SECURITY INVESTIGATION

2.1 NEED FOR SECURITY

- The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents. The Audit Commission Update report (1998) shows that fraud or cases of IT abuse often occur due to the absence of basic controls, with one half of all detected frauds found by accident.
- Information Security Management System (ISMS) enables information to be shared, whilst ensuring the protection of information and computing assets.

At the most practical level, securing the information on your computer means:

- Ensuring that your information remains confidential and only those who should access that information, can.
- Knowing that no one has been able to change your information, so you can depend on its accuracy (information integrity).
- Making sure that your information is available when you need it (by making back-up copies and, if appropriate, storing the back-up copies off-site).

2.2 BUSINESS NEEDS FIRST

Information security performs four important functions for an organization:

1. Protects the organization's ability to function
2. Enables the safe operation of applications implemented on the organization's IT systems.
3. Protects the data the organization collects and uses.
4. Safeguards the technology assets in use at the organization.

Protecting the functionality of an organization

- Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

Enabling the safe operation of applications

- Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications

- The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

Protecting data that organizations collect & use

- Protecting data in motion
- Protecting data at rest
- Both are critical aspects of information security.
- The value of data motivates attackers to seal, sabotage, or corrupt it.
- It is essential for the protection of integrity and value of the organization's data

Safeguarding Technology assets in organizations

- Must add secure infrastructure services based on the size and scope of the enterprise.
- Organizational growth could lead to the need for public key infrastructure, PKI, an integrated system of software, encryption methodologies.

2.3 THREATS

To protect an organization's information, you must

1. Know yourself: (i.e) be familiar with the information to be protected, and the systems that store, transport and process it.
2. Know the threats you face- To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

   A threat is an object, person, or other entity, that represents a constant danger to an asset.

2.3.1 Threats

1. Acts of Human Error or Failure:

- Acts performed without intent or malicious purpose by an authorized user.
- because of in experience ,improper training,
- Making of incorrect assumptions.

One of the greatest threats to an organization's information security is the organization's own employees.

- Entry of erroneous data
- Accidental deletion or modification of data
- Storage of data in unprotected areas.
- Failure to protect information can be prevented with
  - Training
  - Ongoing awareness activities
  - Verification by a second party
  - Many military applications have robust, dual- approval controls built-in.

2. Compromises to Intellectual Property

- Intellectual Property is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.
- Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.
- Organization purchases or leases the IP of other organizations.
- Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as software Piracy.
- Software Piracy affects the world economy.
- U.S provides approximately 80% of world's software.

In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

1. Software and Information Industry Association (SIIA) (i.e)Software Publishers Association
2. Business Software Alliance (BSA)

   Another effort to combat (take action against) piracy is the online registration process.

3. Deliberate Acts of Espionage or Trespass

- Electronic and human activities that can breach the confidentiality of information.

- When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
- Attackers can use many different methods to access the information stored in an information system.
    - Competitive Intelligence [use web browser to get information from market research]
    - Industrial espionage (spying)
    - Shoulder Surfing (ATM)

Trespass

- Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
- Sound principles of authentication & authorization can help organizations protect valuable information and systems.
- **Hackers->** "People who use and create computer software to gain access to information illegally"
- There are generally two skill levels among hackers.
- **Expert Hackers->** Masters of several programming languages, networking protocols, and operating systems.
- **Unskilled Hackers**

4. Deliberate Acts of information Extortion (obtain by force or threat)

- Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

5. Deliberate Acts of sabotage or Vandalism

- Destroy an asset or
- Damage the image of organization
- Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

6. Deliberate Acts of Theft

- Illegal taking of another's property-- is a constant problem.
- Within an organization, property can be physical, electronic, or intellectual.

- Physical theft can be controlled by installation of alarm systems.
- Trained security professionals.
- Electronic theft control is under research.

