Cybersecurity and Applicable Rules and Regulations

Law Offices of
Salar Atrizadeh

When you think advocacy, think of us.®

Issues

- What is cybersecurity?
- What causes data breaches?
- What are the various types of security threats?
- What is the proper security level for electronic devices?
- What are the major security concerns?
- What are the best practices to prevent data breaches?
- What are the applicable rules and regulations?

What is Cybersecurity?

- What is cybersecurity? It is the measure taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack
- On July 8, 2014, the Senate Intelligence Committee advanced a bill that would grant legal immunity for companies to share computer threat data with the government
- The Cybersecurity Information Sharing Act ("CISA") permits voluntary information sharing and includes measures to protect private information

Cybersecurity Information Sharing Act

- However, according to the Center for Democracy and Technology this law:
  - Doesn't address recently-disclosed cybersecurity-related conduct of the NSA
  - Requires cyber-threat indicators (e.g., security vulnerability) a company shares with federal agencies be shared with other federal agencies
  - May turn into a "back-door wiretap" by authorizing use of cyber-threat indicators for overly-broad law enforcement purposes

Cybersecurity Information Sharing Act

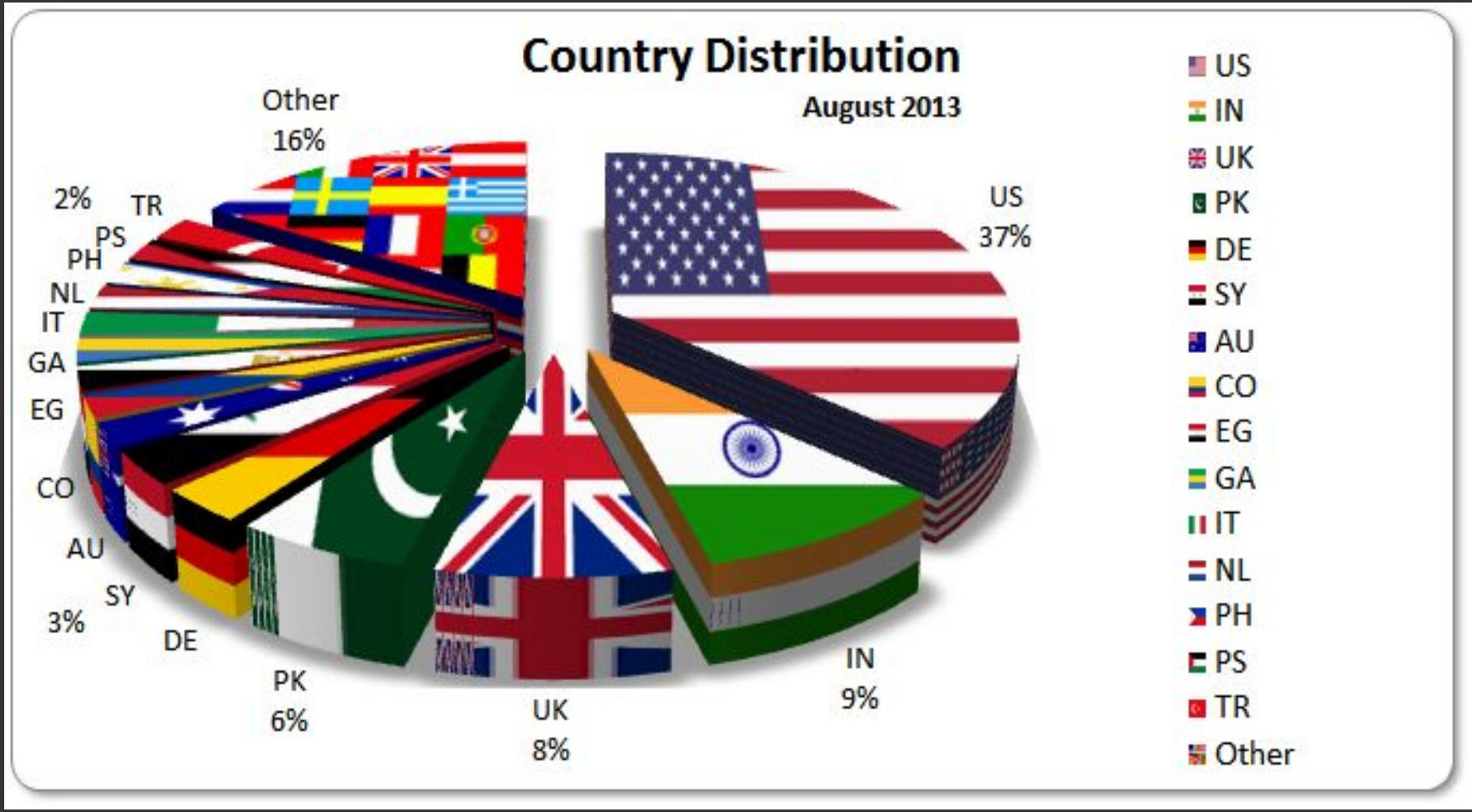
- It fails to require that personally identifiable information that's irrelevant to a cyber-threat indicator (e.g., malicious reconnaissance) be removed before information about the threat indicator is shared
- It authorizes broadly-defined cybersecurity countermeasures and provides a "good faith" defense

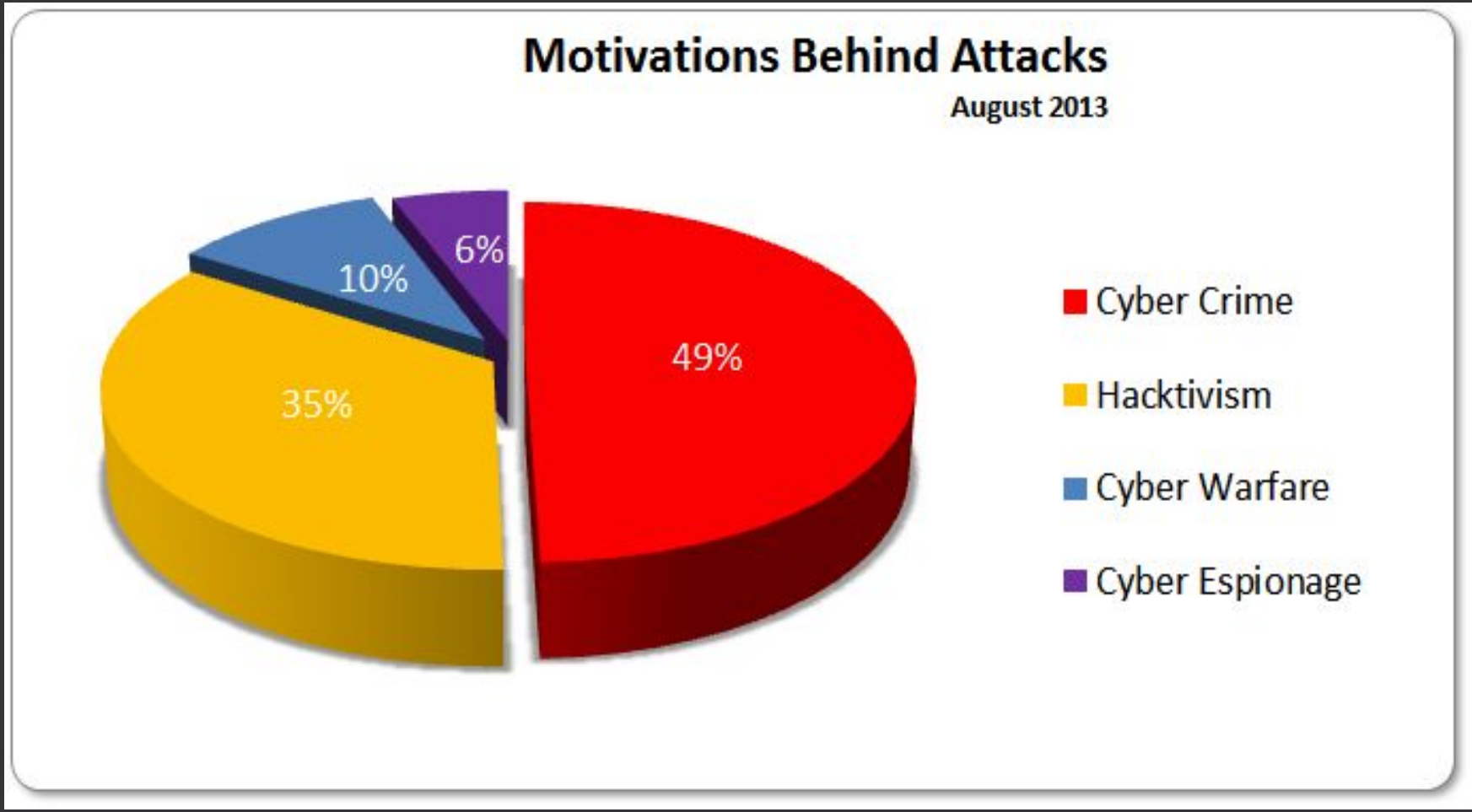
See https://cdt.org/insight/analysis-of-feinstein-chambliss-cybersecurity-information-sharing-act-of-2014

