Info 6010
Domain 1 - Part 1
Security and Risk Management - Law

Information Security Management

FANSHAWE

Information Security & Risk Management

Discussion Topics Part One

Brief overview of course and course outline

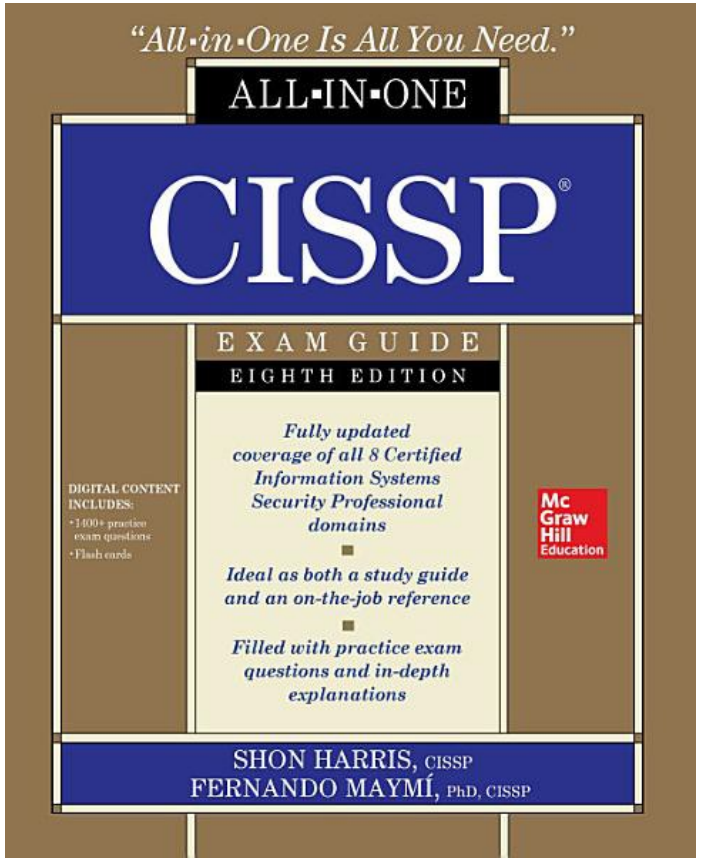
- Security terminology and principles
- Protection control types
- Security frameworks, models, standards, and best practices
- Computer laws and crimes
- Intellectual property
- Data breaches

Discussion Topics Part Two

- Risk management
- Threat modeling
- Business continuity and disaster recovery
- Personnel security
- Security governance

Text Book

Get a text book, either a physical copy or pdf version. The **8th edition** is the latest but an earlier version is better than nothing!!



Learning by rote alone will not help you! You must seek understanding if you wish to master this subject

How will you be evaluated in this course?

Testing! There are Two tests in this course (worth a total of 70%)

- Written quizzes and exams use the **Respondus Lockdown Browser**
- Questions can be Short answer, long answer, M/C, T/F, FIB, Matching,
- Recommend you use wired ethernet (RJ45 patch cable) and a plugged-in power supply (*Respondus does not like blips!*)
- Working ***and tested*** PC or laptop
- Expect an average time of 30-60 seconds per question unless it's a long answer question
- Testable material includes anything discussed "in class" (both verbally and on the slides), in discussion forums, in the textbook, any articles or resources I share, and in the assignments.

Note: Test time lost due to PC problems is not recoverable

Course Outline – Evaluating your work

- Missed Assignments and Tests
  - Tests will have a designated start time or time window. You must start within 15 minutes of the test opening
  - Tests are password protected
  - Students are **not entitled** to complete missed tests
  - In case of a significant event supported by documentation AND professor's approval AND prior notification, a missed test may be completed

- Re-writes & extra grade items
  - Students will **not be permitted** to rewrite tests
  - Students will **not be entitled** to extra work or assignments in order to raise a grade

- If an assignment requires screenshots to show your work. Your name in the screenshot is required. A screenshot of your whole screen is best – not just one window.

Assignments

- Hand in ALL assignments/Labs on time. ***Late penalties apply***.
- Put the assignment name and your last name in the file name
  - (ex. Wright_Lab1.doc)
- Assignments must follow APA 6th (or 7th) edition formatting, styling, and referencing.
- What do you know about APA?
- All assignments submitted via FOL in the correct submission box
  - **Assignments submitted in any other method (including email) will not be accepted**
  - Assignments submitted using the wrong submission box will not get graded.
  - Submission box is open until the noted time, example 11:59pm. You must submit before this time.
- Assignments must be submitted uncompressed, and saved as MSWord files (not .pdf).

Tips on professional writing assignments

- Your assignments **involve research**, **critical thinking**, and **academic writing**.

These are KEY SKILLS for information security professionals, and like any skill, practice makes perfect!

- Tips:
  - Use the discussion forum to practice
  - Use an editor (ex. use each other!)
  - Look up online resources for APA citing and referencing
  - Use credible (ideally peer-reviewed) literature in your work.
  - Include an introduction and conclusion
  - Include a title page
  - TMN font size 12, double spaced, indent paragraphs, 1” margins, etc.
  - Cite your sources BOTH in the text and on the dedicated References page at the end of your document
  - Do not need an abstract or TOC
  - Make sure you are thinking (and writing) critically. Challenge what you find in the literature!

Tips to success in this course

- Do not try to memorize everything. There is too much material. Focus on concepts and ideas, and the content will logically follow.
- Work in groups (online or offline). Collaboration lessens individual work and builds learning communities.
- Study in groups as well
- Use the Discussion Forum for bonus marks! It could be the difference between a letter grade. It is also a great way to construct knowledge together!
- Be prepared to read. **You read for a degree**
- Guard your time! And designate sufficient time to the course. Block it off on your calendar and stick to it.
- If you don't know or aren't sure, please ask!
- Create a personal slide deck (or flash cards) for key terms and concepts.

Great online tools for this!

