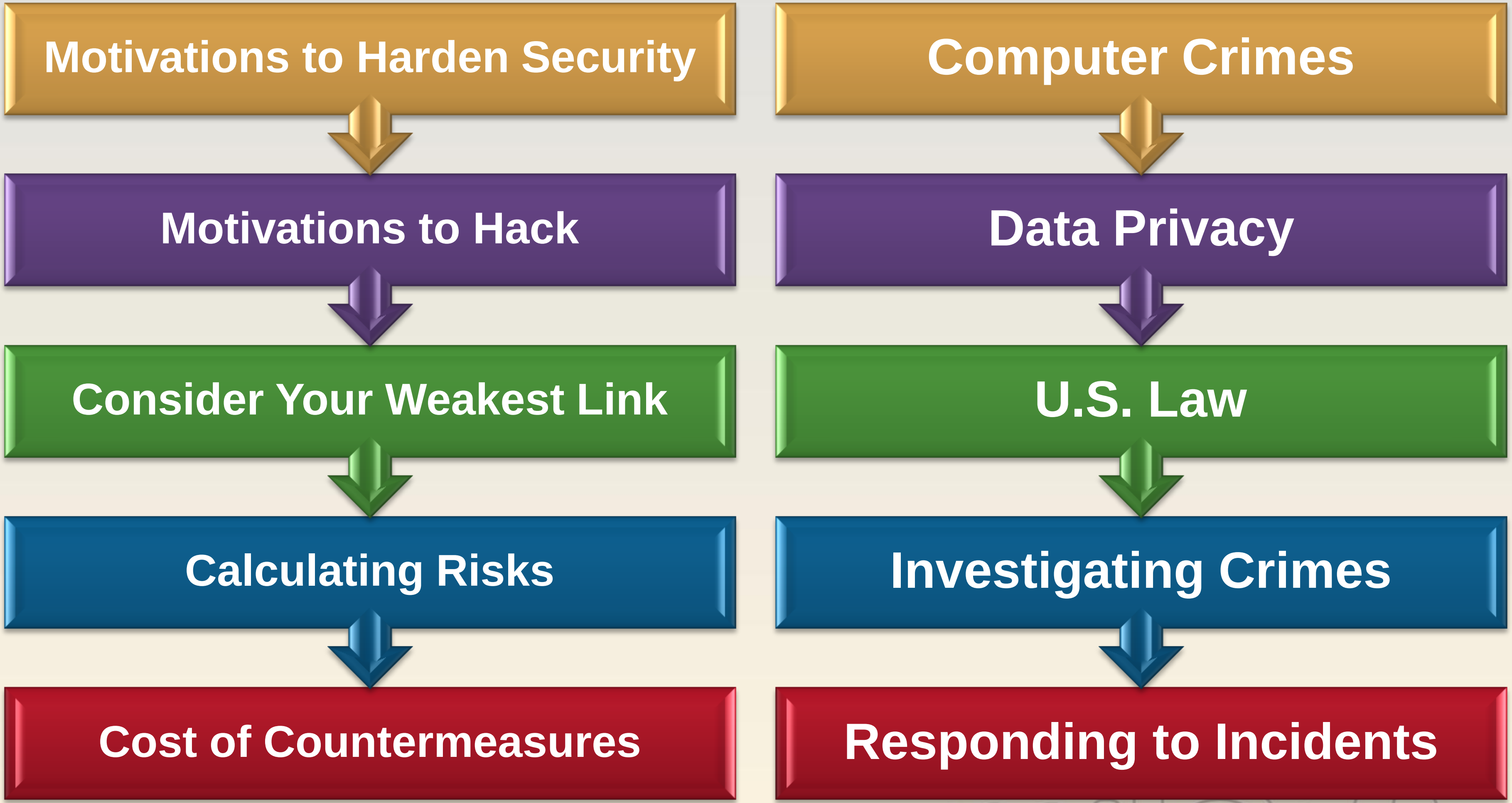
Economics and Law in Relation to Information Security

Review



Motivations to Harden Security

Motivations to Hack

Consider Your Weakest Link

Calculating Risks

Cost of Countermeasures

Computer Crimes

Data Privacy

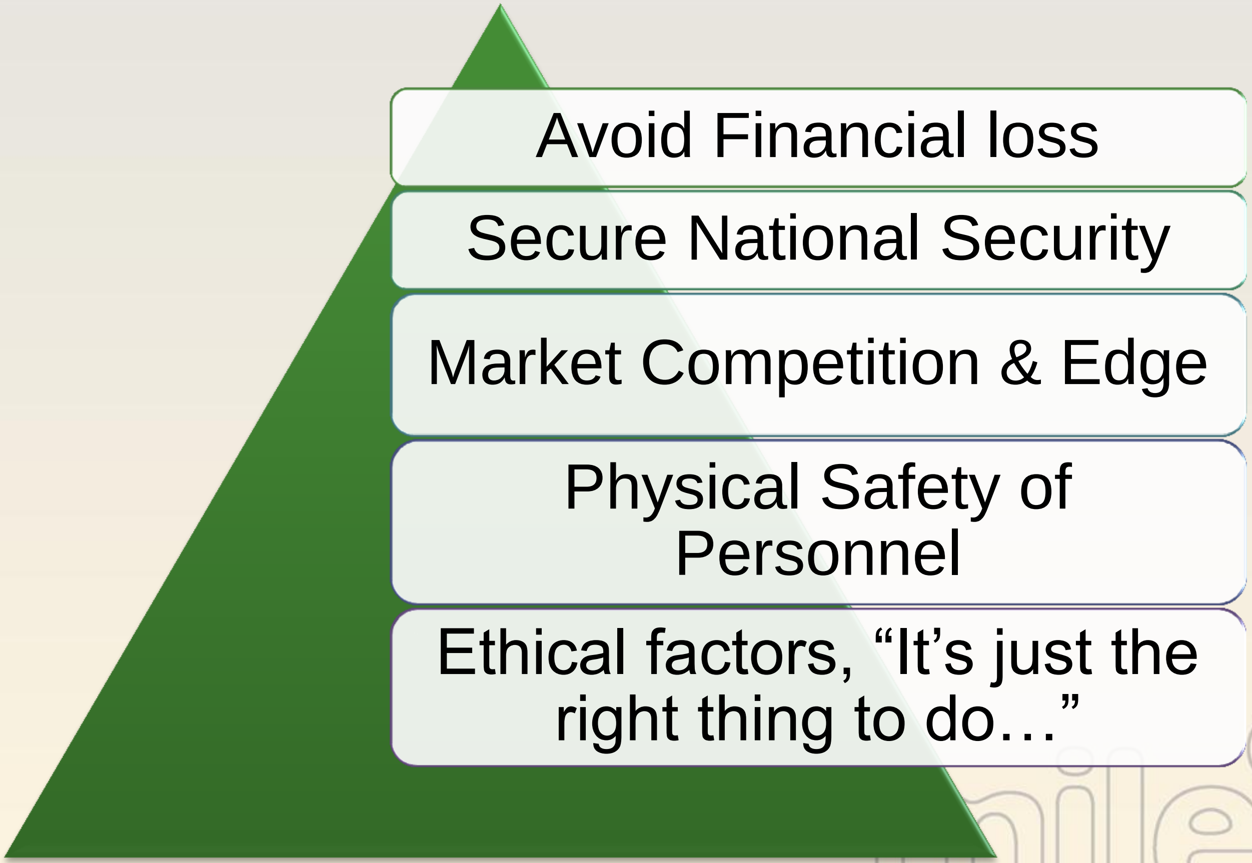
U.S. Law

Investigating Crimes

Responding to Incidents

Security Incentives & Motivations

What motivates us to promote security?