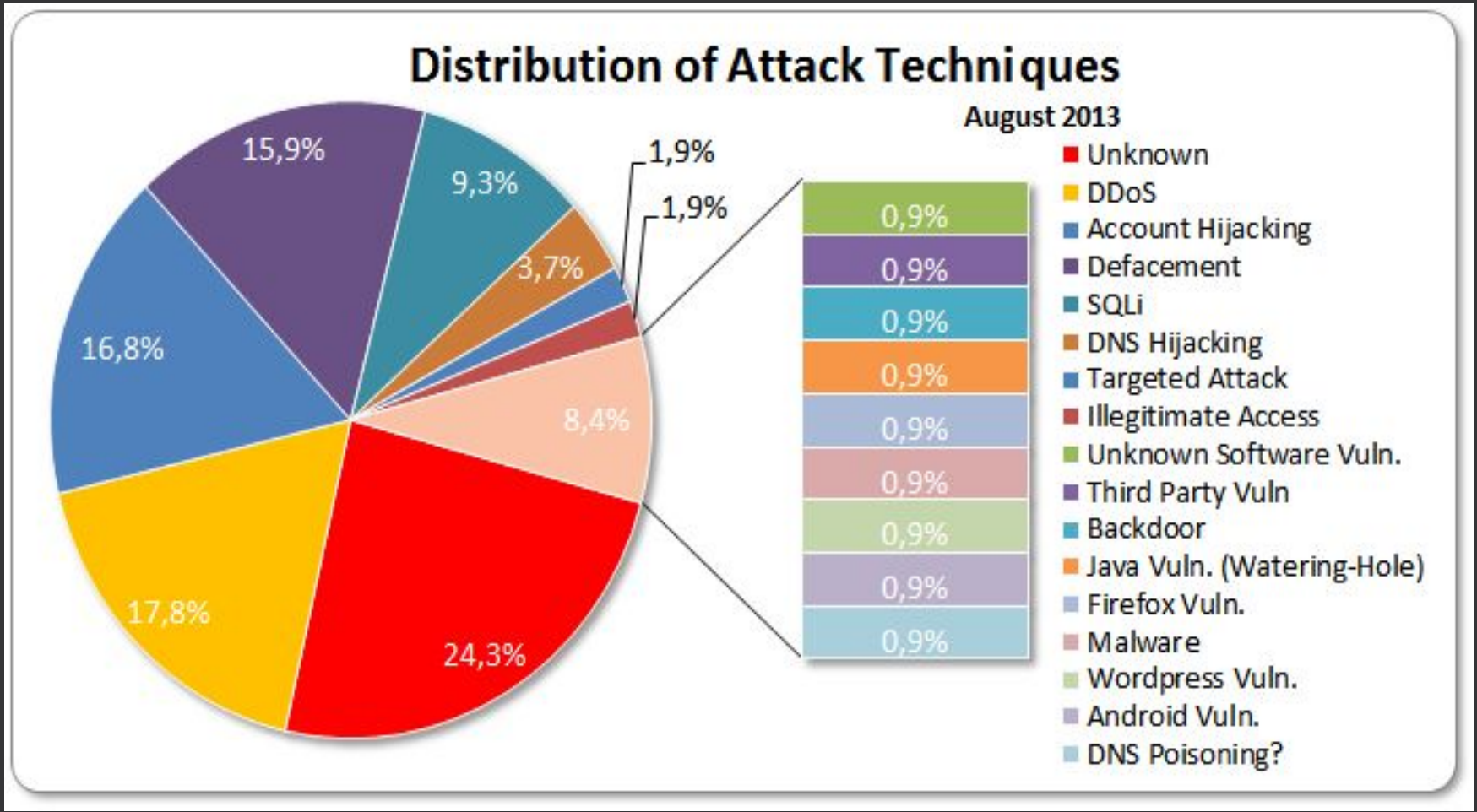
Cybersecurity Information Sharing Act

- According to Electronic Frontier Foundation, this law will grant companies more power to obtain "threat" information (e.g., from private communications of users) and disclose that data to the government without a warrant
- It also gives companies broad immunity to spy on and even launch countermeasures against innocent users

See act.eff.org/action/stop-the-cybersecurity-information-sharing-bills


Country Distribution
August 2013
Other
16%
2%
TR
PS
PH
NL
IT
GA
EG
CO
AU
SY
3%
DE
PK
6%
UK
8%
IN
9%
US
37%
US
IN
UK
PK
DE
SY
AU
CO
EG
GA
IT
NL
PH
PS
TR
Other


Motivations Behind Attacks
August 2013
49%
35%
10%
6%
Cyber Crime
Hacktivism
Cyber Warfare
Cyber Espionage


Distribution of Attack Techniques
August 2013
15,9%
9,3%
1,9%
1,9%
3,7%
16,8%
8,4%
17,8%
24,3%
0,9%
0,9%
0,9%
0,9%
0,9%
0,9%
0,9%
0,9%
Unknown
DDoS
Account Hijacking
Defacement
SQLi
DNS Hijacking
Targeted Attack
Illegitimate Access
Unknown Software Vuln.
Third Party Vuln
Backdoor
Java Vuln. (Watering-Hole)
Firefox Vuln.
Malware
Wordpress Vuln.
Android Vuln.
DNS Poisoning?

What Causes Data Breaches?

- Hackers
- Mobile Devices – e.g., BYOD
- Malicious Insiders
- Human Errors, Accidents, Inadvertence, or Natural Events
- Cloud Computing and Wireless Communications

Hackers

- Advanced Persistent Threats (APTs)
  - Common cyber attack which focuses on espionage
  - Uses undetectable "zero-day" exploits and "social engineering" techniques
- In recent times, law firms' network securities were compromised
  i. In 2011, Wiley Rein, LLP's network was breached by Chinese hackers
  ii. In 2010, UK law firm, ACS:Law's network was breached by using distributed denial-of-service (DDoS) attacks

Mobile Devices

- A large percentage of data breaches is caused by lost or stolen unencrypted mobile devices (e.g., laptops, iPADs, hard drives, back ups, flash drives)
- According to the Identity Theft Resource Center (idtheftcenter.org), from 1/1/2014 until 8/19/2014, there have been 480 industry-wide security breaches, causing 17,508,452 records to be exposed
- Law firm's permitting BYOD face risks and benefits
- A law firm should use Mobile Device Management in order to remotely manage mobile devices (e.g., locate, lock, erase data)

