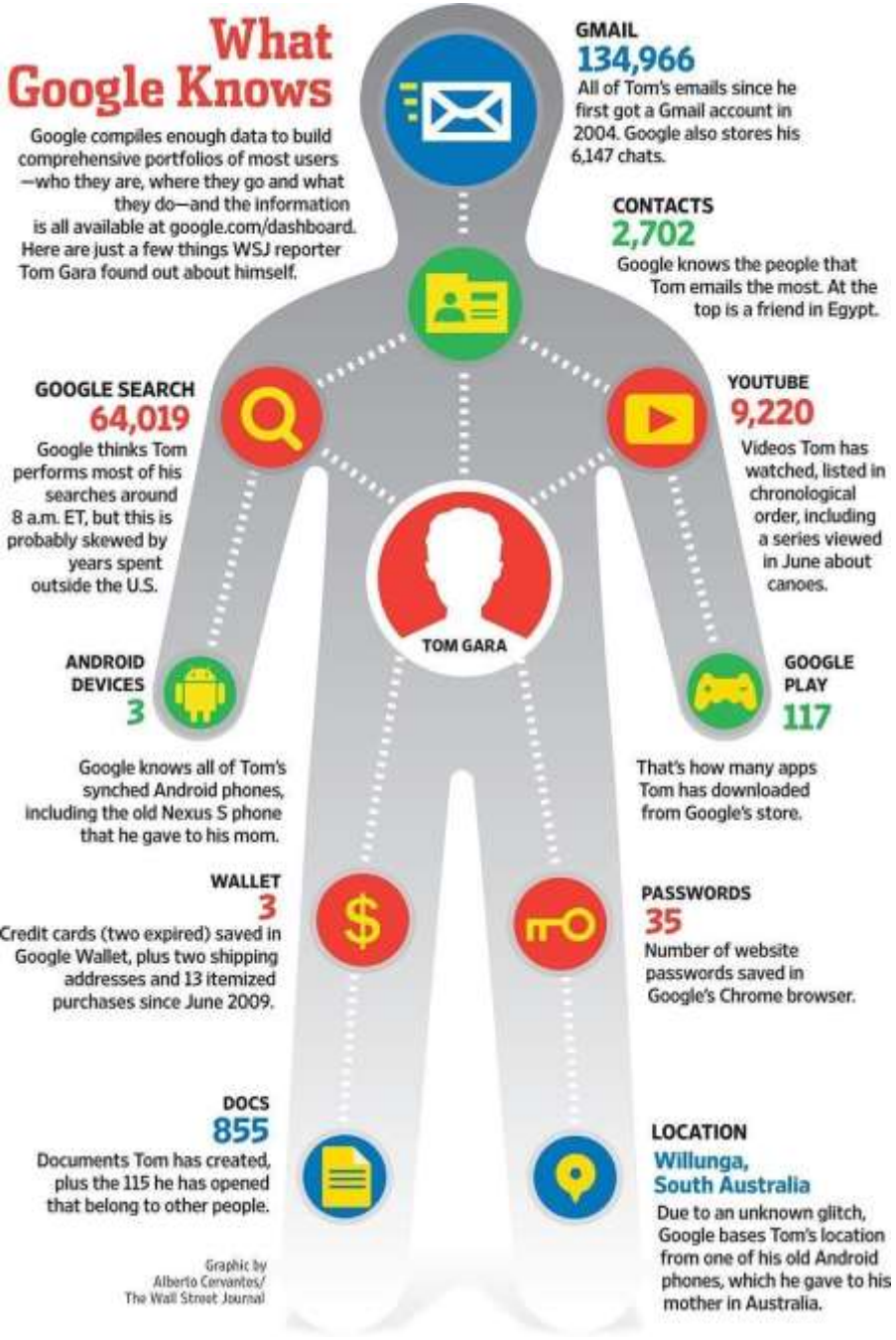


# Other Threats to Your Privacy and Identity

## – Life in The Surveillance Society



Slater Technologies

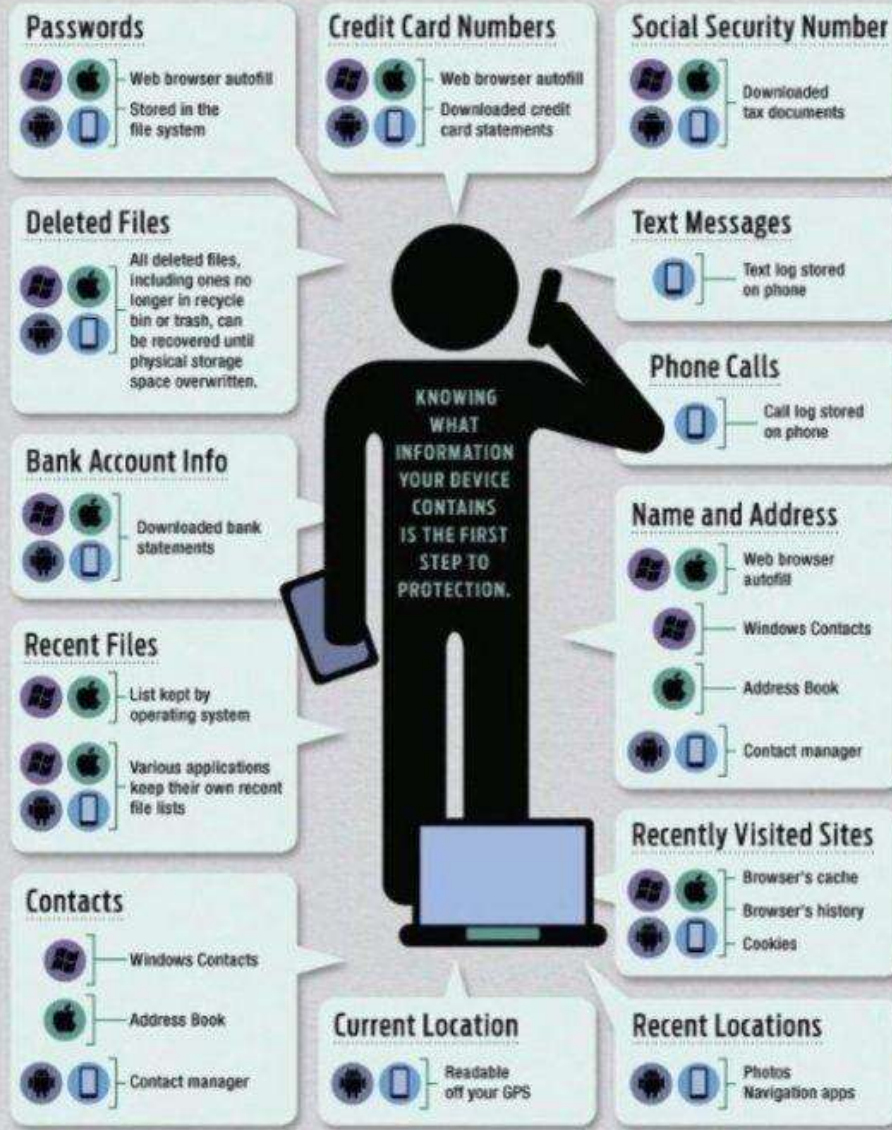
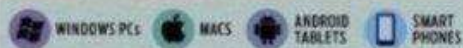


# Other Threats to Your Privacy and Identity – Life in The Surveillance Society



# WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.



# Other Threats to Your Privacy and Identity – Life in The Surveillance Society

# Other Forms of Accomplishing Anonymity in Your Daily Life

- Block your webcam on every computer you use.
- Vary your travel routines for work and recreation.
- Never throw anything away with your name and address on it.
- Get your mail and packages at a commercial package delivery store.
- Never give your phone numbers or address to anyone.
- Trust No One.



**TRUST  
NO ONE**

*Slater Technologies*

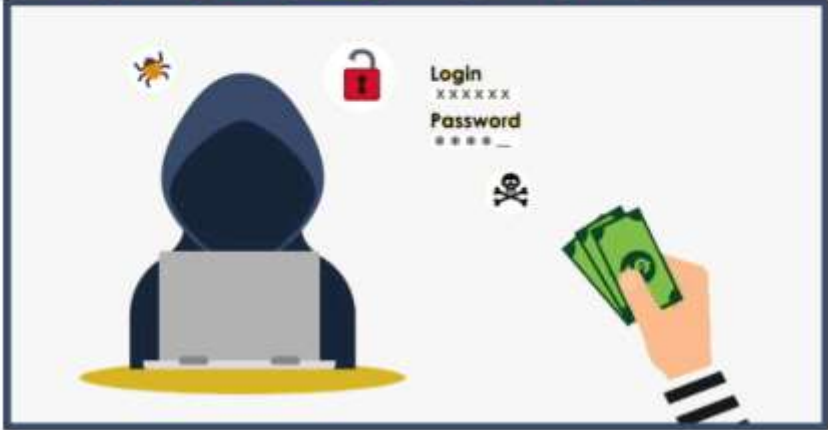
# Big Caution About the Dark Web

- Some people go Anonymous so they can do illegal things on The Dark Web
- If you know such people, let them know they can be caught and prosecuted

**Hacker Who Never Hacked Anyone Gets 33-Month Prison Sentence**

Tuesday, February 27, 2018 Mohit Kumar

Share Share Tweet Share Mail Share



A hacker who was arrested and pleaded guilty last year—not because he hacked someone, but for creating and selling a remote access trojan that helped cyber criminals—has finally been sentenced to serve almost three years in prison.

