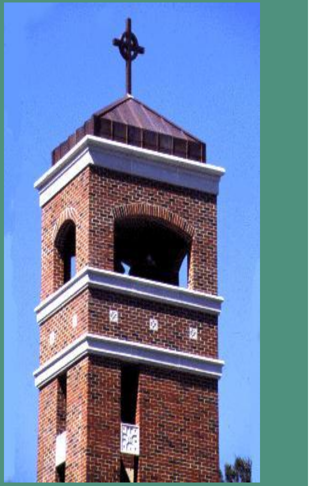


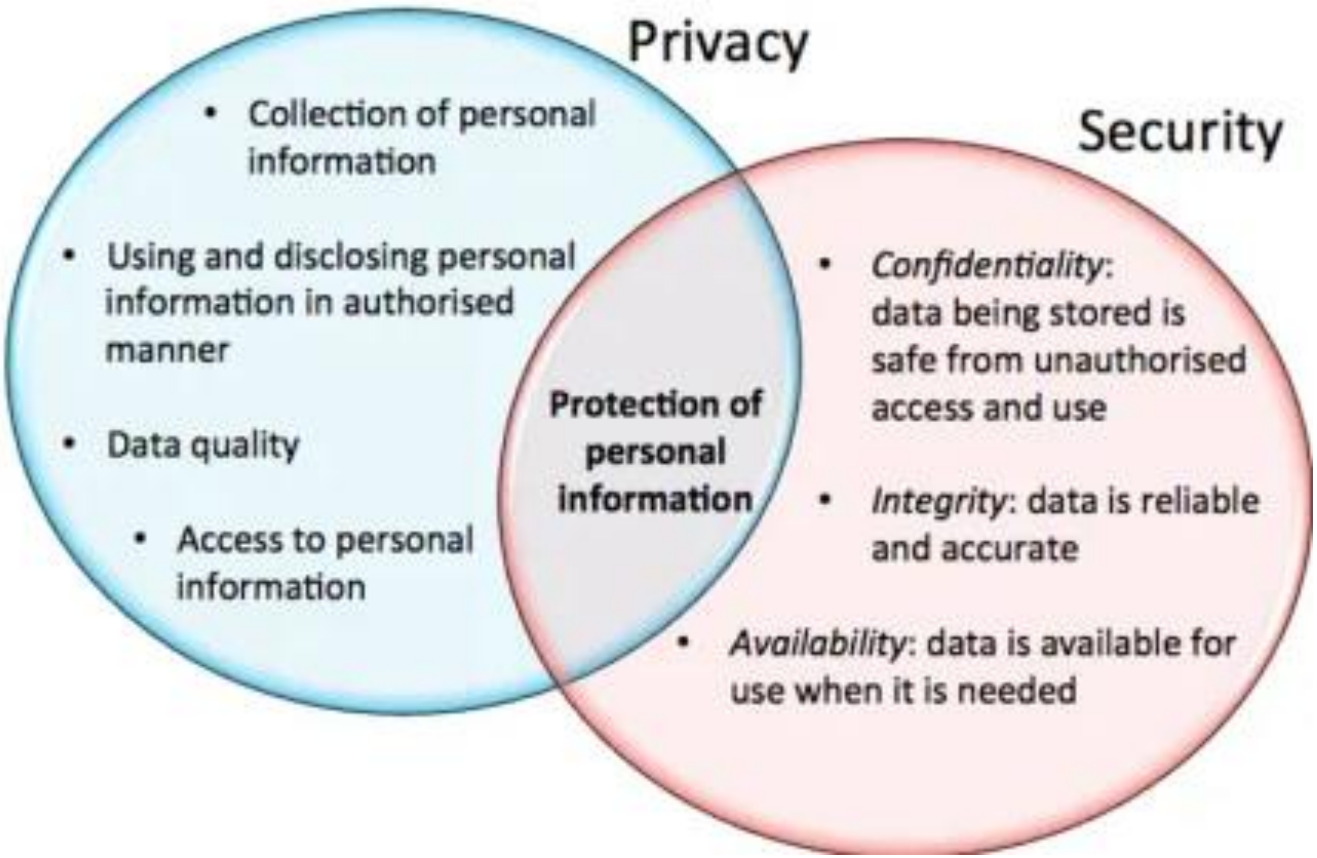
Introduction to MIS

Risk Management and Information Security

Learning Objectives

- Describe information technologies that could be used in computer crimes
- Describe basic safeguards in computer and network security
- Explain the major security threats
- Describe security and enforcement measures
- Summarize the guidelines for a comprehensive security system, including business continuity planning

Privacy & Security



Privacy

- Collection of personal information
- Using and disclosing personal information in authorised manner
- Data quality
- Access to personal information

Protection of personal information

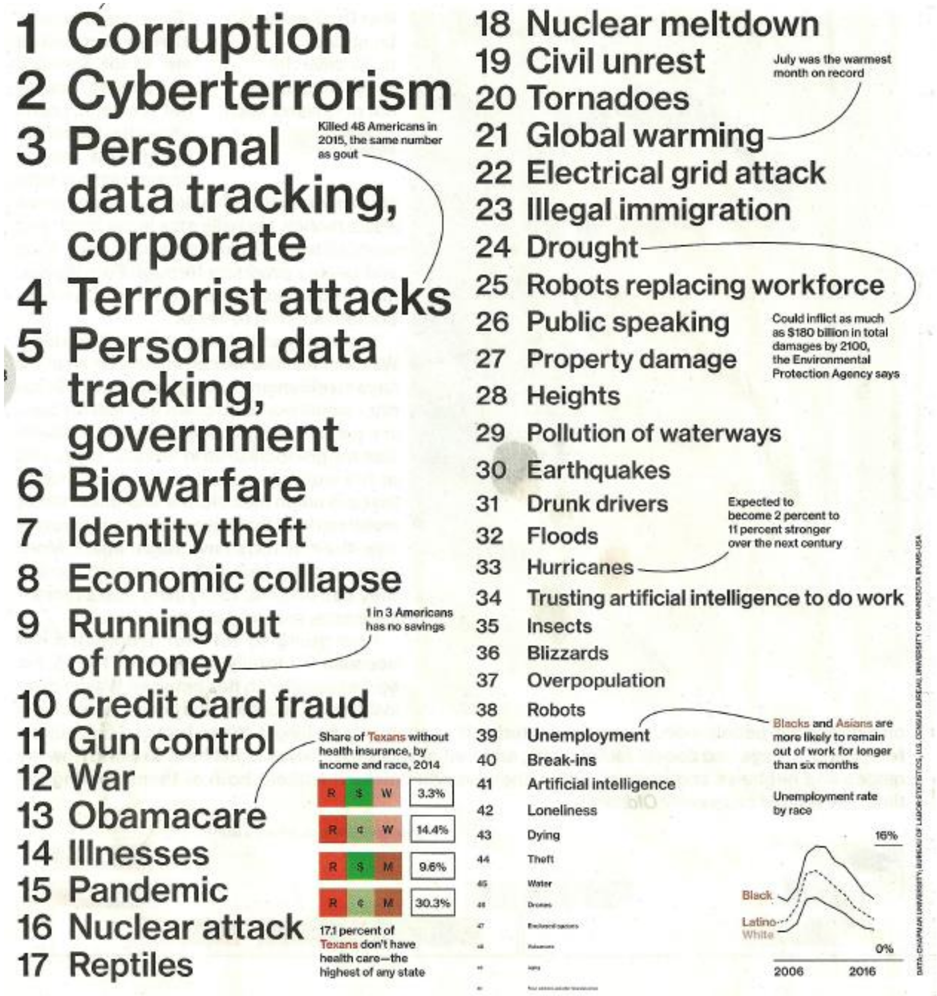
Security

- *Confidentiality*: data being stored is safe from unauthorised access and use
- *Integrity*: data is reliable and accurate
- *Availability*: data is available for use when it is needed

Today’s Insecure World

- Today we seem to be living in a constant state of “insecurity” !
  - Our personal safety
  - Our children
  - Our automobiles
  - Our home & property
  - Our PC and data
  - Our laptops & PDA’s
  - Our job
  - Our reputation

What People Fear



1 Corruption
2 Cyberterrorism
3 Personal data tracking, corporate
4 Terrorist attacks
5 Personal data tracking, government
6 Biowarfare
7 Identity theft
8 Economic collapse
9 Running out of money
10 Credit card fraud
11 Gun control
12 War
13 Obamacare
14 Illnesses
15 Pandemic
16 Nuclear attack
17 Reptiles
18 Nuclear meltdown
19 Civil unrest
20 Tornadoes
21 Global warming
22 Electrical grid attack
23 Illegal immigration
24 Drought
25 Robots replacing workforce
26 Public speaking
27 Property damage
28 Heights
29 Pollution of waterways
30 Earthquakes
31 Drunk drivers
32 Floods
33 Hurricanes
34 Trusting artificial intelligence to do work
35 Insects
36 Blizzards
37 Overpopulation
38 Robots
39 Unemployment
40 Break-ins
41 Artificial intelligence
42 Loneliness
43 Dying
44 Theft
45 Water
46 Drones
47 Enclosed spaces
48 Volcanoes
49 Aging
50 [illegible]

Killed 48 Americans in 2015, the same number as gout

1 in 3 Americans has no savings

Share of Texans without health insurance, by income and race, 2014

R	$	W	3.3%
R	¢	W	14.4%
R	$	M	9.6%
R	¢	M	30.3%

17.1 percent of Texans don't have health care—the highest of any state

July was the warmest month on record

Could inflict as much as $180 billion in total damages by 2100, the Environmental Protection Agency says

Expected to become 2 percent to 11 percent stronger over the next century

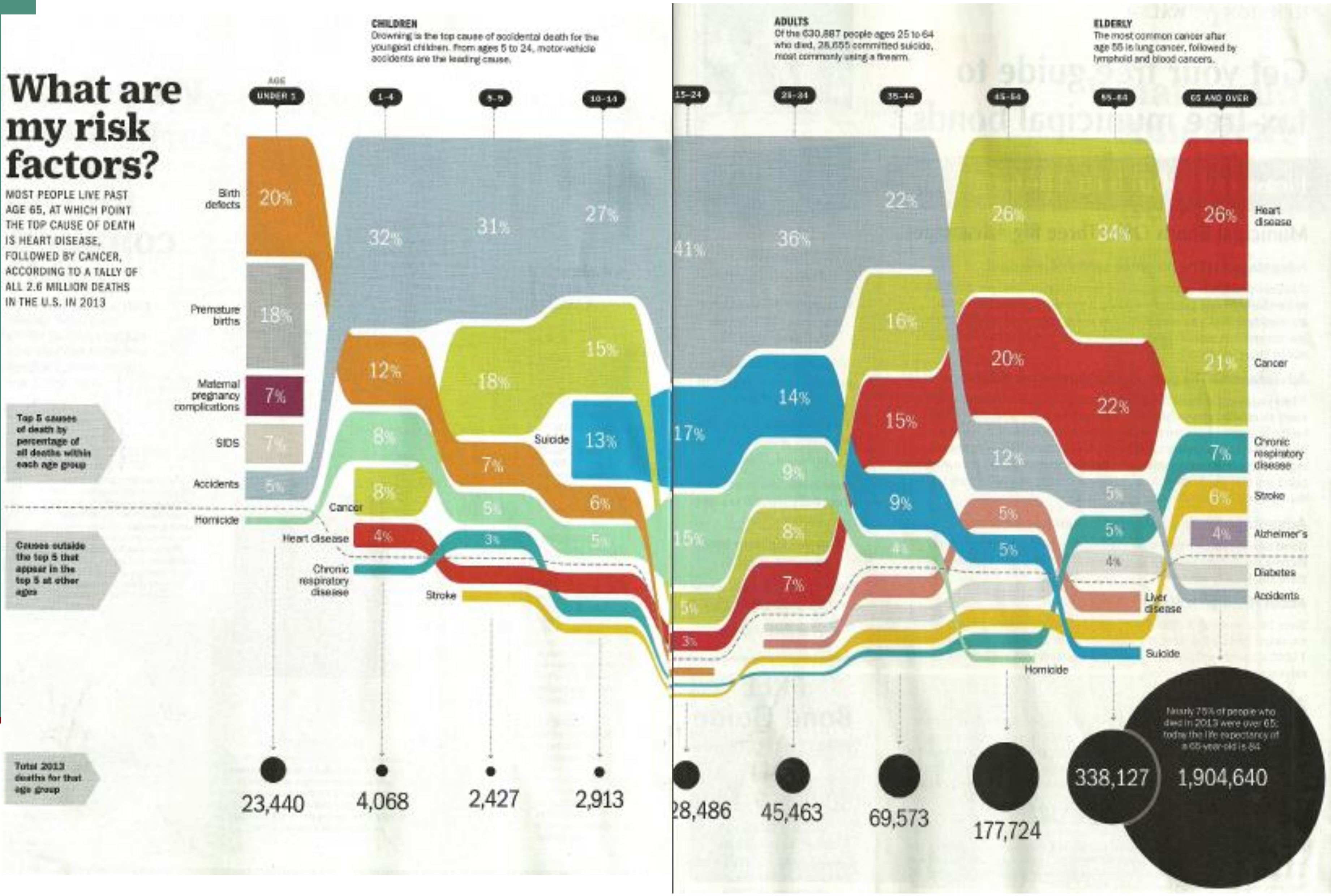
Blacks and Asians are more likely to remain out of work for longer than six months

Unemployment rate by race

DATA: CHAPMAN UNIVERSITY; BUREAU OF LABOR STATISTICS; U.S. CENSUS BUREAU; UNIVERSITY OF MINNESOTA IPUMS-USA

- What is one most likely to die from ?

- Do not look ahead !



What are my risk factors?

MOST PEOPLE LIVE PAST AGE 65, AT WHICH POINT THE TOP CAUSE OF DEATH IS HEART DISEASE, FOLLOWED BY CANCER, ACCORDING TO A TALLY OF ALL 2.6 MILLION DEATHS IN THE U.S. IN 2013

CHILDREN
Drowning is the top cause of accidental death for the youngest children. From ages 5 to 24, motor-vehicle accidents are the leading cause.

ADULTS
Of the 630,887 people ages 25 to 64 who died, 28,655 committed suicide, most commonly using a firearm.

ELDERLY
The most common cancer after age 55 is lung cancer, followed by lymphoid and blood cancers.

Nearly 75% of people who died in 2013 were over 65; today the life expectancy of a 65-year-old is 84

Top 5 causes of death by percentage of all deaths within each age group

Causes outside the top 5 that appear in the top 5 at other ages

Total 2013 deaths for that age group

Risk

- **Risk** is a concept that denotes a potential negative impact to an asset or something important
- In everyday usage, *risk* is often used synonymously with the probability of a known loss, but risk is the "possibility" of a loss
- Paradoxically, a probable loss can be uncertain and relative in an individual event (will my house burn down in the next 10 years?), while having a certainty in the aggregate of multiple events (how many houses burn down each year)

Danger vs Risk

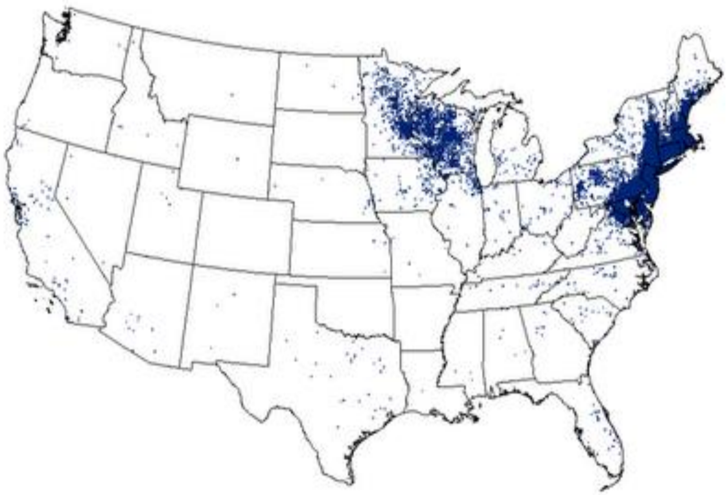
Which of the following animals pose the greatest risk to US human life?

- Do not look ahead !

Bambi Collisions

- Deer are responsible for more human deaths in the U.S. than all the others combined
- About 150 deaths per year due to their habit of running out on roads (over 1.5 million deer/auto crashes annually – over $1 billion property damage)
- **What state has the most deer/auto collisions ?**

Reported Cases of Lyme Disease -- United States, 2006

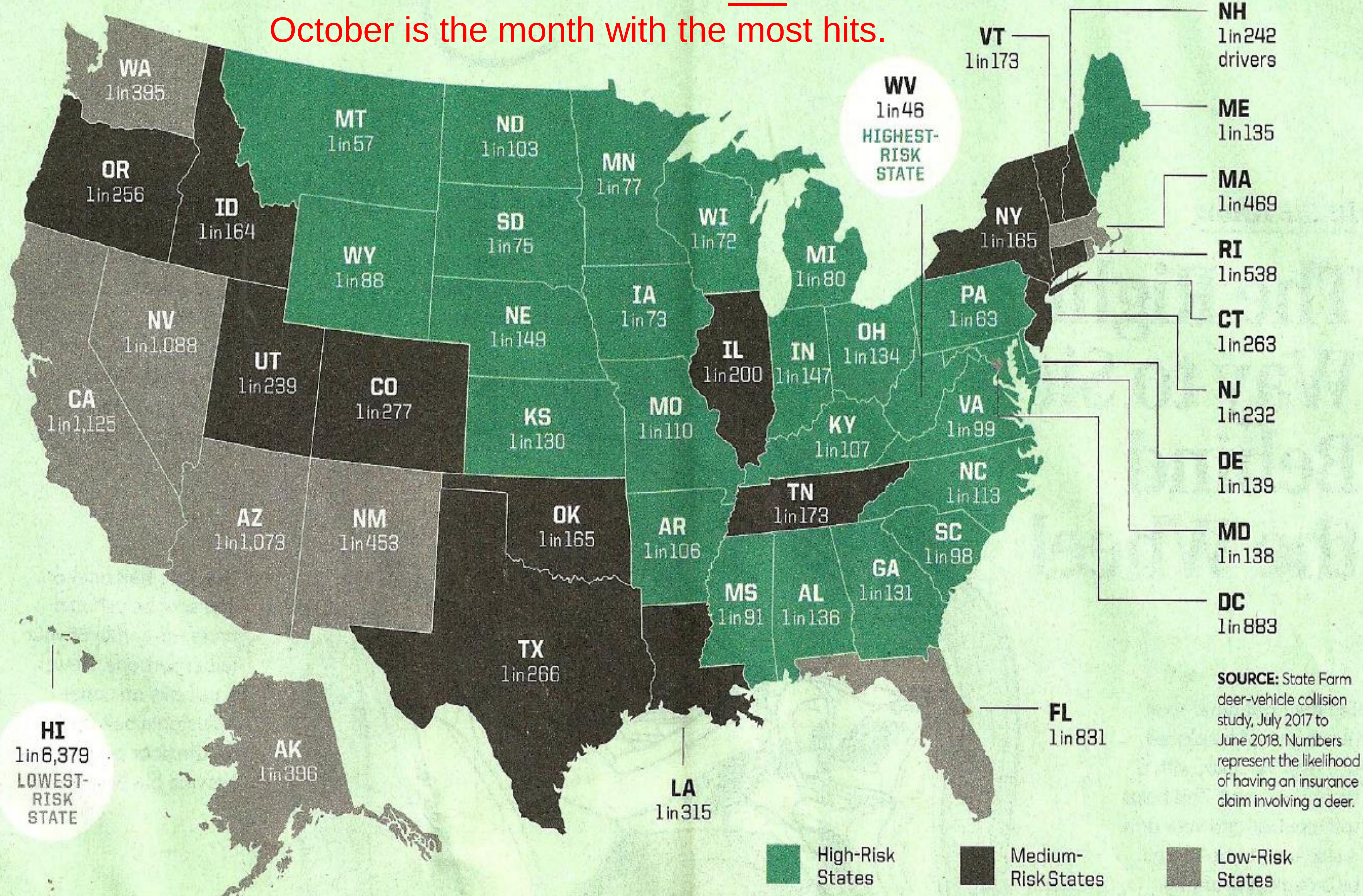


1 dot placed randomly within county of residence for each reported case

Copyright – D. Brandon, Ph.D.

How Likely Are You to Hit a Deer?