7. Deliberate Software Attacks

- Because of malicious code or malicious software or sometimes malware.
- These software components are designed to damage, destroy or deny service to the target system.
- More common instances are

  Virus, Worms, Trojan horses, Logic bombs, Backdoors.
- "The British Internet Service Provider Cloudnine" be the first business "hacked out of existence"

7.1 Virus

- Segments of code that performs malicious actions.
- Virus transmission is at the opening of Email attachment files.
- Macro virus-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.
- Boot Virus-> infects the key operating files located in the computer's boot sector.

7.2 Worms

- A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.
- Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- Eg: MS-Blaster, MyDoom, Netsky, are multifaceted attack worms.
- Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system.
- Furthermore, a worm can deposit copies of itself onto all Web servers that the infected systems can reach, so that users who subsequently visit those sites become infected.

7.3 Trojan Horses

- Are software programs that hide their true nature and reveal their designed behaviour only when activated?

7.4 Back Door or Trap Door

- A Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.
- Eg: Back Orifice

Polymorphism

- A Polymorphic threat is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures.
- These viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs.

7.5 Virus & Worm Hoaxes

Types of Trojans

- Data Sending Trojans
- Proxy Trojans
- FTP Trojans
- Security software disabler Trojans
- Denial of service attack Trojans (DOS)

Virus

- A program or piece of code that be loaded on to your computer, without your knowledge and run against your wishes.

Worm

- A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Trojan horse

- A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

Blended threat

- Blended threats combine the characteristics of virus, worm, Trojan horses & malicious code with server and Internet Vulnerabilities.

Antivirus Program

- A Utility that searches a hard disk for viruses and removes any that found.

7.8 Forces of Nature

- **Fire:** Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.
- **Flood:** Can sometimes be mitigated with flood insurance and/or business interruption Insurance.
- **Earthquake:** Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.
- **Lightning**: An Abrupt, discontinuous natural electric discharge in the atmosphere.
- **Landslide/Mudslide:** The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.
- **Tornado/Severe Windstorm**
- **Huricane/typhoon**
- **Tsunami**
- **Electrostatic Discharge (ESD)**
- **Dust Contamination**

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

- They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

7.9 Deviations in Quality of Service

- A product or service is not delivered to the organization as expected.
- The Organization's information system depends on the successful operation of many interdependent support systems.

- It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.
- This degradation of service is a form of availability disruption.

Internet Service Issues

- Internet service Provider (ISP) failures can considerably undermine the availability of information.
- The web hosting services are usually arranged with an agreement providing minimum service levels known as a Service level Agreement (SLA).
- When a Service Provider fails to meet SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications & Other Service Provider Issues

- Other utility services can affect the organizations are telephone, water, waste water, trash pickup, cable television, natural or propane gas, and custodial services.
- The loss of these services can impair the ability of an organization to function.
- For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
- This would stop normal business operations.

Power Irregularities

- Fluctuations due to power excesses.
- Power shortages &
- Power losses

This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

- When voltage levels spike (experience a momentary increase),or surge (experience prolonged increase), the extra voltage can severely damage or destroy equipment.
- The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

7.10 Technical Hardware Failures or Errors

- Resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in unrecoverable loss of equipment.

- Some errors are intermittent, in that they resulting in faults that are not easily repeated.

7.11 Technical software failures or errors

- This category involves threats that come from purchasing software with unknown, hidden faults.
- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
- These failures range from bugs to untested failure conditions.

7.12 Technological obsolescence

- Outdated infrastructure can lead to unreliable and untrustworthy systems.
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

2.4 ATTACK

- An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.
- It is accomplished by a threat agent that damages or steals an organization's information or physical asset.
- Vulnerability is an identified weakness in a controlled system, where controls are not present or are no longer effective.
- Attacks exist when a specific act or action comes into play and may cause a potential loss.