Taylor Huddleston, 26, of Hot Springs, Arkansas, [pleaded guilty](#) in July 2017 to one charge of aiding and abetting computer intrusions by building and intentionally selling a remote access trojan (RAT), called **NanoCore**, to hackers for \$25.

Huddleston was arrested in March, almost two months before the FBI raided his house in Hot Springs, Arkansas and left with his computers after 90 minutes, only to return eight weeks later with handcuffs.

This case is a rare example of the US Department of Justice (DOJ) charging someone not for actively using malware to hack victims' computers, but for developing and selling it to other cybercriminals.

Huddleston admitted to the court that he created his software knowing it would be used by other cybercriminals to break the law.

# Advantages and Disadvantages of Being Anonymous Online

## Advantages

- Risk avoidance.
- You get to have privacy and protect yourself and your personal data from the perils of data leakage.
- You will make it very difficult for the bad guys to steal your data and cause hurt and/or damage.
- You will become a data privacy subject matter expert and role model for your family, friends, and colleagues.

## Disadvantages

- It's a never-ending effort if you are actively using the Internet via a laptop, desktop, and or smartphone.
- Essentially, you must always stay vigilant to protect yourself.
- Well-intentioned people may find it difficult to reach you.
- People may think you have dark intentions for going anonymous
- People will think you are paranoid.



# 10 Privacy Tips for Businesses

1. Limit your collection and retention of personal information.
2. Know what personal information you collect, where you store it and what you do with it.
3. Ensure staff receive appropriate privacy protection training.
4. Limit and monitor access to personal information and take appropriate action when an employee accesses information without authorization.
5. Think twice before collecting sensitive personal information, such as driver's licenses.
6. Inform customers if you are using video surveillance.
7. Have a privacy policy and be upfront about your collection and use of personal information.
8. Protect personal information on laptops, USB keys and portable hard drives through technological safeguards such as encryption and password protection.
9. Respond to requests for access to personal information in a timely manner.
10. Make sure your customers know who to speak to if they have questions about privacy.

Source: 10 Privacy Tips for Businesses [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/tips-bus\\_info\\_201501/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/tips-bus_info_201501/)

Slater Technologies

# Parting Thoughts - 001:

U.S. Government Surveillance Capability Was Officially Revealed by U.S. Senator Frank Church (D. – Idaho) on Meet the Press in August 1975

- To understand the Genesis of U.S. Government Surveillance and the Power that has now accumulated in the **Executive Branch of the U.S. Federal Government**, please view this very brief **August 17, 1975** video with prescient comments about powerful and growing surveillance capabilities, **“Government Tyranny”** and **“the Abyss”** by **Senator Frank Church**, Chairman of the Senate Committee on Intelligence Activities on NBC’s Meet the Press.



Senator Frank Church

Source: NBC NEWS Meet the press Interview with Senator Frank Church  
Retrieved from <https://www.youtube.com/watch?v=YAG1N4a84Dk>

# Parting Thoughts - 002:

Amazon allows Echo to spy on you.



*Slater Technologies*

# Conclusion

- Threats to our privacy and PII are pervasive and ubiquitous
- You must work diligently to maintain your privacy, particularly in the U.S.
- There are modern tools and methods to help maintain your privacy and anonymity.
- Consequences of leaked PII are significant, especially when it's YOUR data
- As Cybersecurity professionals, we have a responsibility to understand the importance of and best methods for data and privacy protection.



# Questions?



*Slater Technologies*

# References

- AICPA. (2011). Privacy Maturity Model. A presentation presented to ISACA. Retrieved on March 5, 2018 from [https://www.kscpa.org/writable/files/AICPADocuments/10-229\\_aicpa\\_cica\\_privacy\\_maturity\\_model\\_finalebook.pdf](https://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf) .
- Clancy, H. (2012). "Where are U.S. data breach laws toughest? Check this map". An article published at ZDNet on August 28, 2012. Retrieved on March 4, 2018 from <http://www.zdnet.com/article/where-are-us-data-breach-laws-toughest-check-this-map/>.
- Frozen PII. (2018). Hacking IDentity. Retrieved on March 4, 2018 from <http://hackingidentity.com/index.php/226-2/> .
- Grimes, R. A. (2016). "17 essential tools to protect your online identity, privacy". Published by InfoWorld Online. Retrieved on March 4, 2018 from <https://www.infoworld.com/article/3135324/security/17-essential-tools-to-protect-your-online-identity-and-privacy.html> .
- Grimes, R. A. and Gralla, P. (2018). "17 Steps to Being Completely Anonymous Online". Published at CSO Online. Retrieved on March 4, 2018 from <https://www.csoonline.com/article/2975193/data-protection/9-steps-completely-anonymous-online.html> .
- Henderson, L. (2012). Anonymous File Sharing and Darknet: How to be a ghost in the machine. [Place of publication not identified] : [publisher not identified].
- Meet the Press. (1975). Senator Frank Church discusses U.S. Government Surveillance Capabilities on Meeting the Press August 17, 1975. Retrieved October 15, 2011 from <https://www.youtube.com/watch?v=YAG1N4a84Dk&t=2s> .
- Nadeau, M. (2017). "State of Cybercrime 2017: Security events decline, but not the impact." An article published in CSO Online on July 28, 2017. Retrieved on March 4, 2018 from <https://www.csoonline.com/article/3211491/security/state-of-cybercrime-2017-security-events-decline-but-not-the-impact.html> .

# References

- Office of the Privacy Commissioner of Canada. (2018). Privacy Toolkit for Businesses. Retrieved on March 4, 2018 from [https://www.priv.gc.ca/media/2038/guide\\_org\\_e.pdf](https://www.priv.gc.ca/media/2038/guide_org_e.pdf) .
- Office of the Privacy Commissioner of Canada. (2017). Enforcement of PIPEDA. Retrieved on March 4, 2018 from <https://www.priv.gc.ca/biens-act/compliance-framework/en/index> .
- Office of the Privacy Commissioner of Canada. (2018). Personal Information Protection and Electronic Documents Act (PIPEDA). Retrieved on March 4, 2018 from [https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda\\_brief/](https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/) .
- Robideau, R. (2014). Incognito Toolkit: Tools, Apps, and Creative Methods for Remaining Anonymous, Private, and Secure While Communicating, Publishing, Buying, and Researching Online. [Place of publication not identified] : [publisher not identified].
- Rumer, D. B. (2015). Digital Anonymity: Investigating the Open Threat by the Hidden User Retrieved on March 5, 2018 from <https://digitalcommons.apus.edu/cgi/viewcontent.cgi?article=1040&context=theses> .
- Schneier, B. (2016). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York, NY: W. W. Norton & Company.
- Sprenger, P. (1999). Sun on Privacy: 'GET OVER IT'. A Wired Magazine article from January 28, 1999. Retrieved on March 4, 2018 from <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> .
- Winkler, S. and Zeadally, S. (2015). "An Analysis of Tools for Online Anonymity." A scholarly research paper published at the University of Kentucky. Information Science Faculty Publications. 20. Retrieved on March 4, 2018 from <https://pdfs.semanticscholar.org/4796/edaaa1e02ee7c815d2320c80725bc6e849d7.pdf> .

# ***CONCLUSION***



# In Conclusion

- **We covered:**
  - The Internet in 2022
  - The Laws and Examples of Lawbreakers
  - CyberThreats & Cyber Vulnerabilities
  - A Cyber Litigator's Advice – For Defendants
  - How to Be Anonymous
  - CyberForensics & Forensics Principles



Slater Technologies

# ***QUESTIONS AND ANSWERS***

# Questions and Answers



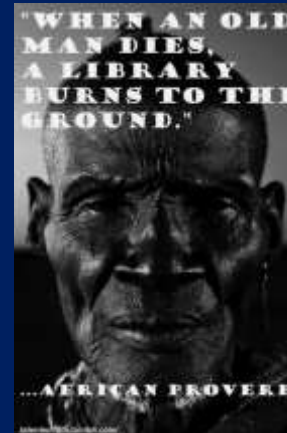
*Slater Technologies*


# *Dedication & Thanks*

# Dedication

This work is dedicated with love, admiration, gratitude, and great respect to Mr. *James P. Jarnagin* (January 25, 1935 – December 2, 2018), the Man who was my Mentor and Father-figure since March 1985. He is one of the biggest reasons for my career success and personal success. What I owe him can never be repaid.