Avoid Financial loss

Secure National Security

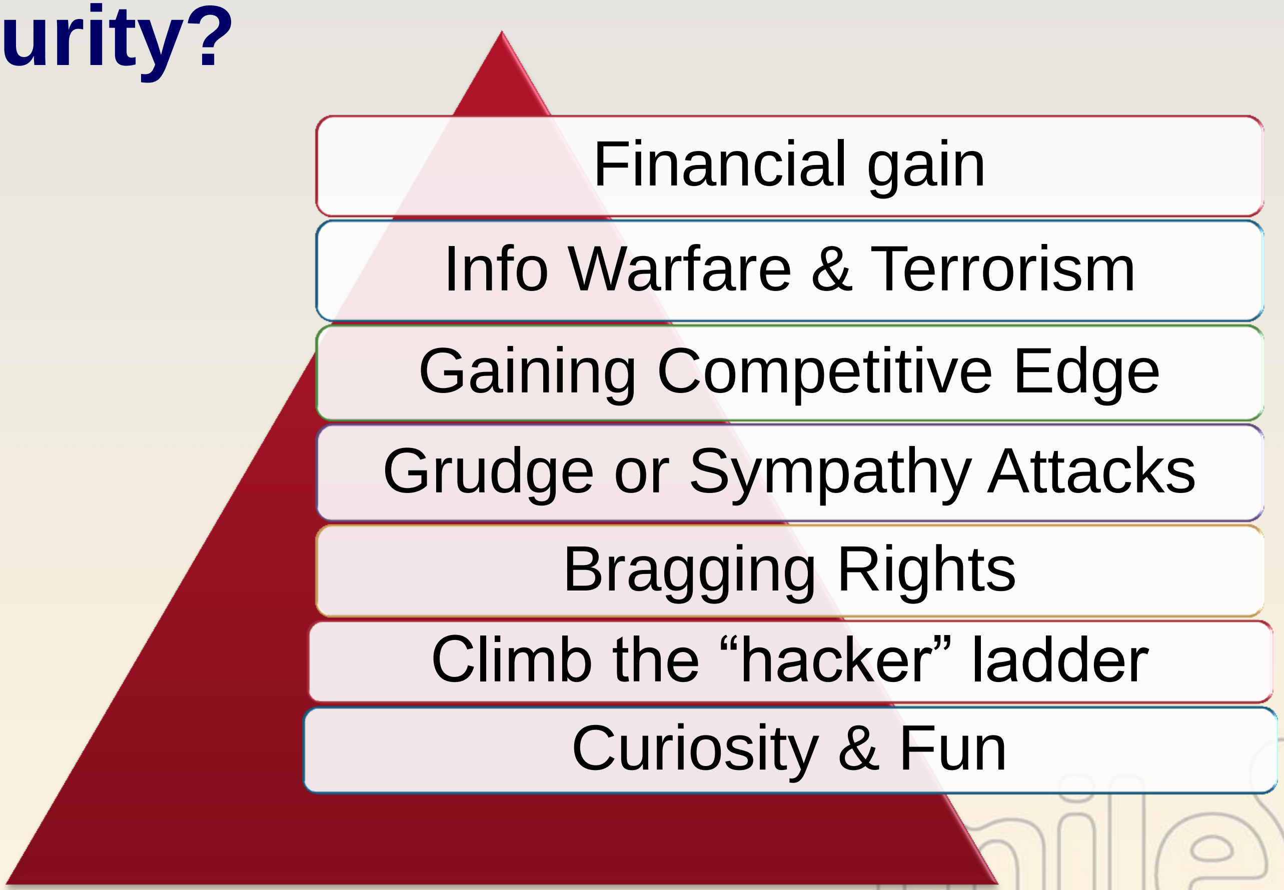
Market Competition & Edge

Physical Safety of Personnel

Ethical factors, “It’s just the right thing to do…”

Security Incentives & Motivations

What motivates others to attack security?



Financial gain

Info Warfare & Terrorism

Gaining Competitive Edge

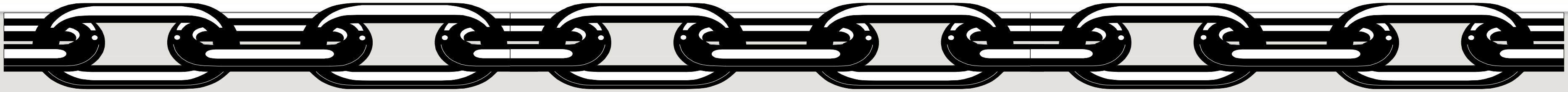
Grudge or Sympathy Attacks

Bragging Rights

Climb the “hacker” ladder

Curiosity & Fun

What is Your Weakest Link?



Links in the Security Chain: Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning, policies, procedures
- ✓ Configuration management and control
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Security in acquisitions
- ✓ Physical security
- ✓ Personnel security
- ✓ Security assessments
- ✓ Certification and accreditation

- ✓ Access control mechanisms
- ✓ Identification & authentication mechanisms (Biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Boundary and network protection devices (Firewalls, guards, routers, gateways)
- ✓ Intrusion protection/detection systems
- ✓ Security configuration settings
- ✓ Anti-viral, anti-spyware, anti-spam software
- ✓ Smart cards

Adversaries attack the weakest link…where is yours?

Slide Contents from : *Information Security Standards Promoting Trust, Transparency, and Due Diligence E-Gov Washington Workshop* April 17, 2009 Dr. Ron Ross Computer Security Division Information Technology Laboratory, NIST

What Is the Value of an Asset?

An Asset’s Value Is Calculated by Reviewing:

- Cost of acquisition
- Replacement cost
- Cost of developing the asset
- Role of the asset in the company
- Amount adversaries are willing to pay for the asset
- Cost of maintaining and protecting the asset
- Production and productivity losses resulting from compromise of asset
- Liability if asset is not properly protected

Examples of Some Vulnerabilities that Are Not Always Obvious

Lack of security understanding

- Real security requires real knowledge
- Technical to the C-level in companies

Misuse of access by authorized users

- Authorization creep
- Can now be a criminal offense according to specific laws

Concentration of responsibilities

- Separation of duties

Not being able to react quickly

- No response team or procedures

Lack of communication structure

Lack of ways to detect fraud

- Rotation of duties
- Technologies and processes

Categorizing Risks

Risks

- Potential loss
  - Ramifications of exposure
- Delayed loss
  - Secondary ramifications of exposure
  - Much harder to identify and calculate

List Examples of…

- Potential losses
- Delayed losses

Some Examples of Types of Losses

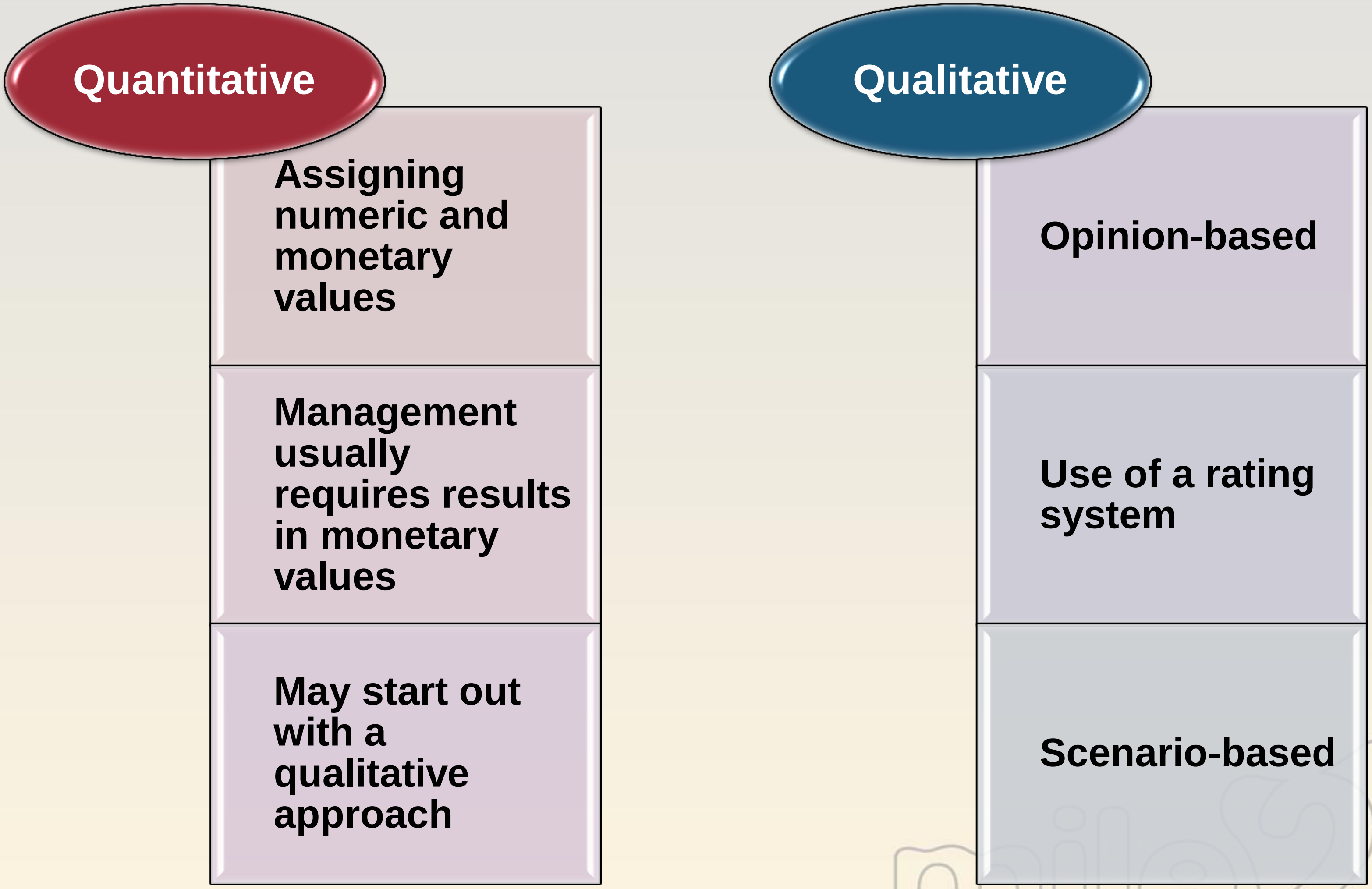
Potential Losses

- Loss in production and productivity
- Cost of repairing damages
- Cost of consultants' or experts' services
- Loss in revenue
- Loss of customers

Delayed Losses

- Loss in reputation
- Loss of potential customers
- Late fees or penalty fees
- Loss in market share

Different Approaches to Analyzing Risks



Quantitative

Assigning numeric and monetary values

Management usually requires results in monetary values

May start out with a qualitative approach

Qualitative

Opinion-based

Use of a rating system

Scenario-based

Who Uses What Analysis Type?