Security Fundamentals

- 3 main principles are:
- Availability
  - Ensures reliability and timely access to data and resources to authorized individuals
- Integrity
  - Assurance of the accuracy and reliability of the information and systems is provided with no unauthorized modification
- Confidentiality
  - Necessary level of secrecy is enforced at each data handling junction and prevents unauthorized disclosure

Security Fundamentals

- Availability
  - Systems and network should have enough capacity for a acceptable level of performance.
  - Able to recover from disruption in a reasonable amount of time.
  - Single points of failure should be avoided
  - Backup and redundancy mechanisms should be in place
  - Appropriate mechanisms in place to avoid inside and outside threats

Security Fundamentals

- Integrity
  - Restrict access to only authorized users
    - System configuration files
  - Ensure attackers or user mistakes don't contaminate data integrity
    - Check data input for reasonable and valid entries
  - Data in transit should be encrypted

Security Fundamentals

- Confidentiality
  - Data in storage or transmitted across can not be read by unauthorized people
  - Attackers can circumvent confidentiality by
    - Network traffic sniffing
    - Looking over someone's shoulder and stealing passwords or by tricking someone to reveal their secret information.
  - Users can intentionally or accidentally disclose information by not encrypting it before transmitting it or transporting on storage devices
    - USB, DVD & Laptop

Security Definitions

- Vulnerability
- Software, hardware, procedural or human weakness that may provide an entry point for an attacker leading to unauthorized access.
  - Absence or weakness of a safeguard that can be exploited
    - Missing patches
    - Open Firewall port
    - Weak or no physical security
      - Unlocked doors
    - Unenforced password requirement

Security Definitions

- Threat
- Any potential danger to information or systems
  - A threat agent is someone or something that will take advantage of a known vulnerability
  - An intruder accessing the network through an open port on a firewall.
  - A process accessing data that violates security policy
  - Natural disaster causing damage to a facility
    - Tornado, hurricane, fire, flood, lightning
  - Environmental control
    - Power outage, heat & humidity damage
  - Terrorists attack

Security Definitions

- Risk
- The *likelihood* of a threat agent taking advantage of a *vulnerability*
  - Firewall with numerous open ports has a greater likelihood of being exploited
  - If a network does not have an Intrusion Detection device there is a greater likelihood of network access being unnoticed
  - User lack of training in security & processes increase likelihood of destroying or exposing data

Security Definitions

- Exposure
- An instance of being exposed to losses from a threat agent
- A vulnerability exposes an organization to possible losses
  - A company does not install fire detectors or fire alarms
    - Exposed to fire
  - A company does not have or enforce a password policy
    - Exposed to having password compromised

Security Definitions

- Safeguards or Countermeasures
- Software configuration, hardware device or a procedure that *reduces* the likelihood a threat agent will exploit a vulnerability
  - A security guard
  - Locked door on server rooms
  - Data backup policy
  - Strong password management
  - Anti-Virus Software
  - Firewall, AAA & IDS/IPS

Security Controls

- Administrative Controls:
  - Developing and publishing of policies, standards, procedures and guidelines
  - Risk management
  - Screening of personnel
  - Security awareness training
  - Implementing change control procedures

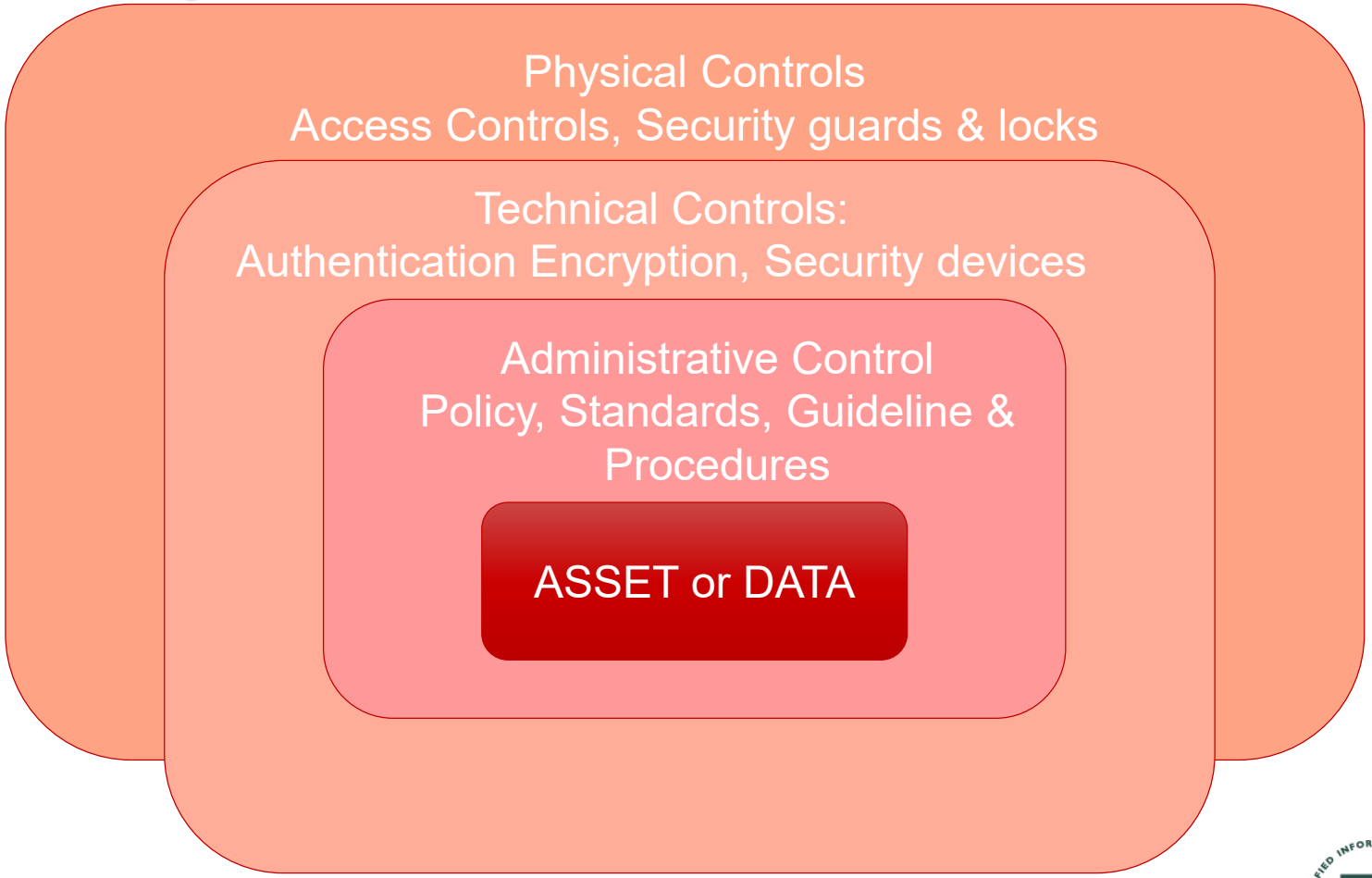
Security Controls

- Technical Controls (Logic Controls):
  - Configuration of security device & infrastructure
  - Implement and maintain access control mechanisms
  - Password and resource management
  - Identification and authentication methods
  - Security devices & infrastructure

Security Controls

- Physical Controls:
  - Controlling individual access into the facility and different departments
  - Locking systems and removing unnecessary drives
    - Floppy/CD-Rom, USB
  - Protecting the perimeter of the facility
    - Monitor for intrusion
  - Environmental controls

Security Controls



Source: All-In-One CISSP Exam Guide 8th Edition by Shon Harris

Standards, Best Practices & Frameworks

- ISO/IEC 27000 series International standards on how to develop and maintain an ISMS developed by ISO and IEC
- Zachman Framework Model for the development of enterprise architectures developed by John Zachman
- TOGAF Model and methodology for the development of enterprise architectures developed by The Open Group
- DoDAF U.S. Department of Defense architecture framework that ensures interoperability of systems to meet military mission goals
- MODAF Architecture framework used mainly in military support missions developed by the British Ministry of Defence
- SABSA model Model and methodology for the development of information security enterprise architectures