*We'll meet again, Jim. You can count on it...*



A black and white portrait of Maya Angelou, an elderly woman with short, curly grey hair, wearing a dark top, a necklace, and earrings. She is looking directly at the camera with a slight smile.

PEOPLE WILL FORGET  
WHAT YOU SAID.  
PEOPLE WILL FORGET  
WHAT YOU DID.  
BUT PEOPLE WILL  
NEVER FORGET HOW  
YOU MADE THEM FEEL.

*Maya Angelou*

The Restaurant Boss

# Thank You, AFCTI!



# ACFTI

# Presenter Bio:

## William Favre Slater, III

Lives and Works in Chicago; Cybersecurity professional by day

**Current Position – CIO, CISO, Project Manager / Sr. IT Consultant at Slater Technologies, Inc.** Working on projects related to

- Security reviews and auditing
- Pentesting
- Blockchain consulting
- ISO 27001 Project Implementations
- Providing subject matter expert services to Data Center product vendors and other local businesses.
- Designing and creating a blockchain database application that streamlines program management, security management, risk management and reporting activities, for management of teams of IT workers and developers in teleworking environments. It will first be a Windows application and then be ported to the web.
- Developing and presenting technical training materials for in the areas of Blockchain and Blockchain development, Data Center Operations, Data Center Architecture, Cybersecurity Management, and Information Technology hardware and software.
- Happily married since 2000, to Ms. Joanna Roguska, a smart, beautiful, Sr. Web Developer from Warsaw, Poland, and she is my Best Friend & Soul Mate
- A Certified Judo Instructor in Kodokan Judo, and holds a Nidan, a second degree Black belt in Judo.



Slater Technologies



# William Favre Slater, II

- 312-758-0307
- [slater@billslater.com](mailto:slater@billslater.com)
- [williamslater@gmail.com](mailto:williamslater@gmail.com)
- <http://billslater.com/interview>
- <http://billslater.com/writing>
- Slater Technologies, Inc.  
1515 W. Haddon Ave., Unit 309  
Chicago, IL 60642  
United States of America



William Favre Slater, III

Slater Technologies

***SUPPLEMENTAL SLIDES***  
***(WITH MORE DETAILS)***

# **INFORMATION SECURITY IN THE NEWS**

GAMING NEWS

## Sony faces lawsuits over costly PSN data breach

Sony PSN hack could cost Sony \$1.5 billion

By Adam Hartley

April 29th | Tell us what you think [ 1 comments ]

Following the PR disaster that is the [massive Sony PSN hack](#) Sony is already facing a number of legal cases from groups of irate PlayStation fans across the globe.



Sony facing class action lawsuits following high-profile PSN hack

Sony shares were down by nearly 5 per cent following the widespread publicity in both tech and mainstream media about the high-profile PlayStation Network hack.

### Angry gamers demand answers

Sony CEO Howard Stringer or his deputy Kazuo Hirai have both refused to comment publicly on the PSN hack to date, angering gamers even further.

Michael Wang, manager of overseas funds at Sony shareholder Prudential Financials, told Reuters: "Gamers are angry that Sony's CEO hasn't come out to explain the situation and investors are disappointed over the company's corporate governance."

The [cost](#) to Sony of the PlayStation Network hack is already being estimated by some analysts to be in the region of \$1.5 billion (£0.89 billion).

### UK ICO investigates

Clearly, it is way too early to estimate the longer term [costs](#) incurred by the damage to the PlayStation brand and the loss of trust from gamers in the PSN service.

Sony is yet to comment on the latest class action cases being brought against the company.

Here in the UK, the Information Commissioner's Office has contacted Sony and is investigating whether the company is guilty of violating British laws pertaining to a company's responsibility to safeguard customers' private and personal [data](#).

Via Reuters

Tags: PSN, PlayStation, Sony, PlayStation Network, hack, PSN Hack  
September 30, 2022

# Sony PlayStation Customer Data Hack could cost the company \$1.5 billion

Note: Legal costs and reputational damage are not represented here.

April 2011

# Epsilon Data Breach: Expect a Surge in Spear Phishing Attacks

By Tony Bradley, PCWorld

Epsilon—the largest distributor of permission-based email in the world—revealed that millions of individual email addresses were exposed in an attack on its servers. While no other information was apparently compromised, security experts are warning users to brace for a tidal wave of more precise spear phishing attacks.

- SIMILAR ARTICLES:**
- Epsilon Fallout: What Happened to Not Sharing My Information?
  - Epsilon E-Mail Breach: 4 Unanswered Questions
  - Lessons Learned from the Epsilon Data Breach
  - LizaMoon Attack: What You Need To Know
  - Watch Out for Adobe Phishing Scams
  - 'Massive' Epsilon E-Mail Breach Hits Citi, Chase, Many More

Epsilon is responsible for sending more than 40 billion marketing emails per year on behalf of its 2500-plus customers. These emails are not spam in the Rustock botnet sense of the word. These email messages are marketing and customer communication emails from major clients such as JP Morgan Chase, Capital One, CitiGroup, and others.

Andrew Storms, Director of Security Operations for nCircle, commented, "There's no doubt you or someone you know has been affected because the list Epsilon has published looks like a slide of the most impressive customers from a sales presentation."



# Epsilon Data Breach that affected millions of customers from several companies will likely lead to follow-on Spear Phishing Attacks

Let's take a look at what we know about the Epsilon data breach, and what you need to do now to protect yourself from any fallout as a result of the attack.

## What Happened?

The press release from Epsilon was terse, and Epsilon has not been very forthcoming with additional details. The good news is that Epsilon seems to have detected the breach quickly, and did not waste any time notifying its customers. Those customers have subsequently not wasted any time communicating with individual users. I have received two emails already today from affected financial institutions.

Randy Abrams, director of technical education at ESET, says "I have not yet seen details of how the breach occurred. An SQL injection attack would be a decent guess, but it is only a guess. How it happened will only be important to lawyers trying to sue for negligence."

## What Is The Risk?

The fact that the breach only exposed email addresses—and not any additional personal or account information—is great news. The primary risk is that the attackers now have a list of millions of verified active email addresses to target with spam and phishing attacks.

If the attackers were able to get not just the email address, but also its affiliation with one of Epsilon's customers, that will yield much more precise spear phishing attacks. Phishing is like casting a net. Spear phishing is narrowed down to a specific domain or company. But, these attacks would be to known email addresses that are also known to have a relationship with the company being spoofed in the attack—more like spear phishing with laser sighting and computer-guided telemetry.

Amol Sawarte, Vulnerabilities Lab Manager for Qualys, explains, "Phishing" scams are the number one concern from this breach. Hackers could send fake emails pretending to be your bank, pharmacy, hotel or other business that were customers of Epsilon. The email will look real and will be convincing as attackers have the customer's name and the company information that they did business with. The email could ask unsuspecting users to click on a link which can ask for credit card numbers, passwords, install software or carry out other attacks."

Note: Legal costs and reputational damage are not represented here.

April 2011

## Spear Phishing Leads to Significant Breaches

(2011-04-07)

Two of the most significant data breaches in the last six months, including Epsilon and RSA where likely enabled by malware downloaded as the result of targeted spear-phishing attacks. An Epsilon technology partner, Return Path, sent out a warning in November 2010 after an employee fell for a phishing attack, exposing thousands of email addresses to the attackers. In early April RSA reported that their breach likely began when attackers targeted a group of RSA employees with a phishing attack in which emails with Excel attachments contained an exploit that placed backdoors on systems through a vulnerability in Adobe Flash Reader.

### External Link:

[http://www.theregister.co.uk/2011/04/04/rsa\\_hack\\_howdunnit/](http://www.theregister.co.uk/2011/04/04/rsa_hack_howdunnit/)

**The attacker in this case sent two different phishing emails over a two-day period. The two emails were sent to two small groups of employees; you wouldn't consider these users particularly high profile or high value targets. The email subject line read "2011 Recruitment Plan".**

**The email was crafted well enough to trick one of the employees to retrieve it from their Junk mail folder, and open the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls".**

**The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609). As a side note, by now Adobe has released a patch for the zero-day, so it can no longer be used to inject malware onto patched machines.**

RSA data breach  
caused by Excel  
file attachments  
sent via e-mail

Note: Legal costs and reputational damage are not represented here.