In Most Situations…

Companies usually use quantitative

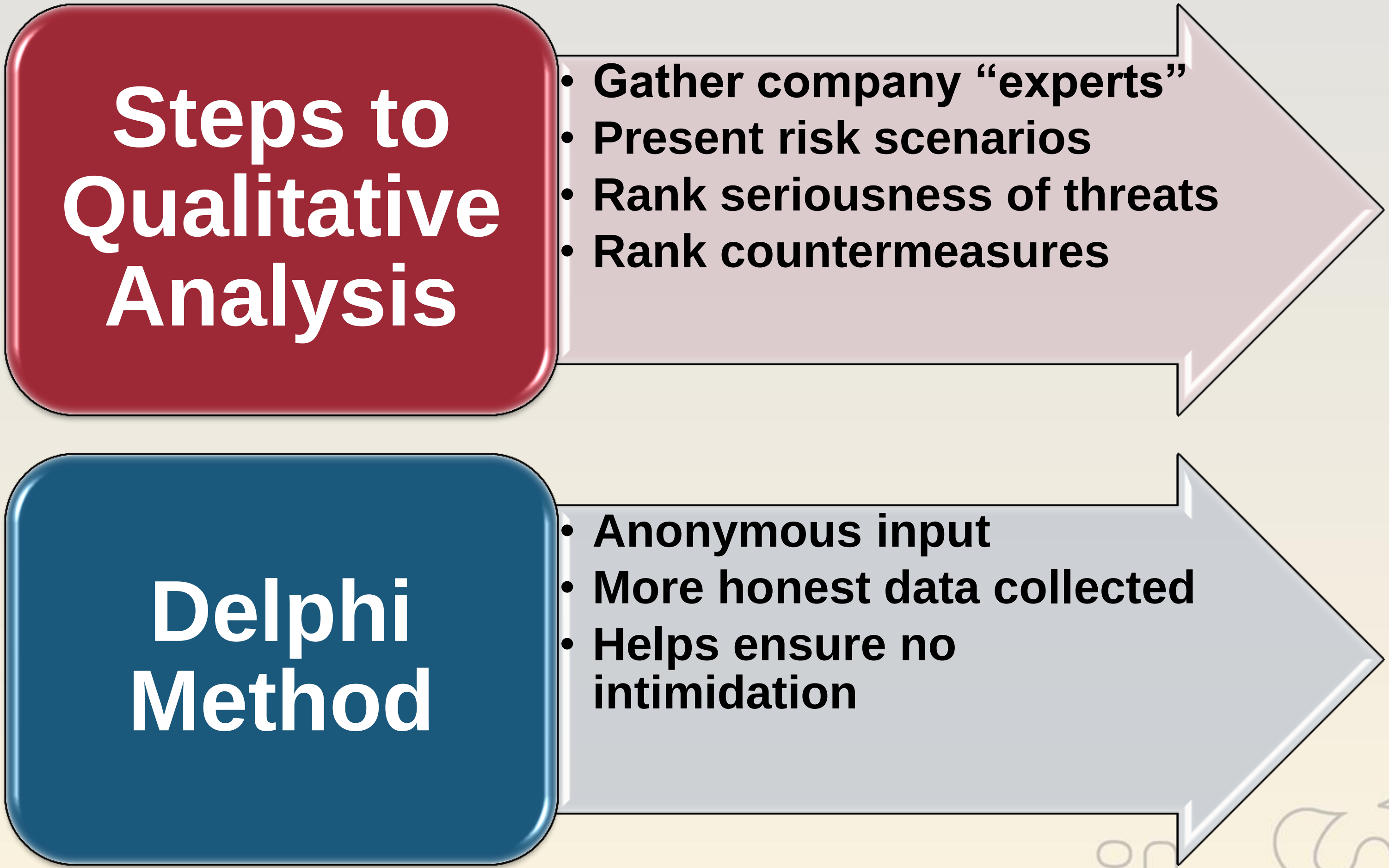
Profit-based organization

Government agencies usually use qualitative

Have to provide protection no matter what

- DoD
- DoE
- Military units
- NSA

Qualitative Analysis Steps



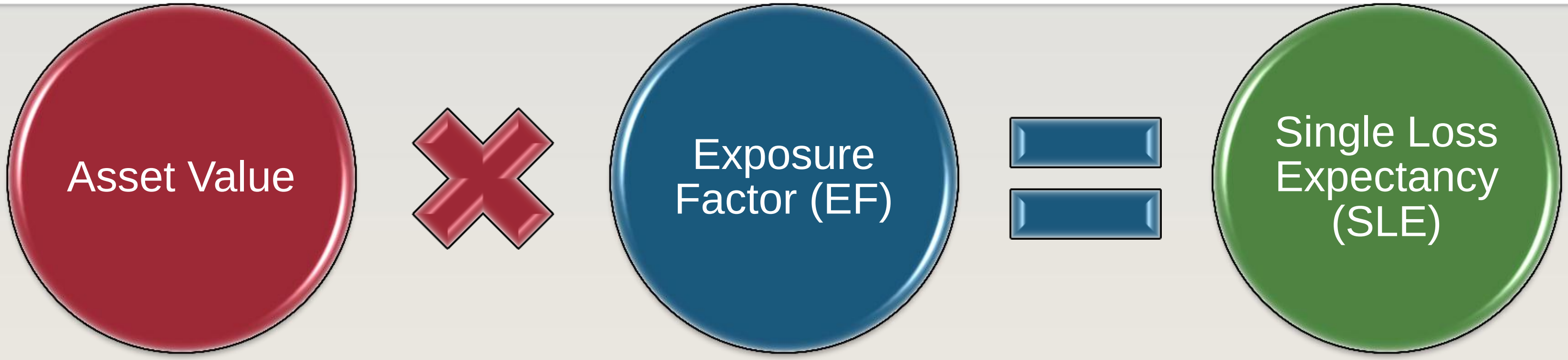
Steps to Qualitative Analysis

- Gather company “experts”
- Present risk scenarios
- Rank seriousness of threats
- Rank countermeasures

Delphi Method

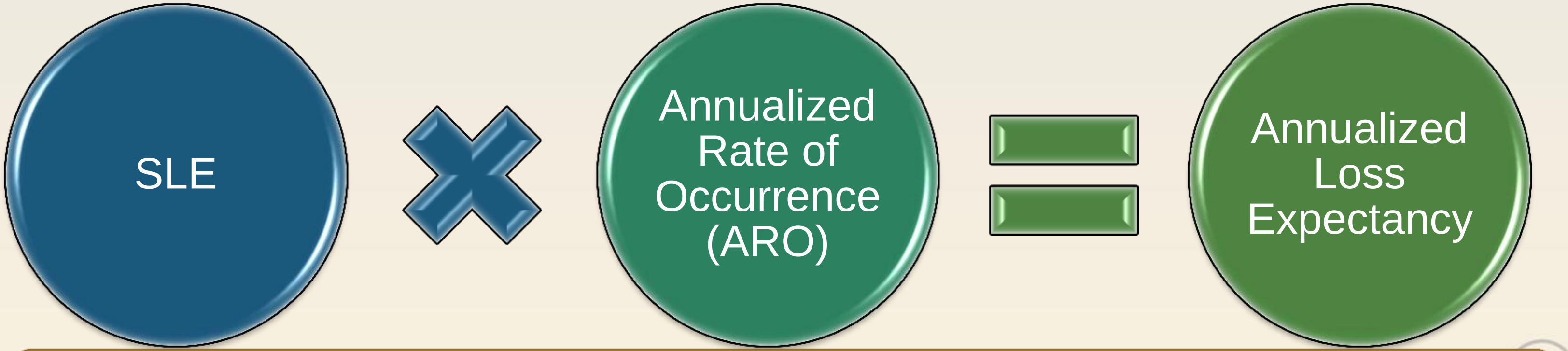
- Anonymous input
- More honest data collected
- Helps ensure no intimidation

Quantitative Analysis



Asset Value × Exposure Factor (EF) = Single Loss Expectancy (SLE)

Exposure factor **= the percentage of loss that could be experienced**



SLE × Annualized Rate of Occurrence (ARO) = Annualized Loss Expectancy

Annualized rate of occurrence (ARO) **= frequency of threat taking place**

What is the ALE value then used for?

Can a Purely Quantitative Analysis Be Accomplished?

NO!

A quantitative analysis requires quantifying many qualitative items.

- How do you assign a value to a reputation?
- How can you know the potential customers that will be lost?
- How can you properly predict market share loss?
- All of these questions are difficult, but are required in a quantitative analysis.