2.4.1 Malicious code

- The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- The state –of-the-art malicious code attack is the polymorphic or multivector, worm.
- These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

2.4.2 Attack Replication Vectors

1. IP scan & attack
2. Web browsing
3. Virus

4. Unprotected shares
5. Mass mail
6. Simple Network Management Protocol (SNMP)

IP scan & attack

- The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

Web browsing

- If the infected system has write access to any Web pages, it makes all Web content files (.html,.asp,.cgi & others) infectious, so that users who browse to those pages become infected.

Virus

- Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

Unprotected shares

- Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

Mass Mail

- By sending E-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program & infect other systems.

Simple Network Management Protocol (SNMP)

- By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

2.4.3 Examples

Hoaxes

- A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.

- Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.

Backdoors

- Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.
- Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.
- A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

Password Crack

- Attempting to reverse calculate a password is often called cracking.
- A password can be hashed using the same algorithm and compared to the hashed results, if they are same, the password has been cracked.
- The (SAM) Security Account Manager file contains the hashed representation of the user's password.

Brute Force

- The application of computing & network resources to try every possible combination of options of a password is called a Brute force attack.
- This is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a password attack.

Spoofing

- It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

Dictionary

- This is another form of the brute force attack noted above for guessing passwords.
- The dictionary attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.

Denial –of- Services(DOS) & Distributed Denial –of- Service(DDOS)

- The attacker sends a large number of connection or information requests to a target.
- This may result in the system crashing, or simply becoming unable to perform ordinary functions.
- DDOS is an attack in which a coordinated stream of requests is launched dagainst a target from many locations at the same.

Man-in-the –Middle

- Otherwise called as TCP hijacking attack.
- An attacker monitors packets from the network, modifies them, and inserts them back into the network.
- This type of attack uses IP spoofing.
- It allows the attacker to change, delete, reroute, add, forge or divert data.
- TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

SPAM

- Spam is unsolicited commercial E-mail.
- It has been used to make malicious code attacks more effective.
- Spam is considered as a trivial nuisance rather than an attack.
- It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

Mail Bombing

- Another form of E-mail attack that is also a DOS called a mail bomb.
- Attacker routes large quantities of e-mail to the target.
- The target of the attack receives unmanageably large volumes of unsolicited e-mail.
- By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
- The target e-mail address is buried under thousands or even millions of unwanted e-mails.

Sniffers

- A sniffer is a program or device that can monitor data traveling over a network.
- Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
- Sniffer often works on TCP/IP networks, where they are sometimes called "packet sniffers"

Social Engineering

- It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

Buffer Overflow

- A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.
- Attacker can make the target system execute instructions.

Timing Attack

- Works by exploring the contents of a web browser's cache.
- These attacks allow a Web designer to create a malicious form of cookie that is stored on the client's system.
- The cookie could allow the designer to collect information on how to access password-protected sites.

2.5 LEGAL, ETHICAL, AND PROFESSIONAL ISSUES

- The information security professional plays an important role in an organization's approach to managing liability for privacy and security risks. In the modern litigious societies of the world, sometimes laws are enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations. Sometimes these damages are punitive—assessed as a deterrent.
- To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information security practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new and emerging issues.

2.5.1 Law and Ethics in Information Security

- Laws are rules that mandate or prohibit certain behaviour in society; they are drawn from ethics, which define socially acceptable behaviours. The key difference between laws and ethics is that

laws carry the sanctions of a governing authority and ethics do not. Ethics in turn are based on Cultural mores.

Types of Law

- **Civil law** -comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people.
- **Criminal law** -addresses activities and conduct harmful to society, and is actively enforced by the state. Law can also be categorized as private or public.
- **Private law** -encompasses family law, commercial law, and labour law, and regulates the relationship between individuals and organizations.
- **Public law** -regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

2.5.2 Relevant U.S. Laws – General

There are several key laws relevant to the field of information security and of particular interest to those who live or work in the United States.