Malicious Insiders

- Malicious insiders can include disgruntled employees
- They usually have access to sensitive data (e.g., confidential documents or trade secrets)
- For example, a computer technician in Bank of New York Mellon stole the identity of 2000 bank employees and opened bank/brokerage accounts
- See Carnegie Mellon University's list of best practices http://www.cert.org/insider-threat/best-practices/index.cfm

Human Errors, Accidents, Inadvertence, or Natural Events

1) Human errors can include: (a) failure to follow instructions (b) mistake in judgment (c) incompetence
2) Accidents can include: (a) fire (b) physical damage (c) accidental deletion
3) Service disruptions can include: (a) electricity outage (b) water outage (c) heat outage (d) fiber optics breakage
4) Natural events can include: (a) earthquake (b) hurricane (c) tornado (d) flood

Case Study

- In *F.T.C. v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602, the Federal Trade Commission brought action alleging that the hospitality company and its subsidiaries engaged in unfair and deceptive trade practice in violation of Federal Trade Commission Act
- FTC alleged that defendants failed to maintain reasonable and appropriate data security for consumers' sensitive personal information
- The court held, *inter alia*, that FTC had authority to regulate companies' failure to maintain reasonable and appropriate data security

Case Study

- In *Piscioatta v. Old National Bancorp, 499 F.3d 629 (2007)*, consumers filed a putative class action against bank, alleging that through its website, bank had solicited personal information on applicants for banking services, but had failed to secure it adequately.
- The district court granted bank's motion for judgment on the pleadings and denied consumers' motion for class certification as moot. The consumers appealed.
- The Court of Appeals held that on a matter of first impression under Indiana law, the consumers did not suffer a compensable injury.

Security Threat Types

Security threats fall into the following categories:

A. Social Engineering Scams
B. Network Breaches
C. Physical Breaches
D. Mobile Breaches

Social Engineering Scams

- It is a common technique that hackers utilize to gain access to your device, network, or information
- For example, it can be an email that seems to come from a trusted vendor that actually contains malware (a/k/a Phishing) or like the Nigerian e-mail or "419" scams
- In 2012, 1 in 291 emails contained a virus or link to malware
- According to Verizon, 29% of unauthorized accesses in 2012 involved some form of social engineering

Network Breaches

- It can be caused by malware, which is short for "malicious software." It's any type of program designed or used for unauthorized access to a computer system.
- Once every three minutes, an organization will experience a malicious email file attachment or web link, as well as malware communication—or call–back—to a command and control (CnC) server - *FireEye Advanced Threat Report (April 2013)*

Different Types of Malware

a) Virus – it relies on human interactions (such as downloading or opening files) to spread

b) Trojan – it masquerades as a legitimate application

c) Worm – it can self-replicate and distribute itself across multiple devices without human intervention

d) Spyware – it discreetly captures and transmits sensitive information from a device (like keystrokes or webcam photos)

Different Types of Malware

e) Adware – its purpose is to serve obtrusive or unexpected ads on the compromised device

f) Chargeware – it charges the victim's money without his/her knowledge or consent

g) Ransomware – it restricts access to a device unless the victim pays to have it unlocked

Physical Breaches

A. Lost or Stolen Devices
   - In recent years, a vast amount of data can be stored on laptops, tablets, and smartphones
   - A smartphone can hold many years of financial and inventory records
   - Confidential data (e.g., trade secrets) may exist on the "cloud"
   - For example, in 2012, in San Francisco almost ½ of all robberies involved smartphones

Physical Breaches

B. Foreign Contact
   - Many businesses have relationships with foreign partners
   - Travel is required by executives
   - Foreign travel can cause additional security risks
   - In fact, some countries have more aggressive search and seizure policies
   - Business communications in another country may be subject to foreign corporate espionage and/or government surveillance

Mobile Breaches

Mobile threats fall into three categories:

(1) Application–based threats

(2) Web-based threats

(3) Network–based threats

Application–based threats

- "Malicious apps" may seem okay on the surface, but they're designed for fraud or disruptions
- They can come in the form of malware, but also include:
  1. Privacy threats — They may not be malicious in design, but can gather or use sensitive information (e.g., location, contact lists, PII) beyond what's necessary to function
  2. Vulnerable apps — They contain flaws that can be exploited for malicious purposes. Vulnerabilities can enable the culprit to access sensitive information, perform undesirable actions, or download other apps to device without user's knowledge

Web–based threats

Mobile devices can access web-based services, exposing them to additional threats like:

1. Phishing Scams — use email, text messages, or social media websites to distribute links to malicious web pages designed to trick you into providing information
2. Drive-By Downloads — can automatically download an application when you visit a web page
3. Browser exploits — take advantage of vulnerabilities in your mobile web browser or software launched by the browser (e.g., Flash player, PDF reader, Image Viewer)

Network–based threats

In general, mobile devices support cellular networks and local wireless networks (e.g., Wi-Fi or Bluetooth). These types of networks can host the following threats:

1. Network exploits — take advantage of mobile operating system flaws. Once connected, they can install malware on your phone without your knowledge.
2. Wi-Fi Sniffing — it intercepts data when traveling through the air between the device and Wi-Fi access point. A lot of applications and websites don’t use proper security measures and sent “unencrypted data” across the network that can be captured by the culprit

Case Study

In re Target Corp. Customer Data Sec. Breach Litigation, 2014 WL 6775314 (December 2, 2014)

- In December 2013, Target announced that over a period of more than 3 weeks during Christmas, hackers had stolen credit and debit-card information for 110 million of its customers
- As a result, lawsuits were filed. Ultimately, the Judicial Panel on Multidistrict Litigation consolidated all federal lawsuits.
- The multidistrict litigation consisted of two types of claims: (1) Consumer claims; and (2) Financial institution claims

Case Study

- In its defense, Target alleged that the hackers' malware did not immediately transmit the stolen data to the hackers' servers, but stored the stolen data on Target's own servers for up to six days before transmitting data to the hackers.
- After consolidation for multidistrict litigation, Target filed a motion to dismiss the banks' putative class-action claims for negligence, violation of Minnesota's Plastic Security Card Act, negligence per se, and negligent misrepresentation by omission
- The court held that the banks plausibly alleged that retailer owed them a duty of care, and the retailer owed them a duty to disclose material facts

Case Study

In re Adobe Systems, Inc. Privacy Litigation, 2014 WL 4379916, Case No.: 13–CV–05226–LHK (September 9, 2014)