April 2011

Home > Industry News > Consumer >

# Michael's warns Chicago customers of data breach

May 05, 2011

ShareThis Tweet 9 LinkedIn Share

Print | Email | 1 comment

(AP) — Michael's Stores Inc. has informed its customers' credit and debit card information may have been compromised.

The Irving, Texas-based arts and crafts supplier says the PIN pad tampering appears to have happened in its Chicago-area stores. Banking and law enforcement officials contacted the company this week after fraudulent transactions were reported last weekend.

Officials believe those fraudulent transactions are linked to legitimate transactions in the Chicago area. The company says it is assisting investigators.

Michael's advises its customers to monitor their statements, report any suspicious account activity and change their personal identification numbers.

If someone thinks their account information was comprised they should contact their credit issuers.



**RELATED CONTENT**

- Crain's investigation: Unpaid wages a growing problem for ...
- Pay-to-play infects Chicago beer market, Crain's ...
- Chicago's big banks ponder new fees to replace overdraft ...
- Mayor Daley runs up big debts building his global city; ...

Chicago Business Today

RELATED CONTENT SPONSORED BY

HARRIS

# Michaels Stores gets its customer data with credit and debit cards compromised

Note: Legal costs and reputational damage are not represented here.

May 2011

## Heartland Breach Settlement with Mastercard

May 21, 2010 – 5:59 pm

Courtesy of [Digital Transactions](#), Heartland Payment Systems entered into a \$41MM settlement agreement regarding their highly publicized data breach incident with Mastercard, Inc.

Continuing its massive clean-up in the wake of the payment card industry's biggest data breach, merchant acquirer Heartland Payment Systems Inc. late on Wednesday announced a \$41.4 million settlement with MasterCard Inc. The settlement will reimburse MasterCard debit and credit card issuers for their costs stemming from the breach Heartland disclosed in January 2009. Heartland has already settled with Visa Inc. for about \$60 million and American Express Co. for \$3.54 million (Digital Transactions News, Jan. 8). That leaves Discover Financial Services as the only major U.S.-based card network with whom Heartland hasn't announced a settlement. The U.S. attorney for New Jersey estimated the breach compromised 130 million payment cards. Several defendants, including notorious computer hacker Albert Gonzalez, have been convicted on federal charges in connection with Heartland's and other big data breaches.

Heartland's MasterCard settlement is contingent upon approval from issuers representing 80% of the affected MasterCard accounts. The Visa settlement had a similar 80% threshold, which issuers approved. MasterCard will make its so-called "alternative recovery offers" to issuers on May 27; issuers have until June 25 to accept them, according to a Heartland filing with the Securities and Exchange Commission. The agreement also provides that those issuers accepting a recovery release Heartland and its sponsor banks, Cleveland-based KeyBank and St. Louis-based Heartland Bank (no relation to the processor) from further breach-related claims. Heartland must obtain a loan of at least \$30.7 million to fund its obligations under the settlement.

According to the Heartland filing, MasterCard will credit the settlement pool with \$6.6 million in "non-compliance assessments"—network fines—that it charged Heartland's sponsors, which those banks passed on to Heartland. That means the maximum Heartland will have to fund for the pool will be \$34.8 million.

Neither Heartland nor MasterCard would comment about the settlement beyond their respective news releases. Like AmEx and Visa, MasterCard didn't say how many of its card accounts sustained breach-related fraud losses, or how many cards its bank and credit-union clients reissued as a precaution. Gartner Inc. security and technology analyst Avivah Litan tells Digital Transactions News by e-mail that based on estimated replacement costs of \$14 to \$20 per card, "it would appear from this settlement that MasterCard could only prove that some 2-3 million of their cards actually had fraud losses and had to be reissued with new accounts." She adds that, "it's good that Heartland is finally settling with MasterCard so it can begin to put this matter behind them."

Robert O. Carr, Heartland's chairman and chief executive officer, said in his company's release that, "We are pleased to have reached an equitable settlement agreement that helps issuers of MasterCard-branded cards obtain a recovery with respect to losses they may have incurred from the intrusion. We look forward to working with MasterCard to

# After data breach Heartland Payment Systems settled with

## MasterCard for \$41 million; Visa for \$60 million; and AMEX for \$3.5 million

**Note: Legal costs and reputational  
damage are not represented here.**

May 2010



# LPL, a Financial Services Company Fined \$275,000 on September 11, 2008 for Failure to Protect Customer Data

## Summary

These proceedings arise out of the violations by LPL, a registered broker-dealer, investment adviser, and transfer agent, of the safeguards rule of Regulation S-P (17 CFR § 248.30(a)) (the “Safeguards Rule”), which requires broker-dealers and SEC-registered investment advisers to adopt written policies and procedures reasonably designed to protect customer information. Despite its being aware as early as 2006 that it had insufficient security controls to safeguard customer information at its branch offices, LPL failed to implement adequate controls, including some security measures, which left customer information at LPL’s branch offices vulnerable to unauthorized access. Between mid-July 2007 and February 2008, LPL experienced a series of computer system security breaches in which an unauthorized person(s) accessed and traded, or attempted to trade, in the customer accounts of several of LPL’s registered representatives. As of the date of the “hacking” incidents, LPL had failed to implement increased security measures and adopt policies and procedures reasonably designed to safeguard customer information as required by Regulation S-P. LPL detected the breaches and absorbed the losses in the customer accounts. Nonetheless, LPL’s failures left customer information vulnerable to identity thieves or other unauthorized users at the firm’s branch offices.

**Note: Legal costs and reputational damage are not represented here.**

September 2008



## Data Breach Alerts

Patients' names, dates of birth, Social Security numbers and limited dental claims data on stolen laptop Thursday, 19 May 2011, 10:54 pm

Unknown Organization data loss incident circa 2011-05-17

Source: [Breach Alerts](#) |

12,000 customers' names, Social Security numbers, addresses and phone numbers acquired by hacker in extortion attempt Thursday, 19 May 2011, 10:43 pm

Leading Investment & Securities Co. data loss incident circa 2011-05-19

Source: [Breach Alerts](#) |

4,000 employees' Social Security numbers and other payroll information exposed when sent via unencrypted email. Thursday, 19 May 2011, 10:39 pm

National Business Center data loss incident circa 2011-05-18

Source: [Breach Alerts](#) |

Laptop with eye photos and names of 611 patients stolen during office burglary Wednesday, 18 May 2011, 8:13 pm

EyeCare Associates of the San Ramon Valley data loss incident circa 2011-05-17

Source: [Breach Alerts](#) |

Social Security numbers of 37,900 Medicare Supplement members exposed in envelope windows Wednesday, 18 May 2011, 7:59 pm

Anthem Blue Cross of California data loss incident circa 2011-05-13

Source: [Breach Alerts](#) |

149 different customers' names, dates of birth and Social Security numbers used to set up 184 bank accounts for fraudulent purposes Wednesday, 18 May 2011, 4:35 pm

Regions Bank data loss incident circa 2011-05-17

Source: [Breach Alerts](#) |

210,000 residents' names, addresses, Social Security numbers, email addresses, Employer ID numbers, and some employer bank account information may have been transmitted after 1,500 computers were infected with a computer virus W32.QAKBOT Tuesday, 17 May 2011, 4:11 pm

# Data Breach Updates from DataBreachWatch.org

**(This website has gone down permanently, probably due to the massive rise in Data Breaches)**

May 2011

# **Guide to Computer Forensics and Investigations Fourth Edition**

## *Chapter 7 Current Computer Forensics Tools*

# Objectives

- Explain how to evaluate needs for computer forensics tools
- Describe available computer forensics software tools
- List some considerations for computer forensics hardware tools
- Describe methods for validating and testing computer forensics tools

# Evaluating Computer Forensics Tool Needs

- Look for versatility, flexibility, and robustness
  - OS
  - File system
  - Script capabilities
  - Automated features
  - Vendor's reputation
- Keep in mind what application files you will be analyzing

# Types of Computer Forensics Tools

- Hardware forensic tools
  - Range from single-purpose components to complete computer systems and servers
- Software forensic tools
  - Types
    - Command-line applications
    - GUI applications
  - Commonly used to copy data from a suspect's disk drive to an image file

# Tasks Performed by Computer Forensics Tools

- Five major categories:
  - Acquisition
  - Validation and discrimination
  - Extraction
  - Reconstruction
  - Reporting

# Tasks Performed by Computer Forensics Tools (continued)

- **Acquisition**
  - Making a copy of the original drive
- Acquisition subfunctions:
  - Physical data copy
  - Logical data copy
  - Data acquisition format
  - Command-line acquisition
  - GUI acquisition
  - Remote acquisition
  - Verification