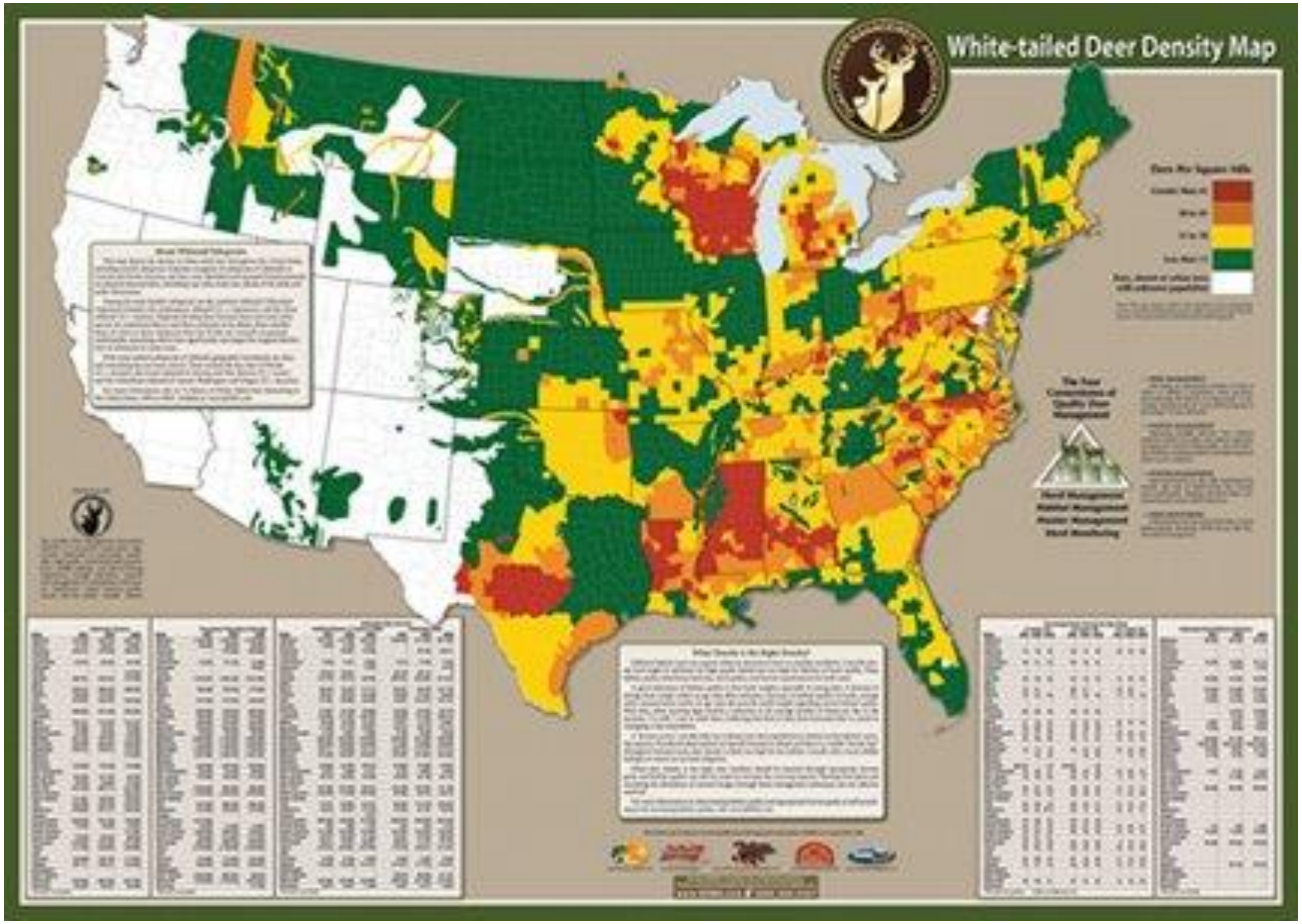
States that have a lot of deer <u>and</u> a lot of drivers.
October is the month with the most hits.



SOURCE: State Farm deer-vehicle collision study, July 2017 to June 2018. Numbers represent the likelihood of having an insurance claim involving a deer.

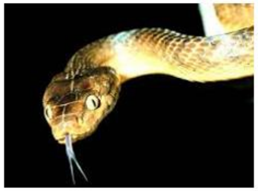
Bambi Collisions (con’t)

[MS has more deer per sq mile, but less drivers]

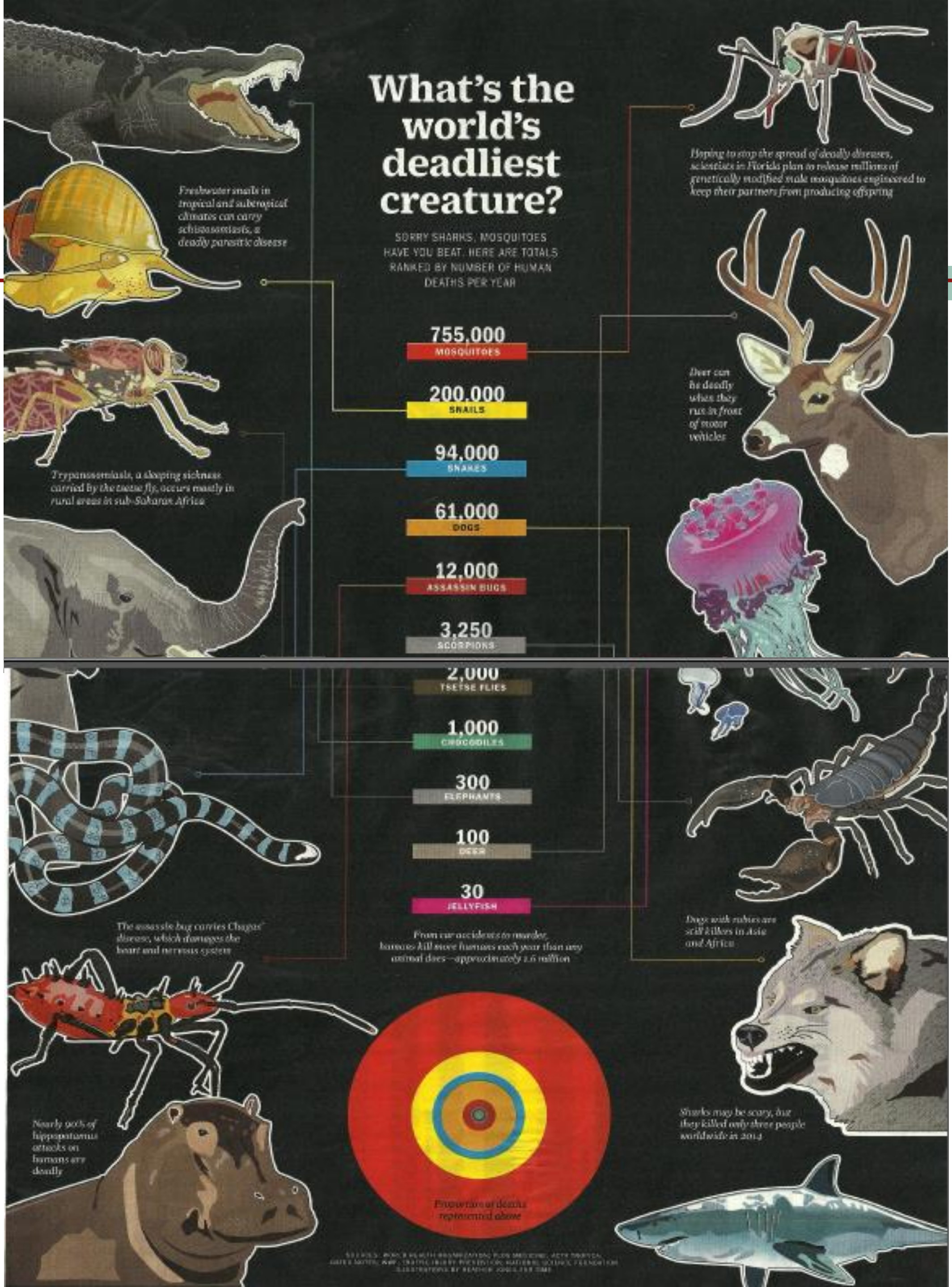


- Horses (not shown) are responsible for 219 human deaths per year – although these are voluntary (mostly riding accidents)
- Dogs are only responsible for 14 deaths per year
- Thus while the impact of being confronted by some of these animals like the bear, shark, or alligator is high, the overall likelihood is small; which makes the overall risk smaller

- What is the deadliest creature in the world ?



- Do not look ahead !



What's the world's deadliest creature?

SORRY SHARKS, MOSQUITOES HAVE YOU BEAT. HERE ARE TOTALS RANKED BY NUMBER OF HUMAN DEATHS PER YEAR

Freshwater snails in tropical and subtropical climates can carry schistosomiasis, a deadly parasitic disease

Trypanosomiasis, a sleeping sickness carried by the tsetse fly, occurs mostly in rural areas in sub-Saharan Africa

Hoping to stop the spread of deadly diseases, scientists in Florida plan to release millions of genetically modified male mosquitoes engineered to keep their partners from producing offspring

Deer can be deadly when they run in front of motor vehicles

The assassin bug carries Chagas' disease, which damages the heart and nervous system

From car accidents to murder, humans kill more humans each year than any animal does—approximately 1.6 million

Dogs with rabies are still killers in Asia and Africa

Nearly 90% of hippopotamus attacks on humans are deadly

Sharks may be scary, but they killed only three people worldwide in 2014

SOURCES: WORLD HEALTH ORGANIZATION; PLOS MEDICINE; ACTA TROPICA; GATES NOTES; WWF; TRAFFIC INJURY PREVENTION; NATIONAL SCIENCE FOUNDATION
ILLUSTRATIONS BY HEATHER JONES FOR TIME

Risk & IT

- IT risks:
  - Information security
  - Cyber security – hardware, software, networks, IT personnel, etc.
- IT used in risk Management activities
  - Physical risks – acts of nature, crime, etc.
  - Virtual risks – financial, reputation, information, etc.

Business Risk

- All three business value chain flows (material, information, currency) involve:
  - Time
  - Cost
  - Risk (Possibility of errors, loss, damage, etc.)
- The goal of ABC (and all business) is to minimize the time, cost, and risk in these flows through whatever means possible, particularly technology !!!

Risk Can Be Reduced

- All activities have some degree of risk; most have considerable risk
- Risk can be reduced !
- To achieve significant risk reduction requires a very proactive effort starting with careful risk planning
- **What % of risk can be reduced ?**

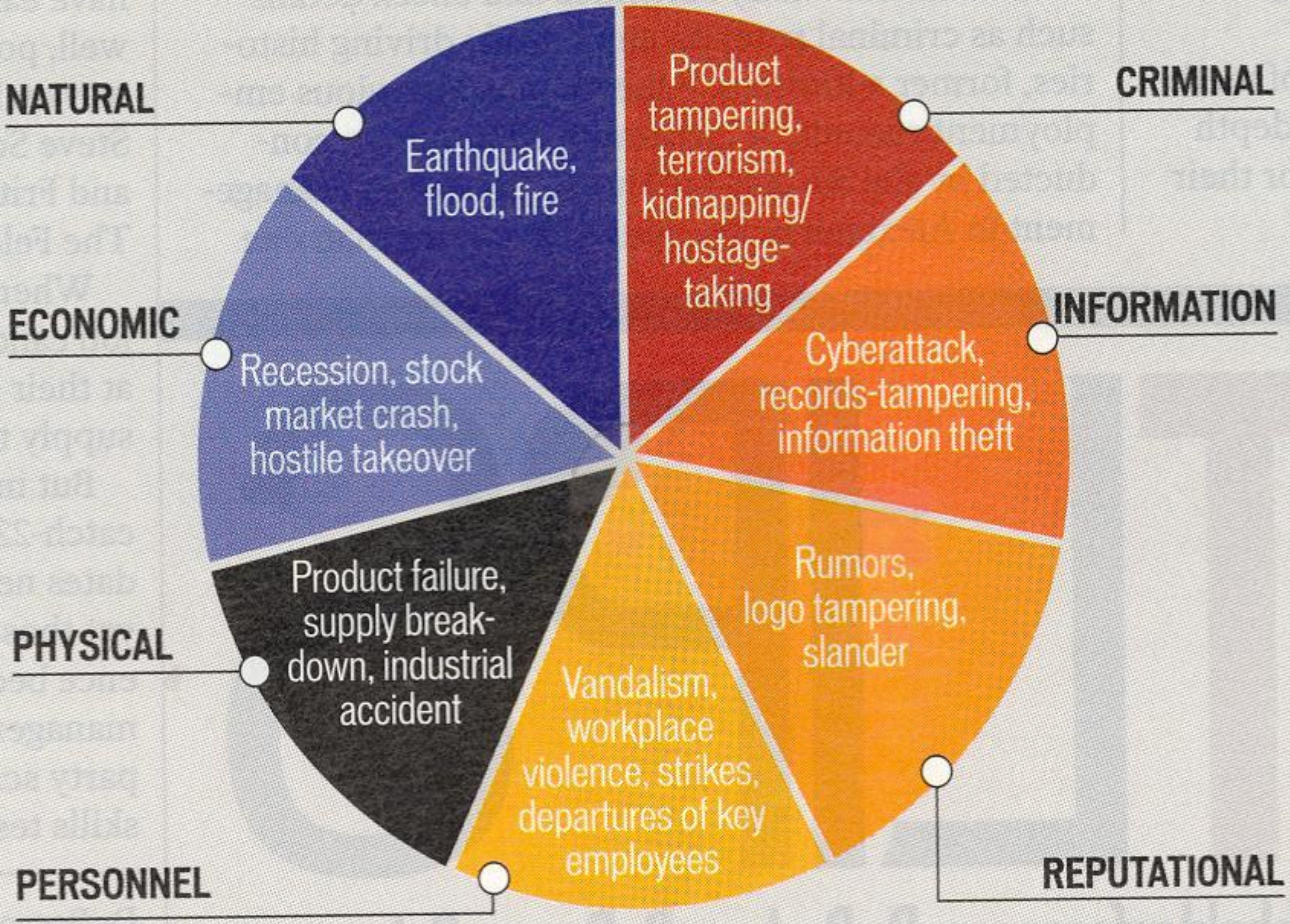
Copyright – Dan Brandon

- Do not look ahead !

- Studies have found that risk can be reduced up to 90%

Risk (con't)

- A **threat** to an information resource is any danger (hazard) to which a system may be exposed and susceptible
- The **exposure** (impact) of an information resources is the harm, loss or damage that can result if a threat compromises that resource
- **Risk** is related to the impact times the likelihood:
  - Loss = ProbabilityOfThreat * Impact
- **IT risk controls** are the procedures, devices, or software aimed at preventing a compromise to the system via **minimizing impact and/or probability**


NATURAL
Earthquake, flood, fire
CRIMINAL
Product tampering, terrorism, kidnapping/ hostage-taking
INFORMATION
Cyberattack, records-tampering, information theft
REPUTATIONAL
Rumors, logo tampering, slander
PERSONNEL
Vandalism, workplace violence, strikes, departures of key employees
PHYSICAL
Product failure, supply break-down, industrial accident
ECONOMIC
Recession, stock market crash, hostile takeover

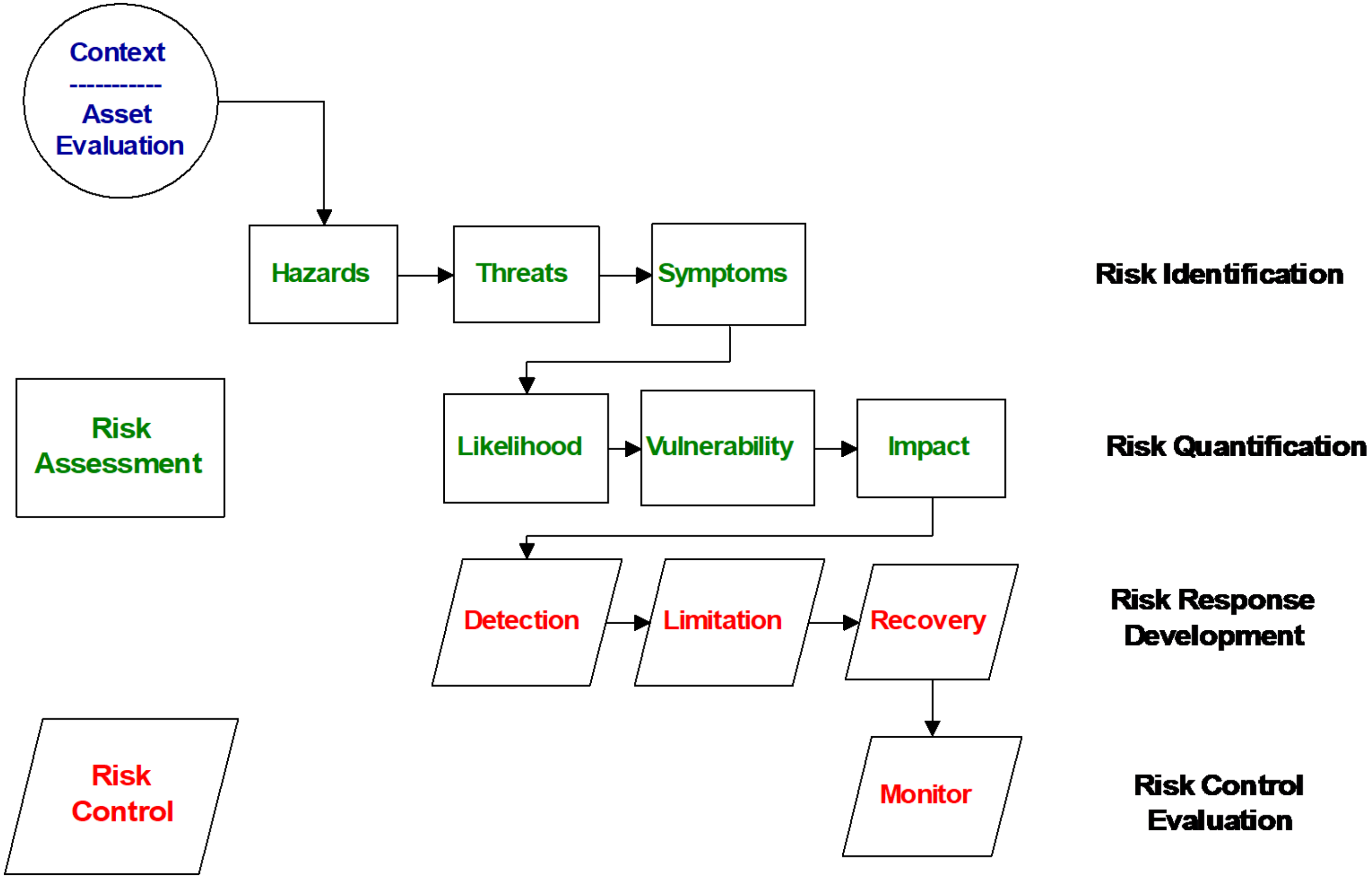
Risk Management

- **Risk management.** To identify, control, and minimize the impact of threats
- **Risk analysis.** To assess the value of each asset being protected, to identify potential hazards to it, to estimate the probability it might be compromised, and compare the probable costs (impact) of it being compromised with the cost of protecting it

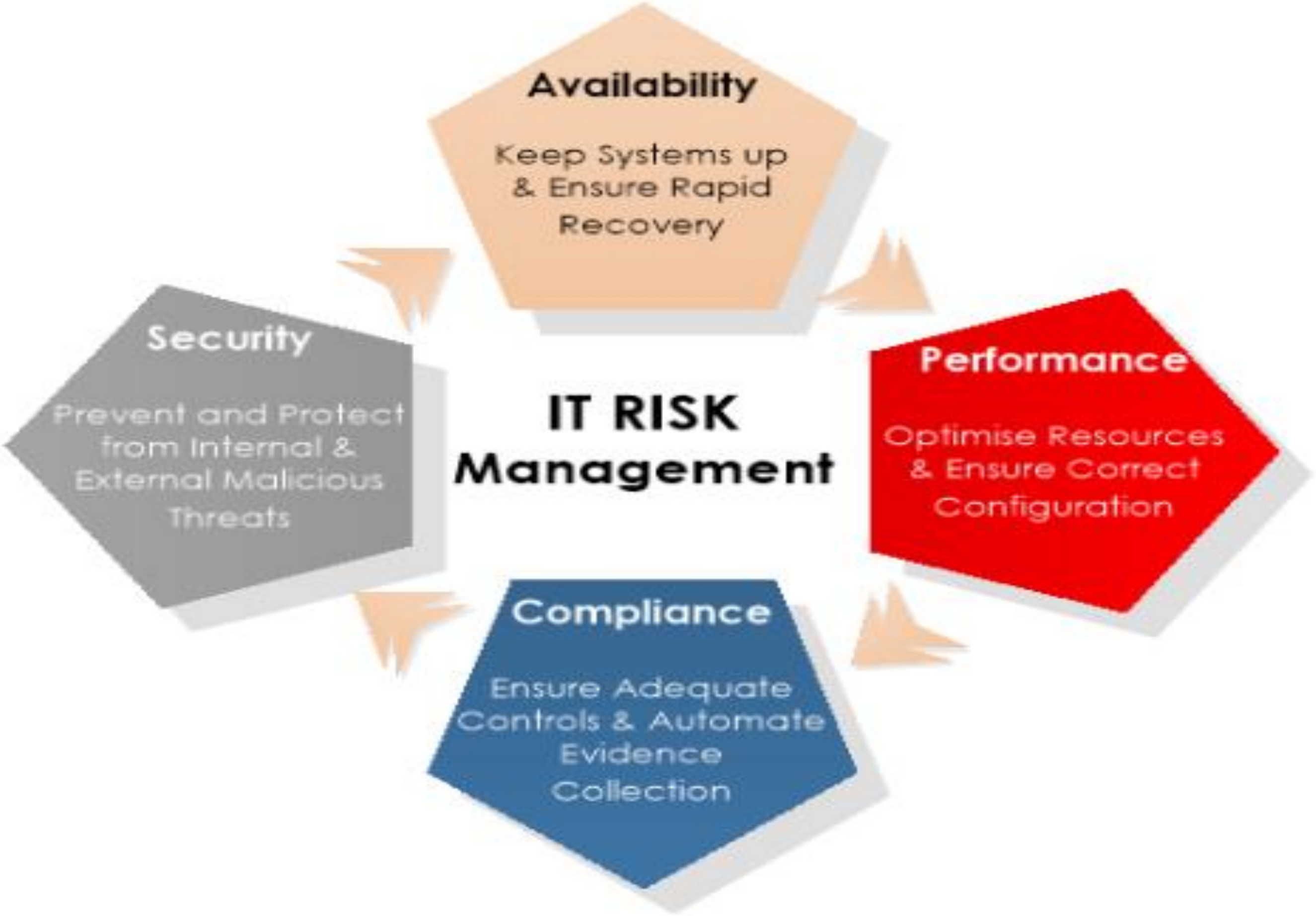
Risk Management (Cont)

- **Risk mitigation** (formally risk control or limitation) is when the organization takes concrete actions against risk
- It has several functions:
  - (1) implement controls to prevent identified threats from occurring
  - (2) protect assets from identified threats
  - (2) developing a means of recovery should the threat become a reality and the asset is compromised

Comprehensive RM Approach

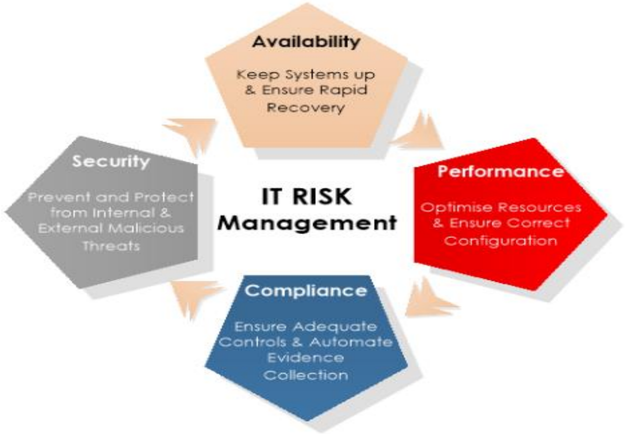


IT Risk Management


Availability
Keep Systems up & Ensure Rapid Recovery
Security
Prevent and Protect from Internal & External Malicious Threats
IT RISK Management
Performance
Optimise Resources & Ensure Correct Configuration
Compliance
Ensure Adequate Controls & Automate Evidence Collection

IT Threats

- Minimize threats to:
  - Availability
  - Security
  - Performance
  - Compliance
- Unintentional Threats
  - Accidents
  - Environmental
- Intentional Threats


Availability
Keep Systems up & Ensure Rapid Recovery
Security
Prevent and Protect from Internal & External Malicious Threats
IT RISK Management
Performance
Optimise Resources & Ensure Correct Configuration
Compliance
Ensure Adequate Controls & Automate Evidence Collection

Unintentional Threats

- *Human errors* can occur in the design of the hardware and/or information system
- They also can occur in programming, testing, data collection, data entry, operation, authorization and procedures.
- They contribute to more than 50% of control and security-related problems in organizations

Program Bugs!