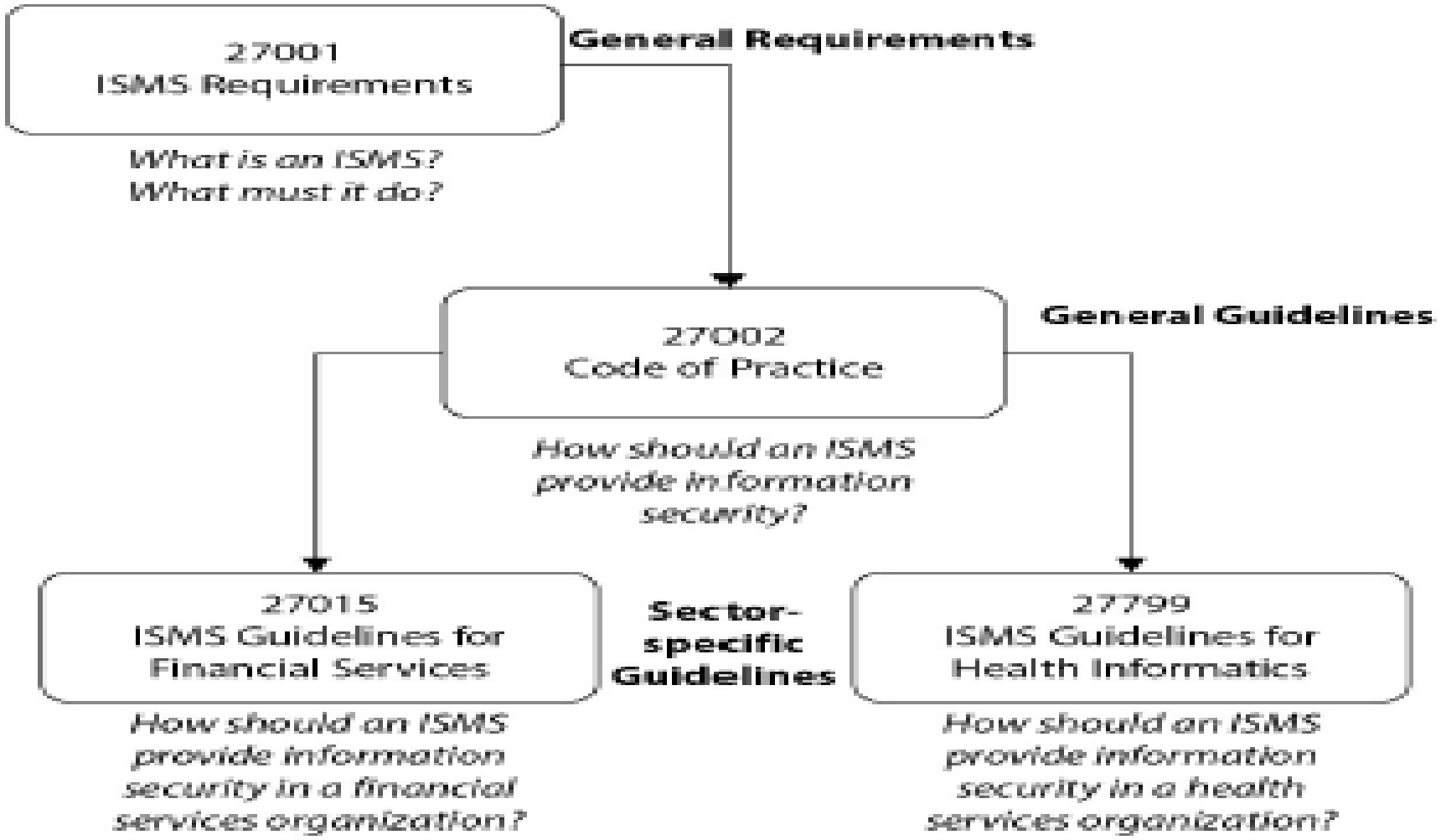
Standards, Best Practices & Frameworks

- **Security Control Development**:
  - COBIT 5 A business framework for IT enterprise management and governance developed by Information Systems Audit and Control Association (ISACA)
  - NIST SP 800-53 Set of controls to protect U.S. federal systems developed by the National Institute of Standards and Technology
  - COSO Internal Control—Integrated Framework Set of internal corporate controls to help reduce the risk of financial fraud developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission
- **Process Management Development:**
  - ITIL Processes to allow for IT service management developed by the United Kingdom's Office of Government Commerce
  - Six Sigma Business management strategy that can be used to carry out process improvement
  - Capability Maturity Model Integration (CMMI) Organizational development for process improvement developed by Carnegie Mellon University

Security Frameworks: ISO/IEC 27000 Series

- Set of standards to describe security processes and mechanisms
- ISO 27000 series has14 domains - similar to CISSP CBK (the revised CISSP has the content from 10 squeezed into 8 new domains- nothing has been taken away but things are added)
- Can be used as blue print to develop security program
- Companies can implement and be certified to provide confidence to customers and business partners
  - Marketing and business advantage

ISO 27000 series - Requirements



Security Framework

- Control Objectives for Information – CobiT
- Set of best practices developed by
  - Information Systems Audit and Control Association (ISACA)
  - IT Governance Institute (ITGI)
- CobiT was derived from COSO framework developed by the Committee of Sponsoring Organizations in 1985 to deal with fraudulent Financial reporting

Security Framework - CobIT

- The Control Objectives for Information and related Technology (COBIT) is a framework for governance and management developed by ISACA.
- It helps organizations optimize the value of their IT by balancing resource utilization, risk levels, and realization of benefits. This is all done by explicitly tying stakeholder drivers to stakeholder needs to organizational goals to IT goals. It is a holistic approach based on five key principles:

Security Framework - CobIT

- 1. Meeting stakeholder needs
- 2. Covering the enterprise end to end
- 3. Applying a single integrated framework
- 4. Enabling a holistic approach
- 5. Separating governance from management

- Many compliance audits are built on CobiT framework
  - Compliance roadmap has 34 control objectives of which 17 relate to the enterprise and 17 to IT related goals.