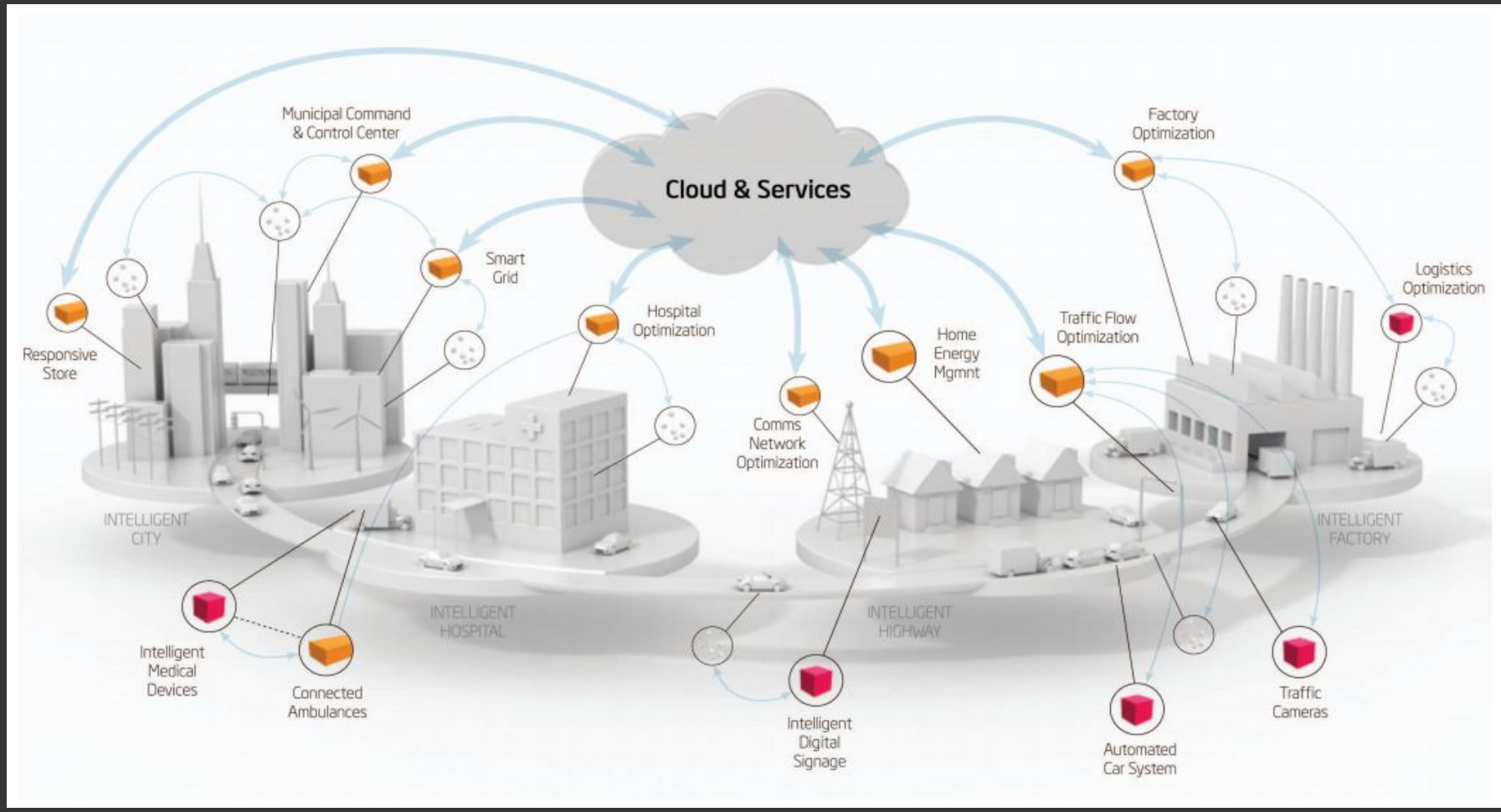
- Customers' personal information was compromised due to online data breach
- They filed a putative class action against Adobe alleging violation of California's Customer Records Act
- Adobe collected personal information from its customers
- In July 2013, hackers gained unauthorized access to Adobe's servers. In August 2013, they reached its databases that contained personal information

Case Study

- Adobe's Privacy Policy stated that: "Adobe provides reasonable administrative, technical, and physical security controls to protect your information. However, despite its efforts, no security controls are 100% effective and it cannot ensure or warrant the security of your personal information."
- Adobe's Safe Harbor Privacy Policy stated that: "Adobe uses reasonable physical, electronic, and administrative safeguards to protect your personal information from loss; misuse; or unauthorized access, disclosure, alteration, or destruction."

Case Study

- The data breach was not discovered until September 2013, when independent security researchers discovered stolen source code on the Internet
- Adobe announced that hackers accessed the personal information of at least 38 million customers
- It confirmed that hackers copied the source code for a number of its products (e.g., ColdFusion)
- It disclosed that hackers were able to use its systems to decrypt customers' credit card numbers, which were stored in encrypted form


Cloud & Services
Municipal Command & Control Center
Factory Optimization
Smart Grid
Logistics Optimization
Responsive Store
Hospital Optimization
Home Energy Mgmnt
Traffic Flow Optimization
Comms Network Optimization
INTELLIGENT CITY
INTELLIGENT FACTORY
INTELLIGENT HOSPITAL
INTELLIGENT HIGHWAY
Intelligent Medical Devices
Connected Ambulances
Intelligent Digital Signage
Automated Car System
Traffic Cameras

Security Level For Electronic Devices

- Electronic devices that connect over the web were created to transfer information, but were not originally designed with proper security features
- What's the proper security level when electronic devices are interconnected?
- For example, firewalls, encryptions, intrusion detection systems, and multi-factor authentications should be implemented as preventive and reactive measures

See internetlawyer-blog.com/2015/09/internet-of-things-and-security.html

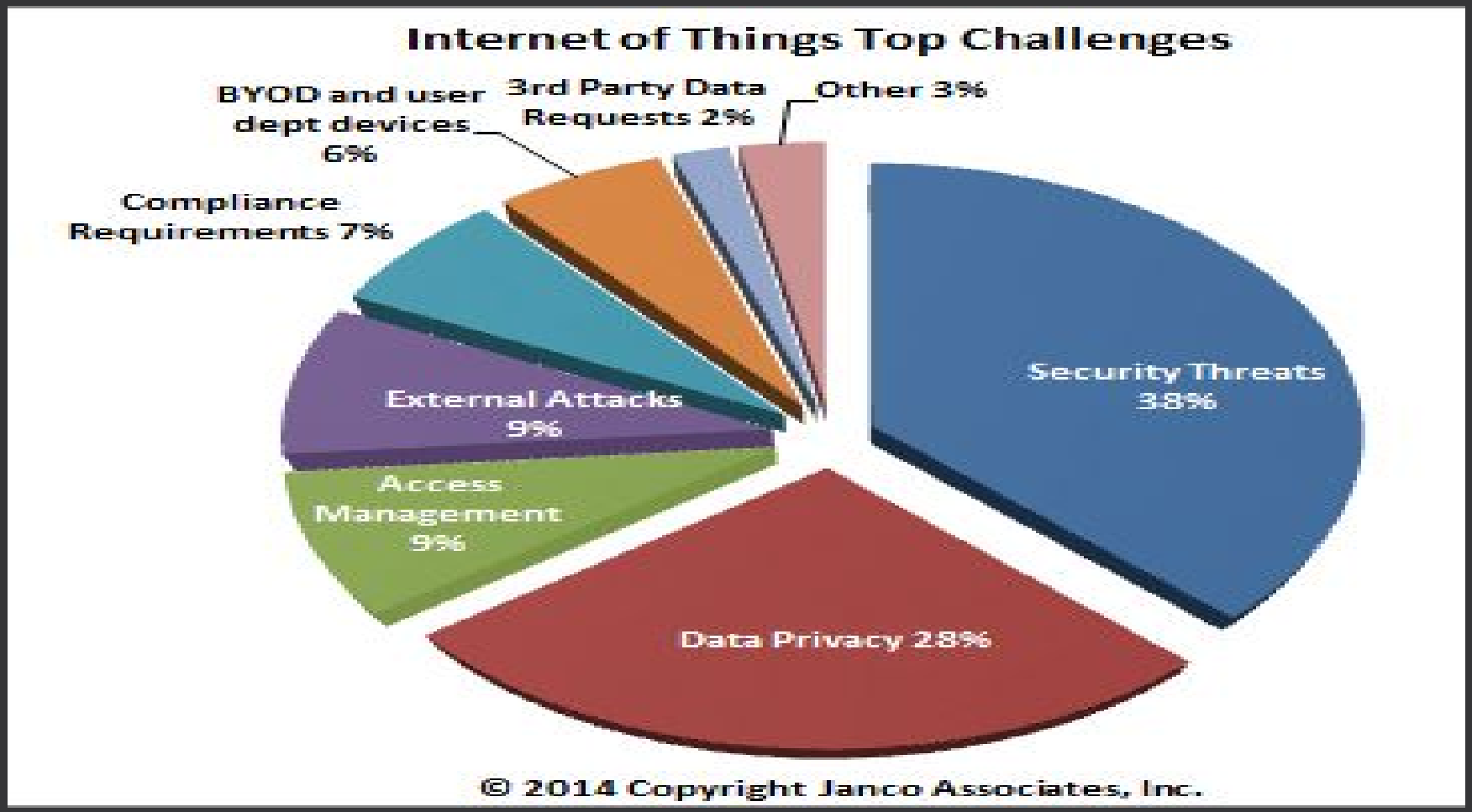
Security Level For Electronic Devices

- Electronic devices that can be accessed via the Internet (e.g., database server) should be segmented into their own network, and include network access restrictions
- Also, we should change default passwords on smart devices and implement strong passwords (e.g., SaLaR@ThOmSoN-SeMiNaR-2015!)
- A corporation's servers must be properly updated and secured to prevent unauthorized access