- For every 55 lines of production C-like code, there is one bug
- Your razor has 80 bugs, You TV has 400 bugs, Your car has ??? Bugs
- Microsoft Windows 2000 was reported by inside sources to be released with 63,000 bugs
- Organizations handle billions of IT support calls, 1/3 of which are bugs
- More bugs all of the time as automation and embedded software grows

Unintentional Threats (Con’t)

- *Environmental hazards* include earthquakes, severe storms, floods, power failures or strong fluctuations, fires (most common hazard), explosions, …etc.

Intentional Threats

- Typically, criminal in nature
- **Cybercrimes** are fraudulent activities committed using computers and communications networks, particularly the Internet
- One problem is that they are often perceived as not being criminal
  - **How much money is stolen in the average armed robbery ?**
  - **How much money is involved in the average cybercrime today ?**

Cybercrime

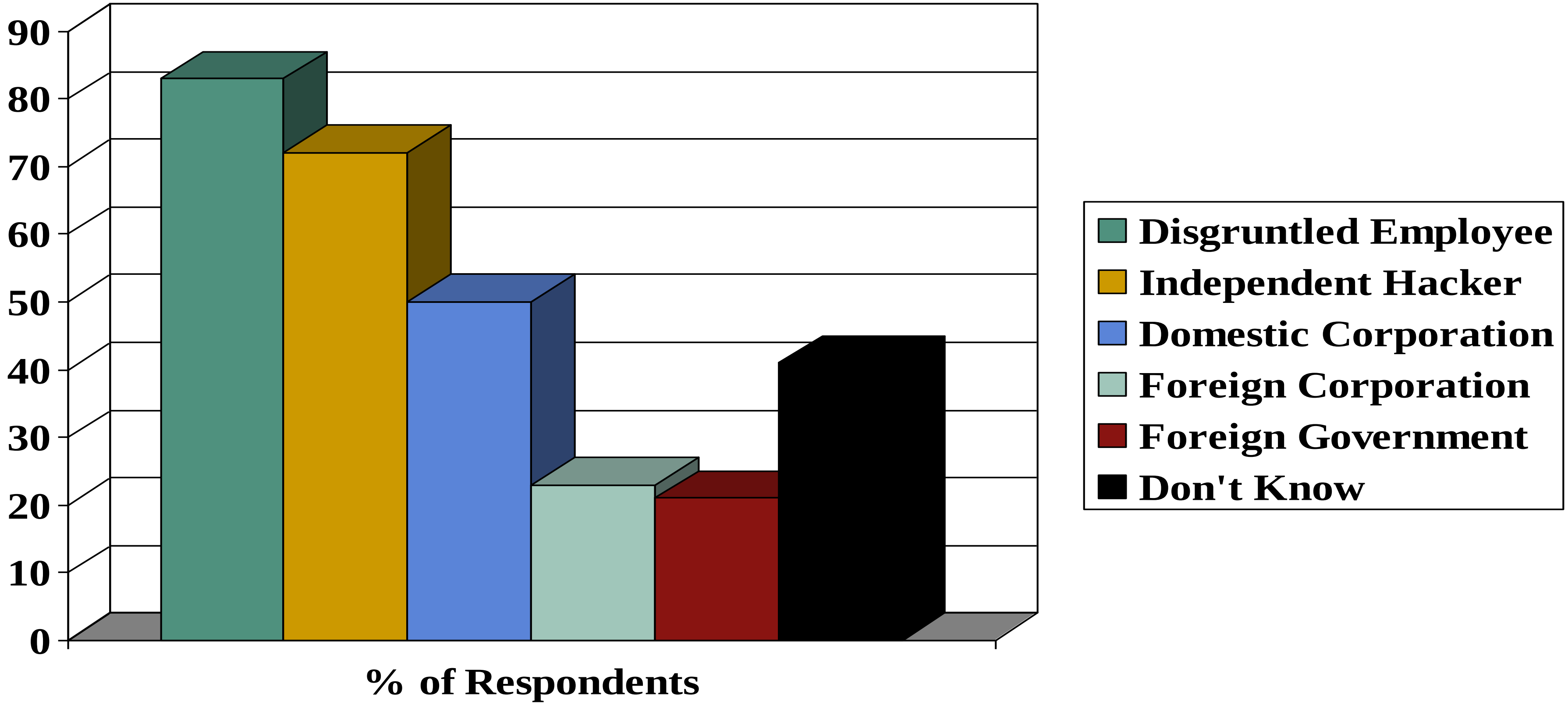
- Average armed robbery of $25
- Average software piracy of $100
- **Average cybercrime involves about $600,000 according to FBI**
- **Today, cybercrime is larger than traditional organized crime !!! – It is a worldwide problem !!!**
- **Cybercrime costs the US over $100 billion per year**

Intentional Threat Perpetrators

- **Hacker -** An outside person who has penetrated a computer system, usually with no criminal intent
- **Cracker -** A malicious hacker
- **Disgruntled employee**
- **Social engineering -** Computer criminals or corporate spies get around security systems by building an inappropriate trust relationship with insiders

Which is more common ?

Who Threatens Systems and Networks



Espionage or Trespass

- The act of gaining access to the information an organization is trying to protect by an unauthorized individual
- *Industrial espionage* occurs in areas where researching information about the competition goes beyond the legal limits
- Governments practice *industrial espionage* against companies in other countries

Chinese Cyber Espionage

- The 2015 disclosed breach of the Office of Personnel Management's security-clearance computer system took place a year earlier, giving Chinese government intruders access to sensitive data for a year
- The considerable lag time between breach and discovery allowed more info to be stolen
- The network holds a wealth of personal, family and financial details on millions of current, former and prospective federal employees and contractors

Information Extortion & Sabotage

- Extortion - When an attacker or formerly trusted employee steal information from a computer system and then demands compensation for its return or an agreement not to disclose it
- A popular type of online vandalism is ***hacktivist*** or ***cyberactivist*** activities
  - ***Hacktivist*** or ***cyberactivist*** uses technology for high-tech civil disobedience to protest operations, policies, or actions of an individual, an organization, or a government agency

- **Cyberterrorism** is a premeditated, politically motivated attack against information, computer systems, computer programs, and data that results in violence against noncombatant targets by subnational groups or clandestine agents
- **Cyberwar**. War in which a country's information systems could be paralyzed from a massive attack by destructive software
  - **The battlefield of the future !**
- **Theft** is the illegal taking of property that belongs to another individual or organization

Identity Theft

- Crime in which someone uses the personal information of others, often obtained from the Internet, to create a false identity and then commits fraud.
- Fastest growing white-collar crime
  - The FTC receives more reports of identity theft than any other consumer complaint
- Biggest problem is restoring victim’s damaged credit rating

Identity Theft

- Identity theft can be accomplished manually or via computer crime or some combination:
  - Getting someone’s key id codes: ss #, credit card numbers, phone #’s, address, driver’s license #, check account #, etc.
  - Theft from trash and mail (outgoing and incoming mail)
  - From both manual and computer transaction data
  - Zombies and trojan-horses downloaded onto computers (you are much more susceptible if you have a dedicated high speed connection)
  - Wireless data interception

Equifax Breach

- Equifax, one of the three credit reporting agencies in the US, announced in September that it was hacked between mid-May and July, potentially exposing Social Security numbers, credit card numbers, and other personal information for up to 143 million Americans
- Hackers exploited a security flaw which was 9 years old, slowly accessing the data over several months
- The vulnerability was in a popular open-source software package known as Apache Struts
  - What’s troublesome is that at least 65% of Fortune 100 companies still use web applications built with the Struts framework
- A breach of this size is a massive challenge for any company, and Equifax certainly hasn't handled it well so far

Equifax Breach (con’t)

- On top of the delay in notification, the company's chief financial officer and two other senior executives cashed in on almost $2 million of Equifax stock once they learned about the hack
- Equifax is only notifying people directly if their credit card number info was leaked
- Equifax set up a site, equifaxsecurity2017.com, to help you find out whether your information was compromised; you can also access the site via Equifax's homepage, and if you'd rather call, there's also a phone line dedicated to the breach: 866-447-7559
  - But do not sign up for the free credit monitoring service; if you do you may be giving up the right to participate in the class action suit

Equifax Breach (con’t)

- The fact that millions of consumers’ personal information including birth date, Social Security number, driver’s license, address and/or credit or debit card information may have fallen prey to hackers demonstrates the enormity of the problem
- Surprisingly, even though this is the largest known hack in 2017, there were over 1,000 additional breaches in 2017, according to the Identity Theft Resource Center — an increase of 23 percent over 2016

- How do you know if you are a victim of identify theft ?

You know you’re a victim when:

- Your bills stop coming
- You start getting bills for credit cards you have not applied for
- You start receiving phone calls or letters about purchases you did not make
- Your application for new credit is denied
  - Check you credit rating at: www.annualcreditreport.com

- How can one protect from identity theft ?

Preventative Measures

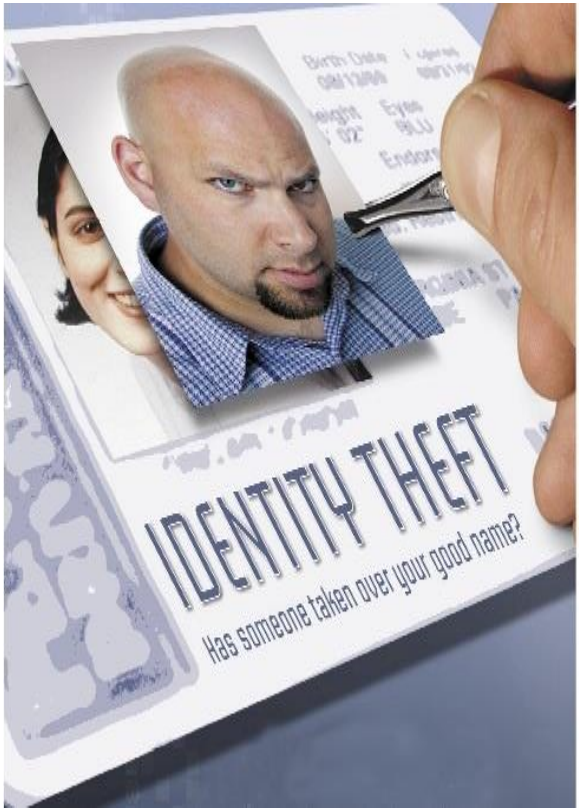
- Be very careful to whom you give any info
- Shred all trash containing id #'s
- Don't put outgoing mail in street mailbox
- Using a locking mailbox, with a drop slot
- Install antimalware and a firewall on your PC, laptop, tablet, and smartphone
- Don't open email attachments unless you are certain of the source
- Don't visit unknown web sites
- Be careful at ATMs, public phones, public Wi-Fi, etc.
- Be careful on social web sites
- Sign-up for a credit monitoring service such as one of the three credit agencies or myidalerts.com

Identity Theft Recovery

- First place a fraud alert (and possibly "freeze") on your accounts
  - It can be very difficult and time consuming to recover from id theft; one needs to contact all three major credit bureaus and possibly dozens of creditors:
    - Experian (1-888-397-3742), TransUnion (1-800-680-7289), Equifax (1-800-525-6285); or order all 3 from 877-322-8228
- Change affected passwords
- Close any accounts that were compromised by speaking directly with those banks, financial institutions, etc.
- File a police report, that you may later need to deal with creditors that need proof of the crime
- Check with your homeowner's insurance company
- File a complaint with the FTC (also with the Social Security Office if someone used your SS# to get a job)

Identity Theft Recovery (con't)

- The federal government has established one form to report id theft to all necessary government and private organizations
  - www.consumer.gov/idtheft
  - Or 877-ID-THEFT
  - If the ID-Theft involves bogus US Treasury forms contact: 1-800-366-4484
- Also see IDTheftInfo.org and IdentityTheft.gov



Copyright - D. Brandon, Ph.D., PMP

SSA – Recovery Plan

- The Social Security Administration publishes a useful booklet called "Identity Theft and Your Social Security Number." In addition to basic protection tips, it provides information about what you should do if you believe your identity and SSN have been stolen or compromised.[6]
- 1. Contact the Social Security Administration (SSA)
- The easiest way to contact Social Security is online (see above). SSA also has a national toll-free phone number, 800-772-1213.
- 2. Contact Medicare if Your MBI Has Been Stolen
- Although Medicare has stopped using SSNs and replaced them with a Medicare Beneficiary Identifier (MBI), it is also subject to theft and can be used to commit Medicare fraud. If you have an MBI and believe it has been compromised, contact Medicare for guidance.[1]
- 3. Request a Review of Your Social Security Earnings
- On rare occasions, more than one person may use the same SSN accidentally through a typo or misremembering when filling out paperwork. This can also happen on purpose if someone uses your number to get a job. Contact Social Security to request an earnings review (or do it yourself with an online account).[3]
- 4. Check Employer Verifications at My E-Verify
- You can also check for the names of employers who have verified your eligibility to work in the U.S. if they went through the Department of Homeland Security E-Verify system. To do that, go to the myE-Verify webpage. If you see an employer whose name you do not recognize, someone else may be using your number to work in the U.S. The site also has a self-lock feature that lets you place a lock on your SSN.

SSA – Recovery Plan (con’t)

- 5. Visit IdentityTheft.gov to Get a Recovery Plan
  - You can visit IdentityTheft.gov to report identity theft and, more importantly, set up a recovery plan, or you can call 877-438-4338 (877-IDTHEFT) to do so. Both will guide you through a process that includes:
    - Calling companies where you suspect fraud has occurred
    - Placing a fraud alert and obtaining your credit reports
    - Reporting the identity theft to the Federal Trade Commission
    - Filing a report with your local police department (optional)
- 6. Contact the Internal Revenue Service (IRS)
  - You may also want to contact the Internal Revenue Service (IRS) if you suspect an identity thief has filed a tax return in your name to get a refund. The IRS should also be on your list of contacts if you suspect someone is using your number for work purposes. Otherwise, the IRS could think you failed to report income when you file your own tax return. Use the IRS Identity Theft Central website or call 800-908-4490.
- 7. File an Online Complaint With the FBI Internet Crime Complaint Center (IC3)
  - The Federal Bureau of Investigation provides a convenient avenue to report suspected criminal or illegal civil acts at the Internet Crime Complaint Center (IC3). Once you report a crime, the site then alerts appropriate law enforcement or regulatory agencies that would have jurisdiction over the matter.
- 8. Apply for a New SSN as a Last Resort
  - If you believe you’ve done everything you can and someone is still using your SSN, you may need to request a new number from the SSA. If you decide to apply for a new number, you will need to prove your identity, age, and U.S. citizenship or immigration status. You will also need to provide evidence that someone is using your old number. The SSA booklet “Your Social Security Number and Card” explains the application process.

THINK OF THE INTERNET AS AN OCEAN ...

The Surface Web Pages that show up when you use Google or other common search engines. Includes content their creators want lots of people to see, like news, entertainment, products or consumer information.

The Deep Web Pages you need a password to see and that can't be found by popular search engines. Content includes online banking, subscription websites, government records, emails and most social media content.

The Dark Web Sites in the deep web that provide anonymity to users and go largely unregulated. Many are legal, serving as, for example, communication outlets for human rights activists. But it's also used by criminals to buy and sell illegal wares.

5-10%

EXAMPLES: *Wikipedia, Amazon, eBay, Fox News, WebMD, Medicare.gov, AARP.org*

90-95%

EXAMPLES: *PayPal, Netflix, LinkedIn, Instagram, Bank of America, Dropbox*

.01%

EXAMPLES: *Silk Road, AlphaBay Market, Shadowcrew*

Dark Web

- Along with the deep web, comes the infamous “dark” web
- While they both contain hidden data, the difference between the two is that the dark web’s contents are intentionally buried
- This darker side has access points through a special browser software isolated from regular internet tools; the Onion Router or, commonly, Tor sets up the necessary connections for a user to get to the hidden “onion” sites where the dark web data is controlled
- This browser primarily allows searchers to remain anonymous and presumably untraceable by routing connections through secret servers in other parts of the world
- A main usage is for trading of illegal services like secured information, pornography, weapons, and drugs
- Because the leading use of the dark web is for illegal data access, frequently visited sites include online black markets like the disreputable Silk Road where you can buy anything from a hitman to someone’s social security number
- In addition to these websites, Bitcoin serves as the dominant currency for dark web because it is equally untraceable leaving virtually no footprints of service purchases

Software Attacks

- ***Malicious software* (*malware*)** designed to damage, destroy, or deny service to the targeted systems
- Most common types of software attacks are viruses, worms, Trojan horses, logic bombs, back doors, denial-of-service, alien software, phishing, and pharming

Software Attacks (Con’t)

- **Viruses.** Segments of computer code that perform unintended actions ranging from merely annoying to destructive
- **Worms.** Destructive programs that replicate themselves without requiring another program to provide a safe environment for replication
- **Trojan Horses.** Software programs that hide in other computer programs and reveal their designed behavior only when they are activated

Software Attacks (Con’t)

- **Logic (time) bombs.** Designed to activate and perform a destructive action at a certain time
- **Back doors or trap doors.** Typically a password, known only to the programmer, that allows access to the system without having to go through any security
- **Denial-of-service.** An attacker sends so many information requests to a target system that the target cannot handle them successfully and can crash the entire system

Alien Software

- **Pestware.** Clandestine software that uses up valuable system resources and can report on your Web surfing habits and other personal information
- **Adware.** Designed to help popup advertisements appear on your screen

- **Spyware.** Software that gathers user information through the user’s Internet connection without their knowledge (i.e. keylogger, password capture)

Alien Software (Continued)

- **Spam.** Unsolicited e-mail, usually for purposes of advertising
- **Spamware.** Designed to use your computer as a launch pad for spammers
- **Cookies.** Small amount of information that Web sites store on your computer, temporarily or more-or-less permanently
- **Cross Site Scripting & SQL Injection**. Attacks that take advantage of weaknesses in web HTML forms, etc.