Security Framework – COSO

- COSO Areas
  - The Committee of Sponsoring Organisations of the Treadway Commission (COSO)
- **Control Environment**
  - Management philosophy & operating style
  - Company culture toward fraud and ethics
- **Risk Assessment**
  - Establish risk level
  - Manage change
- **Control Activities**
  - Policies, procedures & practices to mitigate risk

Security Framework – COSO

- COSO Areas cont.
- **Information and Communication**
  - Organizational structure to ensure information is provided to the right levels of management
- **Monitoring**
  - Detect and respond to control deficiencies

COSO vs CobiT

- CobiT is model for IT (Information Technology) governance
- COSO model for corporate governance
- COSO deals more with strategic level
- CobiT deals more with operational level
- CobiT & COSO identify what is to be achieved not how to achieve it

Security Framework - NIST

- The **National Institute of Standards and Technology** (NIST) is a non-regulatory body of the U.S. Department of Commerce.
- The **NIST Cybersecurity Framework** provides a policy framework of computer security guidance for how private sector organizations in the United States (and is used by many others) can assess and improve their ability to prevent, detect, and respond to cyber attacks.

Process Management – ITIL

- The Information Technology Infrastructure Library
- De facto standard of best practices for IT
- Provides goals and general activities to achieve goals
- Provides steps at process level and expected input and output values of each activity to achieve goals
- Customizable Framework
- Focus is on internal service level agreement (SLA) between the IT department and it's internal customers
  - Security is only one component

Six Sigma

- Six Sigma (6σ) is a set of techniques and tools for process improvement.
- Introduced by engineer Bill Smith while working at Motorola in 1980. Jack Welch made it central to his business strategy at General Electric in 1995.
- A six sigma process is one in which 99.99966% of all opportunities to produce some feature of a part are statistically expected to be free of defects.

Capability & Maturity Model

- A way to determine the maturity of an organizations processes.
- The goal is to continue to review and improve upon the processes to optimize output, increase capabilities.
  - Provides an evolutionary path from an ad hoc “fly by the seat of your pants” approach, to a more disciplined and repeatable method that improves quality, reduces the life cycle of development, provides better project management capabilities, allows for milestones to be created and met in a timely manner, and takes a more proactive approach than the less effective reactive approach

Capability & Maturity Model

- Five maturity levels are used:
- **Unpredictable (Initial)**
  - The company does not use effective management procedures and plans.
  - There is no assurance of consistency, quality is unpredictable
- **Repeatable**
  - A formal management structure, change control, and quality assurance are in place.
  - The company can properly repeat processes throughout each project.
  - The company does not have formal process models defined

Capability & Maturity Model

- Five maturity levels are used cont.:
- **Defined**
  - Formal procedures are in place that outline and define processes carried out in each project.
  - The organization has a way to allow for quantitative process improvement.
- **Managed**
  - The company has formal processes in place to collect and analyze qualitative data, and metrics are defined and fed into the process-improvement program
- **Optimizing**
  - The company has budgeted and integrated plans for continuous process improvement

Security Program Development

- The standards, models and frameworks mentioned on earlier slides are tools that help in the development and maintenance of a security system – no one tool will achieve everything you may need!
- The standards and frameworks are similar and follow a similar approach such as a life cycle process:

1. Plan and organize
2. Implement
3. Operate and maintain
4. Monitor and evaluate

Security Program Development – Top Down Approach

Plan and Organise:

- Establish management commitment.
- Establish oversight steering committee.
- Assess business drivers.
- Develop a threat profile on the organization.
- Carry out a risk assessment.
- Develop security architectures at business, data, application, and infrastructure levels.
- Identify solutions per architecture level.
- Obtain management approval to move forward.

Security Program Development

Implement:

- Assign roles and responsibilities.
- Develop and implement security policies, procedures, standards, baselines, and guidelines.
- Identify sensitive data at rest and in transit.
- Implement the following blueprints:
- Asset identification and management
- Risk management
- Vulnerability management

Security Program Development

Implement cont.:

- Compliance
- Identity management and access control
- Change control
- Software development life cycle
- Business continuity planning
- Awareness and training
- Physical security
- Incident response

- Implement solutions (administrative, technical, physical) per blueprint.
- Develop auditing and monitoring solutions per blueprint.
- Establish goals, SLAs, and metrics per blueprint.

Security Program Development

Operate and Maintain:

- Follow procedures to ensure all baselines are met in each implemented blueprint.
- Carry out internal and external audits.
- Carry out tasks outlined per blueprint.
- Manage SLAs per blueprint.

Security Program Development

Monitor and Evaluate:

- Review logs, audit results, collected metric values, and SLAs per blueprint.
- Assess goal accomplishments per blueprint.
- Carry out quarterly meetings with steering committees.
- Develop improvement steps and integrate into the Plan and Organize phase.

Crux of Computer Crime Laws

Bad things happen and one of the ways of combatting bad behaviour is to enact laws.

The core issues that computer crime laws address are: unauthorized modification or destruction, disclosure of sensitive information, unauthorized access, and the use of malware (malicious software).

We may only think of the victims and their systems that were attacked during a crime, laws have been created to combat three categories of crimes.

Computer Crime Law

- Three categories of computer crimes.
  1. **Computer assisted crime**
  2. **Computer targeted crime**
  3. **Computer is incidental type of crime**

Computer Crime Law

- **Computer Assisted**
  - Is where a computer was used as a tool to help carry out a crime
- **Computer Targeted**
  - Concerns incidents where a computer was the victim of an attack crafted to harm it (and its owners)
- **Computer is incidental**
  - Is not necessarily the attacker or the victim, but just happened to be involved when a crime was carried out

Computer Crime Law

- Examples of co**mputer assisted** crimes:
  - Attacking financial systems (theft of funds and/or sensitive information)
  - Obtaining military and intelligence material
  - Industrial spying
  - Information warfare activities (critical national infrastructure)
  - Hacktivism (protesting a government or company's activities) e.g., recent activities by "Anonymous"

Computer Crime Law

- Examples of **computer targeted** crimes:
  - Distributed Denial-of-Service (DDoS) attacks
  - Capturing passwords or other sensitive data
  - Installing malware with the intent to cause destruction
  - Installing rootkits and sniffers for malicious purposes
  - Carrying out a buffer overflow to take control of a system

Computer Crime Law

- These categories were created to allow current laws to apply to these types of crimes, even though they are in the digital world
- This makes it easier for a judge to know what the proper sentencing (punishments) are for these specific crimes
- Sentencing guidelines have been developed by the government to standardize punishments for the same types of crimes throughout provincial and federal courts

Complexities in Cybercrime

- Most attackers are never caught because they spoof their addresses and identities and use methods to cover their footsteps
- Many attackers break into networks, take whatever resources they were after and clean the logs that tracked their movements and activities
- Because of this many companies do not even know they have been violated

Complexities in Cybercrime

- Attackers commonly hop through several systems before attacking their victim so that tracking them down will be more difficult
- Many of these criminals use innocent people's computers to carry out the crimes for them (Use of Malicious Software – Think Botnets and Zombies)
- Collectively law enforcement are very far behind the times in their skills and tools, and are outnumbered by the number of hackers actively attacking networks

Complexities in Cybercrime

- Law enforcement is continually improving its tactics and individuals are being prosecuted

- www.cybercrime.gov
  - Site showing current and past prosecutions
  - Navigate to cybercrime.gov and look at a few interesting cases.