Security Level For Electronic Devices

- A skilled hacker can connect to a network server and gain access to confidential information (e.g., trade secrets)
- Information transferred wirelessly to and from printers, mobile phones, or other electronic devices is susceptible to unauthorized access
- Also, hackers can implement an IoT Botnet, which comprises of a group of compromised electronic devices that have been setup for illegal purposes

See http://whatis.techtarget.com/definition/IoT-botnet-Internet-of-Things-botnet


Internet of Things Top Challenges
BYOD and user dept devices 6%
3rd Party Data Requests 2%
Other 3%
Compliance Requirements 7%
External Attacks 9%
Access Management 9%
Security Threats 38%
Data Privacy 28%
© 2014 Copyright Janco Associates, Inc.

Security Level For Electronic Devices

- Public Wi-Fi is a concern because it's used to connect electronic devices to the Internet in public places (e.g., cafes, airports)
- Electronic devices can store network login/password upon return to public places and connect automatically
- Although, information may be encrypted, cyber criminals are able to decrypt information or use the illegally-obtained information for fraudulent transactions (e.g., online banking fraud, credit card fraud)
- See internetlawyer-blog.com/2015/09/internet-of-things-and-security.html

What Are The Major Security Concerns?

- The government uses new technology in order to battle crime and enforce the law
- For example, drones are important concerns for law enforcement
- They're accessible to the public and are being used to collect information and view public or private spaces
- For example, a government owned and operated drone can be accessed by hackers by tapping into its system without authorization

What Are The Major Security Concerns?

- Safety concerns, from the use of airspace, to the potential use of terrorism, are being faced by organizations which are trying to enhance security
- Law enforcement agencies use drones for surveillance
- The ability to track individuals via electronic devices has been useful, but it remains controversial
- Also, security measures must be implemented in order to enforce local and national security when using drones and similar surveillance devices

Data Security

- First, in the context of Internet of Things, data security is one of the biggest challenges
- The latest statistics indicate that 90% of connected devices are collecting personal information, and 70% are transmitting this data without encryption
- See Hewlett-Packard, *Internet of Things Research Study* 2 (July 2014)

Data Security

- Manufacturers entering the Internet of Things market should consider data security before they launch products
- Question: If a vulnerability is discovered on a device, should manufacturers notify consumers and patch the vulnerability?
- In reality, a device's security is as important as data security since we need to ensure functionality of connected cars, pacemakers, and other devices

See Tadayoshi Kohno, *Comments at Federal Trade Commission Workshop on Internet of Things 245* (Nov. 19, 2013)

Data Security

- In a legal action, FTC claimed that TRENDnet's cameras were vulnerable to having their feeds hijacked
- Approximately 700 private video feeds—which included images of children and families engaged in their daily activities—were hacked and publicly posted
- TRENDnet's exposure of private activities within consumers' homes constituted unfair conduct

See ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf

Data Security

The common reasons of network breaches include:

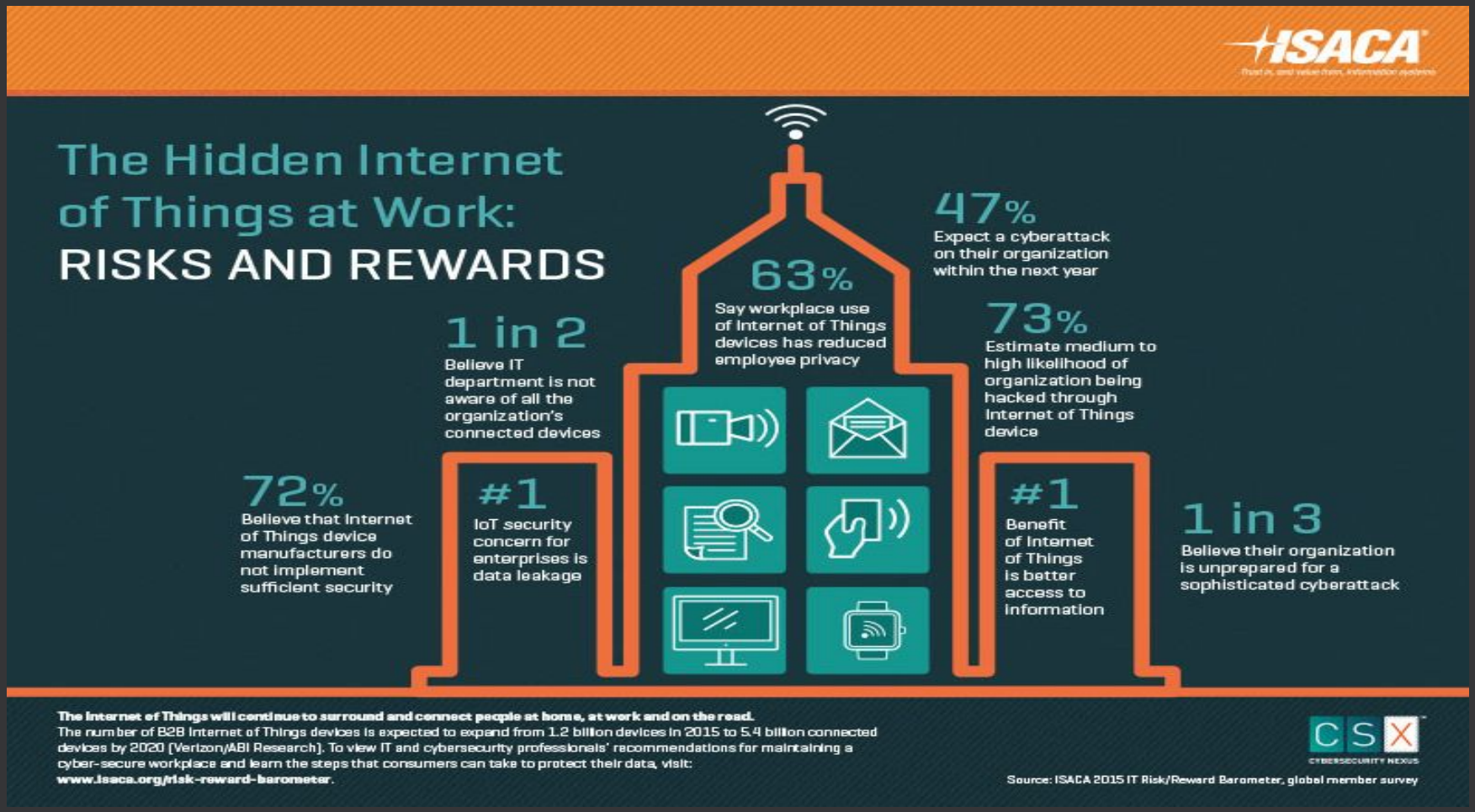
1. Hackers
2. Malware (e.g., virus, worm, spyware, adware, chargeware)
3. Network breach (e.g., DoS/DDoS/PDoS attacks)
4. Malicious insider (e.g., disgruntled employee)
5. Mobile devices (e.g., BYOD)

Data Security

- A Denial-of-Service ("DoS") attack bombards a high volume of information requests to overwhelm a network system
- A Distributed Denial-of-Service ("DDoS") attack occurs when many computers attack an individual system
- A Permanent Denial-of-Service ("PDoS") attack damages a system so badly that it requires hardware replacement or reinstallation
- See internetlawyer-blog.com/2014/12/e-residencies-e-states-risk-cyberattacks-digital-societies.html