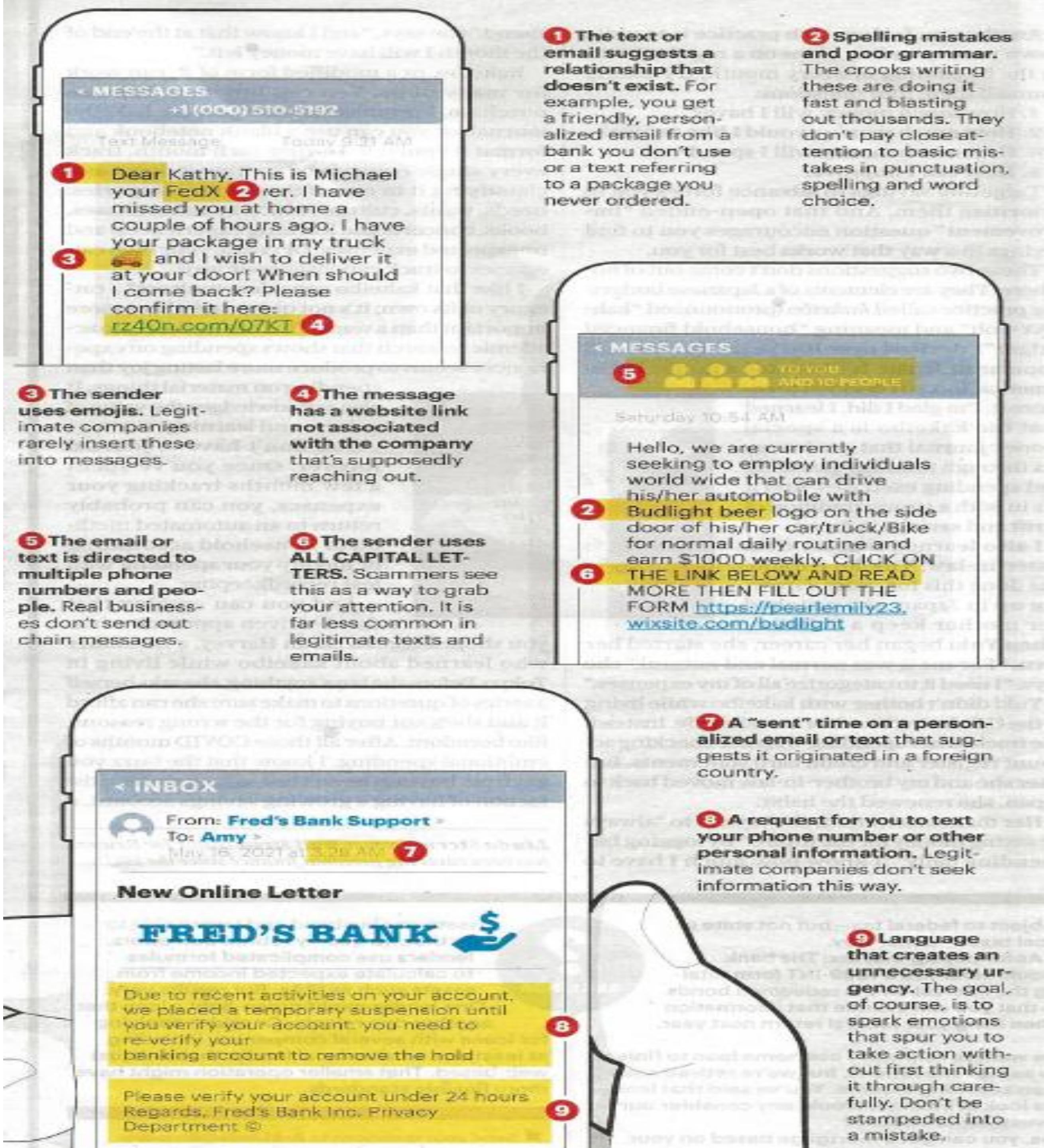
Alien Software (Con't)

- **Web bugs.** Small, usually invisible, graphic images that are added to a Web page or e-mail
- **Phishing.** Uses deception to fraudulently acquire sensitive personal information such as account numbers and passwords disguised as an official-looking e-mail
- **Pharming.** Fraudulently acquires the Domain Name for a company's Web site and when people type in the Web site url they are redirected to a fake Web site

Alien Software (Con’t)

- **Baiting**
  - Similar to phishing attacks; baiter gives recipient a promise
- **Quid pro quo**
  - Involves a hacker requesting the exchange of critical data or login information in exchange for a service or prize
- **SMiShing** (SMS [text message] phishing)
  - Technique tricks a user to download a malware
- **Vishing** (voice or VoIP phishing)
  - Technique tricks a user to reveal important financial or personal information to unauthorized entities

How to Spot a Phish Text



< MESSAGES
+1 (000) 510-5192

Text Message Today 9:31 AM

1 Dear Kathy. This is Michael your FedX 2 ver. I have missed you at home a couple of hours ago. I have your package in my truck
3 🚚 and I wish to deliver it at your door! When should I come back? Please confirm it here:
rz40n.com/07KT 4

1 **The text or email suggests a relationship that doesn't exist.** For example, you get a friendly, personalized email from a bank you don't use or a text referring to a package you never ordered.

2 **Spelling mistakes and poor grammar.** The crooks writing these are doing it fast and blasting out thousands. They don't pay close attention to basic mistakes in punctuation, spelling and word choice.

3 **The sender uses emojis.** Legitimate companies rarely insert these into messages.

4 **The message has a website link not associated with the company** that's supposedly reaching out.

5 **The email or text is directed to multiple phone numbers and people.** Real businesses don't send out chain messages.

6 **The sender uses ALL CAPITAL LETTERS.** Scammers see this as a way to grab your attention. It is far less common in legitimate texts and emails.

< MESSAGES
5 TO YOU AND 10 PEOPLE

Saturday 10:54 AM

Hello, we are currently seeking to employ individuals world wide that can drive his/her automobile with
2 Budlight beer logo on the side door of his/her car/truck/Bike for normal daily routine and earn $1000 weekly. CLICK ON
6 THE LINK BELOW AND READ MORE THEN FILL OUT THE FORM https://pearlemily23.wixsite.com/budlight

< INBOX

From: Fred's Bank Support >
To: Amy >
May 16, 2021 at 3:26 AM 7

New Online Letter

FRED'S BANK

Due to recent activities on your account, we placed a temporary suspension until you verify your account. you need to re-verify your
banking account to remove the hold 8

Please verify your account under 24 hours
Regards, Fred's Bank Inc. Privacy Department © 9

7 **A "sent" time on a personalized email or text** that suggests it originated in a foreign country.

8 **A request for you to text your phone number or other personal information.** Legitimate companies don't seek information this way.

9 **Language that creates an unnecessary urgency.** The goal, of course, is to spark emotions that spur you to take action without first thinking it through carefully. Don't be stampeded into a mistake.

Social Networking & Phishing

- Social networking (i.e. Facebook), by its very nature, is about socializing, which means users are letting their guard down and sharing information
- They're expanding their professional networks, connecting with old friends, and communicating in real time with pals and peers
- And for bad guys who favor social-engineering and phishing attacks, taking advantage is like shooting fish in a barrel !

Social Networking & Phishing (con't)

- Most people know enough to not respond to e-mail requests from exiled Nigerian royalty promising millions of dollars if only you will help them smuggle the money out of the country
- But what if your good friend from high school whom you haven't seen in 18 years sends you a message on Facebook explaining how their wallet was stolen and their car broke down, and asks you to wire money to help them get home? You might not be as apprehensive -- but you should be
- Attackers have figured out that family and friends are easy prey for such sob stories; using other attacks or methods, they gain access to a Facebook account and hijack it
  - They change the password so that the legitimate owner can't get back in, and then they proceed to reach out to the friends of the hijacked account and attempt to extort money from those friends through social engineering

Social Networking & Phishing (con’t)

- On Facebook and the like:
  - Change privacy settings to “friends only”
  - Weed out “friends” you don’t really know well
  - Delete any info you would not want anyone to see

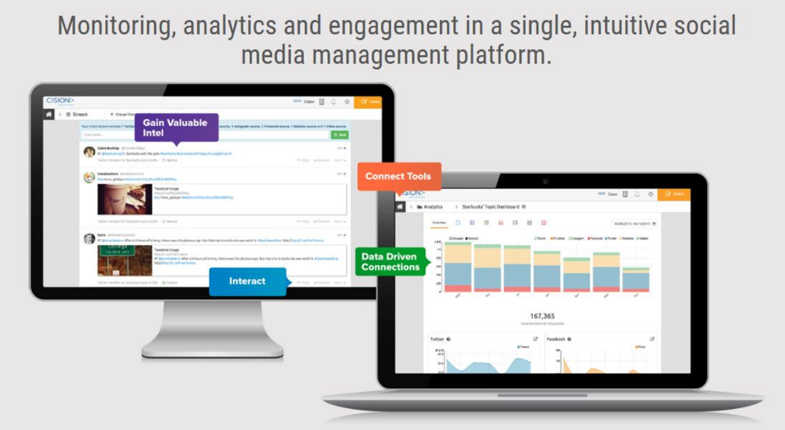
Six Things Never to Reveal on Facebook, Etc.

- **Your Birth Date and Place**
  - Sure, you can say what day you were born, but if you provide the year and where you were born too, you've just given identity thieves a key to stealing your financial life, said Givens. A study done by Carnegie Mellon showed that a date and place of birth could be used to predict most — and sometimes all — of the numbers in your Social Security number, she said.
- **Vacation Plans**
  - There may be a better way to say "Rob me, please" than posting something along the lines of: "Count-down to Maui! Two days and Ritz Carlton, here we come!" on Twitter. But it's hard to think of one. Post the photos on Facebook when you return, if you like. But don't invite criminals in by telling them specifically when you'll be gone.
- **Home Address**
  - Do I have to elaborate? A study recently released by the Ponemon Institute found that users of Social Media sites were at greater risk of physical and identity theft because of the information they were sharing. Some 40% listed their home address on the sites; 65% didn't even attempt to block out strangers with privacy settings. And 60% said they weren't confident that their "friends" were really just people they know.
- **Confessionals**
  - You may hate your job; lie on your taxes; or be a recreational user of illicit drugs, but this is no place to confess. Employers commonly peruse social networking sites to determine who to hire — and, sometimes, who to fire. Need proof? In just the past few weeks, an emergency dispatcher was fired in Wisconsin for revealing drug use; a waitress got canned for complaining about customers and the Pittsburgh Pirate's mascot was dumped for bashing the team on Facebook. One study done last year estimated that 8% of companies fired someone for "misuse" of social media.
- **Password Clues**
  - If you've got online accounts, you've probably answered a dozen different security questions, telling your bank or brokerage firm your Mom's maiden name; the church you were married in; or the name of your favorite song. Got that same stuff on the information page of your Facebook profile? You're giving crooks an easy way to guess your passwords.
- **Risky Behaviors & Photos/Videos**
  - You take your classic Camaro out for street racing, soar above the hills in a hang glider, or smoke like a chimney? Insurers are increasingly turning to the web to figure out whether their applicants and customers are putting their lives or property at risk, according to Insure.com. So far, there's no efficient way to collect the data, so cancellations and rate hikes are rare. But the technology is fast evolving, according to a paper written by Celent, a financial services research and consulting firm.

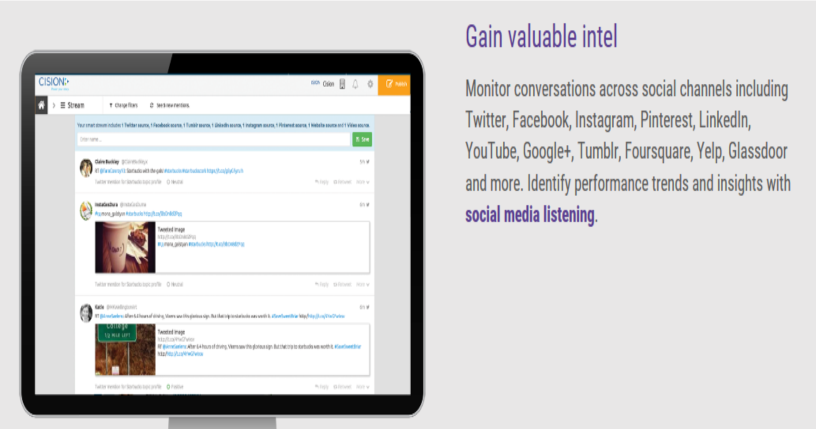
Removing Info About Yourself

- **Services to remove info about yourself include PrivacyDuck, OneRep, and DeleteMe**
- **The online privacy software company Abine, which makes Do Not Track Plus, offers a service called DeleteMe, which removes your data from numerous tracking sites and keeps it from coming back**
- **They have also made public how to do for yourself everything that DeleteMe does**
- **Be warned, though, the following are not easy instructions, and it's not because they're technically complex; they require a tenacity and wherewithal that is likely to either exhaust you, drive you borderline bonkers, or both:**
- ***Step 1:*** *Prepare yourself: You're going to have to be polite.*
  These instructions require patience for the antics of others and determination to get the job done. It's not a bad idea to get something inanimate to take your frustrations out on, because often getting your data successfully removed or changed will require the good faith of the person you're dealing with. Things are not likely to go your way the first time around.
- ***Step 2:*** *Aggressively track sites that aggressively track you.*
  This is where the DeleteMe service comes in. They currently charge you $99 to un-track you from the tracking data clearinghouses, which in turn sell your data to others entities. You can follow Abine's list of services and do the deed yourself, and that means writing many e-mails, sending numerous faxes, and placing enough phone calls to make you wish for a time machine so you can go back to the 19th century to do violence unto Alexander Graham Bell.
- One thing that isn't clear from Abine's list is that most of these data aggregators will re-add you within a few months, so I recommend at least bi-annual checks to see if they've sucked up your data again. Be tenacious, be polite, and if this is important to you, stick with it until you get what you want.

Reputation Management



Monitoring, analytics and engagement in a single, intuitive social media management platform.



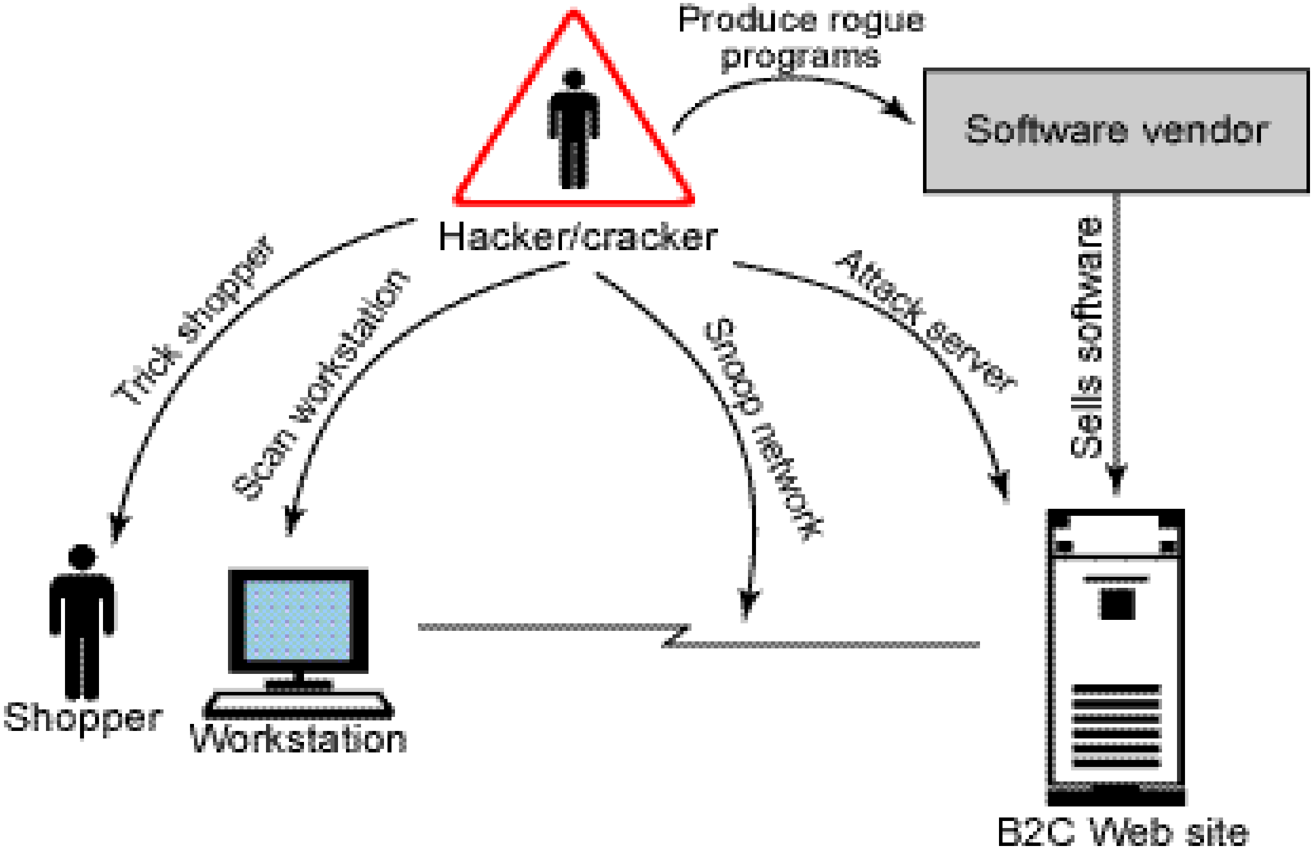
Gain valuable intel

Monitor conversations across social channels including Twitter, Facebook, Instagram, Pinterest, LinkedIn, YouTube, Google+, Tumblr, Foursquare, Yelp, Glassdoor and more. Identify performance trends and insights with **social media listening**.

Interact with your brand's community

Source and distribute engaging content on social media. Cision social software amplifies your message by extending your brand's reach and sparking **social engagement** across channels by ensuring that the right content reaches the right audience.

E-Commerce Attacks



New/Rising Attacks from Cybercriminals

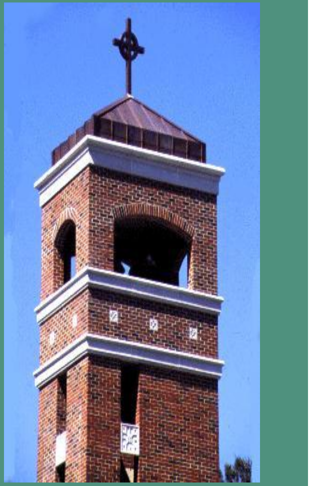
- Text-message malware – usually opening attachments and/or photos
  - Upon opening, malware is installed which gets info from the phone plus spreads itself via contact lists
  - he malware also starts to buy stuff including ringtones that are charged to your phones
- Ransomware – locking up a computer until a ransom is paid
- Hacking into smart grids – utilities, manufacturing, industrial control systems, public systems, smart meters, etc.

New/Rising Attacks from Cybercrim (con't)

- Social media – stealing info, blackmail, spoofing, false chats with connections, phising, etc.
- Cyberstalking, cyber bullying, cyber harassment, blackmail
- Hacking into automobile computer systems – gaining information, linking to personal devices (mobile and home computers), and even controlling your car
- GPS jamming and spoofing – interfering with GPS used in armored cars, emergency vehicles, financial transactions, etc.

Hacking Auto Computer Systems

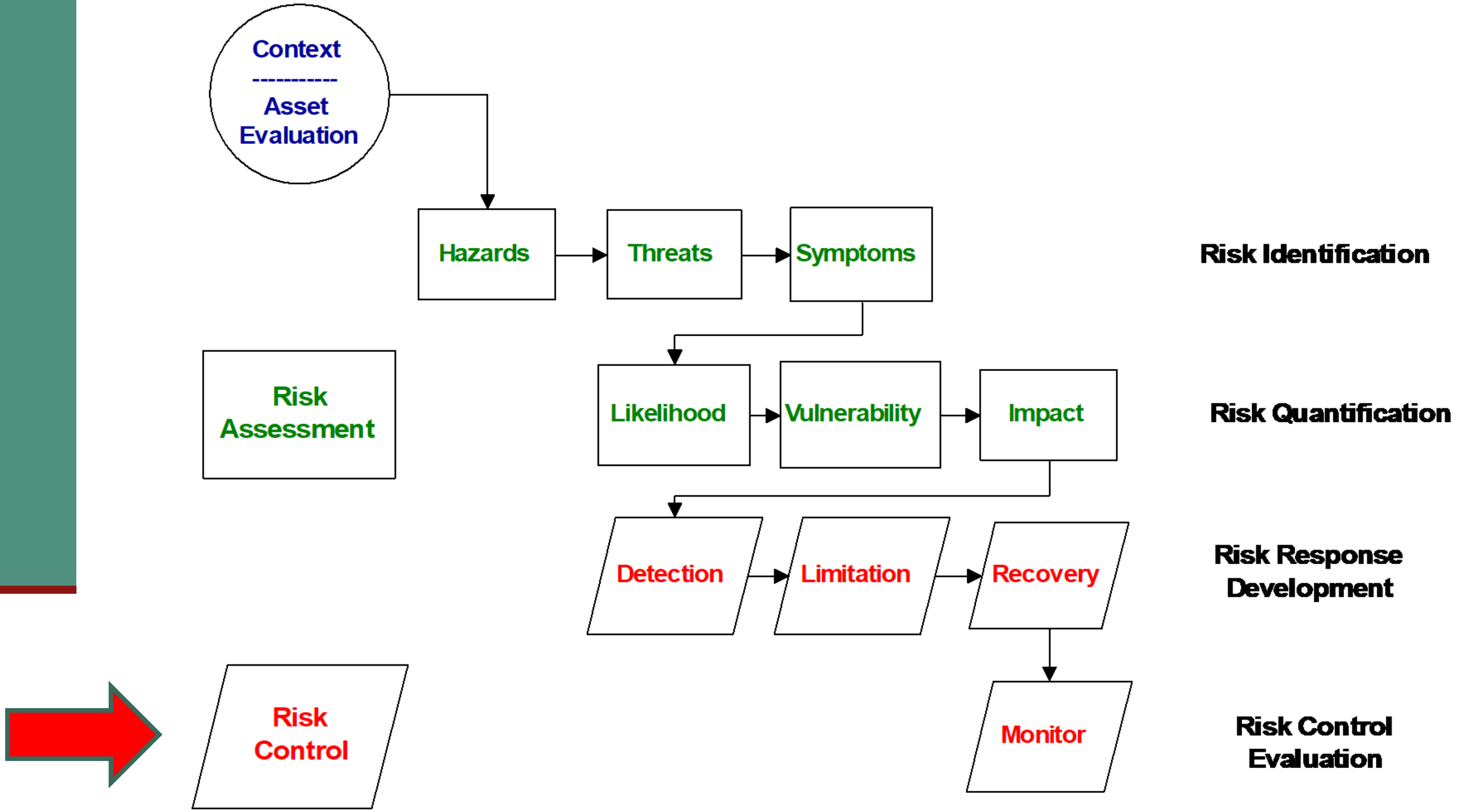
- A pair of computer experts recently demonstrated their abilities cracking the digital defenses of Internet-connected vehicles, remotely hacking into the highway-cruising vehicle from miles away
- Their code is an automaker’s nightmare
- The software that lets hackers send commands through a car’s entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country