Electronic Assets

- **Assets have changed (electronic)**
  - Defining what has to be protected and to what extent has become harder
  - Shift in the business world pertaining to assets that need to be protected
  - Previously assets were more tangible (equipment, building, manufacturing tools, inventory)
  - Companies have a hard time protecting their data in digital format and defining what constitutes sensitive data and where that data should be kept

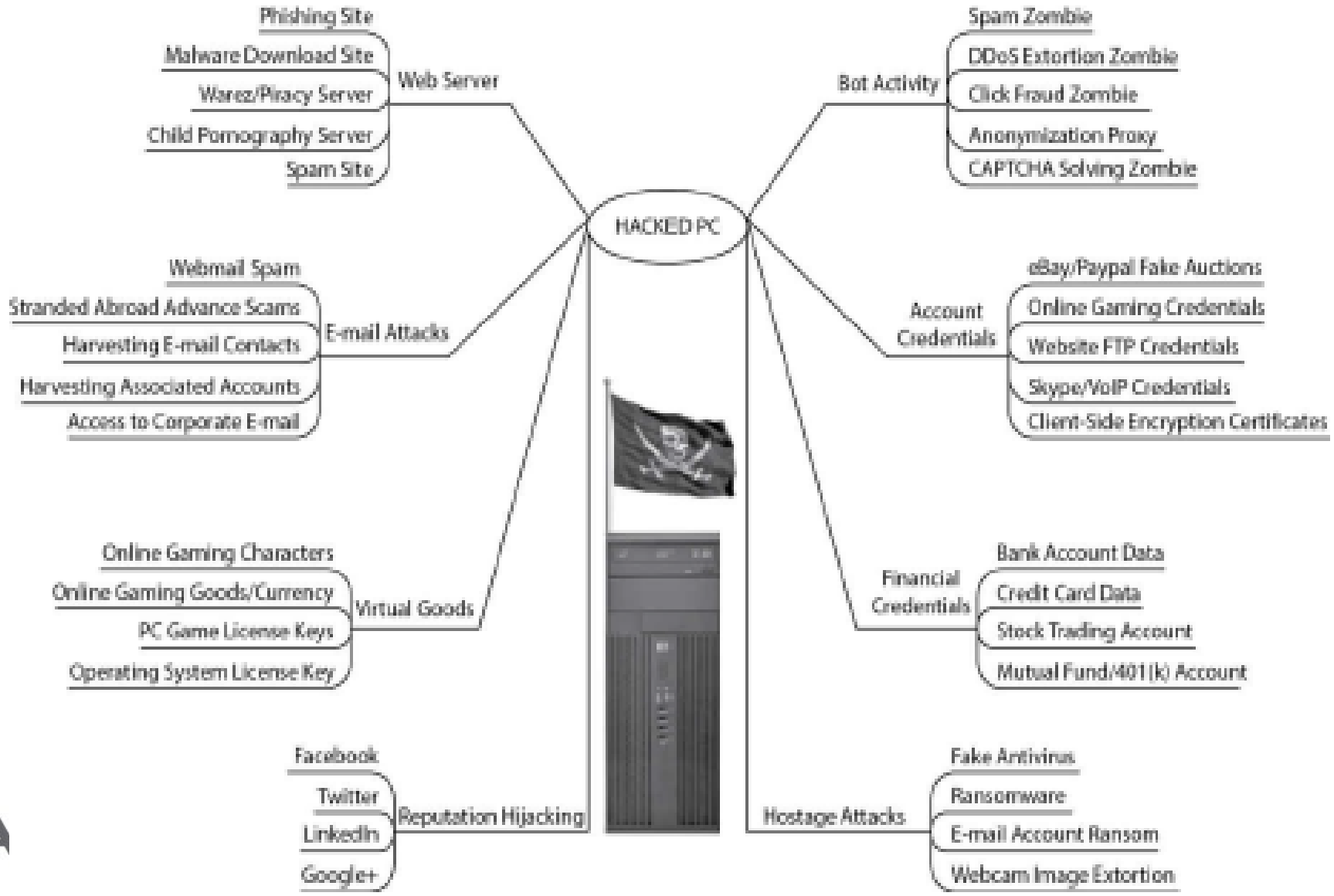
Electronic Assets

- Today companies must add data to their list of assets
  - Product blueprints
  - Social Security numbers
  - Medical information
  - Credit card numbers
  - Personal information
  - Trade secrets

Evolution of Attacks

- In the 60's, 70's and 80's hackers were mainly made up of people who just enjoyed the thrill of hacking
- It was seen as a challenging game without any real intent of harm
- Take down large web sites (Yahoo!, MSN, Excite)
- Made headlines and won bragging rights among their fellow hackers
- Virus writers created viruses that simply replicated or carried out some benign activity

Malicious uses for a Compromised Computer



Common Internet Crime Schemes

- Auction fraud
- Counterfeit cashier's check
- Debt elimination
- Parcel courier e-mail scheme
- Employment/business opportunities
- Escrow services fraud
- Investment fraud
- Lotteries
- Nigerian letter, or "419"
- Ponzi/pyramid
- Reshipping
- Third-party receiver of funds
- Sophistication of the attacks continues to increase, so does the danger of these attacks

International Issues

- **Different Countries**
- If a hacker in Ukraine attacked a bank in France whose legal jurisdiction is that?
- How do these countries work together to identify the criminal and carry out justice?
- Which country is required to track down the criminal?
- Which country should take this person to court?

Internet Crime Issues

- Different countries have different legal systems
- Some countries have no laws pertaining to computer crime
- Jurisdiction disputes may erupt
- Some governments may not want to cooperate with each other, for example
  - Israel and Iran
  - North Korea and USA

Internet Crime Issues

- **The Council of Europe (CoE) Convention on Cybercrime**
- First attempt to create a standard international response to cybercrime
- International treaty seeking to coordinate national laws and improve investigative techniques and international cooperation
- Framework for establishing jurisdiction and extradition of the accused

FANSHAWE

OECD - Principles

- Global organizations that move data across other country boundaries must be aware of and follow the **Organisation for Economic Co-operation and Development (OECD)** Guidelines
- OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy

OECD - Principles

The core principles defined by the OECD:

1. Collection of personal data should be limited, obtained by lawful and fair means, and with the knowledge of the subject
2. Personal data should be kept complete and current, and be relevant to the purposes for which it is being used
3. Subjects should be notified of the reason for the collection of their personal information at the time that it is collected, and organizations should only use it for that stated purpose

OECD – Principles cont.

The core principles defined by the OECD cont.

4. Only with the consent of the subject or by the authority of law should personal data be disclosed, made available, or used for purposes other than those previously stated.
5. Reasonable safeguards should be put in place to protect personal data against risks such as loss, unauthorized access, modification, and disclosure

OECD - Principles cont.