Data Security

- Employees introduce connected electronic devices into their company networks all the time
- Therefore, companies must implement preventive measures to avoid unnecessary risks
- According to ISACA's 2015 IT Risk/Reward Barometer:
  - 73% of technologists believe that a company will be hacked via a connected device
  - 72% of technologists believe that manufacturers are not implementing proper security measures in connected devices
- See isaca.org/pages/2015-risk-reward-barometer.aspx


ISACA
The Hidden Internet of Things at Work:
RISKS AND REWARDS
63%
Say workplace use of Internet of Things devices has reduced employee privacy
47%
Expect a cyberattack on their organization within the next year
1 in 2
Believe IT department is not aware of all the organization's connected devices
73%
Estimate medium to high likelihood of organization being hacked through Internet of Things device
72%
Believe that Internet of Things device manufacturers do not implement sufficient security
#1
IoT security concern for enterprises is data leakage
#1
Benefit of Internet of Things is better access to information
1 in 3
Believe their organization is unprepared for a sophisticated cyberattack
The Internet of Things will continue to surround and connect people at home, at work and on the road.
The number of B2B Internet of Things devices is expected to expand from 1.2 billion devices in 2015 to 5.4 billion connected devices by 2020 (Verizon/ABI Research). To view IT and cybersecurity professionals' recommendations for maintaining a cyber-secure workplace and learn the steps that consumers can take to protect their data, visit:
www.isaca.org/risk-reward-barometer.
CSX
CYBERSECURITY NEXUS
Source: ISACA 2015 IT Risk/Reward Barometer, global member survey

Data Security

- The term “hidden” Internet of Things has been used in the context of connectivity of electronic devices within the corporate environment
- This is true because there are numerous entry points hackers can use to gain access to confidential information
- For example, fitness bands and smart watches can infiltrate the office on employee’s wrists and pockets
- So, electronic device manufacturers should adopt an industry-wide security standard

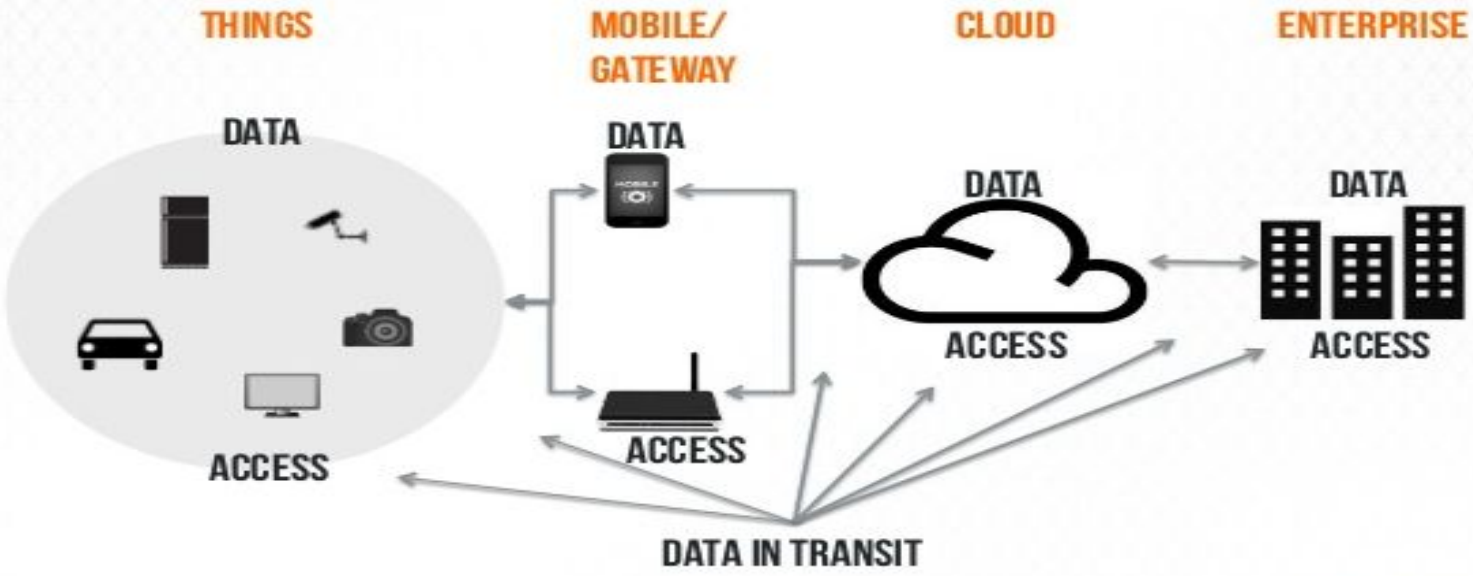
Data Security

Methods for companies to maintain a secure environment:

1. Embrace IoT devices to gain advantage over competition
2. Update electronic devices regularly with security upgrades
3. Ensure electronic devices are wirelessly connected to the workplace guest network
4. Implement cybersecurity training for employees to raise knowledge and awareness

See www.isaca.org for more information

SECURITY AND PRIVACY



Data Security

- Second, the other challenge is the collection and use of health, location, financial, and similar personal information
- Organizations may collect and use personal information from consumers outside the initially-permitted scope
- Health-related mobile apps have transmitted personal information to third parties without permission

See Jared Ho, *Comments at Federal Trade Commission Consumer Generated and Controlled Health Data Seminar 26–27* (May 7, 2014)