Introduction to MIS

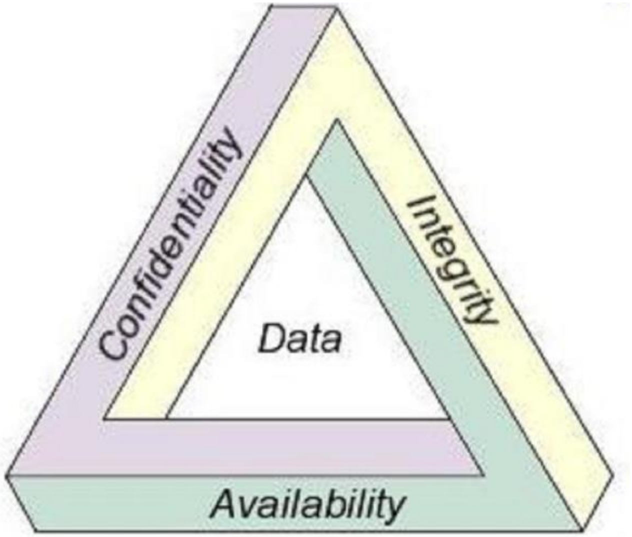
Information Security – Detection, Limitation, Protection, Recovery

Comprehensive RM Approach



CIA Triangle

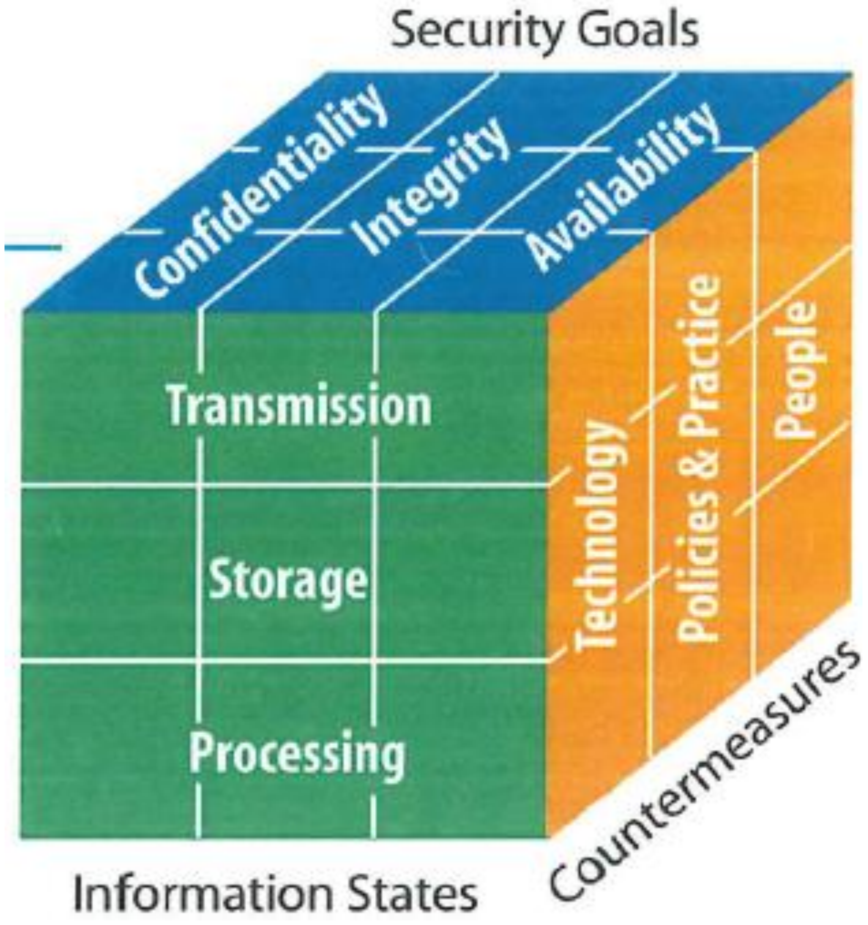
- Organizations need to protect their information and other IT assets in regard to:
  - Confidentiality
    - Privacy compromise
  - Integrity
    - Altering data
  - Availability
    - Deletion of data
    - Encryption of data
    - Denial of service



McCumber Cube

- McCumber cube
  - Framework for evaluating information security
  - Represented as a three-dimensional cube
  - Includes different states in which information can exist in a system
    - Transmission, storage, and processing
  - Defines three types of protection
    - Technology, policy, people (awareness, training, etc.)
  - Overall 27 areas of risk management

McCumber Cube



Fault-tolerant Systems

- Planning a comprehensive security system: designing fault-tolerant systems
  - Ensure availability in the event of a system failure by using a combination of hardware and software
  - Commonly used methods
    - Uninterruptible power supply (UPS)
    - Generator
    - Redundant array of independent disks (RAID)
    - Rapid backup and recovery

Security Measures And Enforcement

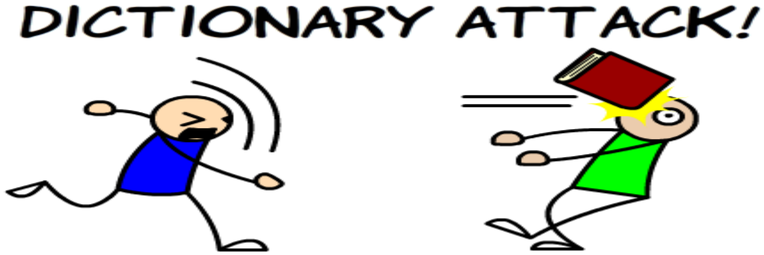
- Key components of a comprehensive security system
  - Access controls
    - Biometric, nonbiometric, and physical security measures
  - Data encryption
    - Virtual private networks
    - E-commerce transaction security measures
    - Encrypted data storage
  - Attack detection and prevention
  - Computer Emergency Response Team (CERT)

Access Control

- Identification (username)
  - Terminal resource security
    - Signs the user off after a specified length of inactivity
- Authentication:
  - What one knows (i.e. password)
  - What one has (thumbprint, retina scan, etc.)
  - What one does (online behavior)

- Access Control List
  - Who/what has what type of access to what
- Multi-factor authentication
- Audits of usage

Password Attacks

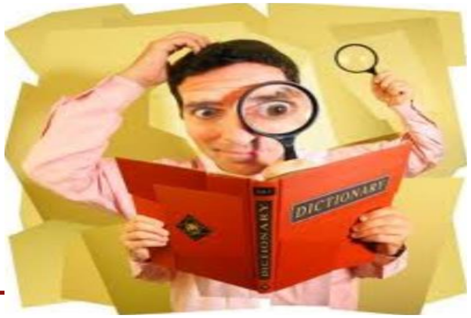


- The three types of password attacks are: Password Crack, Brute Force, and Dictionary:
  - Password crack: Attempting to reverse calculate the password is called “cracking”
    - Cracking is used when a copy of the Security Account Manager data file can be obtained
    - Tries to reverse-engineer hashing algorithm
  - Brute Force: The application of computing and network resources to try every possible combination of options for a password
  - Dictionary: A form of brute force for guessing passwords; the dictionary attack selects specific accounts and uses a list of commonly used passwords with which to guess

Brute Force Password Determination

[all keyboard characters, upper and lower]

Number of Characters	Time to Crack
1	.00001 sec
2	.011 sec
3	0.1 sec
4	10 sec
5	15 min
6	24 hours
7	3 months



- What can system administrators do to protect against password attacks ?

MY KEYBOARD IS BROKEN. IT ONLY TYPES ASTERISKS FOR PASSWORDS.
www.dilbert.com scottadams@aol.com
DOGBERT'S TECH SUPPORT
TRY CHANGING YOUR PASSWORD TO FIVE ASTERISKS.
© 2001 United Feature Syndicate, Inc.
I HOPE I CAN REMEMBER IT.

Wait….

- ?

Don’t look ahead, until you have your answer !

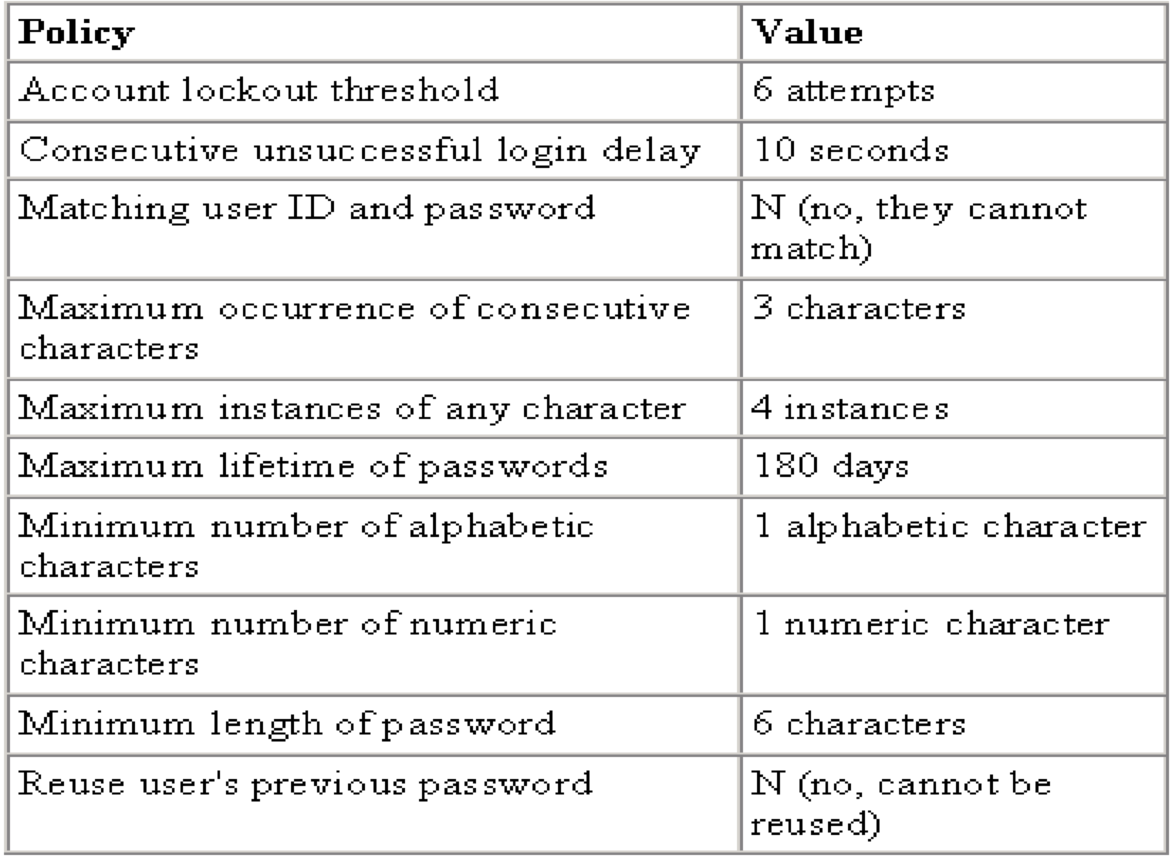
Password Attacks (con’t)

- To protect against password attacks, security administrators can:
  - Implement controls that limit the number of attempts allowed
  - Use a “disallow” list of passwords from a dictionary
  - Force more frequent password changes
  - Require use of additional numbers and special characters in passwords (“strong password”)
    - A common password policy is to force creation of passwords with at least 8 characters one of which is a capital letter, two of which are numbers, one of which is a symbol (*, &, ^, %, $, @, !)
- For greater security, administrators can also implement other forms of authentication such as biometrics

Example Password Policy

[Federal Information Processing Standard (FIPS)]

Policy First → then Tools to Enforce Policy



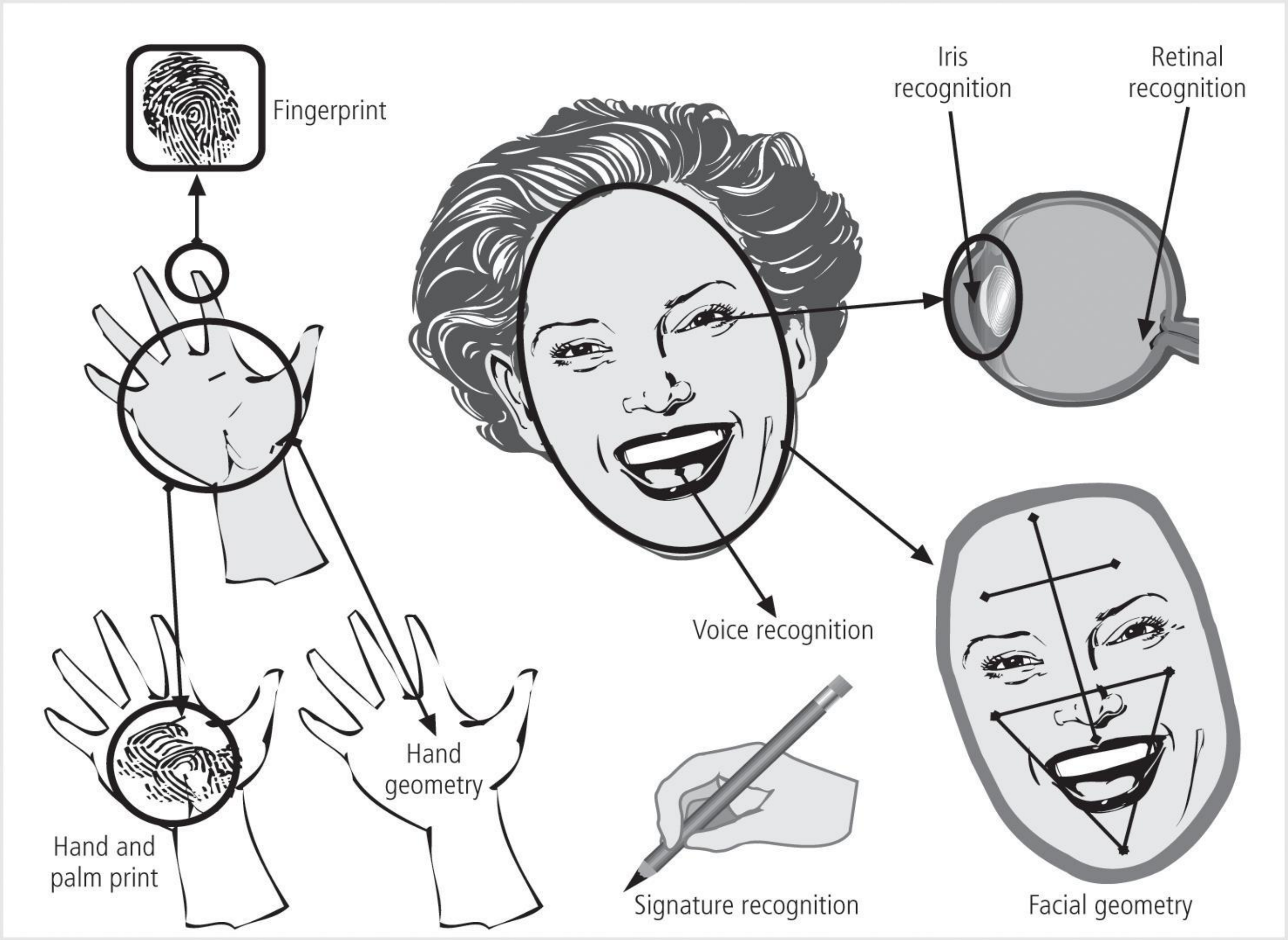
Policy	Value
Account lockout threshold	6 attempts
Consecutive unsuccessful login delay	10 seconds
Matching user ID and password	N (no, they cannot match)
Maximum occurrence of consecutive characters	3 characters
Maximum instances of any character	4 instances
Maximum lifetime of passwords	180 days
Minimum number of alphabetic characters	1 alphabetic character
Minimum number of numeric characters	1 numeric character
Minimum length of password	6 characters
Reuse user's previous password	N (no, cannot be reused)

Someone discovered my
PASSWORD.
Now I have to rename my dog.

Use strong passwords. A simple password, such as your pet's name, is not sufficient protection. Hackers systematically check every possible word to decipher passwords in no time.

Watch for an online awareness program
PUBLIC JOBS: PRIVATE DATA
Minnesota

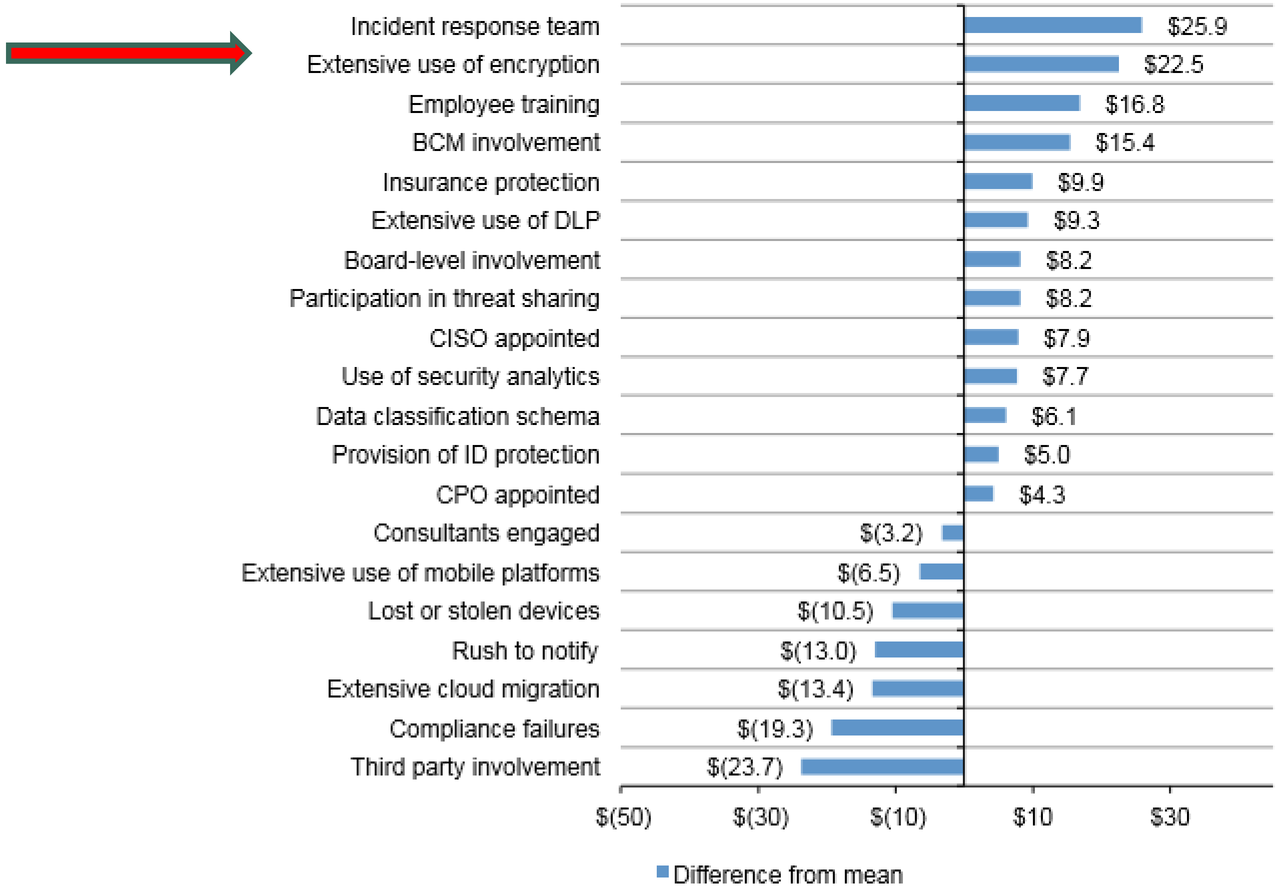
Biometric Characteristics
(new forms: odor & gait)



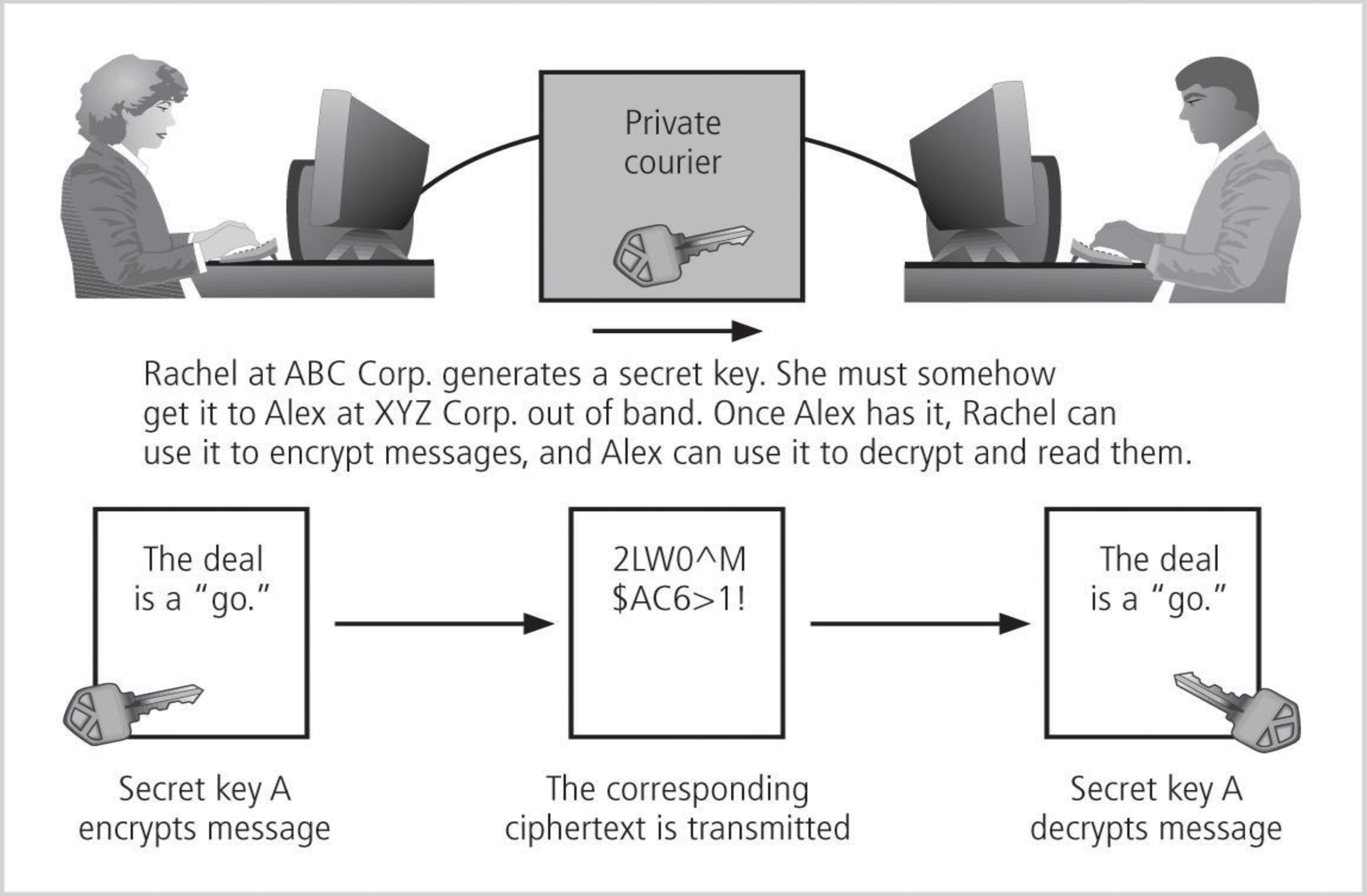
Data Encryption

- Transforms data, called plaintext or cleartext, into a scrambled form called ciphertext that cannot be read by others
  - Ender encrypts data
  - Receiver unscrambles data using a decryption key
- Rules for encryption
  - Known as the encryption algorithm

Impact of 20 Security Factors



Symmetric Encryption
[need “out of band” exchange]



Rachel at ABC Corp. generates a secret key. She must somehow get it to Alex at XYZ Corp. out of band. Once Alex has it, Rachel can use it to encrypt messages, and Alex can use it to decrypt and read them.