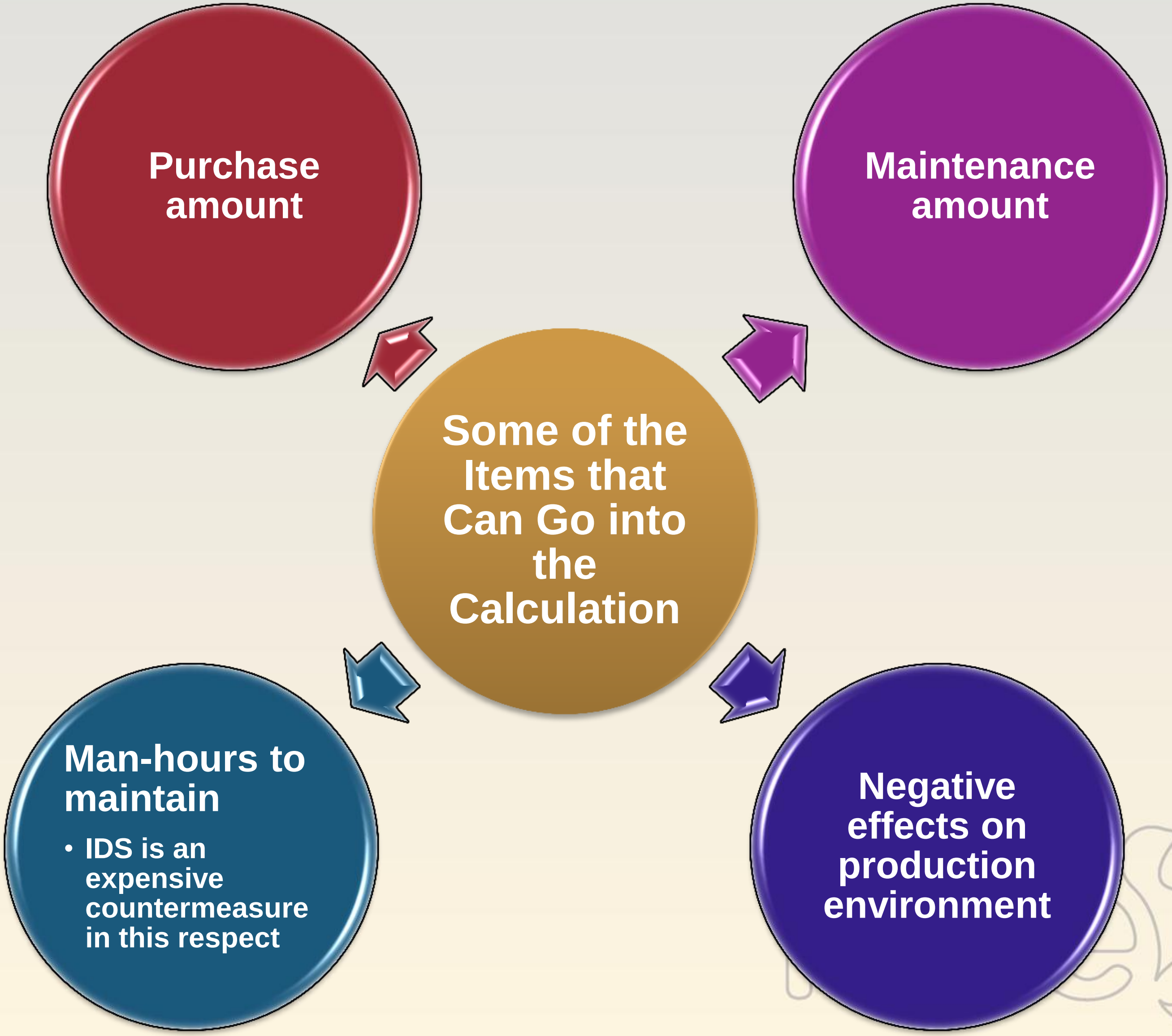
Comparing Cost and Benefit

Cost/Benefit Analysis

- The annualized cost of countermeasures should not be more than potential losses
- If a server is worth $3,000, a countermeasure that costs $4,000 should not be used
- Not as cut and dried as it may seem

How do you determine the cost of a countermeasure?

Cost of a Countermeasure



Some of the Items that Can Go into the Calculation

Purchase amount

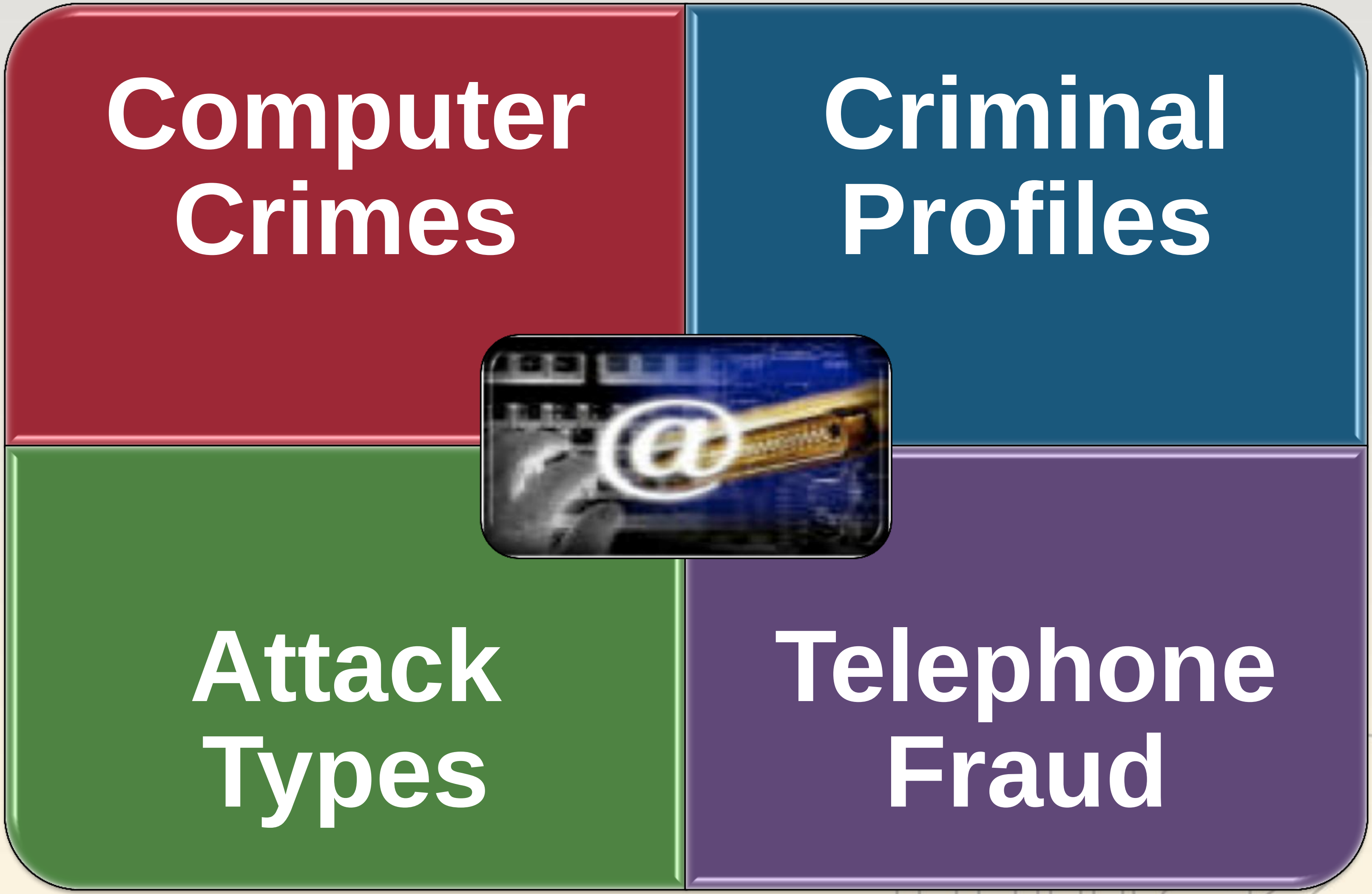
Maintenance amount

Man-hours to maintain

- IDS is an expensive countermeasure in this respect

Negative effects on production environment

Cyber Crime!



Computer Crimes

Criminal Profiles

Attack Types

Telephone Fraud

Not Just Fun and Games

Seriousness of Computer Crimes

- Continually on the rise
- Costs organizations around the world billions of dollars each year
- We do not have representative statistics
  - Crimes go unnoticed or unreported
- Affects the public and government sectors

Examples of Computer Crimes

- ILOVEYOU, SoBIG.f, Morris worm, Blaster, Klez malware
- DDoS that brought down Excite, Yahoo!, and other large sites
- Extortion attempts after stealing credit card numbers
- Stealing of credit card information
- Stealing funds from financial accounts
- Internal employee fraud
- Stealing military secrets and critical information
- Competitors stealing each other’s customer information

Just a Few…

Who Perpetrates These Crimes?

Criminal Profiles

- Script kiddies
  - Do not understand the technology and ramifications of such activities
  - “Ankle biters” – curious individuals who test their skills
  - “Machine gunners” – persons who dispatch thousands of probes at once
- Dedicated cracker
  - Chooses victim and carries out intelligence gathering before conducting attack
  - More dangerous than script kiddies and usually much more talented
  - Has a specific goal in mind

A Few Attack Types

Salami

- Carrying out smaller crimes with the hope that the larger crime will go unnoticed
  - Taking a small amount of money from each account each month

Data Diddling

- Modifying data before it is entered into a computer or as soon as it comes out
  - Trying to alter the reality of a situation
  - “Changing the books”

Dumpster Diving

- Obtaining information in the trash that can be used against the victim
  - Unethical, but not illegal

Telephone Fraud

Phreakers

Telephone fraud

2600 Club

Captain Crunch

Red Boxing

- Simulating coins dropping into a pay phone
- Still can be carried out because some pay phones still uses in-band signalling
  - Rest of telecommunication network uses out-of-band signalling

Blue Boxing

- Using analog tones to gain free long distance service

Black Boxing

- Manipulating line voltage

PBX fraud

Identification Protection & Prosecution

Hacking, cracking, and attacking have only increased over the years and will not stop anytime soon. There are several issues that deal with why these activities have not been properly stopped or even curbed. These include proper identification of the attackers, the necessary level of protection for networks, and successful prosecution once an attacker is captured.

Privacy of Sensitive Data

United States and European Legal Approaches

Moving Sensitive Data Across International Boundaries

Employee Privacy Topics

Privacy Issues – U.S. Laws as Examples

Privacy Act of 1974

- Data held on individuals by government agencies

Electronic Communications Privacy Act of 1986

- Prohibits unauthorized eavesdropping or interception of messages without proper court approval
  - Protects data while stored or in transit

Health Insurance Portability and Accountability Act (HIPAA)

- Protecting the privacy medical information

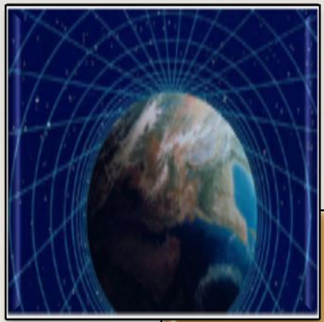
Gramm Leach Bliley Act of 1999

- Protects an individual's non-public information

European Union Principles on Privacy

1. The reason for gathering of data must be specified at the time of collection.
2. Data cannot be used for other purposes.
3. Unnecessary data should not be collected.
4. Data should only be kept for as long as it is needed to accomplish the stated task.
5. Only the necessary individuals who are required to accomplish the stated task should be allowed access to the data.
6. Whoever is responsible for securely storing the data should not allow unintentional “leaking” of data.

