FESTUS OLUBUKUNMI AJIBUWA

Data and Information Security in Modern Day Businesses

A Final Thesis Presented to
The Academic Department
Of the School of Science and Engineering
In Partial Fulfillment of the Requirements
For the Degree of Master in Computer Science

ATLANTIC INTERNATIONAL UNIVERSITY

Acknowledgement

My profound gratitude goes to Almighty God who does things in his own time. I did not dream of having a Master degree so soon. I wish to acknowledge Dr. Jean Paillet who has being my financial support right from the Bachelor’s level together with Dr. Tony Johnson of International Business College, The Gambia. To my lovely wife, I say thank you for your support and understanding. To my advisor – Nam Nguyen I say a big THANK you for your prompt attention and grading of my assignments. And to my good friend – Gordon Essese; thanks for linking me up with Atlantic International University.

I appreciate all your efforts. The Lord will reward you.

Table of Contents

Abstract

Information security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

This Thesis reveals a comprehensive analysis of Data and Information Security in modern-day businesses. It covers the Meaning and Background history of Data Security, Categories of Data Security, Security Concepts, Security Standards, Principles of Information Security, The negative impact of breaching organization's security, Data Protection and Risk Management; Laws and Regulations governing Information Security.

It equally covers some verse areas of Information Security as a process, Information Security at Management level, Sources of Standards for Information Security, Protecting Privacy in Information Systems, Data Theft, Database Security, Managing Systems for Employee Turn-over, Laws and Regulations governing Information Security, Sources of Standards for Information Security, Types of Data Theft, Security Administration, Reporting Data Security Breaches and the Responsibilities of everyone that has to do with Data and Information Security. Detailed analyses of these sub-headings are well arranged and simplified within the write-up.

Chapter 1

General Introduction

Data / Information

In the area of Information Security, data (and the individual elements that comprise the data) is processed, formatted and re-presented, so that it gains meaning and thereby becomes information. Information Security is concerned with the protection and safeguard of that information which, in its various forms can be identified as Business Assets or Information Assets.

The terms data and information can be used somewhat interchangeably; but, as a general rule, information always comprises data, but data is not always information.

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review.

In 1989, Carnegie Mellon University established the Information Networking Institute, the United State's first research and education center devoted to information networking. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations during the later years of the 20th century and early years of the 21st century.

Entry into the field can be accomplished through self-study, college or university schooling in the field or through week long focused training camps. Many colleges, universities and training companies offer many of their programs on- line. The GIAC-GSEC and Security+ certifications are both respected entry level security certifications. The Certified Information Systems Security Professional (CISSP) is a well respected mid- to senior-level information security certification.
The profession of information security has seen an increased demand for security professionals who are experienced in network security auditing, penetration testing, and digital forensics investigation.

Definitions of Data Security

Security according to Collins English Dictionary is “the state of being secure. Precautions taken to ensure against theft, espionage, etc;” Data security is very important, data that contain personal information has to be protected under the data protection act, and data that could be useful for commercial competitors has to be safeguarded from theft.

The Higher National Computing (page 226) declares that data security as an essential aspect of computing especially with database system to ensure privacy of sensitive and personal information. Data security is also paramount in complying with legislation that protects users and third parties of data.

According to Terence Driscoll and Bob Dolden “Security in information management terms means the protection of data from accident or deliberate threats which might cause unauthorized modification, disclosure or destruction of data, and the protection of information system from the degradation or non availability of services.”

Security refers to technical issues related to the computer system, psychological and behavioral factors in the organization and its employees, and protection against the unpredictable occurrences of the natural world.

Kelvin Townsend (editor, Information Security Bulletin) mentioned on page 10 of the IMIS IT Security journal that people frequently asked him “What is the best security system to install?” And his answer is “The best security system is the one that allows you to fulfill your security policy.” He further said that “A formal security policy is the key to a secure system.”

Security is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security.

The word "security" in general usage is synonymous with "safety," but as a technical term "security" means that something not only *is secure* but that it *has been secured*. In telecommunications, the term security has the following meanings:

(a) A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.

(b) With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.