- Computer Fraud and Abuse Act of 1986
- National Information Infrastructure Protection Act of 1996
- USA Patriot Act of 2001
- Telecommunications Deregulation and Competition Act of 1996
- Communications Decency Act (CDA)
- Computer Security Act of 1987

Privacy

- The issue of privacy has become one of the hottest topics in information
- The ability to collect information on an individual, combine facts from separate sources, and merge it with other information has resulted in databases of information that were previously impossible to set up
- The aggregation of data from multiple sources permits unethical organizations to build databases of facts with frightening capabilities

Privacy of Customer Information

- Privacy of Customer Information Section of Common Carrier Regulations
- Federal Privacy Act of 1974
- The Electronic Communications Privacy Act of 1986 - is a collection of statutes that regulates the interception of wire, electronic, and oral communications.
- The Health Insurance Portability & Accountability Act Of 1996 (HIPAA) also known as the Kennedy-Kassebaum Act - protects the confidentiality and security of health care data by establishing and enforcing standards and by standardizing electronic data interchange.
- The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999

Area	Act	Date	Description
Telecommunications	Telecommunications Deregulation and Competition Act of 1996—Update to Communications Act of 1934 (47 USC 151 et seq.)	1934	Regulates interstate and foreign telecommunications (amended 1996 and 2001)
Freedom of information	Freedom of Information Act (FOIA)	1966	Allows for the disclosure of previously unreleased information and documents controlled by the U.S. government
Privacy	Federal Privacy Act of 1974	1974	Governs federal agency use of personal information
Copyright	Copyright Act of 1976—Update to U.S. Copyright Law (17 USC)	1976	Protects intellectual property, including publications and software
Cryptography	Electronic Communications Privacy Act of 1986 (Update to 18 USC)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act
Access to stored communications	Unlawful Access to Stored Communications (18 USC 2701)	1986	Provides penalties for illegally accessing stored communications (such as e-mail and voicemail) stored by a service provider
Threats to computers	Computer Fraud and Abuse Act (also known as Fraud and Related Activity in Connection with Computers) (18 USC 1030)	1986	Defines and formalizes laws to counter threats from computer-related acts and offenses (amended 1996, 2001, and 2006)
Federal agency information security	Computer Security Act of 1987	1987	Requires all federal computer systems that contain classified information to have security plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems
Personal health information protection	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	1996	Requires medical practices to ensure the privacy of personal medical information
Encryption and digital signatures	Security and Freedom through Encryption Act of 1997	1997	Affirms the rights of persons in the United States to use and sell products that include encryption and to relax export controls on such products

Area	Act	Date	Description
Copy protection	Digital Millennium Copyright Act (update to 17 USC 101)	1998	Provides specific penalties for removing copyright protection from media
Identity theft	Identity Theft and Assumption Deterrence Act of 1998 (18 USC 1028)	1998	Attempts to instigate specific penalties for identity theft by identifying the individual who loses their identity as the true victim, not just those commercial and financial credit entities who suffered losses
Banking	Gramm-Leach-Bliley Act of 1999 (GLB) or the Financial Services Modernization Act	1999	Repeals the restrictions on banks affiliating with insurance and securities firms; has significant impact on the privacy of personal information used by these industries
Terrorism	USA PATRIOT Act of 2001 (update to 18 USC 1030)	2001	Defines stiffer penalties for prosecution of terrorist crimes
Accountability	Sarbanes-Oxley Act of 2002 (SOX) or Public Company Accounting Reform and Investor Protection Act	2002	Enforces accountability for executives at publicly traded companies; this law is having ripple effects throughout the accounting, IT, and related units of many organizations
Spam	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 CAN-SPAM Act (15 USC 7701 et seq.)	2003	Sets the first national standards for regulating the distribution of commercial email; the act includes mobile phone spam as well
Fraud with access devices	Fraud and Related Activity in Connection with Access Devices (18 USC 1029)	2004	Defines and formalizes law to counter threats from counterfeit access devices like ID cards, credit cards, telecom equipment, mobile or electronic serial numbers, and the equipment that creates them
Terrorism and extreme drug trafficking	USA PATRIOT Improvement and Reauthorization Act of 2005 (update to 18 USC 1030)	2006	Renews critical sections of the USA PATRIOT Act

Key U.S. Laws of Interest to Information Security Professionals

Export and Espionage Laws

- Economic Espionage Act in 1996- To protect American ingenuity, intellectual property, and competitive advantage, Congress passed the Economic Espionage Act in 1996.
- The Security and Freedom through Encryption Act of 1999 - provides guidance on the use of encryption and provides protection from government intervention.