Routing Data Through Different Countries



Transborder Information Flow

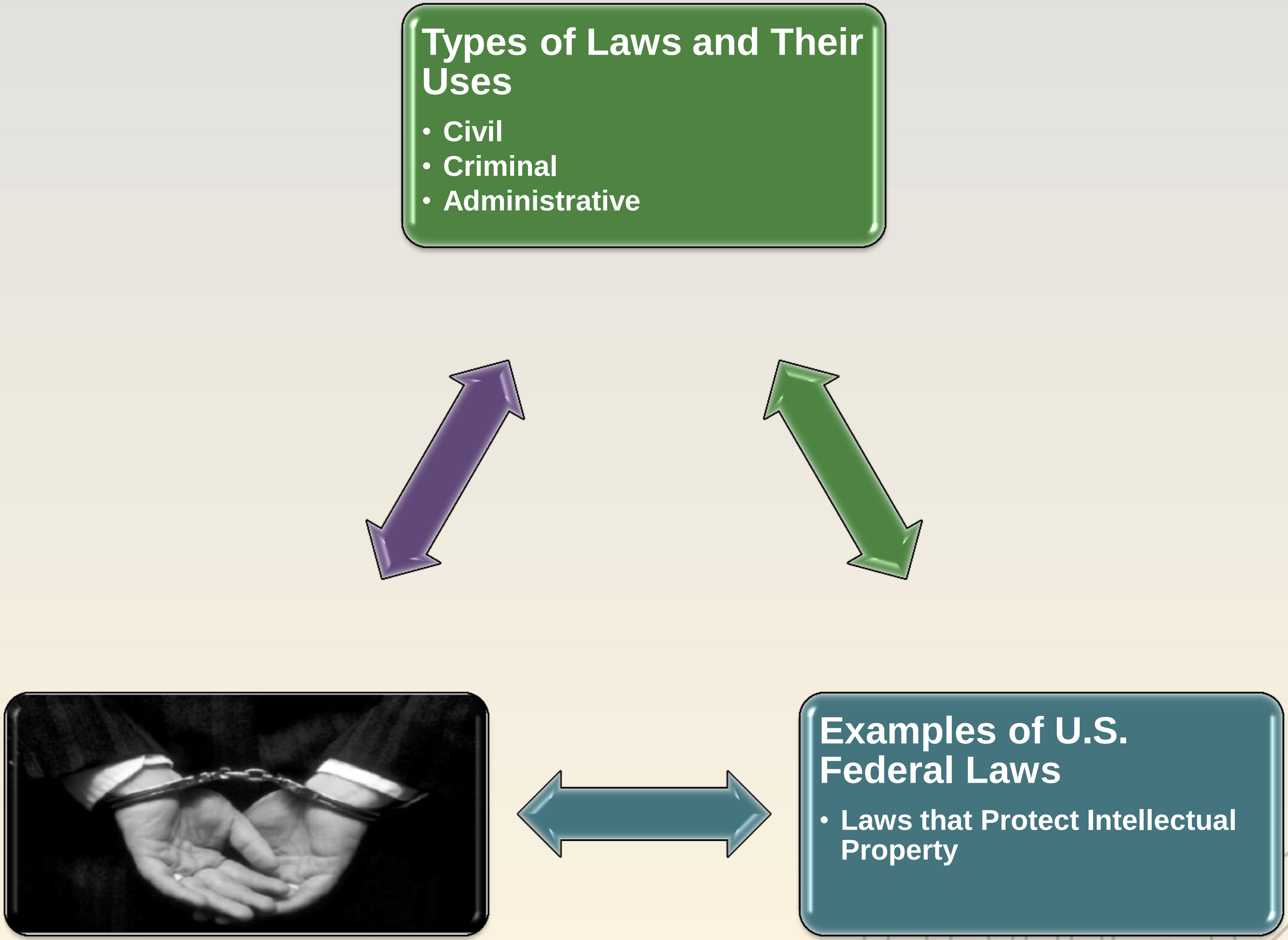
- Movement and storage of data by automatic means across international boundaries
- Different regions have different laws pertaining to the type of data that can be transmitted
- Many European countries have strong restrictions on flow of personal and financial data
  - Bank statements, personal records, mailing lists
- Companies should research the laws before transmitting data through different countries
  - Route data through other countries, if necessary

Employee Privacy Issues

Employee Monitoring

- Must be in security policy and employees must be aware that monitoring may take place
  - Employee handbooks, banners, security awareness training
- Ensure monitoring is lawful
  - Research and uphold state and federal laws
  - Do not target specific individuals
  - Only monitor work related activities
  - Acceptable use and ramifications of not meeting expectations should be told to employees
- Possible types of monitoring
  - Keystroke logging
  - Cameras
  - Telephone
  - E-mail

U.S. LAW



Types of Laws and Their Uses

- Civil
- Criminal
- Administrative

Examples of U.S. Federal Laws

- Laws that Protect Intellectual Property

Common Laws – Civil

Civil Law

- Tort law = Wrongs against individuals or companies that result in damage or loss
- Contract law and property issues
- Case law is built on precedents
- Determines if someone is liable for a specific activity
  - Usually from negligence
- Less of a burden of proof compared to criminal law
  - Punishments are less severe
  - Punishment is usually financial, handled through community service work, or designated to stop some type of activity – no jail time is involved

Common Laws – Criminal

Criminal Law

- Laws that were created by the government to protect the public
- In a crime, the public is seen as the victim
- Someone can win a criminal case and lose a civil case on the same issue
- More stringent burden of proof compared to civil law
  - Punishments can include time in jail or the death penalty

Common Laws – Administrative

Administrative Law

- Different industries have specific laws and regulations they must abide by
  - Food and drug
  - Financial
  - Healthcare
  - Educational
- Performance and conduct of organizations, officials, and officers
  - Expectations of government agencies for these different entities
- Administrative law deals with industry regulations
- Punishments can be financial or merit imprisonment

U.S. Federal Laws

Dealing with Computer Crimes at the Federal Level

- Electronic Communications Act of 1996
  - Wiretap Act
  - Stored Communication Act
- Computer Fraud and Abuse Act of 1986
  - Most commonly used law in prosecuting computer crimes
  - “Anti-Hacking law”
- Electronic Espionage Act of 1996
  - Prosecutions for industrial espionage
  - This act dictates that taking, downloading, or possessing trade secrets can merit up to $10 million in fines and up to 15 years in prison

Intellectual Property Laws

Trade Secret

Maintains confidentiality of proprietary business-related data

- Must be adequately protected by the owner

Owner invested resources to develop this data

The data must provide competitive value, be proprietary to a company, and important for its survival

Copyright

Protects "original works of authorship"

Protects expression of ideas rather than the ideas themselves

Author to control how work is distributed, reproduced, and modified

Source code, object code, and microcode are copyrightable

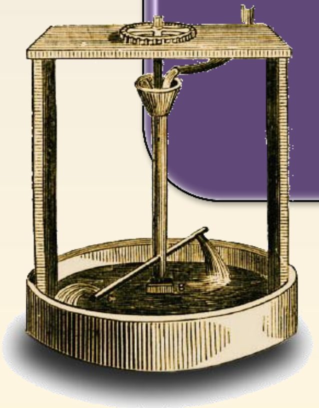
More Intellectual Property Laws

Trademark

- Protects word, name, symbol, sound, shape, color or combination thereof which is used to identify a product or company and distinguish it from others
- Protects a company's "look and feel"

Patent

- Allows owner to exclude others from practicing invention for a specific time period
- Invention must be novel and non-obvious



Software Licensing

Controlling Who Can Use a Product

- Many types of software licensing practices
  - Single user
  - Multi-user
    - Site license
    - Per server license
    - Per personal computer license
    - Number of user licenses
    - Number of concurrent user licenses
    - Floating licenses

Software Piracy

- Copying and using the creator’s work without compensation
- Software Protection Association (SPA)
  - Many software vendors working together
- Business Software Alliance (BSA)
  - International group based in Washington, D.C.
- Federation Against Software Theft (FAST)
  - International group based in London

Digital Millennium Copyright Act

DMCA Characteristics

- It is now illegal to tamper with or break into controls that protect copyrighted material
- Only protects items that fall under the copyright law
- Main goal is to prevent reverse-engineering attacks
- Controversial today because some carry out reverse-engineering tasks as a white hat and could be prosecuted
- First attempt to use this law was against a presenter at DefCon
  - Adobe eventually dropped the charge

Investigating

Complications of Investigating and Prosecuting

Computer Crimes

Investigation Steps and Forensics

Types of Evidence

Evidence Handling

Computer Crime and Its Barriers

Difficult to Investigate and Prosecute

- Law enforcement agencies' jurisdiction issues
  - Crime took place in Texas, but criminal carried it out from China
- Law enforcement agencies are behind in manpower and skill
  - Local law enforcement, FBI, and Secret Service
- Current laws may not directly apply to new computer crimes
  - Trying to fit a round peg in a square hole
- Lack of reporting of crimes by organizations
- Evidence is intangible and hard to collect
  - Traditional crimes have more tangible evidence – blood, gun, fingerprints
- Explaining complex technical concepts to judge and jury
- Identifying lawyers that specialize in this type of law

Countries Working Together

Transborder Issues

- Many countries do not view computer crimes the same way, thus they are treated differently
  - This is due to different legal systems, rules of evidence, and jurisdiction
- Governments may not work with each other to prosecute suspects in international cases
- Each country treats computer crimes differently
- Evidence rules differ between legal systems
- Jurisdiction issues
- Governments may not assist each other in international cases
- G8
  - The G8 group represents the world's leading industrialized countries
  - They have agreed to cooperate to fight cybercrime
- International police organization (Interpol) collects and distributes information about cross-border crimes

Security Principles for International Use

Generally Accepted System Security Principles (GASSP)

- NIST document that provides guidelines for organizations around the world to use as best practices
  - Trying to get everyone on the "same page" pertaining to security
- Based on Organization for Economic Cooperation and Development (OECD)
  - Supports the mission of the organization
  - Integral element of sound management and judgment
  - Cost-effective
  - Responsibilities and accountability is explicit
  - Comprehensive and integrated
  - Periodically reassessed
  - Constrained by societal factors
    - Privacy issues is one example