# Tasks Performed by Computer Forensics Tools (continued)

- Acquisition (continued)
  - Two types of data-copying methods are used in software acquisitions:
    - Physical copying of the entire drive
    - Logical copying of a disk partition
  - The formats for disk acquisitions vary
    - From raw data to vendor-specific proprietary compressed data
  - You can view the contents of a raw image file with any hexadecimal editor

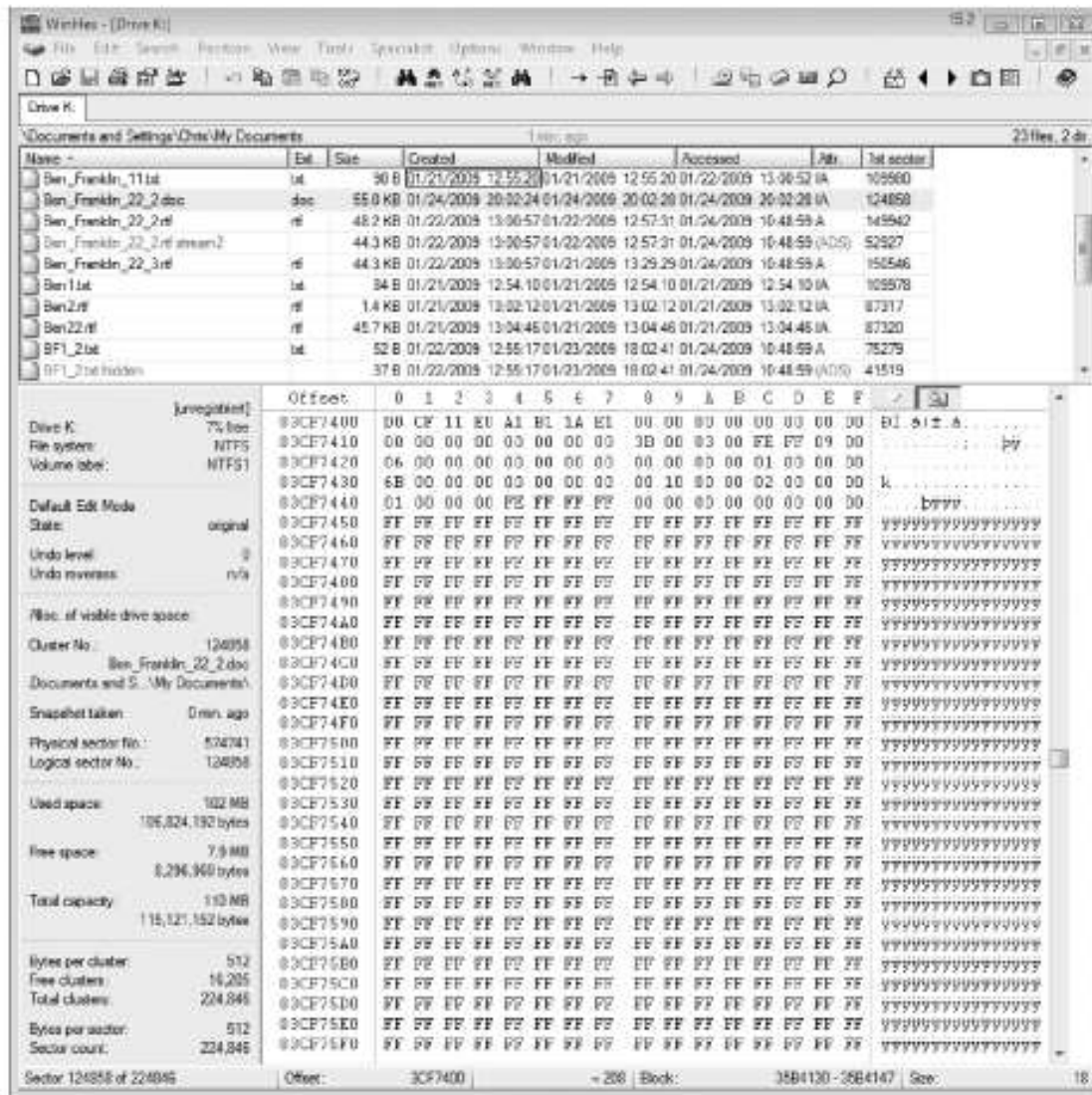


Figure 7-1 Viewing data in a hexadecimal editor.

# Tasks Performed by Computer Forensics Tools (continued)

- Acquisition (continued)
  - Creating smaller segmented files is a typical feature in vendor acquisition tools
  - All computer forensics acquisition tools have a method for verification of the data-copying process
    - That compares the original drive with the image

# Tasks Performed by Computer Forensics Tools (continued)

- Validation and discrimination
  - **Validation**
    - Ensuring the integrity of data being copied
  - **Discrimination** of data
    - Involves sorting and searching through all investigation data

# Tasks Performed by Computer Forensics Tools (continued)

- Validation and discrimination (continued)
  - Subfunctions
    - Hashing
      - CRC-32, MD5, Secure Hash Algorithms
    - Filtering
      - Based on hash value sets
    - Analyzing file headers
      - Discriminate files based on their types
  - National Software Reference Library (NSRL) has compiled a list of known file hashes
    - For a variety of OSs, applications, and images

# Tasks Performed by Computer Forensics Tools (continued)

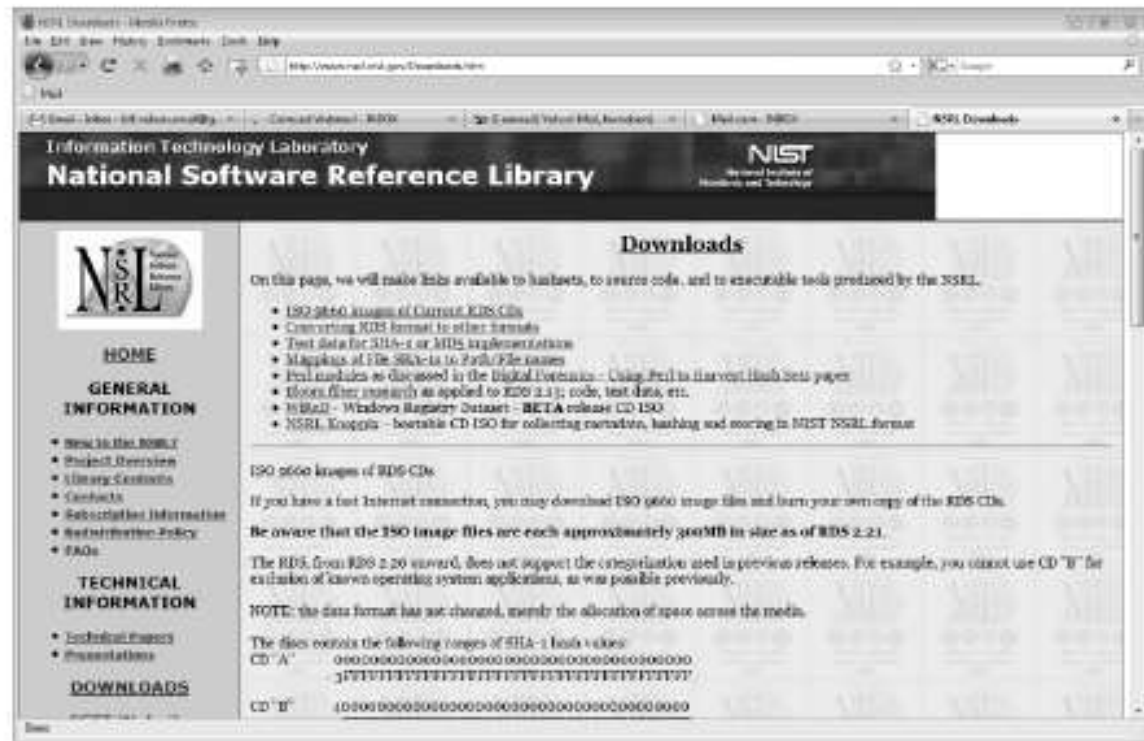


Figure 7-2 The download page of the National Software Reference Library

# Tasks Performed by Computer Forensics Tools (continued)

- Validation and discrimination (continued)
  - Many computer forensics programs include a list of common header values
    - With this information, you can see whether a file extension is incorrect for the file type
  - Most forensics tools can identify header values