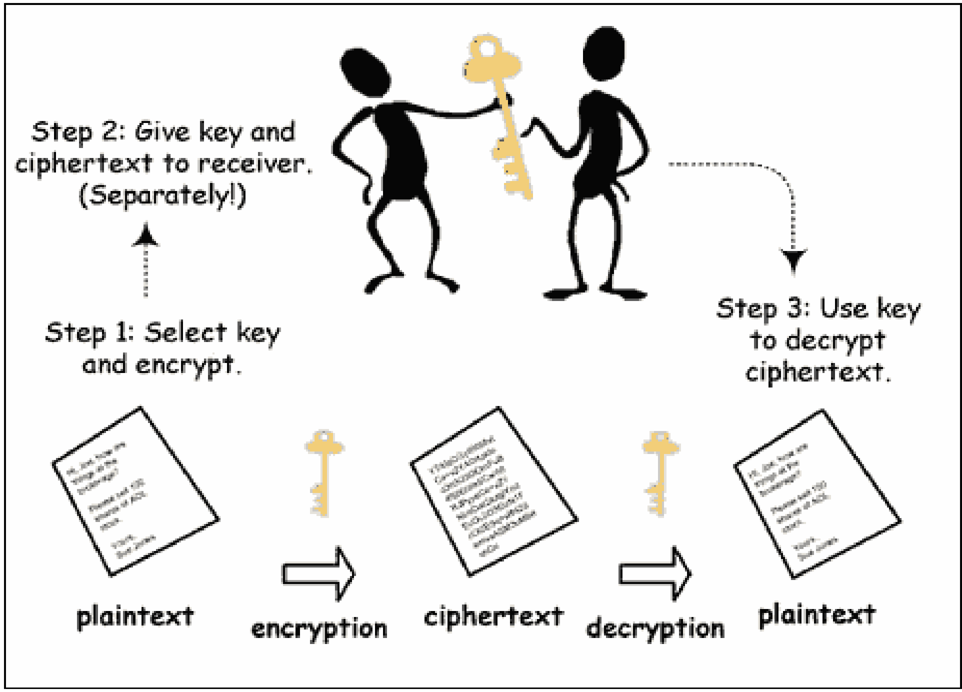
Secret key A encrypts message

The corresponding ciphertext is transmitted

Secret key A decrypts message

Symmetric Encryption Algorithms

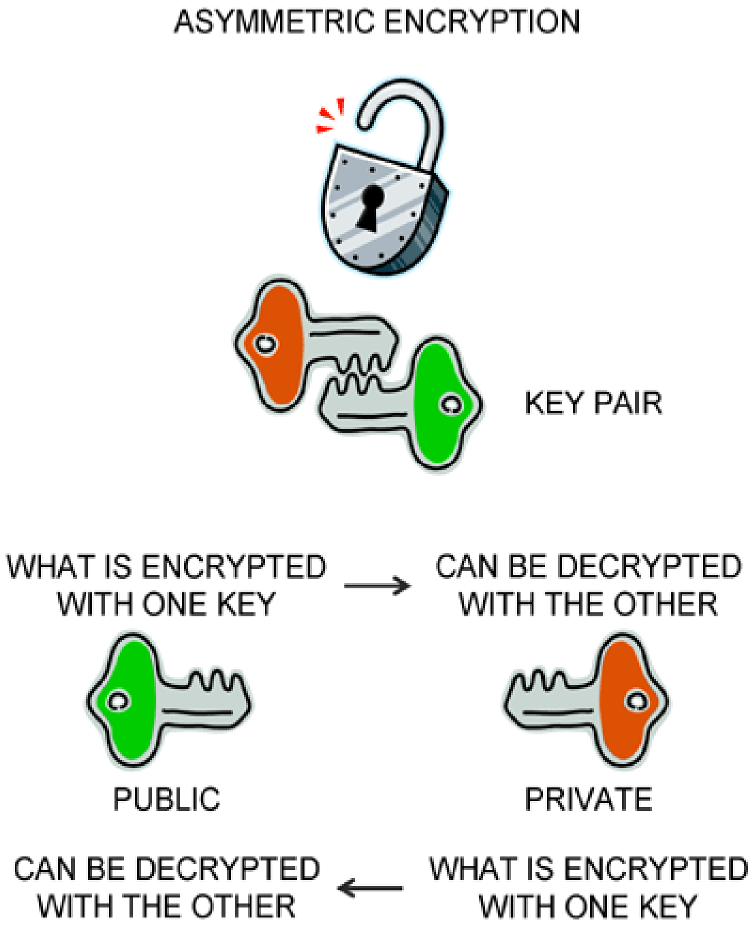
- Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
- Triple DES (3DES): created to provide security far beyond DES
- Advanced Encryption Standard (AES): developed to replace both DES and 3DES


Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

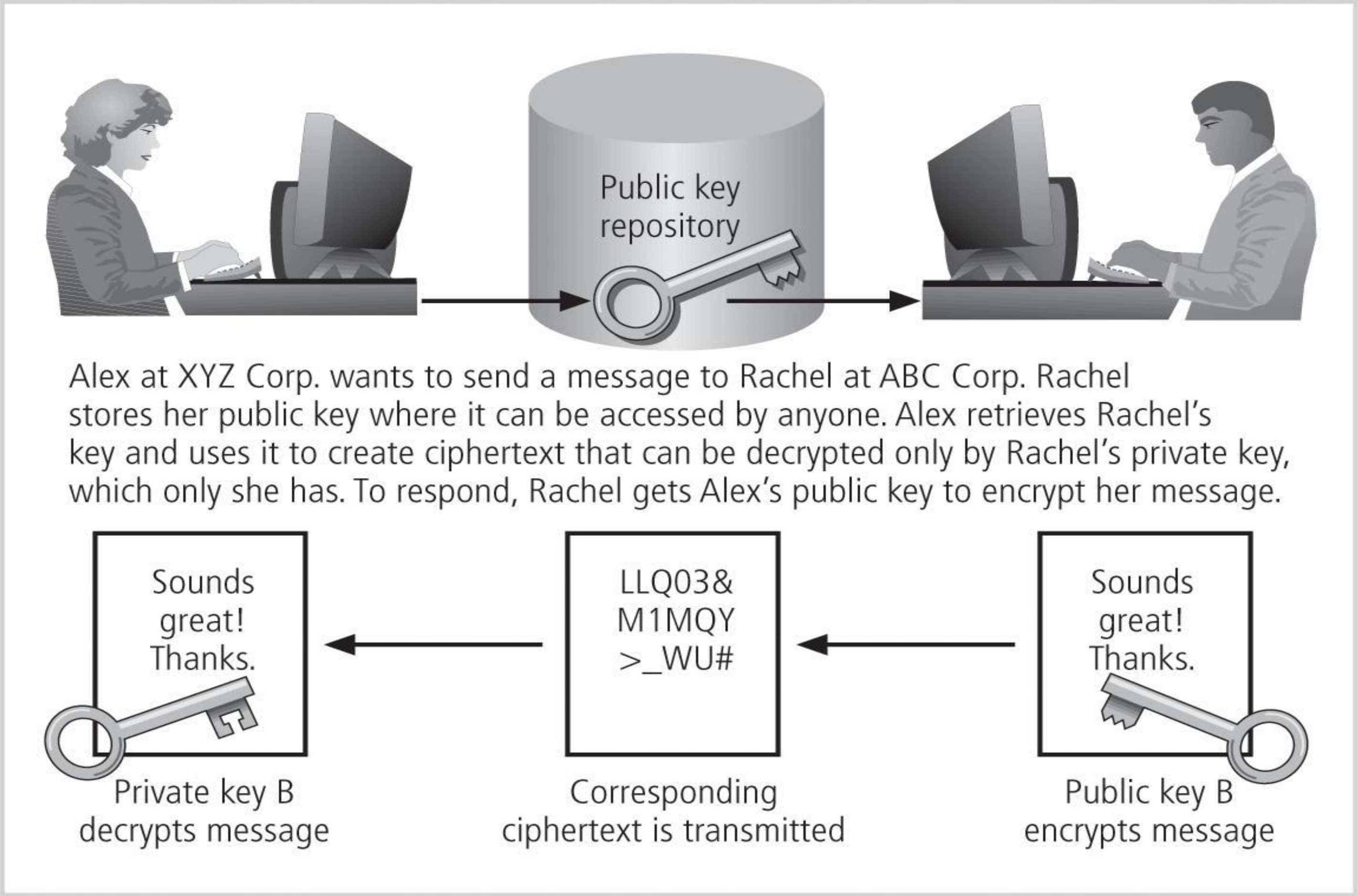
Copyright – Dan Brandon

Asymmetric Encryption

- Asymmetric encryption (public-key encryption)
  - Uses two different but related keys; either key can encrypt or decrypt message
  - If Key A encrypts message, only Key B can decrypt
  - One key serves as private key and the other serves as public key – solves the key distribution problem of symmetric encryption


ASYMMETRIC ENCRYPTION
KEY PAIR
WHAT IS ENCRYPTED WITH ONE KEY
CAN BE DECRYPTED WITH THE OTHER
PUBLIC
PRIVATE
CAN BE DECRYPTED WITH THE OTHER
WHAT IS ENCRYPTED WITH ONE KEY

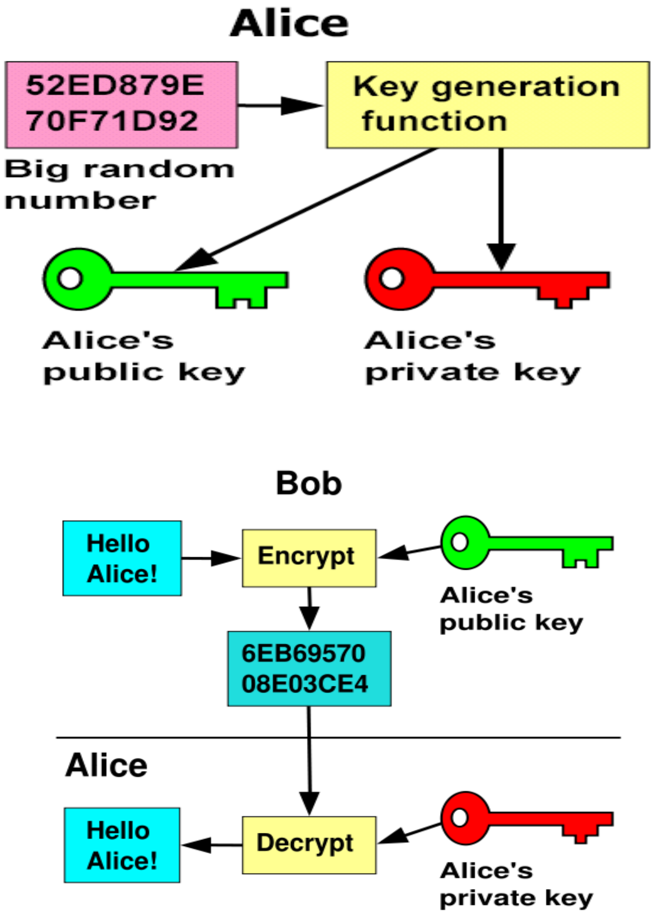
Asymmetric Encryption (con't)



Alex at XYZ Corp. wants to send a message to Rachel at ABC Corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves Rachel's key and uses it to create ciphertext that can be decrypted only by Rachel's private key, which only she has. To respond, Rachel gets Alex's public key to encrypt her message.

Asymmetric Encryption (con't)

- The keys are related mathematically, but the private key cannot be feasibly derived from the public key
- It was the discovery of such algorithms which revolutionized the practice of cryptography beginning in the middle 1970s - Used in SSL, TSL, PGP, and GPG



Copyright – Dan Brandon

Virtual Private Networks

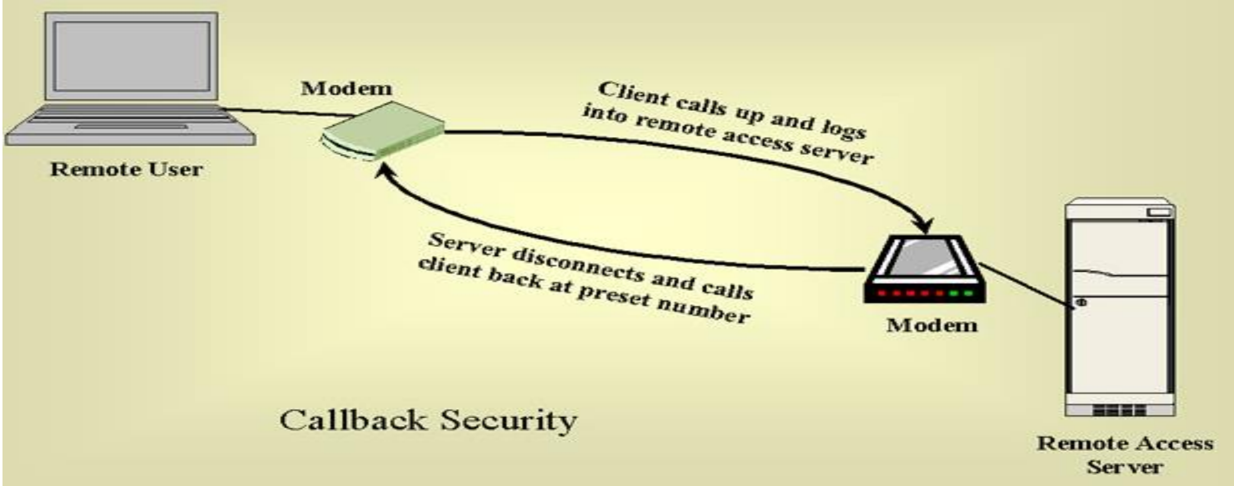
- Provides a secure tunnel through the Internet for transmitting messages and data by creating a private network
  - Gives remote users have a secure connection to the organization’s network
  - Provides security for extranets
- Data is encrypted before it is sent with a protocol
  - Layer Two Tunneling Protocol (L2TP)
  - Internet Protocol Security (IPSec)
- Advantage
  - Set-up costs are low
- Disadvantages
  - Slower transmission speed
  - Lack of standardization

Modern Security “Devices”

- Modern security devices (hardware/software) to mitigate cyber attacks include:
  - Callback modems
  - Firewalls
  - Intrusion detection systems
  - Proxy Servers

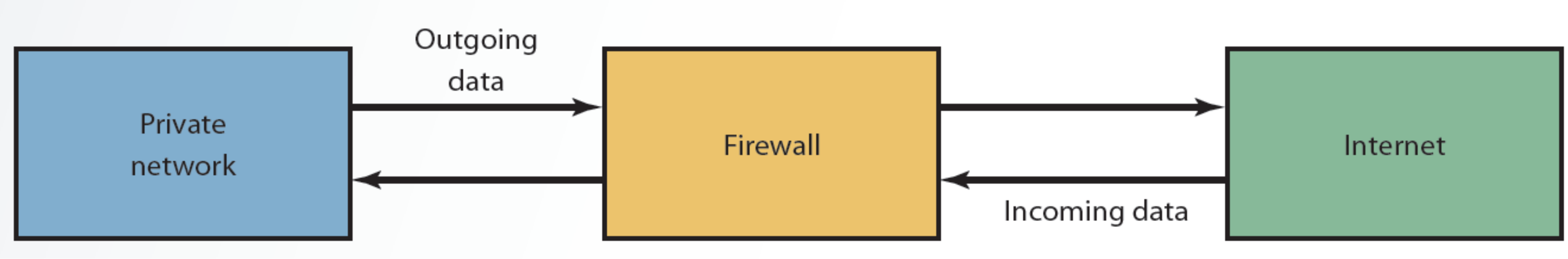
Callback Modems

- Verify whether a user's access is valid
  - Done by logging the user off and then calling the user back at a predetermined number
  - Useful when many employees work off-site and need to connect to the network from remote locations


Modem
Remote User
Client calls up and logs into remote access server
Server disconnects and calls client back at preset number
Modem
Callback Security
Remote Access Server

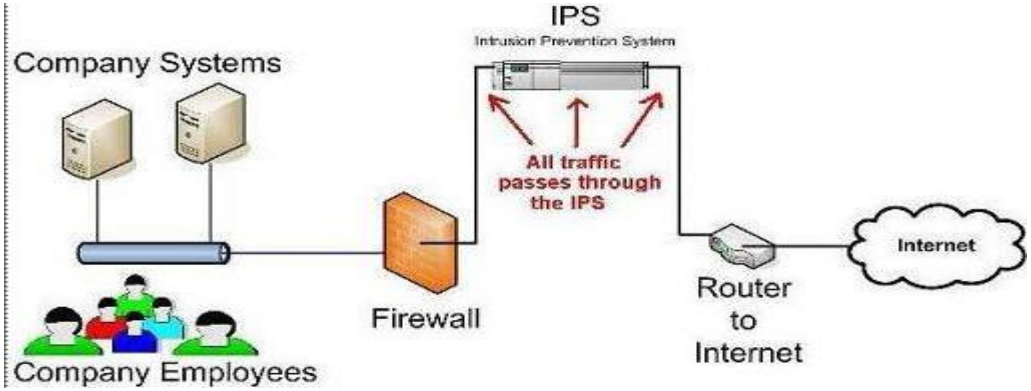
Firewalls

- Combinations of hardware and software that acts as a filter between a private network and external networks
  - Network administrator defines rules for access based upon IP addresses, and all other data transmissions are blocked
  - Types: packet-filtering firewalls, application-filtering firewalls, and proxy servers