Determine if a Crime Has Indeed Been Committed

Violation Analysis

- When something suspicious takes place, make sure that it is not a user error or a mis-configuration
- One or more individuals should be responsible for investigating and making sure an actual crime has taken place
- Once this is confirmed, investigate the crime and gather evidence
- Management must decide how to handle a computer crime
  - Conduct internal investigation
  - Bring in law enforcement

Bringing in Law Enforcement

Management Needs to Make this Decision Because…

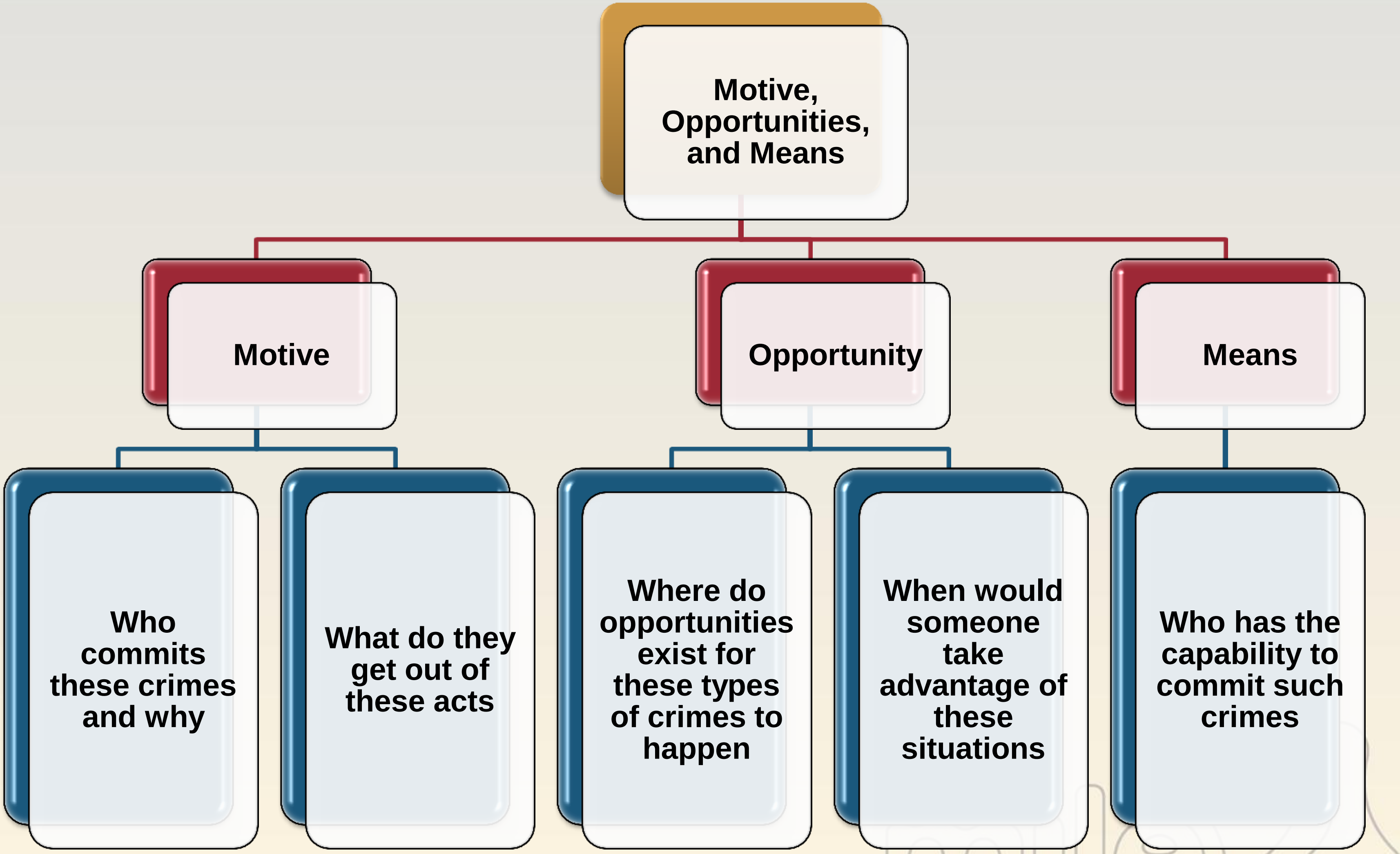
- Company loses control over investigation once law enforcement is involved
- Secrecy of compromise is not promised
    - Could become part of public record
- Effects on reputation need to be considered
    - Ramifications of this information reaching customers, share holders, etc.
- Evidence will be collected and may not be available for a long period of time
    - May take a year or so to get into court

Citizen versus Law Enforcement Investigation

- Search and seizure – must have a probable cause
  - Fourth Amendment right
  - Search warrant is required
- Citizen investigation
  - Private citizen is not subject to protecting the Fourth Amendment rights of others unless acting as a police agent
  - Acting as a police agent when carrying out activities on behalf of a law enforcement agent

Law Enforcement

Investigation of Any Crime



Motive, Opportunities, and Means

Motive

Opportunity

Means

Who commits these crimes and why

What do they get out of these acts

Where do opportunities exist for these types of crimes to happen

When would someone take advantage of these situations

Who has the capability to commit such crimes

Role of Evidence in a Trial

Evidence

Material offered to the court and jury to prove the truth or falsity of a fact

Used to prove directly or indirectly that an individual may be responsible for committing a crime or innocent

Challenge pertaining to computer crimes is that the evidence is intangible

- Electrical voltages that are held in a binary representation
- Hard to properly collect and maintain
- It is hard to prove that this intangible evidence has not been modified in an unauthorized manner

Evidence Requirements

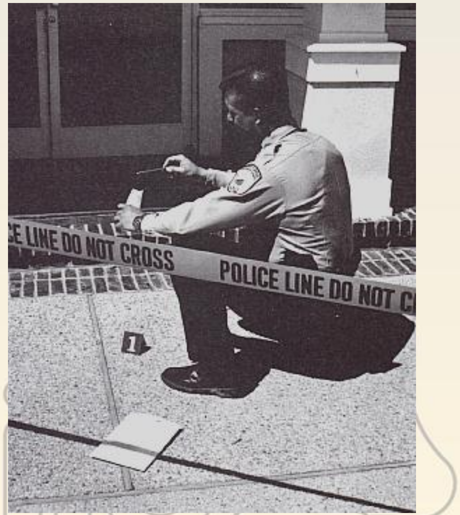
Evidence Must Be…

- **Material -** Must be relevant to the case
- **Competent**
  - Proper process of collecting evidence was used
  - It was obtained legally
  - Chain of custody was properly followed
- **Relevant**
  - Provide information pertaining to the suspect’s motives
  - Evidence should prove or disprove a fact in the case

Chain of Custody

Chain of Custody of Evidence

- Who obtained the evidence and how?
- Where and when was it obtained?
- Who secured it?
- Who had control or possession of the evidence?
- How was it moved from one place to another?
- Segregation of duties is a good control to ensure a proper chain of custody

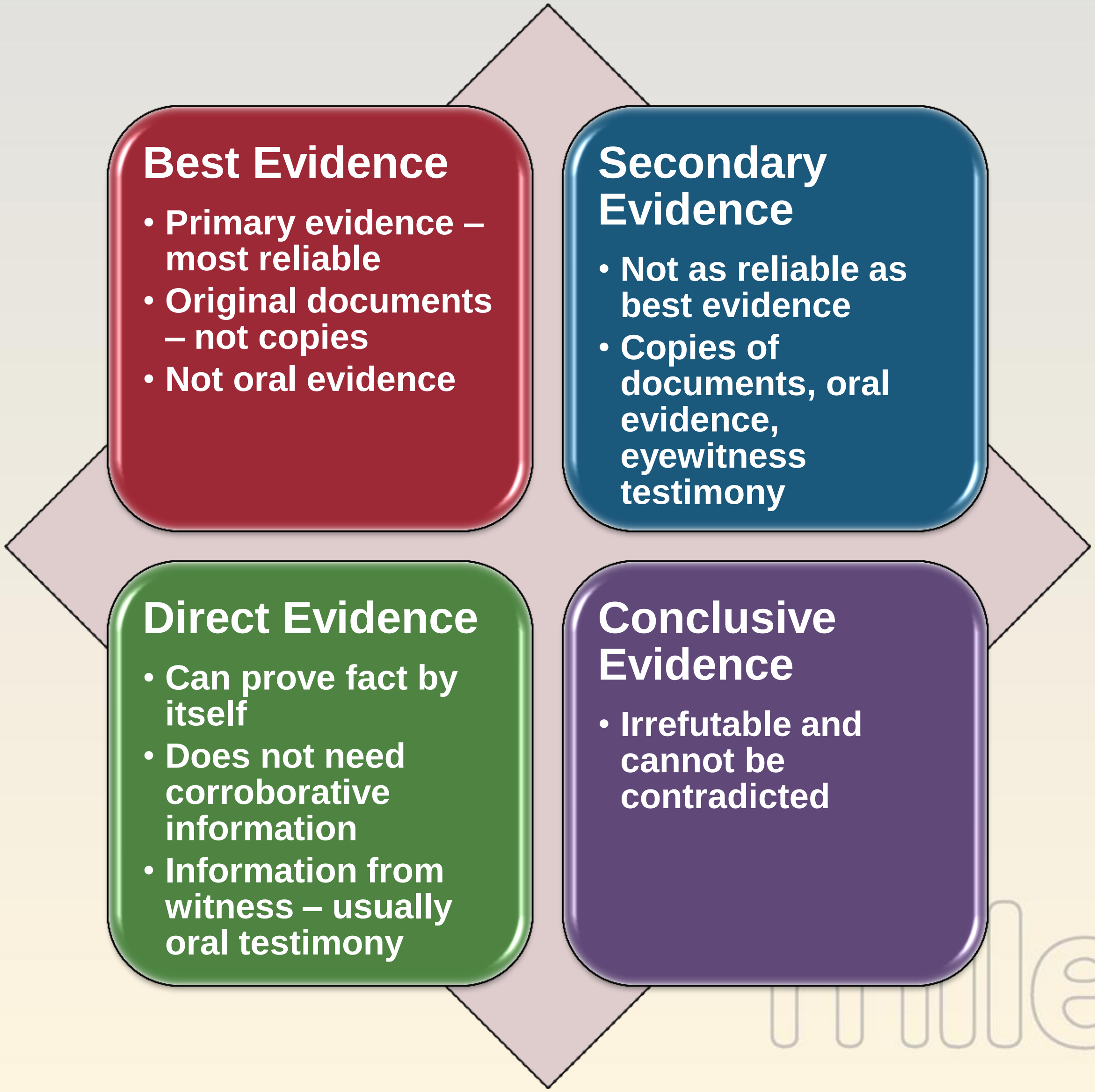


How Is Evidence Processed?