Indicates a .jpeg file

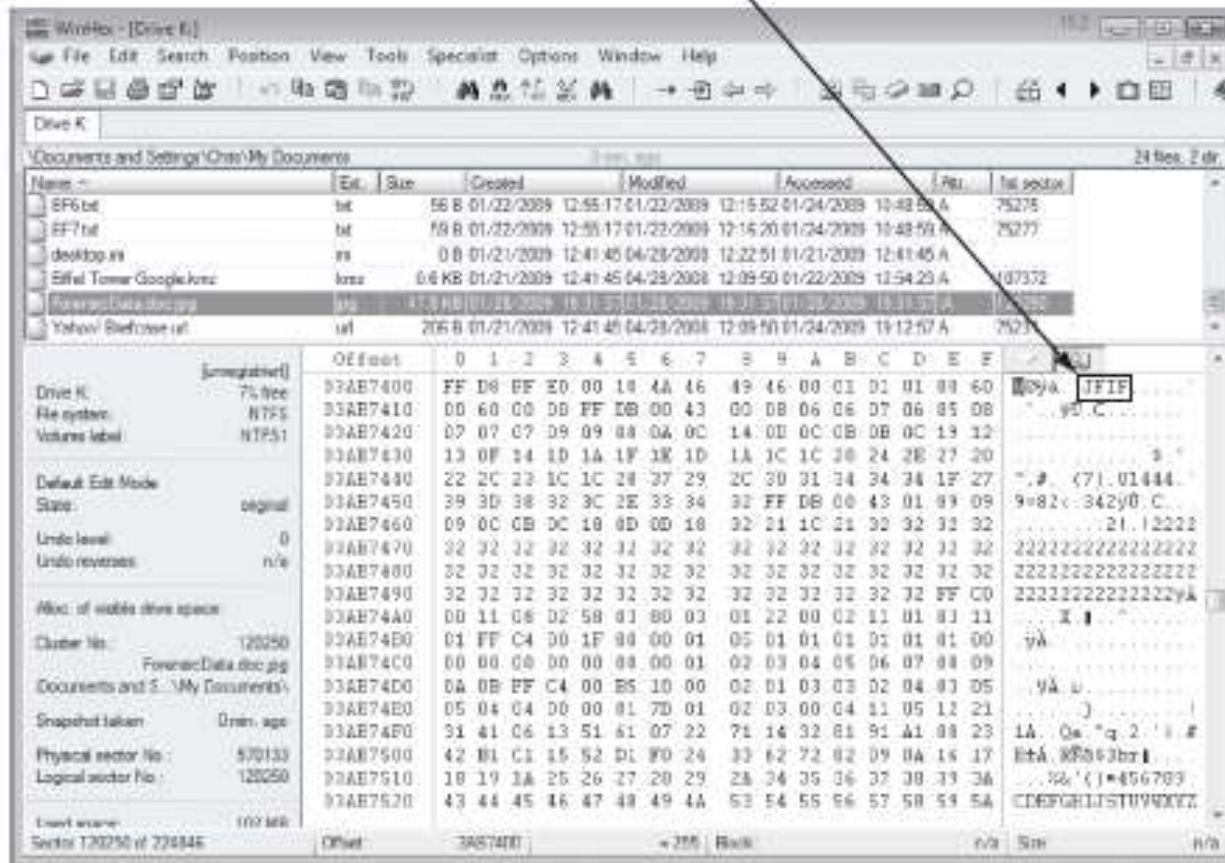
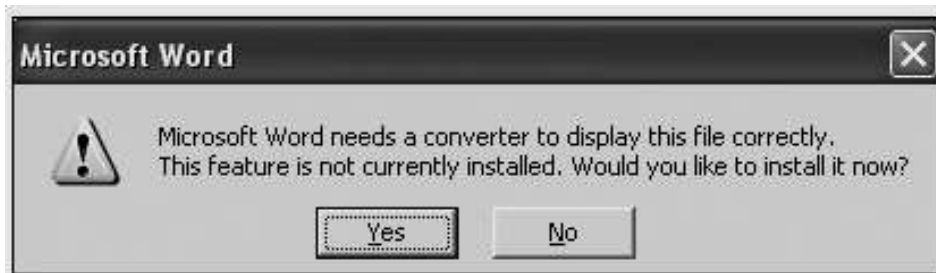


Figure 7-3 The file header indicates a .jpeg file



# Tasks Performed by Computer Forensics Tools (continued)



**Figure 7-4** Error message displayed when trying to open a JPEG file in Word



Figure 7-5 ForensicData.doc open in an image viewer

# Tasks Performed by Computer Forensics Tools (continued)

- **Extraction**
  - Recovery task in a computing investigation
  - Most demanding of all tasks to master
  - Recovering data is the first step in analyzing an investigation's data

# Tasks Performed by Computer Forensics Tools (continued)

- Extraction (continued)
  - Subfunctions
    - Data viewing
    - Keyword searching
    - Decompressing
    - Carving
    - Decrypting
    - Bookmarking
  - **Keyword search** speeds up analysis for investigators

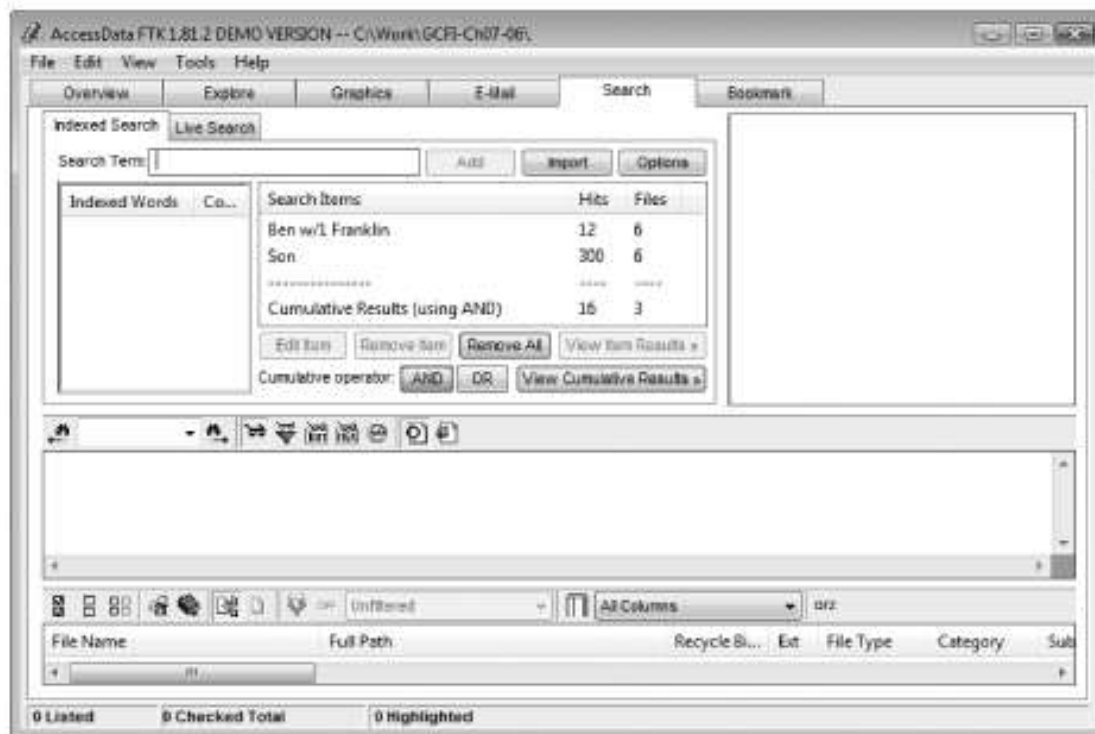


Figure 7-6 The Indexed Search feature in FTK

# Tasks Performed by Computer Forensics Tools (continued)

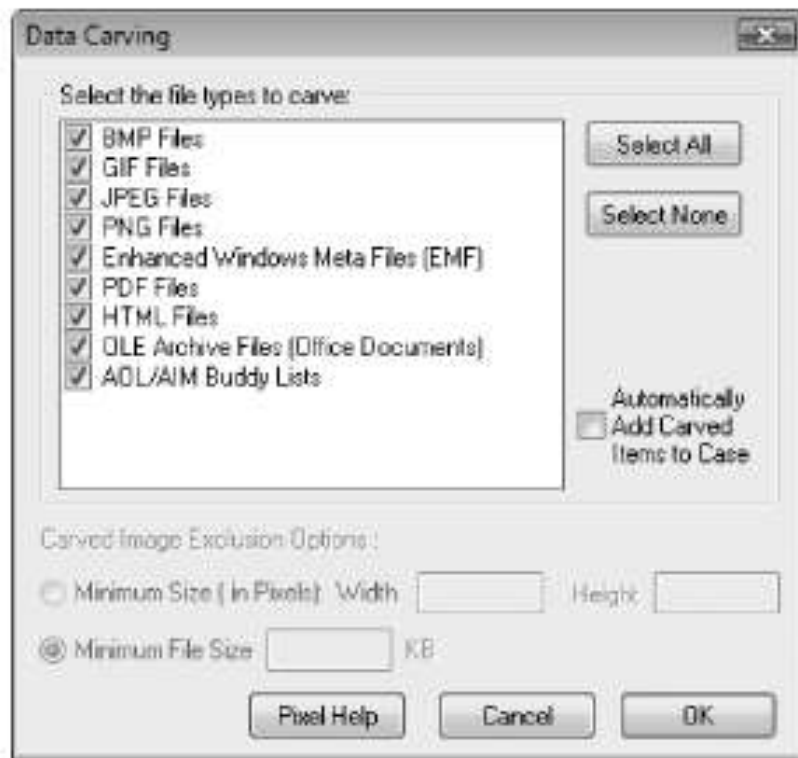


Figure 7-7 Data-carving options in FTK

# Tasks Performed by Computer Forensics Tools (continued)

- Extraction (continued)
  - From an investigation perspective, encrypted files and systems are a problem
  - Many password recovery tools have a feature for generating potential password lists
    - For a **password dictionary attack**
  - If a password dictionary attack fails, you can run a **brute-force attack**