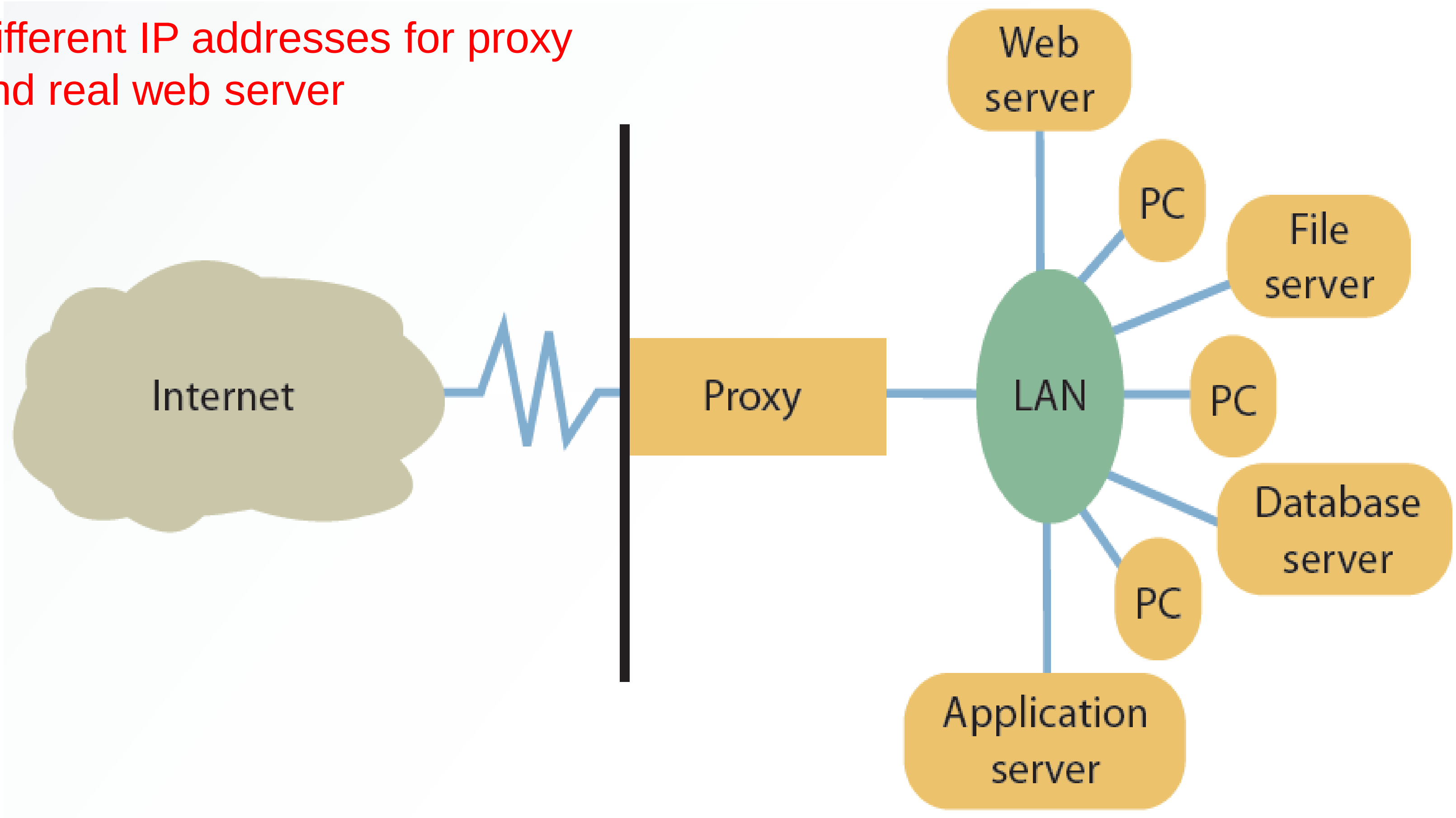
Intrusion Detection System (IDS)

- Protects against external and internal access
  - Placed in front of a firewall
  - Identifies attack signatures, traces patterns, and generates alarms for the network administrator
  - Causes routers to terminate connections with suspicious sources
  - Prevents DoS and many other type attacks
- Modern systems are intrusion detection and prevention systems (IDPS)



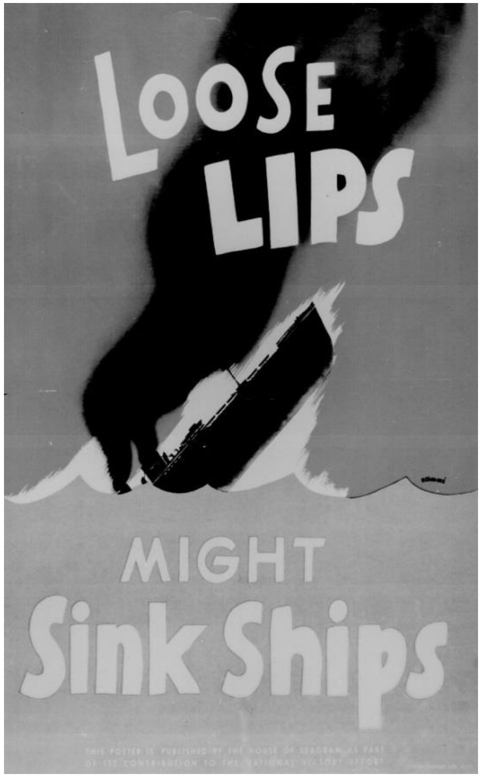
Proxy Server

Different IP addresses for proxy and real web server

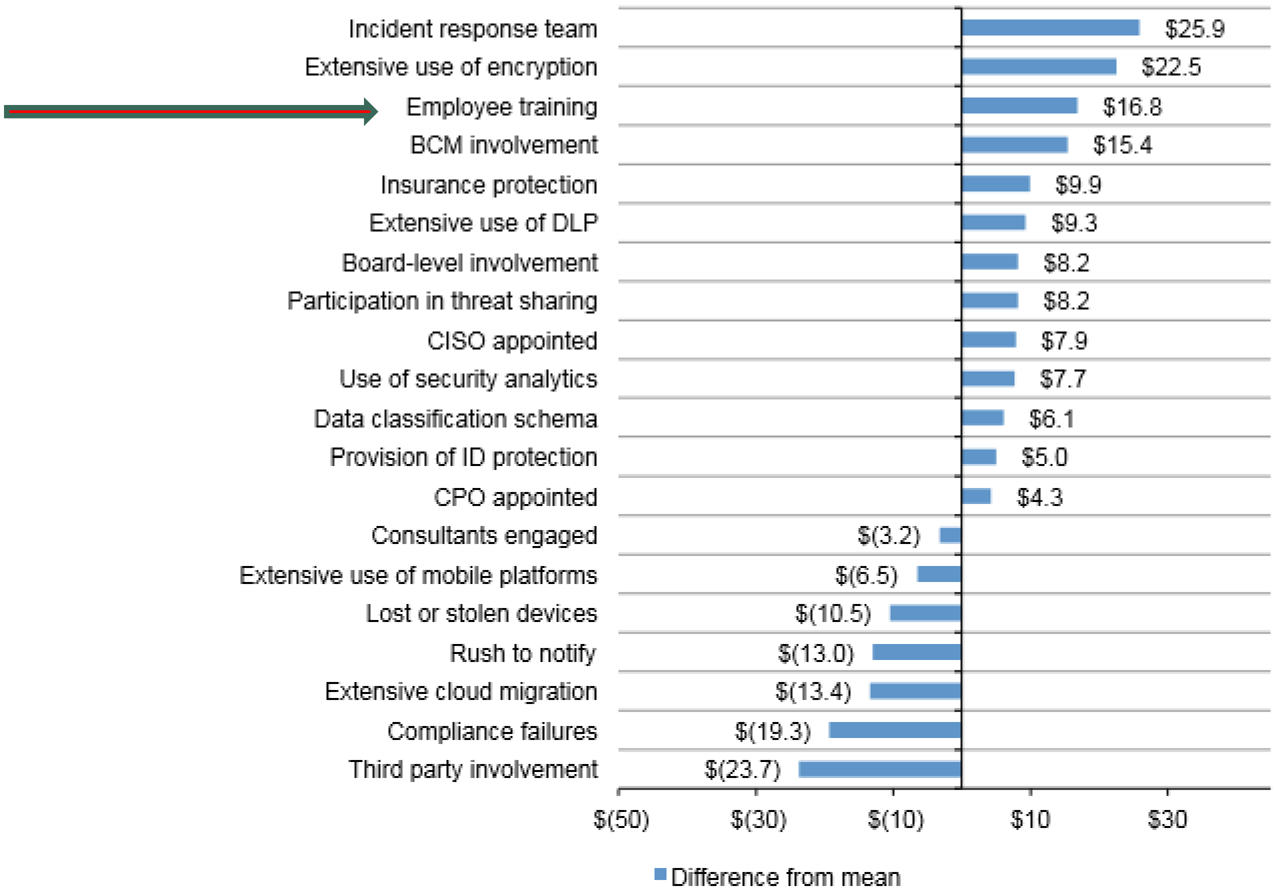


Security Education, Training, and Awareness Program (SETA)

- **As soon as a general security policy exists, policies to implement security education, training, and awareness (SETA) program should follow**
- SETA is a control measure designed to reduce accidental security breaches, and to minimize the impact of all types of security breaches



Impact of 20 Factors on Security



Physical Security Measures

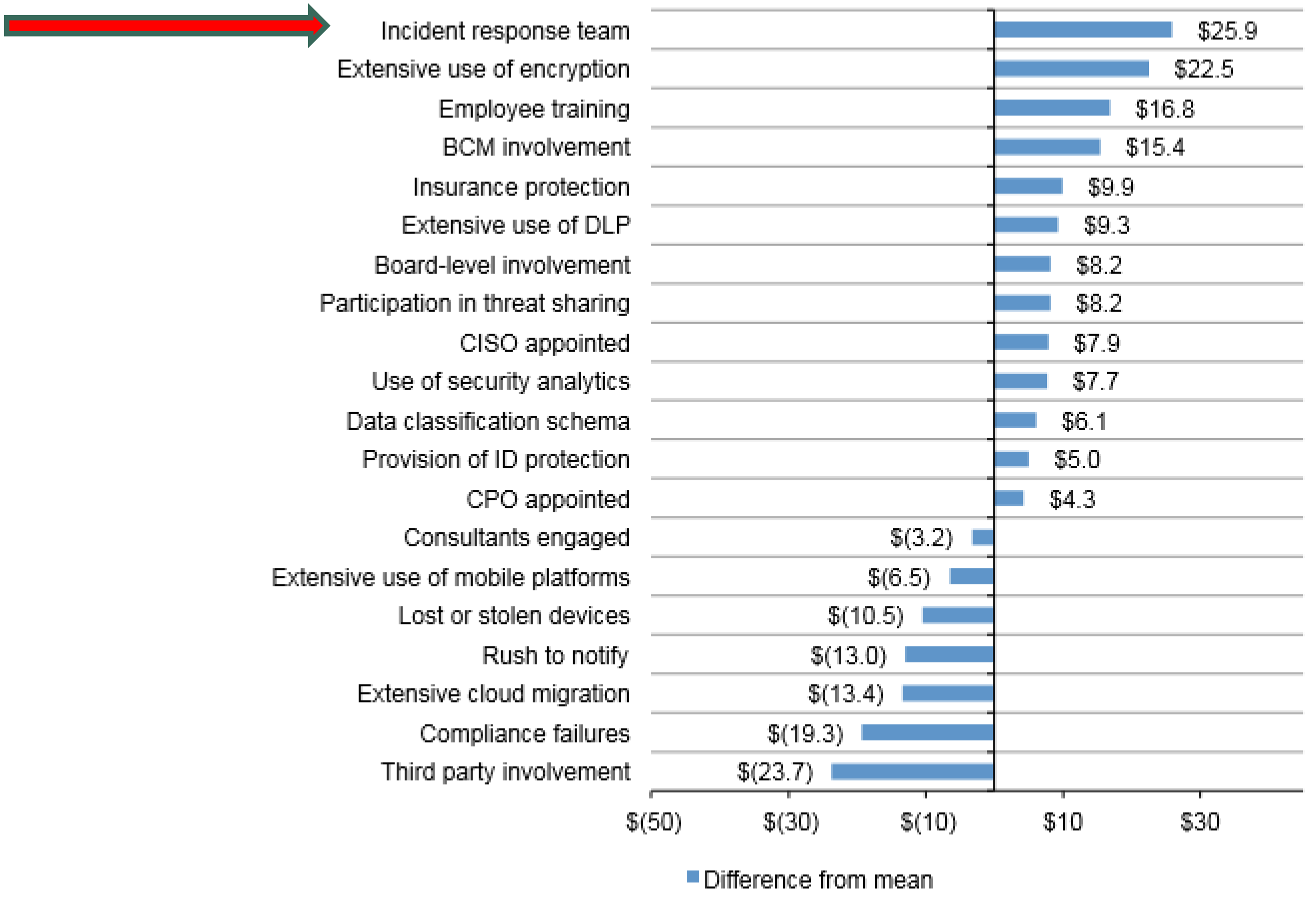
- Control access to computers and networks
  - Include devices for securing computers and peripherals from theft, damage, improper usage
    - Locked computer rooms
    - Cable shielding and room shielding
    - Steel encasements
    - Electronic trackers
    - Identification (ID) badges
    - Video surveillance

Disaster Recovery Planning
[Business Continuity]

- **Disaster recovery.** The chain of events linking planning to protection to recovery; manifested in a formal *disaster recovery plan*
- **Disaster avoidance.** Oriented towards prevention, such as an *uninterrupted power supply (UPS)*

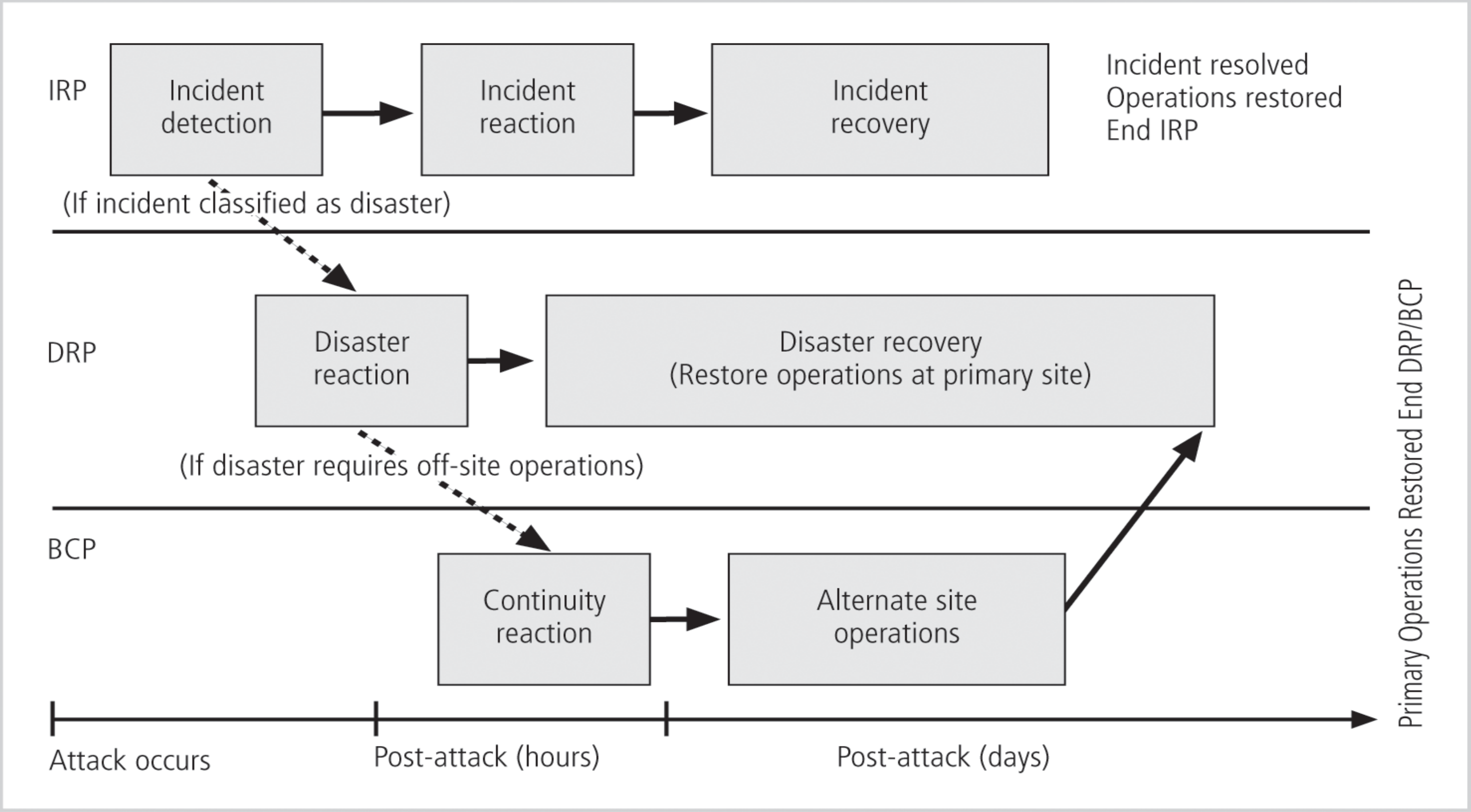
- ***Disaster protection.*** *Oriented towards protection of assets in the event of a disaster*
  - **Hot sites.** External data center that is fully configured and has full working current copies of the organization’s data, programs, etc.

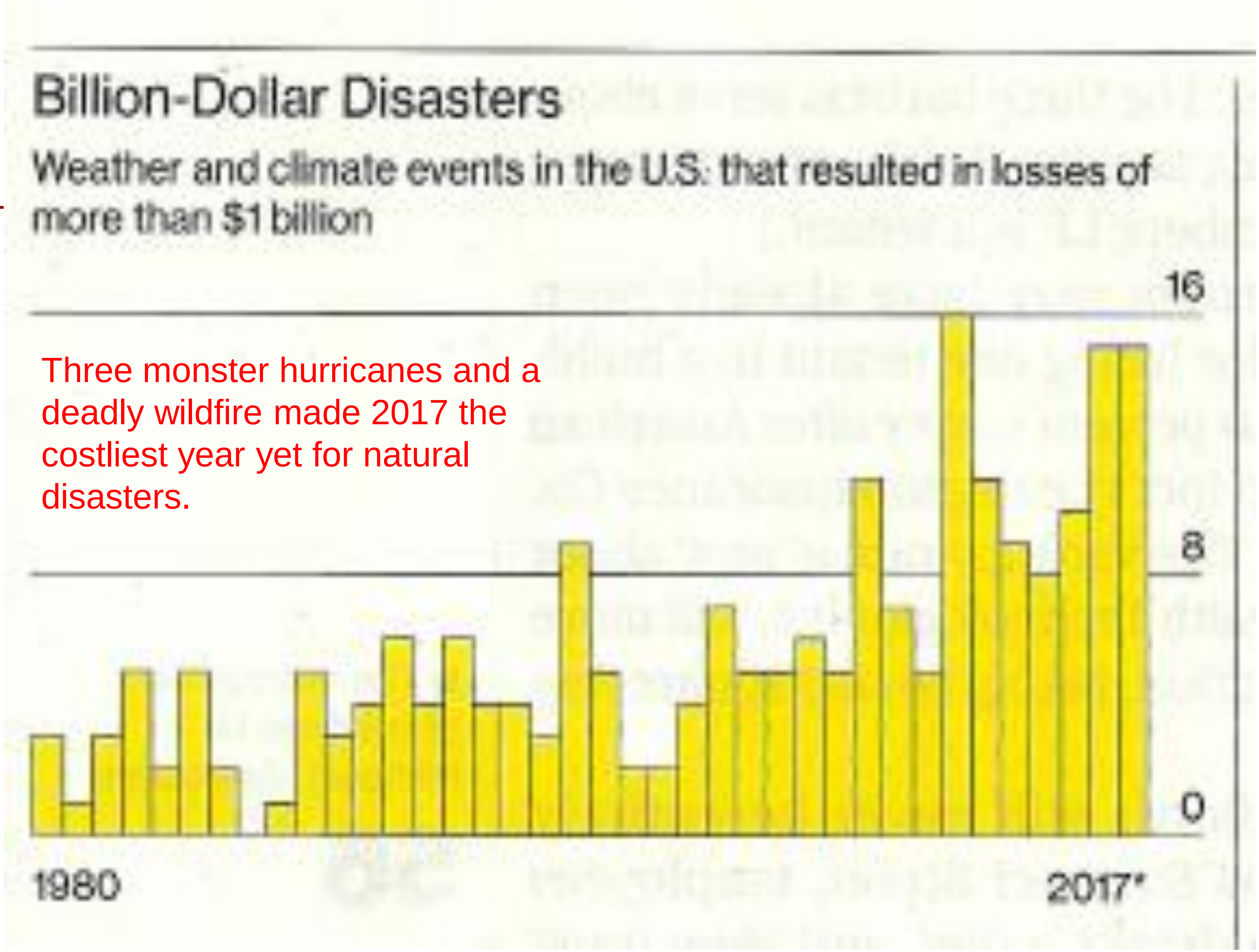
Impact of 20 Factors on Security



Copyright Dan Brandon

IRP, DRP, & BCP Interrelationship





Billion-Dollar Disasters

Weather and climate events in the U.S. that resulted in losses of more than $1 billion

Three monster hurricanes and a deadly wildfire made 2017 the costliest year yet for natural disasters.

- Which parts of the US have the worst weather related disasters ?