Evidence Life Cycle

- Discovery
- Protection
- Recording
- Collection and identification
- Analysis
- Storage, preservation, transportation
- Present in court
- Return to owner

Evidence Types



Best Evidence

- Primary evidence – most reliable
- Original documents – not copies
- Not oral evidence

Secondary Evidence

- Not as reliable as best evidence
- Copies of documents, oral evidence, eyewitness testimony

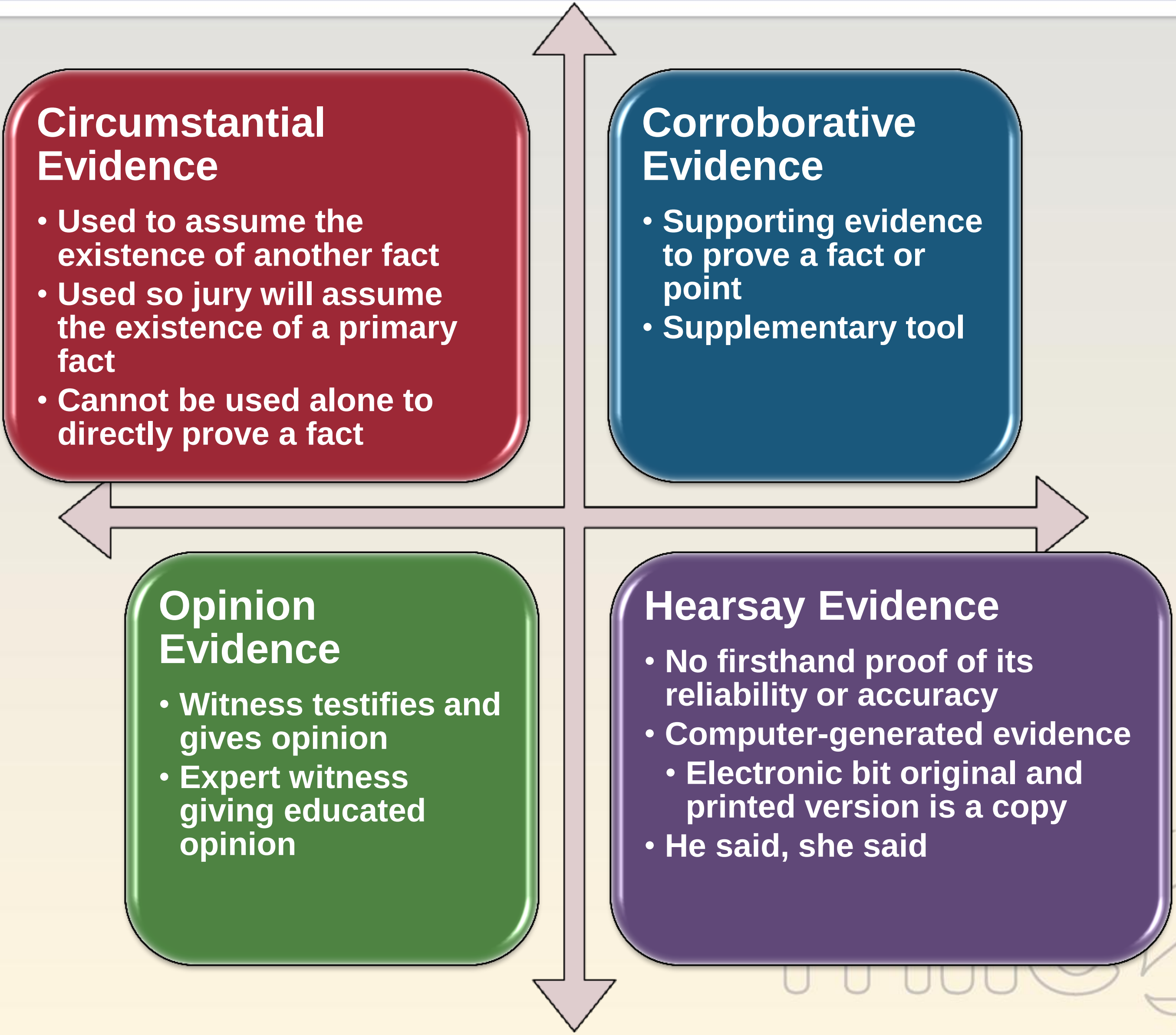
Direct Evidence

- Can prove fact by itself
- Does not need corroborative information
- Information from witness – usually oral testimony

Conclusive Evidence

- Irrefutable and cannot be contradicted

Evidence Types



Circumstantial Evidence

- Used to assume the existence of another fact
- Used so jury will assume the existence of a primary fact
- Cannot be used alone to directly prove a fact

Corroborative Evidence

- Supporting evidence to prove a fact or point
- Supplementary tool

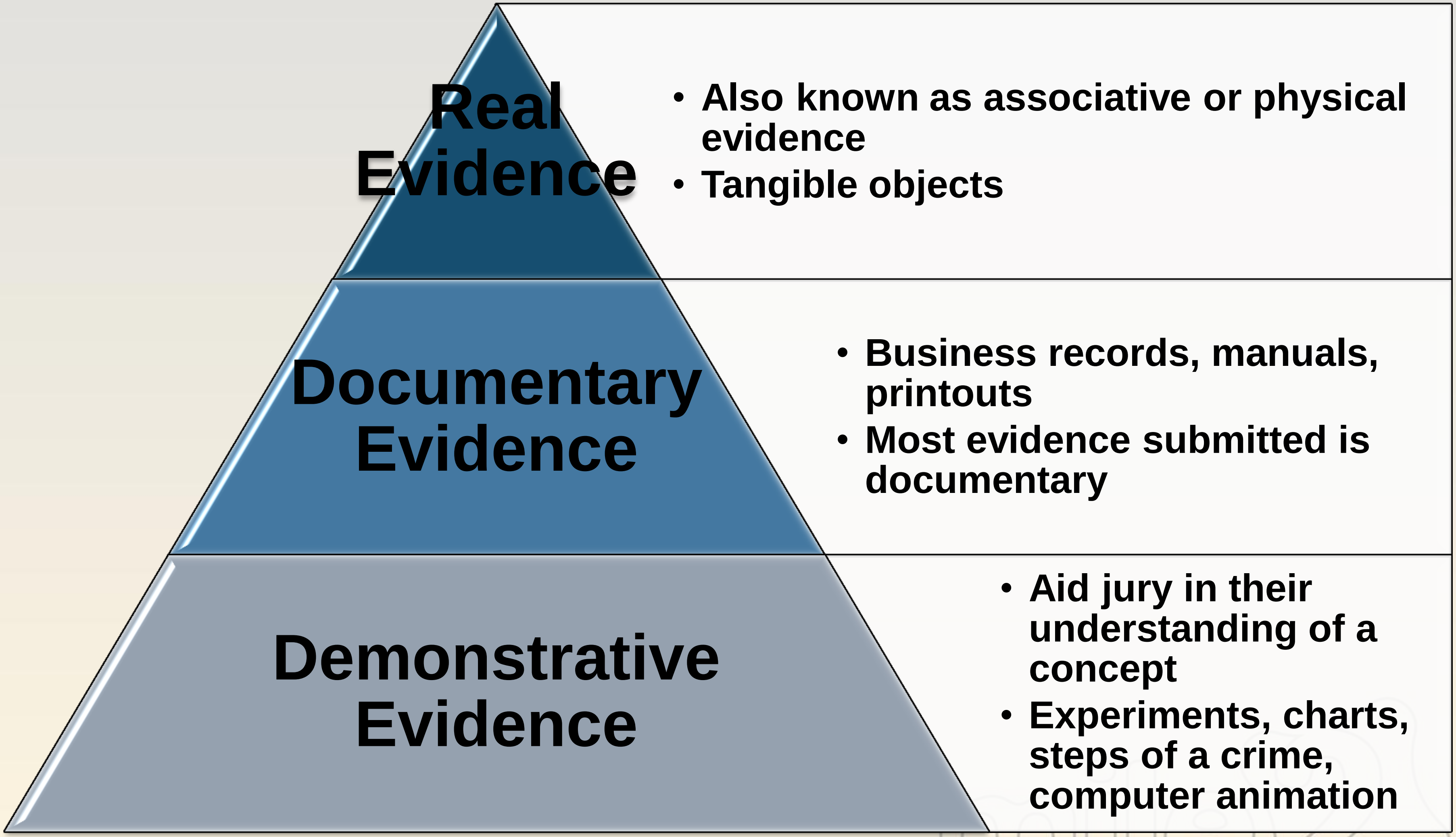
Opinion Evidence

- Witness testifies and gives opinion
- Expert witness giving educated opinion

Hearsay Evidence

- No firsthand proof of its reliability or accuracy
- Computer-generated evidence
  - Electronic bit original and printed version is a copy
- He said, she said