# Tasks Performed by Computer Forensics Tools (continued)

- **Reconstruction**

- Re-create a suspect drive to show what happened during a crime or an incident
- Subfunctions
  - Disk-to-disk copy
  - Image-to-disk copy
  - Partition-to-partition copy
  - Image-to-partition copy



# Tasks Performed by Computer Forensics Tools (continued)

- Reconstruction (continued)
  - Some tools that perform an image-to-disk copy:
    - SafeBack
    - SnapBack
    - EnCase
    - FTK Imager
    - ProDiscover

# Tasks Performed by Computer Forensics Tools (continued)

- Reporting
  - To complete a forensics disk analysis and examination, you need to create a report
  - Subfunctions
    - Log reports
    - Report generator
  - Use this information when producing a final report for your investigation

# Tool Comparisons

Table 7-1 Comparison of forensics tool functions

Function	ProDiscover Basic	AccessData Ultimate Toolkit	Guidance Software EnCase
<b>Acquisition</b>			
Physical data copy	√	√	√
Logical data copy	√	√	√
Data acquisition formats	√	√	√
Command-line process			√
GUI process	√	√	√
Remote acquisition			√*
Verification	√	√	√
<b>Validation and discrimination</b>			
Hashing	√	√**	√**
Filtering		√	√
Analyzing file headers		√	√
<b>Extraction</b>			
Data viewing	√	√***	√***
Keyword searching	√	√	√
Decompressing		√	√
Carving		√	√
Decrypting		√	
Bookmarking	√	√	√
<b>Reconstruction</b>			
Disk-to-disk copy	√	√	√
Image-to-disk copy	√	√	√
Partition-to-partition copy	√		√
Image-to-partition copy	√		√
<b>Reporting</b>			
Log reports		√	√
Report generator	√	√	

# Other Considerations for Tools

- Considerations
  - Flexibility
  - Reliability
  - Expandability
  - Keep a library with older version of your tools
- Create a software library containing older versions of forensics utilities, OSs, and other programs

# Computer Forensics Software Tools

- The following sections explore some options for command-line and GUI tools in both Windows and UNIX/Linux

# Command-line Forensic Tools

- The first tools that analyzed and extracted data from floppy disks and hard disks were MS-DOS tools for IBM PC file systems
- Norton DiskEdit
  - One of the first MS-DOS tools used for computer investigations
- Advantage
  - Command-line tools require few system resources
    - Designed to run in minimal configurations

# UNIX/Linux Forensic Tools

- \*nix platforms have long been the primary command-line OSs
- SMART
  - Designed to be installed on numerous Linux versions
  - Can analyze a variety of file systems with SMART
  - Many plug-in utilities are included with SMART
  - Another useful option in SMART is its hex viewer

# UNIX/Linux Forensic Tools (continued)

- Helix
  - One of the easiest suites to begin with
  - You can load it on a live Windows system
    - Loads as a bootable Linux OS from a cold boot
- Autopsy and SleuthKit
  - Sleuth Kit is a Linux forensics tool
  - Autopsy is the GUI/browser interface used to access Sleuth Kit's tools





Figure 7-8 The Helix menu

# UNIX/Linux Forensic Tools (continued)

- Knoppix-STD
  - Knoppix Security Tools Distribution (STD)
    - A collection of tools for configuring security measures, including computer and network forensics
  - Knoppix-STD is forensically sound
    - Doesn't allow you to alter or damage the system you're analyzing
  - Knoppix-STD is a Linux bootable CD