The core principles defined by the OECD cont.

6. Developments, practices, and policies regarding personal data should be openly communicated. In addition, subjects should be able to easily establish the existence and nature of personal data, its use, and the identity and usual residence of the organization in possession of that data
7. Subjects should be able to find out whether an organization has their personal information and what that information is, to correct erroneous data, and to challenge denied requests to do so

OECD

- Organizations that are not aware of and/or do not follow these types of rules and guidelines can be:
  - Fined
  - Sued
  - Business can be disrupted
  - Can go out of business

General Data Protection Regulation - GDPR

- The General Data Protection Regulation (GDPR) is an EU regulation that protects the personal data and privacy of EU citizens.
- The GDPR, is law in all 28 member states of the EU. This means that each state does not have to write its own version, which harmonizes data protection regulations and makes it easier for companies to know exactly what is expected of them throughout the block.
- The catch is that these requirements are quite stringent, and violating them exposes a company to a maximum fine of 4 percent of that company's global turnover.

General Data Protection Regulation - GDPR

- **Data subject:** The individual to whom the data pertains.
- **Data controller:** Any organization that collects data on EU residents.
- **Data processor:** Any organization that processes data for a data controller.
- The regulation applies if any one of the three entities is based in the EU, but it also applies if a data controller or processor has data pertaining to an EU resident. The GDPR impacts every organization that holds or uses European personal data both inside and outside of Europe.

General Data Protection Regulation - GDPR

Protected Privacy Data includes:

- Name
- Address
- ID numbers
- Web data (location, IP address, cookies)
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

Import/Export Legal Requirements

Import and export laws can be complex as each country has its own specifications when it comes to what is allowed in its borders and what is allowed out.

For example, the Wassenaar Arrangement implements export controls for “Conventional Arms and Dual-Use Goods and Technologies.” It is currently made up of 42 countries and lays out rules on how the following items can be exported from country to country:

Import/Export Legal Requirements

- Category 1 Special Materials and Related Equipment
- Category 2 Materials Processing
- Category 3 Electronics
- Category 4 Computers
- Category 5 Part 1: Telecommunications
- Category 5 Part 2: Information Security
- Category 6 Sensors and Lasers
- Category 7 Navigation and Avionics
- Category 8 Marine
- Category 9 Aerospace and Propulsion

Import/Export Legal Requirements

The Wassenaar Arrangement is complex and frequently changes. Countries are categorised as “good or bad” this determines what can be exported to them. Products containing cryptographic functions are generally restricted.

Some countries (China, Russia, Iran, Iraq, etc.) have cryptographic import restrictions that have to be understood and followed.

Types of Legal Systems

- Different countries often have different legal systems
- **Civil (Code) Laws**
  - System of law used in continental European countries (France, Spain)
  - Civil law is rule-based law not precedence based
    - Different from common law used in the United Kingdom and United States
  - For the most part, a civil law system is focused on codified law (written laws)
  - The history of civil laws dates to the sixth century when the Byzantine emperor Justinian codified the laws of Rome.

Civil Laws

- Civil law was established by states or nations for self-regulation
  - Civil law can be divided into subdivisions such as French civil law, German civil law, and so on
- It is the most widespread legal system in the world and the most common legal system in Europe
- Under civil law, lower courts are not compelled to follow the decisions made by higher courts.
- Civil legal systems should not be confused with the civil (or tort) laws found in the U.S.

Common Law

- Developed in England.
- Based on previous interpretations of laws.
- Judges did not have a written set of laws so they based their laws on custom and precedent.
- In the 12th century the King of England imposed a unified legal system that was “common” to the entire country.
- Reflects the community’s morals and expectations.
- Led to the creation of barristers, or lawyers, who actively participate in the litigation process through the presentation of evidence and arguments.

Common Law

- Today, common law uses judges and juries of peers. If the jury trial is waived, the judge decides the facts.
- Typical systems consist of a higher court, several intermediate appellate courts, and many local trial courts. Precedent flows down through this system. Tradition also allows for “Magistrate’s courts,” which address administrative decisions.
- The common law system is broken down into criminal, civil/tort, and administrative.
- Used in Canada, United Kingdom, Australia, United States, and New Zealand.

Common Law, Criminal, Civil/tort Law

- Common Law is broken down into the following:
- **Criminal**
  - Based on common law, statutory law, or a combination of both.
  - Addresses behavior that is considered harmful to society.
  - Punishment usually involves a loss of freedom, such as incarceration, or monetary fines
  - Responsibility is on the prosecution to prove guilt beyond a reasonable doubt.

- **Civil/tort**
  - Offshoot of criminal law
  - Under civil law, the defendant owes a legal duty to the victim
  - The defendant's breach of that duty causes injury to the victim; usually physical or financial

Civil Law

- **Categories of civil law:**
- Intentional
  - Assault, infliction of emotional distress, or false imprisonment
- Wrongs against Property
  - Nuisance against landowner
- Wrongs against a Person
  - Car accidents, dog bites, and a slip and fall
- Negligence
  - Wrongful death

Civil Law

- Categories of civil law:
- Nuisance
  - Trespassing
- Dignitary Wrongs
  - Invasion of privacy and civil rights violations
- Economic Wrongs
  - Patent, copyright, and trademark infringement
- Strict Liability
  - Failure to warn of risks and defects in product or design
- Administrative
  - Regulatory

Customary Law

- Deals mainly with personal conduct and patterns of behavior
- Based on traditions and customs of the region
- Emerged when cooperation of individuals became necessary as communities merged
- Not many countries work under a purely customary law system, but instead use a mixed system where customary law is an integrated component. (Codified civil law systems emerged from customary law.)

Customary Law

- Mainly used in regions of the world that have mixed legal systems (for example, China and India)
- Restitution is commonly in the form of a monetary fine or service

Religious Law

- Based on religious beliefs of the region
- In Islamic countries the law is based on the rules of the Koran
- The law is different in every Islamic country
- Jurists and clerics have a high degree of authority
- Cover all aspects of human life but commonly divided into:
  - Responsibilities and obligations to others
  - Religious duties

Religious Law

- Knowledge and rules as revealed by God which define and govern human affairs
- Rather than create laws law makers and scholars attempt to discover the truth of law
- Law includes codes of ethics and morality which are upheld and required by God
- Examples:
  - Hindu law
  - Sharia (Islamic law),
  - Halakha (Jewish law)

Mixed Legal Systems

- Two or more legal systems are used together and apply cumulatively or interactively
- Most often mixed law systems consist of civil and common law
- A combination of systems is used as a result of more or less clearly defined fields of application
- Civil law may apply to certain types of crimes, while religious law may apply to other types within the same region
- Examples of mixed law systems include
  - Holland, Canada, and South Africa.