Evidence Types



Real Evidence

- Also known as associative or physical evidence
- Tangible objects

Documentary Evidence

- Business records, manuals, printouts
- Most evidence submitted is documentary

Demonstrative Evidence

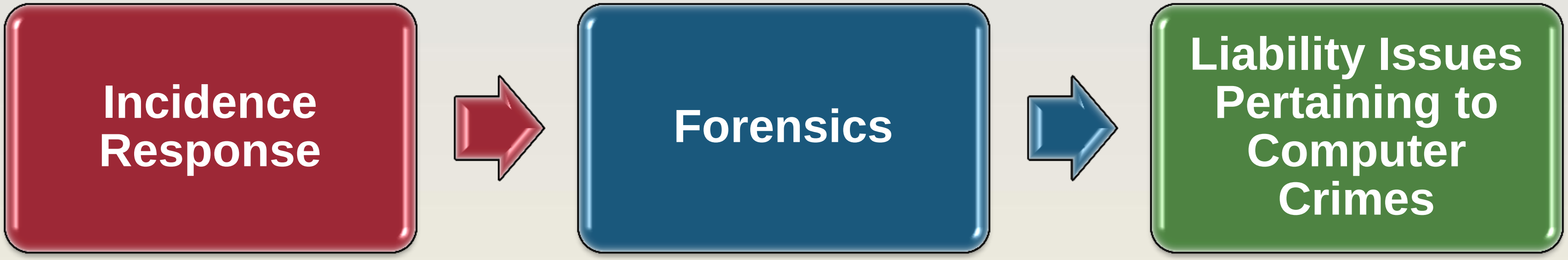
- Aid jury in their understanding of a concept
- Experiments, charts, steps of a crime, computer animation

Hearsay Rule Exception

Business Record Exemption to Hearsay Rule

- Business documentation can be admissible if it is created during regular business activity
  - This does not include documentation that is created for a specific court case
  - Regular business records have more weight as evidence

Responding to an Incident



Incidence Response

Forensics

Liability Issues Pertaining to Computer Crimes

Preparing for a Crime Before It Happens

Developing an Incident Response Team

- Policies and procedures need to be developed for incidence response
- Decide whether an internal response team will be developed
  - Does the company have the resources with the necessary skill level?
  - Will the company use outside resources?
  - Understand liability issues of each approach
- If the company will use an internal team…
  - Team should be composed of representatives from specific company department, such as:
    - IT
    - Management
    - Human resources
    - Legal
    - PR
  - Human resources must get involved if suspect is an employee

Incident Handling

First Goals of Incident Handling:

- Containing and repairing damage from an incident
- Preventing further damage
- After the team is ensured that the spread of damage is contained, evidence gathering can start

Evidence Collection Topics

Collecting Evidence

- Photograph area, record what is on the screen
  - Important to show what environment was like before anyone touches anything
- Dump contents from memory
  - Could still contain commands and activities from the intruder
- Power down system
  - This means to “pull the plug” instead of allowing for a graceful shutdown
- Photograph inside of system
- Label each piece of evidence
  - Every item of evidence must be labeled
  - Usually placed in bag with label over opening
  - Label indicates who collected it, the date, and the
  - case number

Computer Forensics

Specialized Skill

- Study of computer technology and how it relates to law
- First step is to image disk
  - Bit-level copy, sector by sector, to capture deleted files, slack spaces, and unallocated clusters
  - Specialized tools or the dd Unix utility
  - All work is done on image of disk, not on the original
- Create message digest for files and directories
  - Ensure their integrity
- A few of the things that are analyzed
  - Hidden files
  - Streams
  - Slack space
  - Malware
  - Deleted files
  - Extract data from the swap file in
    - Windows systems

Trying to Trap the Bad Guy

Enticement

- Legal attempt to lure a criminal into carrying out a crime
  - Providing a honeypot on your company’s DMZ
  - Pseudo flaw = code purposely added to software to trap an intruder
    - Padded cell = virtual machine used to confine intruders without them knowing it

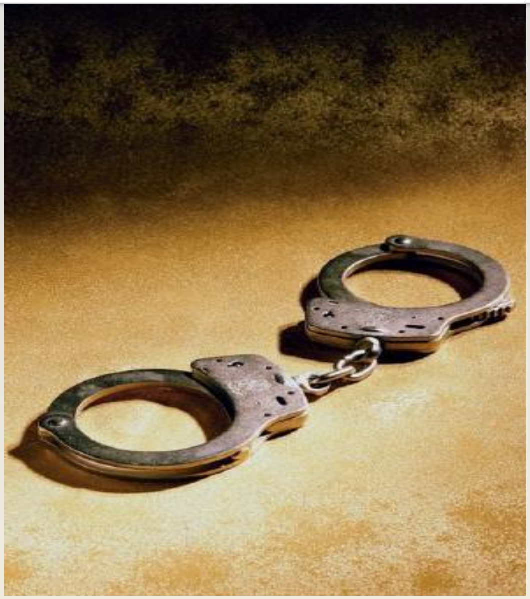
Entrapment

- Illegal attempt to trick a person into committing a crime
  - Pointing a user to a site and then charging him with trespassing

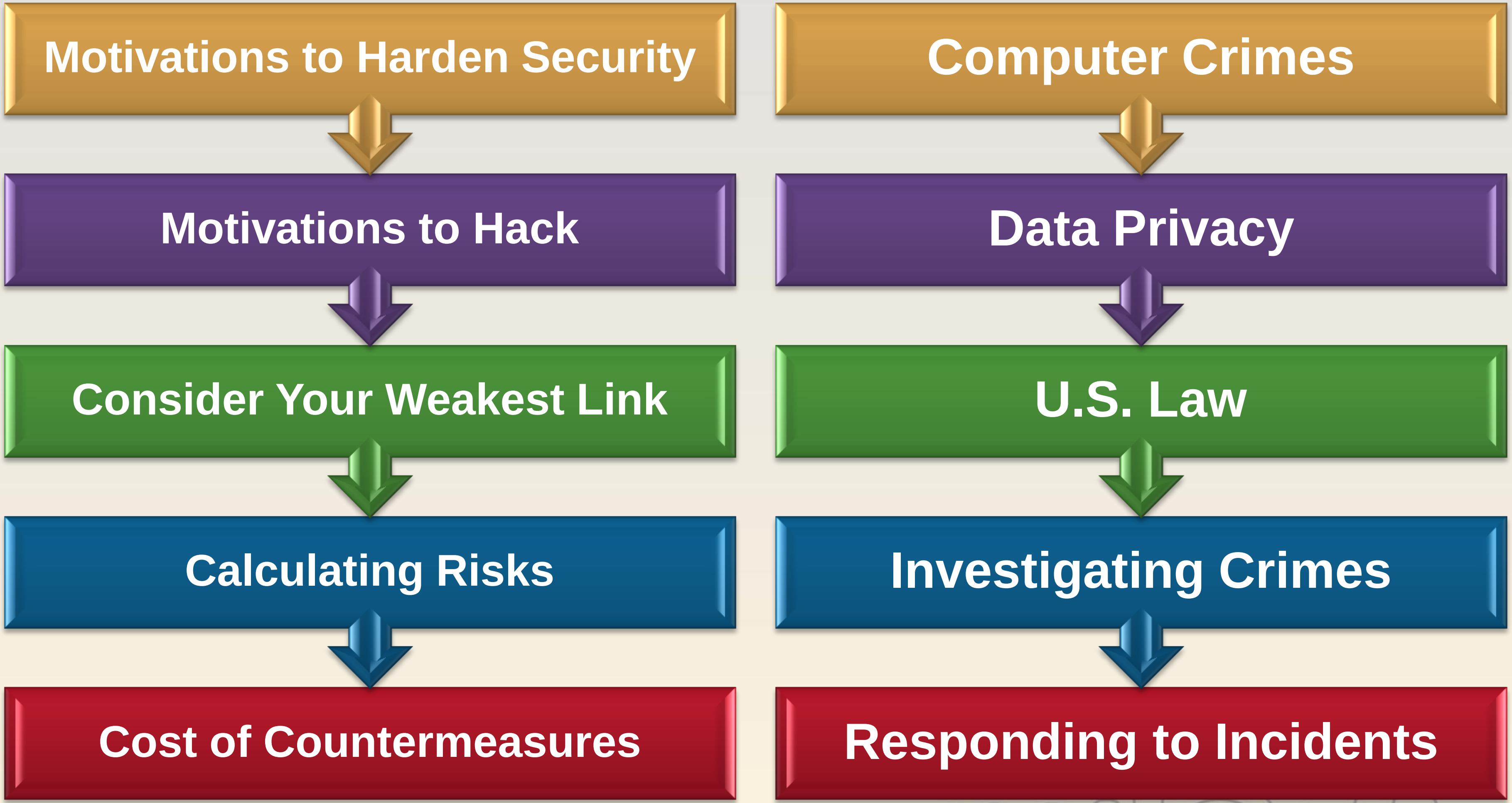
Companies Can Be Found Liable

Company May Be Found Negligent if It Doesn't…

- Practice due care
- Practice due diligence
- Follow the prudent person rule
  - Perform duties that a responsible person would exercise in similar circumstances
- Practice due care for downstream liabilities
  - Actions, or lack of actions, that negatively affect another company or partner



Overview



Motivations to Harden Security

Motivations to Hack

Consider Your Weakest Link

Calculating Risks

Cost of Countermeasures

Computer Crimes

Data Privacy

U.S. Law

Investigating Crimes

Responding to Incidents