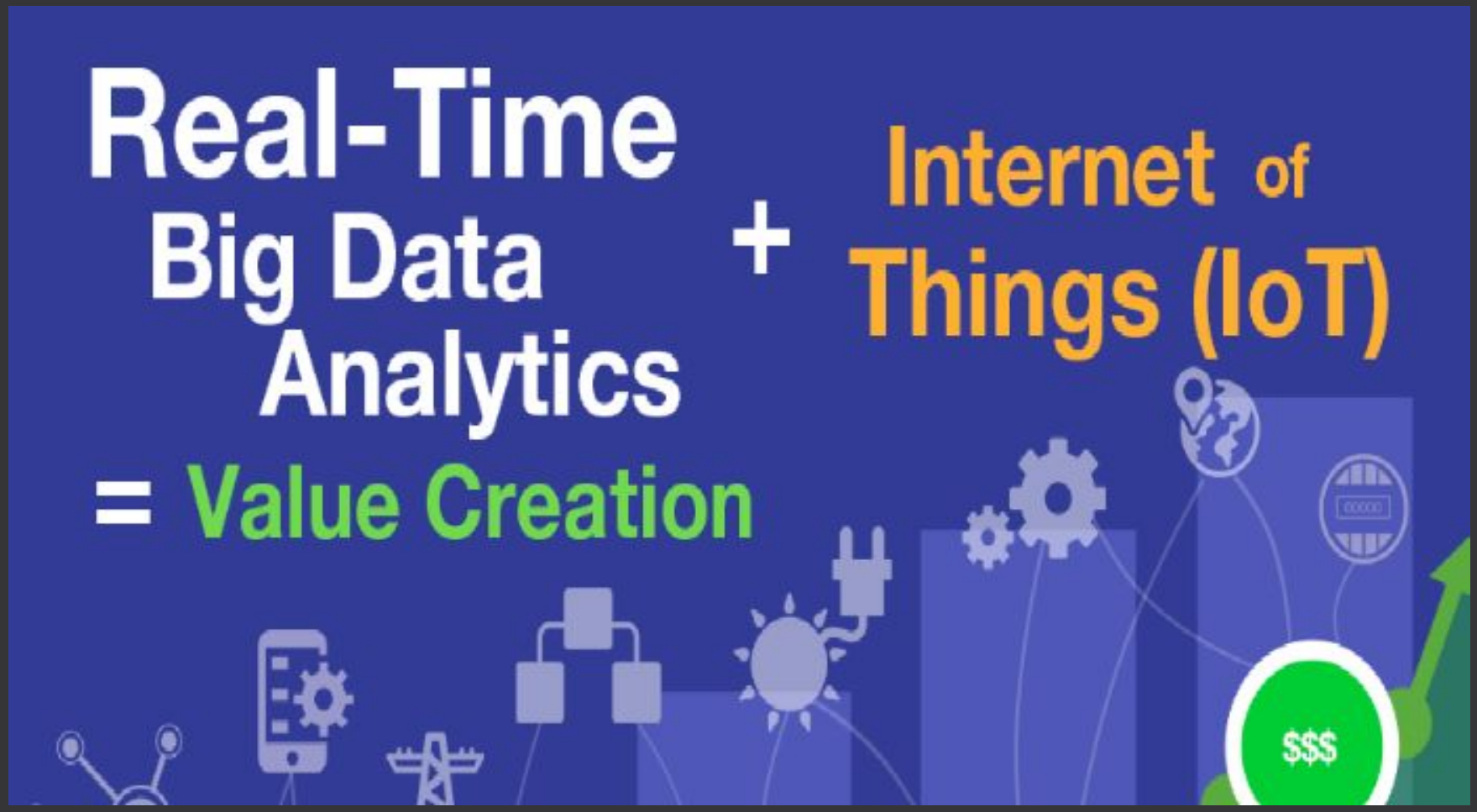
Ethical Use of Big Data

- Third, the next challenge is to ensure fair and ethical use of big data, which comes from connected devices
- Now, certain algorithms can make inferences and predictions about our behavior
- Data brokers collect data about us and merge them into profiles
- Also, banks can contact financially-challenged individuals with offers for low-cost banking products

See Michael Schrage, *Big Data's Dangerous New Era of Discrimination*, HARV. BUS. REV. (Jan. 29, 2014)

Ethical Use of Big Data

- These profiles may be used as tools for inclusion or to harm consumers
- These profiles may be used to target consumers with high-cost loans
- From an ethical standpoint, organizations must follow protocols on how to use personal information since the Internet of Things adds depth, precision, and accuracy


Real-Time
Big Data
Analytics
+
Internet of
Things (IoT)
= Value Creation
$$$

Case Study: *State v. McMurray*, 860 N.W.2d 686 (2015)

- The Supreme Court of Minnesota mentioned "Internet of Things" when Defendant moved to suppress narcotics evidence based on a warrantless search and seizure of his trash
- The court stated that:
  - More household waste is being recycled and the digital revolution is in full flourish
  - People are encouraged by government to recycle digital devices (e.g., routers, tablets, cell phones)

Case Study: *State v. McMurray*, 860 N.W.2d 686 (2015)

- In addition, the court mentioned that:
  - U.S. Supreme Court has recognized, digital devices and media, "[w]ith all they contain and all they may reveal, … hold for many Americans the privacies of life"
  - See *Riley v. California*, 134 S.Ct. 2473, 2494–95 (2014)
- This trend will accelerate as we enter the "Internet of Things" in which hundreds of billions of objects will become digital devices

Proposed Rules and Regulations

1) Black Box Privacy Protection Act

- On June 18, 2013, this bill was introduced to Congress, but was not enacted
- It sought to prohibit the sale of cars that were equipped with event data recorders (i.e., black boxes) unless the consumer controlled it
- It also required that recorded data be considered as the car owner's property
- Any violation constituted unfair or deceptive practices pursuant to the Federal Trade Commission Act
- See govtrack.us/congress/bills/113/hr2414

Proposed Rules and Regulations

2) We are Watching You Act

- On June 13, 2013, this bill was introduced to Congress, but was not enacted
- It sought to require notification to consumers before a video service collects visual or auditory information from the viewing area
- Its sought to provide consumers with choices that do not involve the collection of such information, and for other purposes
- See govtrack.us/congress/bills/113/hr2356

Federal Trade Commission Act

- FTC Act
  - Under Section 5, the FTC can take action against companies that engage in "unfair or deceptive" practices
  - In 1938, when Congress added this authority, it probably wasn't considering data privacy or cybersecurity
  - So far, FTC has instigated 40+ privacy-related enforcement actions and 55+ data security enforcement actions
  - See ftc.gov/reports/privacy-data-securityupdate-2014

Health Insurance Portability and Accountability Act

- HIPAA
  - It was implemented to protect private health information
  - It contains security regulations, which according to the Department of Health & Human Services, set national standards for the security of patient health information
  - The HIPAA Breach Notification Rule requires third parties to provide notification following a breach of unsecured protected health information
  - See hhs.gov/ocr/privacy/hipaa/understanding/summary

Gramm-Leach Bliley Act

- Gramm-Leach Bliley Act
  - It requires financial institutions to explain their information-sharing practices and to safeguard sensitive information
  - Under the Safeguards Rule, financial institutions must protect consumer information
  - It gives consumers the right to opt-out from a limited amount of non-public personal information sharing
  - It's codified under *15 U.S.C. §§ 6801-09*
  - See https://epic.org/privacy/glba

Fair Credit Reporting Act

- FCRA
  - It was enacted to promote the accuracy, fairness, and privacy of consumer information held by consumer reporting agencies
  - It requires consumer reporting agencies to provide information in your file upon your request
  - It prohibits consumer reporting agencies from providing credit reports to any party that lacks a permissible purpose
  - It prohibits consumer reporting agencies from giving your credit information to employers without written consent
  - It's codified under *15 U.S.C. § 1681 et seq.*

Communications Act - 47 U.S.C. § 222

- In 1996, Congress passed the new Privacy of Customer Information provision, codified as Section 222 of the Communications Act
- It states, in part, that: "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of … other telecommunication carriers, equipment manufacturers, and customers …"
- It contains restrictions on the use of customer information by all carriers
- See https://epic.org/privacy/iei/cpnipet.html

Communications Act - 47 U.S.C. § 338

- It states that "[e]ach satellite carrier providing … secondary transmissions to subscribers located within the local market of a television broadcast station … shall carry … the signals of all television broadcast stations located within that local market"
- It requires satellite carriers to provide written notice to subscribers about: (A) nature of personally identifiable information collected; (B) nature, frequency, and purpose of disclosure; (C) period during which information will be maintained; (D) times and places which subscriber may have access to information; and (E) limitations on collection/disclosure of information and subscriber's rights
- See *47 U.S.C. § 338(i)(1)*

Communications Act - 47 U.S.C. § 631

- It was designed to protect personal information gathered from consumers through an organization's verification procedures
- Multichannel Video Programming Distributors ("MVPDs") have a statutory obligation pursuant to Sections 338(i)(4)(A) and 631(c)(1) to protect subscribers' personal information
- These provisions are designed to protect consumer privacy since they prohibit disclosure of subscribers' personally identifiable information without prior consent
- See fcc.gov/document/fcc-adopts-new-video-device-accessibility-rules

State Privacy Regulations

- In 2014, approximately 60 new privacy laws were passed at the state level
- These privacy laws were enacted on the following issues:
  - Limiting employer's ability to view employee's social network account
  - Prohibiting employers/insurers from using information about certain medical conditions
  - Requiring companies to notify consumers when they suffer a data security breach
  - See ncsl.org/research/telecommunications-and-information-technology/security-breachnotification-laws.aspx

State Privacy Regulations

- The Privacy Rights for California Minors in the Digital World Act (a/k/a "Eraser Bill") allows minors to remove, or to request and obtain removal of, information posted on websites, online services, online applications, or mobile applications
- It prohibits a website from marketing/advertising products or services to minors that minors are not allowed to purchase (e.g., alcohol, tobacco, firearms)
- See *California Business & Professions Code §§ 22580-22582*