Civil Law

- **Civil law** deals with wrongs against individuals or companies that result in damages or loss
  - This is referred to as **tort** law.
- Examples include trespassing, battery, negligence, and products liability
- A civil lawsuit would result in financial restitution and/or community service instead of a jail sentence
  - When someone sues another person in civil court, the jury decides upon liability instead of innocence or guilt. If the jury determines the defendant is liable for the act then the jury decides upon the punitive damages of the case

Criminal Law

- **Criminal law** is used when an individual's conduct violates the laws passed to protect the public
- Jail sentences are commonly the punishment for criminal law cases
  - In civil law cases the punishment is usually an amount of money that the liable individual must pay the victim
  - For example in the O.J. Simpson case he was first tried and found not guilty in the criminal law case but then was found liable in the civil law case
- This seeming contradiction can happen because the burden of proof is lower in civil cases than in criminal cases.

Administrative Law

- **Administrative/regulatory law** deals with regulatory standards that regulate performance and conduct
- Government agencies create these standards, which are usually applied to companies and individuals within those specific industries
- Examples of administrative laws could be that every building used for business must have a fire detection and suppression system must have easily seen exit signs and cannot have blocked doors in case of a fire

Intellectual Property Law

- Intellectual property laws specify how a company can protect what it rightfully owns from unauthorized duplication or use and what it can do if these laws are violated
- The issue in intellectual property cases is what the company did to protect the resources it claims have been violated
  - A company must go through many steps to protect resources that it claims to be intellectual property and must show that it exercised **due care** in its efforts to protect those resources

Intellectual Property Law

- Intellectual property can be protected by several different laws depending upon the type of resource it is
- Two categories
- Industrial property
  - inventions (patents), industrial designs & trademarks
- Copyright
  - Literary and artistic works

Trade Secret

- Trade secret law protects certain types of information or resources from unauthorized use or disclosure
- For a company to have its resource qualify as a trade secret, the resource must provide the company with some type of competitive value or advantage
- A trade secret is something that is proprietary to a company and important for its survival and profitability

Trade Secret

- Many companies require their employees to sign a nondisclosure agreement, confirming that they understand its contents and promise not to share the company's trade secrets with competitors
- Example of a trade secret is the formula used for a soft drink, such as Coke or Pepsi

Copyright

- In the United States copyright law protects the right of an author to control the public distribution, reproduction, display, and adaptation of his original work
  - Copyright protection is for life plus 50 years
- There are many categories of work:
  - Pictorial
  - Graphic
  - Musical
  - Dramatic
  - Literary
  - Pantomime
  - Motion picture
  - Sculptural
  - Sound recording
  - Architectural

Trademark

- A trademark is slightly different from a copyright in that it is used to protect a word, name, symbol, sound, shape, color, or combination of these
- Represents (brand identity) to a group of people or to the world
- Companies cannot trademark a number or common word
- Unique colors can be trademarked as well as identifiable packaging which is referred to as “trade dress”
  - Think UPS Brown

Patents

- A patent is the strongest form of intellectual property protection
- Patents are given to grant legal ownership and exclude others from using or copying the invention covered by the patent
  - Patents grant a limited property right to exclude others from making, using, or selling the invention for a specific period of time
    - 20 years
- Invention must be novel, useful, and not obvious
- WPIO – World Property Intellectual Organization
  - United Nations oversees international registration of trademarks

Intellectual Property

- Employees must be informed of the level of secrecy or confidentiality of the resource, and of their expected behavior pertaining to that resource
- Identified resources should have the necessary level of access control protection, auditing enabled, and a proper storage environment
  - Company's data classification scheme.
- If it is deemed secret then not everyone in the company should be able to access it
- If a company fails in one or all of these steps it may not be covered by laws

Software Piracy

- Software piracy occurs when the intellectual or creative work of an author is used or duplicated without permission or compensation to the author
- It is an act of infringement on ownership rights and if the pirate is caught he could be sued civilly for damages or be criminally prosecuted
- There are four categories of software licensing:
  - **Freeware**
  - **Shareware**
  - **Commercial**
  - **Academic**

Software Piracy

- **Freeware**
  - Software that is publicly available free of charge and can be used, copied, studied, modified, and redistributed without restriction
- **Shareware**
  - Users obtain a free trial version
  - User is asked to purchase a copy after trial period expires (usually 30 days)
- **Commercial**
  - Software is sold for commercial profit purposes
- **Academic**
  - Software that is provided for academic purposes at a reduced cost

Software Piracy

- The Business Software Alliance (BSA) and International Data Corporation (IDC) found that the frequency of installed illegal software is 36 percent worldwide
  - This means that for every two dollars' worth of legal software purchased one dollar's worth is pirated
- Not every country recognizes software piracy as a crime, but several international organizations have made strides in curbing the practice
- Software Protection Association (SPA) has been formed by major companies to enforce proprietary rights of software

Privacy Laws

- The following issues have increased the need for more privacy laws and governance:
- Data aggregation and retrieval technologies advancement
  - Large data warehouses are continually being created full of private information
- Loss of borders (globalization)
  - Private data flows from country to country for many different reasons
  - Business globalization.
- Convergent technologies advancements
  - Gathering, mining, distributing sensitive information

Laws, Directives & Regulations

- Laws, regulations, and directives developed by governments or appointed agencies do not usually provide detailed instructions to follow to properly protect computers and company assets
  - Each environment is too diverse in topology, technology, infra-structure, requirements, functionality, and personnel
- Regulations state high-level requirements that commonly have companies scratching their heads on how to be compliant with them
- Today, security professionals are being pulled out of the server rooms and asked to be more involved in business-oriented issues

Federal Privacy Act of 1974

- The **Privacy Act** of **1974** provide restrictions and safeguards against the invasion of personal **privacy** through the misuse of data and records by **Federal** Agencies (in the US).

Privacy

- **Current methods of privacy protection:**
- Government regulations
  - SOX, HIPAA, GLBA, BASEL
- Self-regulation
  - Payment Card Industry (PCI)
- Individual user
  - Passwords, encryption, awareness

HIPPA

- **The Health Insurance Portability and Accountability Act (HIPAA)**
- The Health Insurance Portability and Accountability Act (HIPAA), a U.S. federal regulation has been mandated to provide national standards and procedures for the storage, use, and transmission of personal medical information and health care data
- As health records migrate from a paper-based system to an electronic system, they become easier to maintain, access, and transfer, but they also become easier to manipulate and access in an unauthorized manner

USA Patriot Act

Reduces restrictions on law enforcement agencies' ability to search telephone, e-mail, medical, financial, and other records.

- Eases restrictions on foreign intelligence gathering within the United States.
- Expands the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities.
- Broadens the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts.
- Expands the definition of terrorism to include domestic terrorism, thus enlarging the number of activities to which the USA PATRIOT Act's expanded law enforcement powers can be applied.