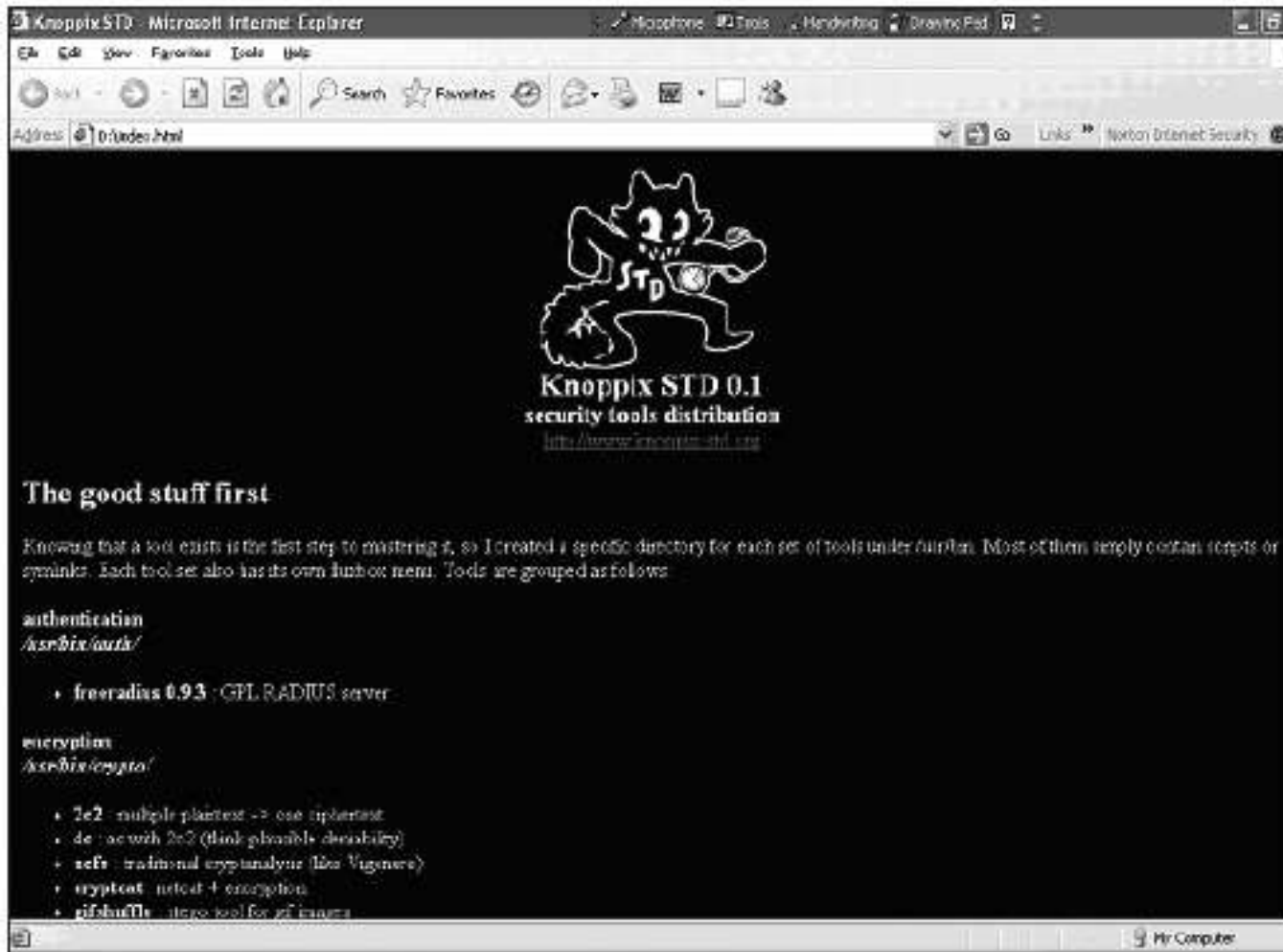


Figure 7-9 The Knoppix-STD information window in Windows

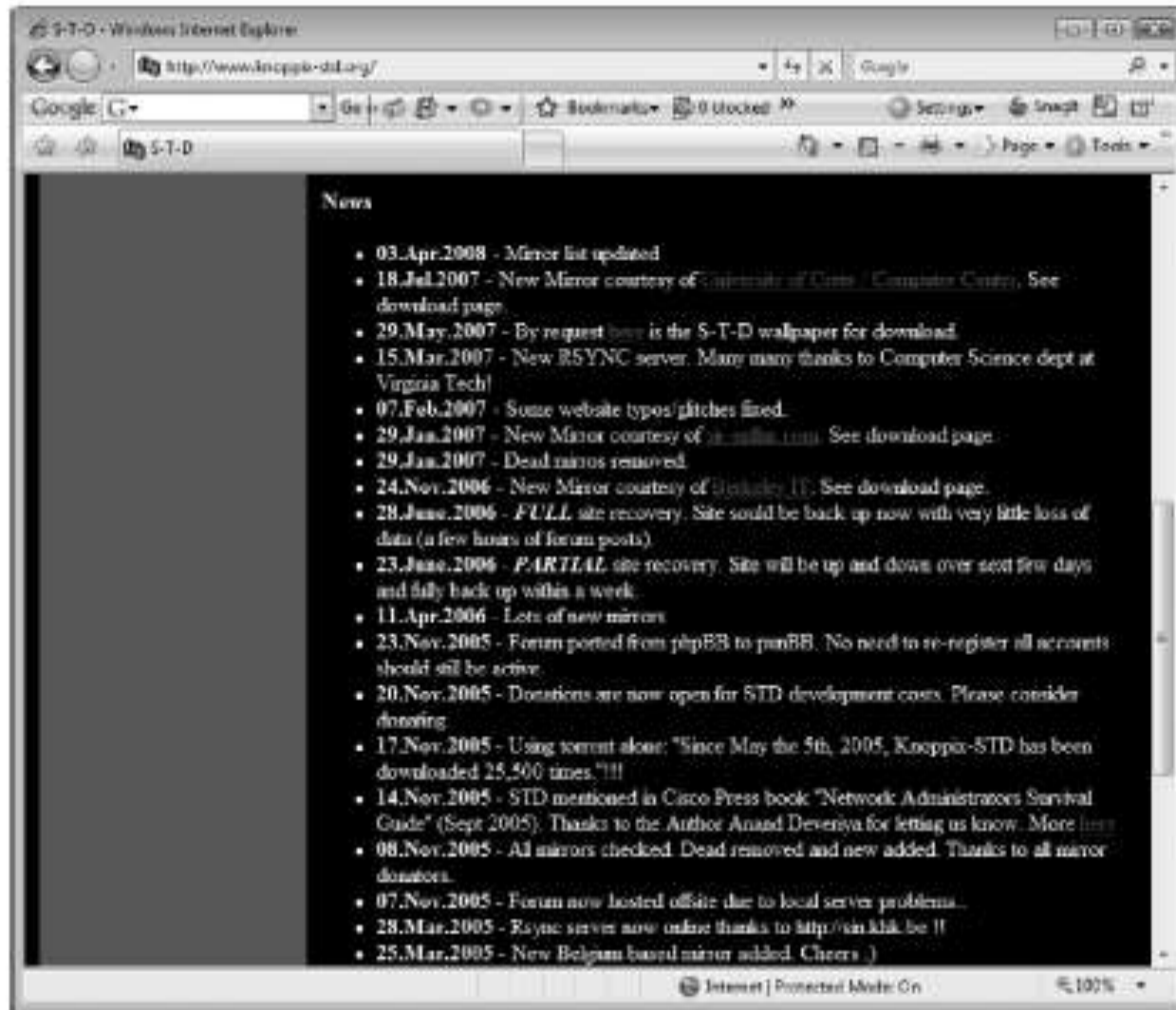


Figure 7-10 A list of forensics tools available in Knoppix-STD

# Other GUI Forensic Tools

- Simplify computer forensics investigations
- Help training beginning investigators
- Most of them come into suites of tools
- Advantages
  - Ease of use
  - Multitasking
  - No need for learning older OSs

# Other GUI Forensic Tools (continued)

- Disadvantages
  - Excessive resource requirements
  - Produce inconsistent results
  - Create tool dependencies

# Computer Forensics Hardware Tools

- Technology changes rapidly
- Hardware eventually fails
  - Schedule equipment replacements
- When planning your budget consider:
  - Failures
  - Consultant and vendor fees
  - Anticipate equipment replacement

# Forensic Workstations

- Carefully consider what you need
- Categories
  - Stationary
  - Portable
  - Lightweight
- Balance what you need and what your system can handle



# Forensic Workstations (continued)

- Police agency labs
  - Need many options
  - Use several PC configurations
- Private corporation labs
  - Handle only system types used in the organization
- Keep a hardware library in addition to your software library

# Forensic Workstations (continued)

- Not as difficult as it sounds
- Advantages
  - Customized to your needs
  - Save money
- Disadvantages
  - Hard to find support for problems
  - Can become expensive if careless
- Also need to identify what you intend to analyze

# Forensic Workstations (continued)

- You can buy one from a vendor as an alternative
- Examples
  - F.R.E.D.
  - F.I.R.E. IDE
- Having vendor support can save you time and frustration when you have problems
- Can mix and match components to get the capabilities you need for your forensic workstation

# Using a Write-Blocker

- **Write-blocker**
  - Prevents data writes to a hard disk
- **Software-enabled blockers**
  - Software write-blockers are OS dependant
  - Example: PDBlock from Digital Intelligence
- **Hardware options**
  - Ideal for GUI forensic tools
  - Act as a bridge between the suspect drive and the forensic workstation

# Using a Write-Blocker (continued)

- Can navigate to the blocked drive with any application
- Discards the written data
  - For the OS the data copy is successful
- Connecting technologies
  - FireWire
  - USB 2.0
  - SCSI controllers

# Recommendations for a Forensic Workstation

- Determine where data acquisitions will take place
- Data acquisition techniques
  - USB 2.0
  - FireWire
- Expansion devices requirements
- Power supply with battery backup
- Extra power and data cables

# Recommendations for a Forensic Workstation (continued)

- External FireWire and USB 2.0 ports
- Assortment of drive adapter bridges
- Ergonomic considerations
  - Keyboard and mouse
  - A good video card with at least a 17-inch monitor
- High-end video card and monitor
- If you have a limited budget, one option for outfitting your lab is to use high-end game PCs

# Validating and Testing Forensic Software

- Make sure the evidence you recover and analyze can be admitted in court
- Test and validate your software to prevent damaging the evidence



# Using National Institute of Standards and Technology (NIST) Tools

- **Computer Forensics Tool Testing (CFTT)** program
  - Manages research on computer forensics tools
- NIST has created criteria for testing computer forensics tools based on:
  - Standard testing methods
  - ISO 17025 criteria for testing items that have no current standards
  - ISO 5725

# Using National Institute of Standards and Technology (NIST) Tools (continued)

- Your lab must meet the following criteria
  - Establish categories for computer forensics tools
  - Identify computer forensics category requirements
  - Develop test assertions
  - Identify test cases
  - Establish a test method
  - Report test results
- Also evaluates drive-imaging tools using
  - Forensic Software Testing Support Tools (FS-TST)

# Using National Institute of Standards and Technology (NIST) Tools (continued)

- **National Software Reference Library (NSRL)** project
  - Collects all known hash values for commercial software applications and OS files
    - Uses SHA-1 to generate a known set of digital signatures called the Reference Data Set (RDS)
  - Helps filtering known information
  - Can use RDS to locate and identify known bad files

# Using Validation Protocols

- Always verify your results
- Use at least two tools
  - Retrieving and examination
  - Verification
- Understand how tools work
- One way to compare results and verify a new tool is by using a disk editor
  - Such as Hex Workshop or WinHex

# Using Validation Protocols (continued)

- Disk editors
  - Do not have a flashy interface
  - Reliable tools
  - Can access raw data
- Computer Forensics Examination Protocol
  - Perform the investigation with a GUI tool
  - Verify your results with a disk editor
  - Compare hash values obtained with both tools

# Using Validation Protocols (continued)

- Computer Forensics Tool Upgrade Protocol
  - Test
    - New releases
    - OS patches and upgrades
  - If you find a problem, report it to forensics tool vendor
    - Do not use the forensics tool until the problem has been fixed
  - Use a test hard disk for validation purposes
  - Check the Web for new editions, updates, patches, and validation tests for your tools

# Summary

- Create a business plan to get the best hardware and software
- Computer forensics tools functions
  - Acquisition
  - Validation and discrimination
  - Extraction
  - Reconstruction
  - Reporting
- Maintain a software library on your lab

# Summary (continued)

- Computer Forensics tools types
  - Software
  - Hardware
- Forensics software
  - Command-line
  - GUI
- Forensics hardware
  - Customized equipment
  - Commercial options
  - Include workstations and write-blockers



# Summary (continued)

- Tools that run in Windows and other GUI environments don't require the same level of computing expertise as command-line tools
- Always test your forensics tools