US Copyright Law

- Intellectual property is recognized as a protected asset in the US
- US copyright law extends this right to the published word, including electronic formats
- Fair use of copyrighted materials includes

- The use to support news reporting, teaching, scholarship, and a number of other related permissions
- The purpose of the use has to be for educational or library purposes, not for profit, and should not be excessive.

Freedom of Information Act of 1966 (FOIA)

- The Freedom of Information Act provides any person with the right to request access to federal agency records or information, not determined to be of national security
  - US Government agencies are required to disclose any requested information on receipt of a written request.
- There are exceptions for information that is protected from disclosure, and the Act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA

State & Local Regulations

- In addition to the national and international restrictions placed on an organization in the use of computer technology, each state or locality may have a number of laws and regulations that impact operations.
- It is the responsibility of the information security professional to understand state laws and regulations and insure the organization's security policies and procedures comply with those laws and regulations.

2.5.3 International Laws and Legal Bodies

- Recently the Council of Europe drafted the European Council Cyber-Crime Convention, designed.
  - To create an international task force to oversee a range of security functions associated with Internet activities,
  - To standardize technology laws across international borders
- It also attempts to improve the effectiveness of international investigations into breaches of technology law.
- This convention is well received by advocates of intellectual property rights with its emphasis on copyright infringement prosecution.

Digital Millennium Copyright Act (DMCA) Digital Millennium Copyright Act (DMCA)

- The Digital Millennium Copyright Act (DMCA) is the US version of an international effort to reduce the impact of copyright, trademark, and privacy infringement
- The European Union Directive 95/46/EC increases protection of individuals with regard to the processing of personal data and limits the free movement of such data
- The United Kingdom has already implemented a version of this directive called the Database Right

United Nations Charter

- To some degree the United Nations Charter provides provisions for information security during Information Warfare.
- Information Warfare (IW) involves the use of information technology to conduct offensive operations as part of an organized and lawful military operation by a sovereign state
- IW is a relatively new application of warfare, although the military has been conducting electronic warfare and counter-warfare operations for decades, jamming, intercepting, and spoofing enemy communications.

Policy versus Law

- Most organizations develop and formalize a body of expectations called policy
- Policies function in an organization like laws
- For a policy to become enforceable, it must be:
    - Distributed to all individuals who are expected to comply with it
    - Readily available for employee reference
    - Easily understood with multi-language translations and translations for visually impaired, or literacy-impaired employees
    - Acknowledged by the employee, usually by means of a signed consent form
- Only when all conditions are met, does the organization have a reasonable expectation of effective policy.

2.5.4 Ethical Concepts in Information Security

Cultural Differences in Ethical Concepts

- Differences in cultures cause problems in determining what is ethical and what is not ethical

- Studies of ethical sensitivity to computer use reveal different nationalities have different perspectives
- Difficulties arise when one nationality's ethical behaviour contradicts that of another national group

Ethics and Education

- Employees must be trained and kept aware of a number of topics related to information security, not the least of which is the expected behaviors of an ethical employee
- This is especially important in areas of information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal
- Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user

Deterrence to Unethical and Illegal Behaviour

- Deterrence - preventing an illegal or unethical activity
- Laws, policies, and technical controls are all examples of deterrents
- Laws and policies only deter if three conditions are present:
  - Fear of penalty
  - Probability of being caught
  - Probability of penalty being administered