GBLA

- **The Gramm-Leach-Bliley Act of 1999 (GLBA)**
- The Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to develop privacy notices and give their customers the option to prohibit financial institutions from sharing their information with nonaffiliated third parties

PCI DSS

- **Payment Card Industry Data Security Standards (PCI DSS)**
- Self regulated by the Credit Card industry, PCI DSS is a private-sector industry initiative and is not a law
- Applies to any entity that processes, transmits, stores, or accepts credit card data
- Noncompliance or violations may result in revocation of merchant status
  - But not jail time
- Varying levels of compliance depending on the size of the customer and the volume of transactions

Employee Privacy

- Within a corporation, several employee privacy issues must be thought through and addressed if the company wants to be properly protected
- Employees must be informed keyboard, email and surveillance monitoring will take place

Employee Privacy

- Monitoring must be work related, meaning that a manager may have the right to listen in on his employees' conversations with customers, but he does not have the right to listen in on personal conversations that are not work related
- Monitoring also must happen in a consistent way, such that all employees are subjected to monitoring, not just one or two people

Employee Privacy

- If a company feels it may be necessary to monitor e-mail messages and usage, this must be explained to the employees, first through a security policy and then through a constant reminder such as a computer banner or regular training.
- It is best to have an employee read a document describing what type of monitoring they could be subjected to, what is considered acceptable behavior, and what the consequences of not meeting those expectations are.

Employee Privacy

- Employees should sign this document, which can later be treated as a legally admissible document if necessary
- Company must not promise privacy to employees that it does not then provide, because that could result in a lawsuit

Data Breaches

- **Data breach**: when data owners lose control of who has access to their data. A data breach is a **security event** that results in the actual or potential compromise of the confidentiality or integrity of protected information by unauthorized persons.
- Protected information can be PII, IP, personal health information (PHI), classified information, or any other information that can cause damage to an individual or organization.
- Major data breaches happen all the time some are often unreported or unnoticed at the time of the breach.
- If an organization fails to properly protect the privacy of its customers' data, it increases the likelihood of experiencing a data breach.
- A data breach does not always involve a violation of Personal Identifiable Information (PII) but often intellectual property (IP).

Data Breaches

If a data breach occurs there will likely be legal and regulatory requirements that must be complied with i.e. notify all affected persons that their data may have been compromised.

As the laws will vary between countries it is always best to seek legal advice.

Security Policy

- An overall general statement produced by senior management that dictates what role security plays within the organization
- Security policy can address one of the following:
  - Organizational Policy
  - Issue Specific Policy
  - System Specific Policy

Security Policy

- Organizational Policy
  - Management determines goals and assigns responsibilities,
  - Shows the strategic value of security and outlines how enforcement should be carried out.
- Organizational Policy Example
  - Management outlines general employee conduct policy addressing local, provincial or federal laws
  - This policy may also include vendor specific market regulations.

Security Policy

- Issue Specific Policy
  - Also called a functional policy
  - Addresses specific security issue(s) that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues.
- Issue Specific Policy Example
  - Email monitoring policy outlining what management may do with employees email.
  - May also state employees cannot share confidential information or state company issued email cannot be used for non business websites, forums or chat groups.

Security Policy

- System Specific Policy
  - Managements decisions that are specific to computers, networks, applications and data
- System Specific Policy Example
  - Managements provides an approved software list
  - It may also address how computers are to be locked down or how firewalls and Intrusion Detection systems are implemented and monitored.

Security Policy

- Identifies assets the company considers valuable
- Provides authority to the security team and its activities
- States the company security goals and objectives
- Outlines personal responsibility
  - Provides a reference when conflicts arise
- Helps to prevent unaccounted for events
- Outlines incident response

Security Policy Types

- Regulatory Policy
  - Ensures company is following legal and industry specific regulations. (Health Care, Financial)
- Advisory Policy
  - Outlines acceptable and unacceptable employee behavior.
  - Includes possible consequences should policy be broken.
- Informative Policy
  - Informs employees of certain topics
  - This policy is NOT enforceable
  - Used for training

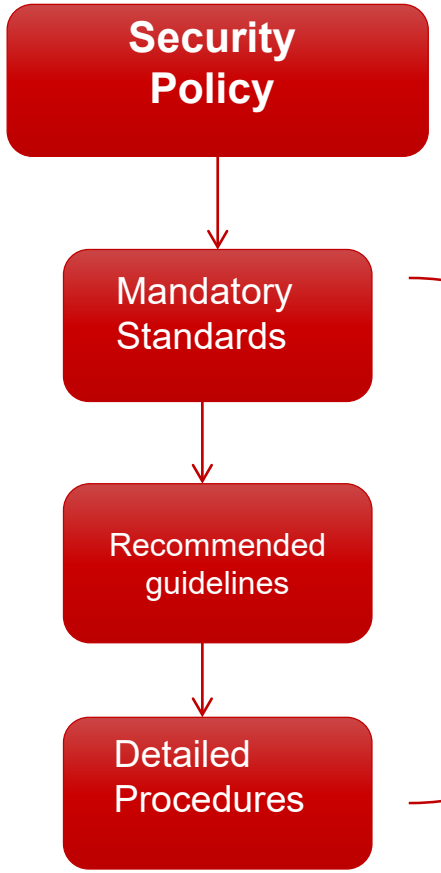
Standards, Baselines, …

- Standards
  - Mandatory activities, actions or rules
  - Standards support Policies.
  - Standards can be company specific (derived internally) or mandated by regulatory bodies or governments
- Baselines
  - Minimum level of protection required
  - Baseline can be a point in time reference for comparison for future changes.
  - All patches and upgrades must be checked and tested to ensure baseline compliance

Guidelines, and Procedures

- Guideline
  - General guide and recommended actions when a specific Standard does not apply
- Procedure
  - Step by step detailed instruction on specific tasks
    - Set up new user accounts
  - Lowest level of security policy
  - Details of how standards and guidelines are implemented

Policy, Standard, Baseline & Guidelines



Strategic Goal
End result

Tactical Goal

Steps Required to Achieve End Result

Source: All-In-One CISSP Exam Guide 8th Edition by Shon Harris

Policy, Standard, Baseline & Guidelines

- Security policy is a modular document
- Parts such as a standard or procedure can be modified as required without changing the whole document

Policy, Standard, Baseline & Guidelines

- Example #1
- Policy
  - All corporate data must be backed up
- Standard
    - Full back up every week
    - Incremental every day
    - Store off site
- Procedure
  - Step by step instructions for how backup performed
  - Detail on how to store backup

Policy, Standard, Baseline & Guidelines

- Example #2
- Policy
  - All employee user accounts requires password protection
- Standard
    - Passwords 10 characters long
    - Change every 45 days
    - Complex
- Procedure
  - Steps for setting up user account
  - Password change on first login

Homework

- Read the relevant chapter(pages) in the set book ‘All In One CISSP Exam Guide’ – by Shon Harris.

- Depending on which edition you have the relevant sections will be in different places – so use the index.

- Then identify and do the practice m/c questions relating to this subject.

Questions?