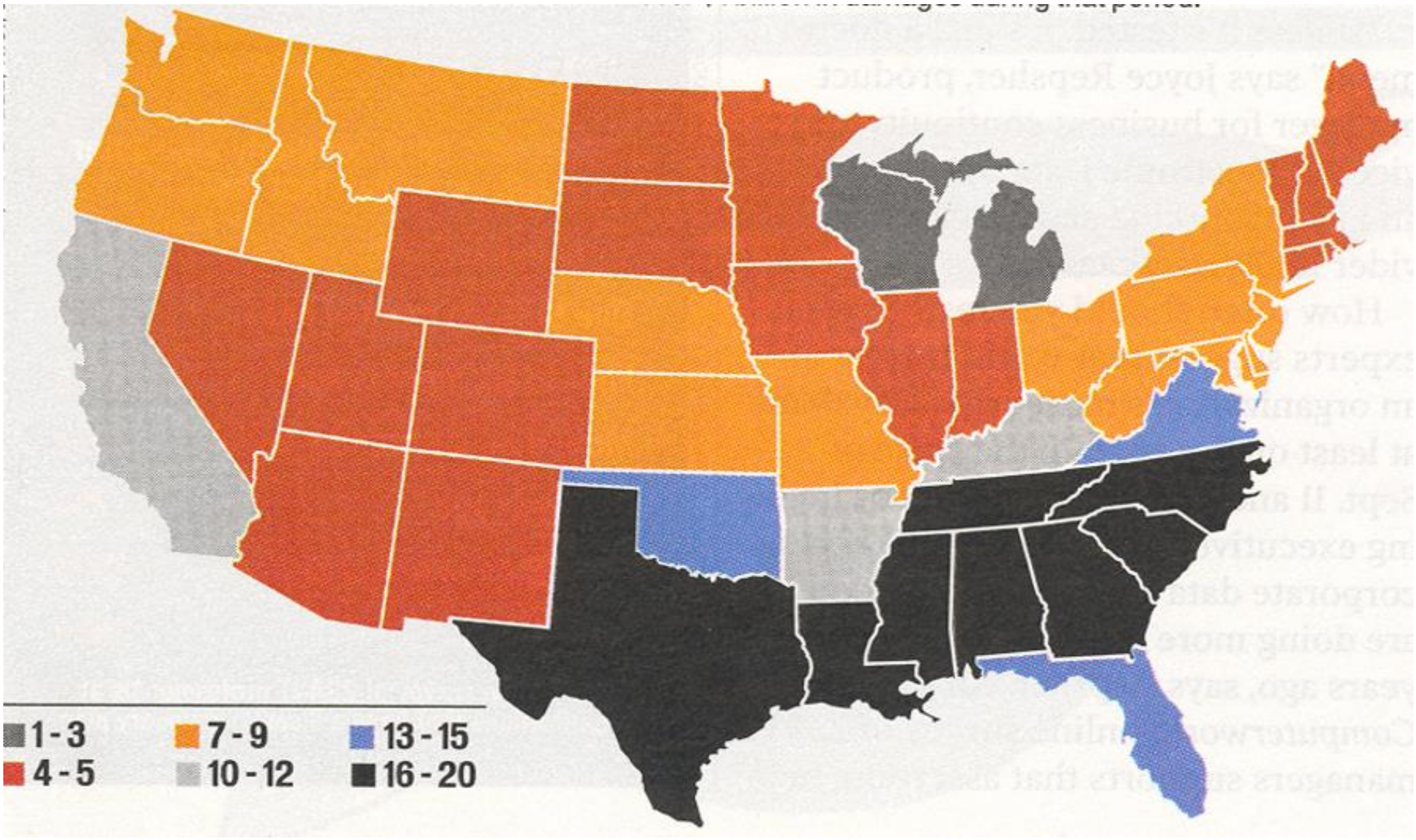
Aftermath of an earthquake in Japan, 2004
Photograph by Kimimasa Mayama/Reuters

Wait….

- ?

Don’t look ahead, until you have your answer !

Billion Dollar Disasters



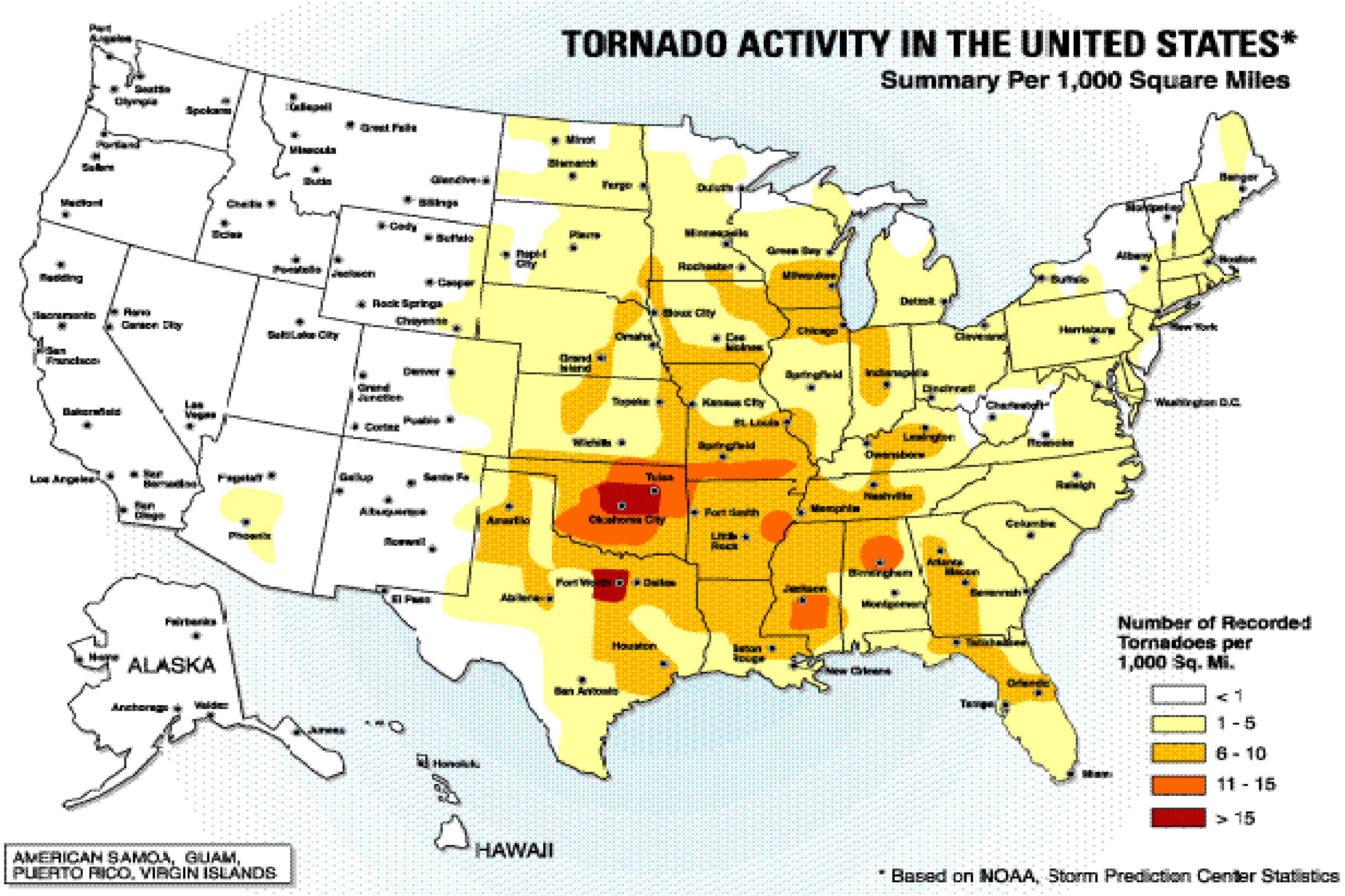
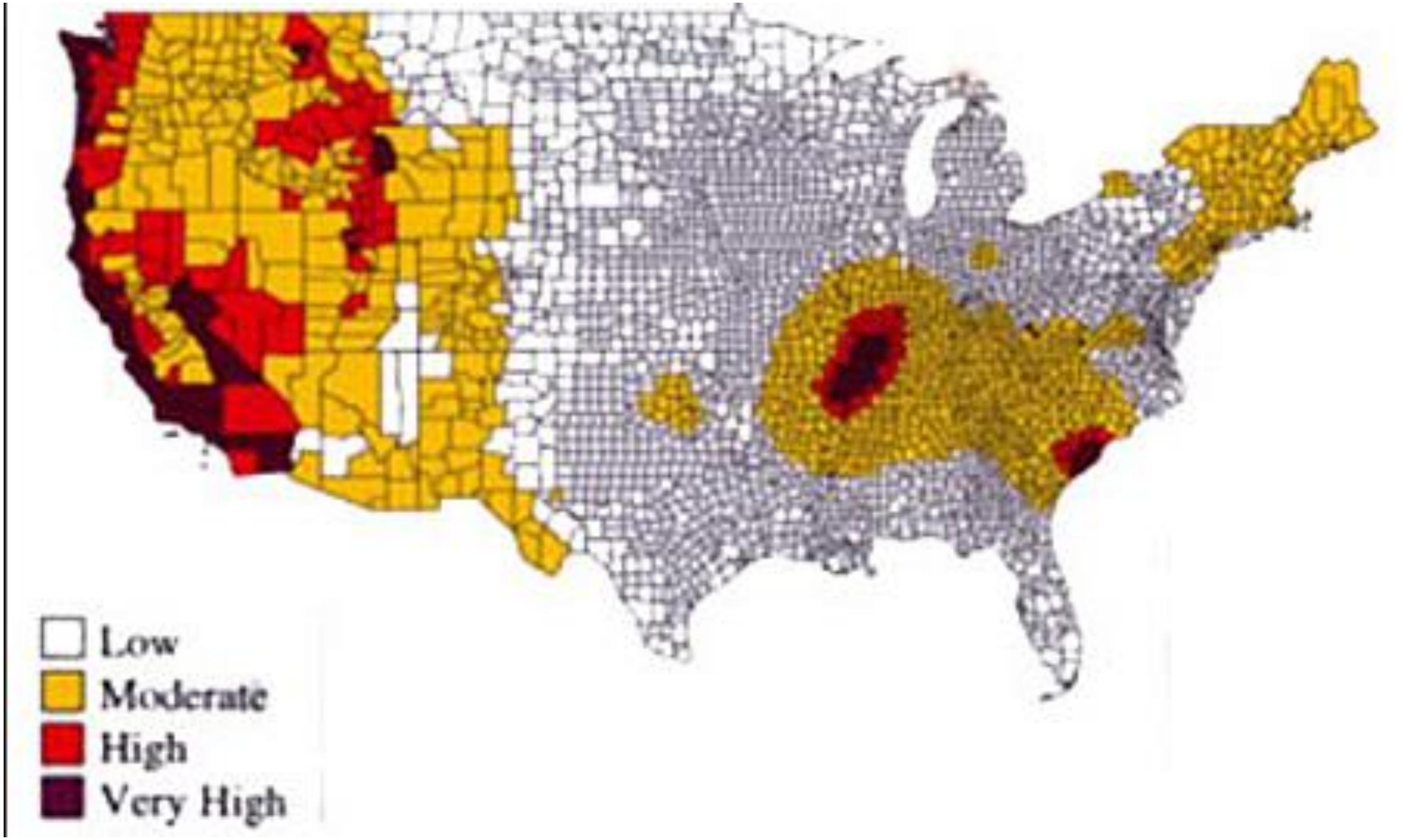


Figure I.1 The number of tornadoes recorded per 1,000 square miles

Earth Moving Under Us

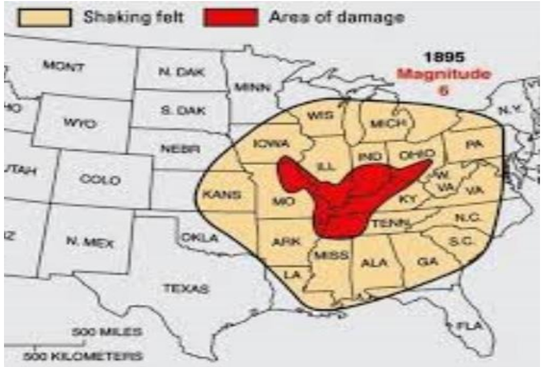
- Most people think that the ground under their feet is solid
- But that is not true, its moving all the time
- We all know that California is likely to have a major earthquake within the next 20 years
- But other areas such as New York City sit on top of a very brittle grid of rock that is long overdue for a major quake
- Other quake danger areas include OK, AR, TX and other ‘fracking” regions; MS river towns; and other coastal and mountain areas

Earth Moving Under Us (con't)



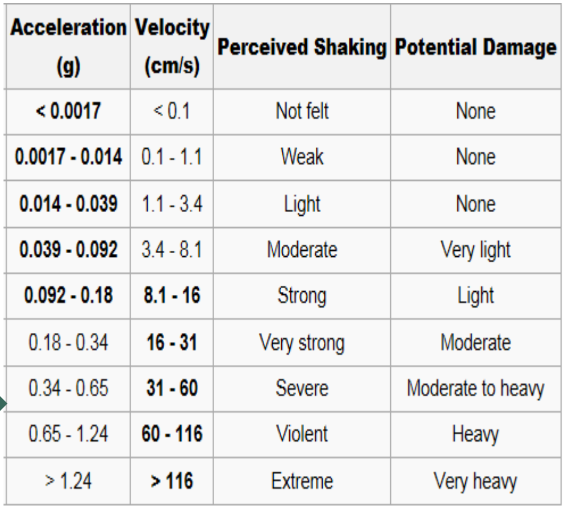
Memphis Disasters

- Memphis sits very close to the New Madrid fault
  - This is one of the most active faults in the US
  - We experience, on average, a small quake every 2-3 days
  - The largest earthquake ever recorded in the US was right here, and it created the 18000 acre Reelfoot lake and changed the course of the Mississippi river
  - A significant quake on this fault would create extensive power, gas, and water difficulties for hundreds of miles around
- Recent local disasters:
  - Ice storm of 1994
  - “Hurricane Elvis” in 2003

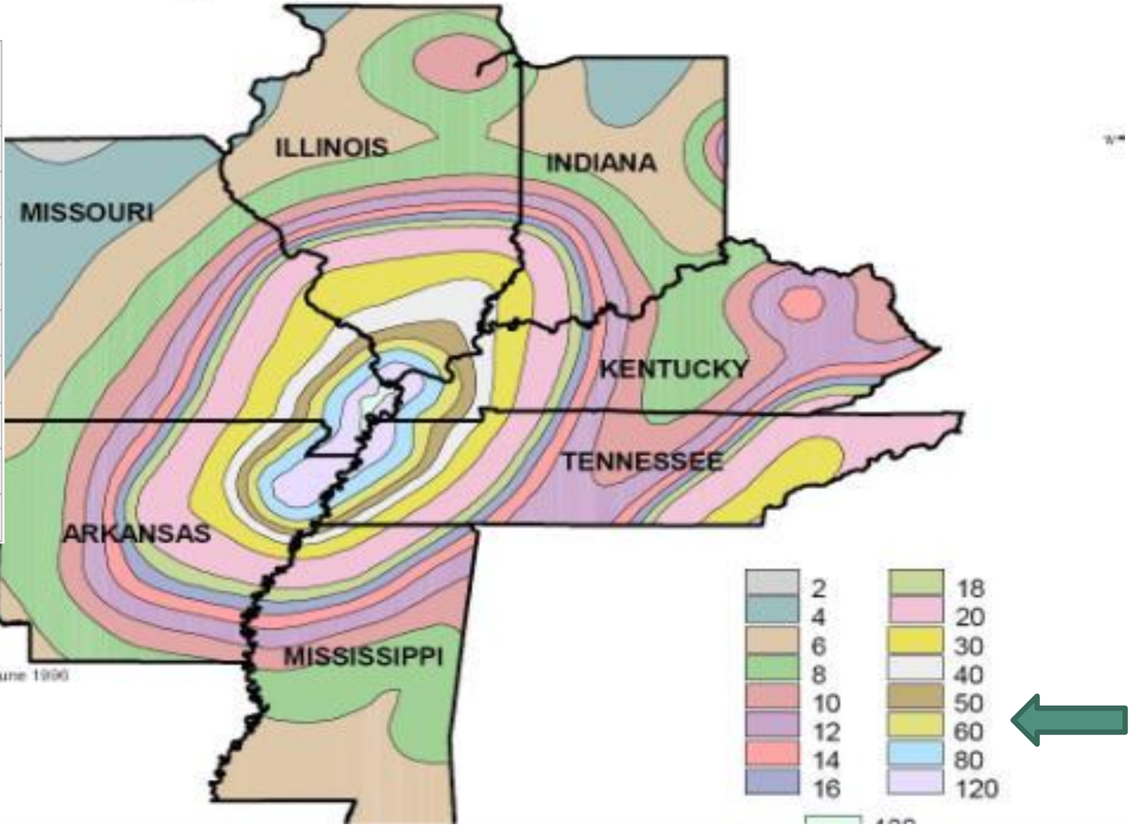


New Madrid Fault

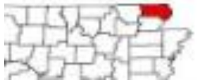
Figure 3-7: Peak Ground Acceleration (%g) with 2% Probability of Exceedance in 50 years; CUSEC* States



Acceleration (g)	Velocity (cm/s)	Perceived Shaking	Potential Damage
< 0.0017	< 0.1	Not felt	None
0.0017 - 0.014	0.1 - 1.1	Weak	None
0.014 - 0.039	1.1 - 3.4	Light	None
0.039 - 0.092	3.4 - 8.1	Moderate	Very light
0.092 - 0.18	8.1 - 16	Strong	Light
0.18 - 0.34	16 - 31	Very strong	Moderate
0.34 - 0.65	31 - 60	Severe	Moderate to heavy
0.65 - 1.24	60 - 116	Violent	Heavy
> 1.24	> 116	Extreme	Very heavy



Source: U.S. Geological Survey, June 1996



Copyright – Dan Brandon

Computer Forensics

- *The art and science of applying computer science to aid the legal process*
- It is more than the technological, systematic inspection of a computer system and its contents for evidence or supportive evidence of a civil wrong or a criminal act
- Computer forensics requires specialized expertise and tools that goes above and beyond the normal data collection and preservation techniques available to end-users or system support personnel

Computer Forensics (con’t)

- Computer forensics experts: identify sources of digital evidence, preserve the evidence, analyze the evidence, and present the findings.
- Computer forensics is done in a fashion that adheres to the standards of evidence (chain of custody) that are admissible in a court of law
- Thus, computer forensics must be techno-legal in nature rather than purely technical or purely legal

New IT Jobs

- Cyber Security
- IT Risk Management
- Disaster Recovery (business continuity)
- IS Auditor
- Computer Forensics

Best Jobs
[US News and World Reports]

- **Dentist**
- **Nurse Practitioner**
- **Software Developer**
- **Physician**
- **Dental Hygienist**
- **Physical Therapist**
- **Computer Systems Analyst**
- **Information Security Analyst**
  - The US BLS predicts our No. 8 job will grow at an astounding rate of 36.5 percent between 2012 and 2022
- **Registered Nurse**
- **Physician Assistant**

Top Tech Initiatives
[CIO Magazine Survey]

- Business Intelligence (analytics)
- Mobile Technologies
- Cloud Services
- Application Modernization
- Customer Experience Technologies
- Security and Risk Management

Ten Commandments of Computer Ethics (cf. Rinaldi, 2000)

- 1. Thou shalt not use a computer to harm other people.
- 2. Thou shalt not interfere with other people’s computer work.
- 3. Thou shalt not snoop around in other people’s files.
- 4. Thou shalt not use to steal.
- 5. Thou shalt not use use a computer to bear false witness.
- 6. Thou shalt not use or copy software for which you have not paid.
- 7. Thou shalt not use other people’s computer resources without authorization.
- 8. Thou shalt not appropriate other people’s intellectual output.
- 9. Thou shalt think about the social consequences of the program you write.
- 10. Thou shalt use a computer in ways that show consideration and respect.

Ten Signs Your Network May Not Be Secure

- 10.Your CEO thought your last information security risk assessment was a Sudoku puzzle
- 9.You arrive at work to find Dateline and 60 Minutes waiting in the lobby to interview you about the security breach
- 8.The new network administrator has posted your network schematic on his personal, “Master of the Domain” web site where he appears scantily clad in leather and old computer parts
- 7.When post-it notes run out, new hires begin to tattoo their passwords on their wrists
- 6.The door to the server room is of the revolving variety

- 5. The CFO thinks the Intrusion Prevention System is that “wire thingy” that keeps squirrels and pigeons out of the attic
- 4.The company’s security awareness program involves lots of yelling, cursing, and crying
- 3.Your last IT audit used the phrase “bless their hearts” 20 times
- 2.The janitor complains that his sink where he rings out the mops, is too close to that “rack of boxes with blinking lights”
- 1.Internet content filters block your company’s new e-commerce site as a gambling site

Summary

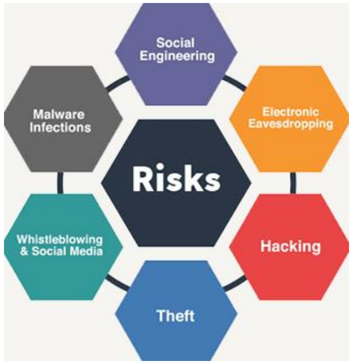
- Risks associated with information technologies can be minimized by:
  - Installing operating system updates regularly
  - Using antivirus/antispyware software and e-mail security features
- Comprehensive security system protects an organization’s resources
  - Including information, computers, and network equipment
- Network security threats can be categorized
  - Unintentional: natural disasters, accidental deletion of data, and structural failures
  - Intentional: hacker attacks and attacks by disgruntled employees
- Organizations must employ a variety of comprehensive security measures to guard against threats

Library and Web References

- Computer Security Basics by Rick Lehtinen
- Computer Security Fundamentals (Prentice Hall Security Series) by Chuck Easttom
- Computer Security: Art and Science by Matt Bishop
- Corporate Computer and Network Security by Raymond Panko
- Computer Security by Dieter Gollmann
- Computer Security: 20 Things Every Employee Should Know by Ben Rothke
- Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security by Tony Bradley

Homework

- Textbook Chapter Five
- Quiz on that chapters
- For ABC, individually:
  - How will ABC handle ethical and legal issues
  - Information Security – What are the major issues for ABC here, and how will ABC protect its customers, employees, business and assets


Social Engineering
Malware Infections
Electronic Eavesdropping
Risks
Whistleblowing & Social Media
Hacking
Theft