State Privacy Regulations

- California's Govt. Code § 6267 protects a library patron's use records (e.g., database search records, borrowing records, class records) from disclosure
- California Reader Privacy Act, codified under Civil Code § 1798.90:
  - Protects information about the books Californians browse, read, or purchase from electronic services and online booksellers
  - Requires a search warrant, court order, or user's affirmative consent before a business can disclose the user's personal information related to his/her book usage with exceptions (e.g., imminent danger of death)

State Privacy Regulations

California Bus. & Prof. Code § 22575

- It requires a commercial website to disclose in its privacy policy how it responds to a web browser "Do Not Track" signal
- It also requires a commercial website to disclose whether third parties are tracking consumers on its website
- This mechanism allows consumers to exercise choice about online tracking of their personal information
- See leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

State Privacy Regulations

California Bus. & Prof. Code §§ 22575-22578

- The Online Privacy Protection Act requires a website operator (i.e., entity that collects personally identifiable information from California residents through online services for commercial purposes) to post a conspicuous privacy policy
- It requires the privacy policy to identify the categories of personally identifiable information that the website operator collects about consumers (e.g., name, address, telephone, zip code)
- See leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

State Privacy Regulations

California Education Code § 99122

- It requires private nonprofit or for-profit postsecondary educational institutions to post a social media privacy policy on the their websites
- The statute defines “social media” as an electronic service or electronic content (e.g., videos, images, blogs, podcasts)
- See leginfo.ca.gov/cgi-bin/displaycode?section=edc&group=99001-100000&file=99120-99122

State Privacy Regulations

- For example, Nevada and Minnesota require Internet Service Providers ("ISPs") to keep certain information private unless the customer permits its disclosure
- They both prohibit disclosure of personally identifying information. However, Minnesota also requires ISPs to obtain permission from subscribers before disclosing information about their online surfing habits
- See *Minnesota Statutes §§ 325M.01 to .09*
- See *Nevada Revised Statutes § 205.498*

State Privacy Regulations

- California and Utah require all non-financial businesses to disclose the types of personal information they share with or sell to a third party for direct marketing purposes
- Under the California law, businesses may post a privacy statement that gives customers the option to choose not to share information
- See *California Civil Code §§ 1798.83-84*
- See *Utah Code §§ 13-37-101, 102, 201-203*

State Privacy Regulations

False and Misleading Statements In Website Privacy Policies

- Under *Nebraska Stat. § 87-302(14)*, Nebraska prohibits knowingly making a false or misleading statement in a privacy policy about the use of personal information submitted by the public
- Under *18 Pa. C.S.A. § 4107(a)(10)*, Pennsylvania prohibits false and misleading statements in privacy policies that are published on websites
- See ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

State Privacy Regulations

Monitoring of Employee E-mail Communications and Internet Access

- Connecticut and Delaware require employers to give notice to employees prior to monitoring e-mail communications or Internet access
- Colorado and Tennessee require states and other public entities to adopt a policy related to monitoring of public employees' e-mails
- See *Connecticut Gen. Stat. § 31-48d*
- See *Delaware Code § 19-7-705*

State Privacy Regulations

Connecticut Gen. Stat. § 31-48d

- Employers who engage in any type of electronic monitoring must give prior written notice to all employees, informing them of the types of monitoring which may occur
- If an employer has reasonable grounds to believe that employees are engaged in illegal conduct and electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice.
- It provides for civil penalties of $500 for the first offense, $1,000 for the second offense, and $3,000 for the third and each subsequent offense

State Privacy Regulations

Delaware Code § 19-7-705

- It prohibits employers from monitoring or intercepting electronic mail or Internet access or usage of an employee unless the employer has given a one-time written or electronic notice to the employee
- It provides exceptions for processes that are performed solely for the purpose of computer system maintenance and/or protection, and for court ordered actions
- It provides for a civil penalty of $100 for each violation
- See delcode.delaware.gov/title19/c007/sc01/index.shtml#705

State Privacy Regulations

Colorado Rev. Stat. § 24-72-204.5

- It requires the state or any agency, institution, or political subdivision that operates or maintains e-mail communications system to adopt a written policy on monitoring of e-mails
- The written policy must include a statement that employee's e-mails may be part of public records and subject to inspection
- See lexisnexis.com/hottopics/Colorado

State Privacy Regulations

Tennessee Code § 10-7-512

- It requires the state and its agencies that operate or maintain an e-mail system to adopt a written policy on e-mail monitoring
- The written policy must include a statement that employee's emails may be part of public records and subject to inspection
- See http://law.justia.com/codes/tennessee/2010/title-10/chapter-7/part-5/10-7-512

State Privacy Regulations

- At least 17 states require government websites or state portals to implement privacy policies, or to incorporate machine-readable privacy policies
- California Govt. Code § 11019.9 requires privacy policies to state that: (1) personally identifiable information is obtained legally; (2) purpose of collected personally identifiable information is specified: (3) personal data will not be disclosed for other purposes without consent; (4) personal data is relevant to the purpose for which it is collected; (5) general means by which personal data is protected against unauthorized access; and (6) each state agency will designate a department responsible for the privacy policy.

What Are the Applicable Rules and Regulations?

Federal statutes

1. Children's Online Privacy Protection Act – 15 U.S.C. § 6501 et seq.
2. E-SIGN – 15 U.S.C. § 7001(d)
3. FCRA/FACTA – 15 U.S.C. § 1681 et seq.
4. FISMA – 44 U.S.C. §§ 3541-3549
5. FTC Act – 15 U.S.C. § 45(a)(1)
6. GLBA – 15 U.S.C. §§ 6801, 6805
7. HIPAA – 42 U.S.C. §§ 1320d-2 and 1320d-4
8. Homeland Security Act of 2002 – 44 U.S.C. § 3532(b)(1)
9. Privacy Act of 1974 – 5 U.S.C. § 552a

What Are the Applicable Rules and Regulations?

State statutes

1. Civil Code § 1798.81.5(b) – obligates to provide security for personal information
2. Civil Code § 1798.85(a)(3) – imposes duty to encrypt personal information
3. Civil Code § 1798.81 – relates to data disposal and destruction
4. Civil Code § 1798.82 – relates to security breach notifications
5. Civil Code § 1798.85 / Family Code § 2024.5 – relates to social security number protection

Note: New Mexico's Data Breach Notification Act (HB 224) did not pass

What Are the Applicable Rules and Regulations?

Federal regulations

1. Federal regulations imposing an obligation to provide security
   a) COPPA regulations – 16 C.F.R. § 312.8
   b) DHS regulations – 8 C.F.R. Part 274a (e), (f), (g), and (h)
   c) FCC Order re: Pretexting – 47 C.F.R. §§ 64.2001-64.2011
   d) FDA regulations – 21 C.F.R. Part 11
   e) FFIEC Guidance – see www.ffiec.gov
   f) GLBA security regulations – 12 C.F.R. Part 30, Appendix B
   g) GLBA security regulations (FTC) – 16 C.F.R. Part 314

What Are the Applicable Rules and Regulations?

Federal regulations

2. Federal regulations imposing authentication requirements
   a) ACH operating rules (2013) Section 2.5.2.5(d)
   b) Banking Know Your Customer Rules
      i. 31 C.F.R. § 103.121 – bank customer ID programs
      ii. 31 C.F.R. § 103.122 – broker-dealer customer ID programs
      iii. 31 C.F.R. § 103.123 – futures commission merchants customer ID programs
      iv. 31 C.F.R. § 103.131 –mutual funds' customer ID programs

Any Questions?

Salar Atrizadeh, Esq.
Law Offices of Salar Atrizadeh
9701 Wilshire Blvd., 10th Floor
Beverly Hills, CA 90212
T: 310-694-3034
F: 310-694-3057
Email: salar@atrizadeh.com
Website: atrizadeh.com
Blog: internetlawyer-blog.com