(c) Measures taken by a military unit, an activity or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (Sources: from Federal Standard 1037C and adapted from the Department of Defense Dictionary of Military and Associated Terms)

Security has to be compared and contrasted with other related concepts: Safety, continuity, reliability. The key difference between security and reliability is that security must take into account the actions of active malicious agents attempting to cause destruction.

Data Classification

Data Classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled / secured and is also indicative of its value in terms of Business Assets.

The classification of data and documents is essential if you are to differentiate between that which is a little (if any) value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level. For many organizations, a simple 5 scale grade will suffice as follows:-

Document / Data Classification	Description
Top Secret	Highly sensitive internal documents e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highest possible.
Highly Confidential	Information that, if made public or even shared around the organization, could seriously impede the organization’s operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants etc., patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization’s operational control without specific authority. Security at this level should be very high.
Proprietary	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level is high.
Internal Use only	Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.
Public Documents	Information in the public domain; annual reports, press statements etc.; which has been

	approved for public use. Security at this level is minimal.

Information Asset

An Information Asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization. The information which comprises an Information Asset may be little more than a prospect name and address file; or it may be the plans for the release of the latest in a range of products to compete with competitors.

Irrespective, the nature of the information assets themselves, they all have one or more of the following characteristics:-

- They are recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization’s corporate identity, without which, the organization may be threatened.
- Their Data Classification would normally be Proprietary, Highly Confidential or even Top Secret.

It is the purpose of Information Security to identify the threats against, the risks and the associated potential damage to, and the safeguarding of Information Assets.

Information Custodian

An Information Custodian is the person responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level classified by the Information Owner.

This could be the System Administrator, controlling access to a computer network; or a specific application program or even a standard filing cabinet.

Information Owner

The person who creates, or initiates the creation or storage of the information, is the initial owner. In an organization, possibly with divisions, departments and sections, the owner becomes the unit itself with the person responsible, being the designated 'head' of that unit.

The Information owner is responsible for ensuring that:

- An agreed classification hierarchy is agreed and that this is appropriate for the types of information processed for that business / unit.

- Classify all information stored into the agreed types and create an inventory (listing) of each type.
- For each document or file within each of the classification categories, append its agreed (confidentiality) classification. Its availability should be determined by the respective classification.
- Ensure that, for each classification type, the appropriate level of information security safeguards are available e.g. the logon controls and access permissions applied by the Information Custodian provide the required levels of confidentiality.
- Periodically, check to ensure that information continues to be classified appropriately and that the safeguards remain valid and operative.

Perceived security compared to real security

It is very often true that people's perception of security is not directly related to actual security. For example, a fear of flying is much more common than a fear of driving; however, driving is generally a much more dangerous form of transport.

Another side of this is a phenomenon called security theatre where ineffective security measures such as screening of airline passengers based on static databases are introduced with little real increase in security or even, according to the critics of one such measure - Computer Assisted Passenger Prescreening System - with an actual decrease in real security.

Chapter 2

Categorizing security

There is an immense literature on the analysis and categorization of security. Part of the reason for this is that, in most security systems, the "weakest link in the chain" is the most important. The situation is asymmetric since the defender must cover all points of attack while the attacker can simply identify a single weak point upon which to concentrate their efforts.

Types of security

The following are some major types of securities:

- international security
- national security
- physical security
- home security
- information security
- network security
- computing security
- application security
- financial security
- human security
- food security
- airport security
- shopping centre security
- humanitarian Security

Security concepts

Certain concepts recur throughout different fields of security.

- risk - a risk is a possible event which could cause a loss
- threat - a threat is a method of triggering a risk event that is dangerous
- countermeasure - a countermeasure is a way to stop a threat from triggering a risk event
- defense in depth - never rely on one single security measure alone
- assurance - assurance is the level of guarantee that a security system will behave as expected

Information security

Information security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Heads of state and military commanders have long understood the importance and necessity of protecting information about their military capabilities, number of troops and troop movements. Such information falling into the hands of the enemy could be disastrous. Governments, military, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. Should confidential information about a businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. For the individual, information security has a significant effect on Privacy, which is viewed very differently in different cultures.

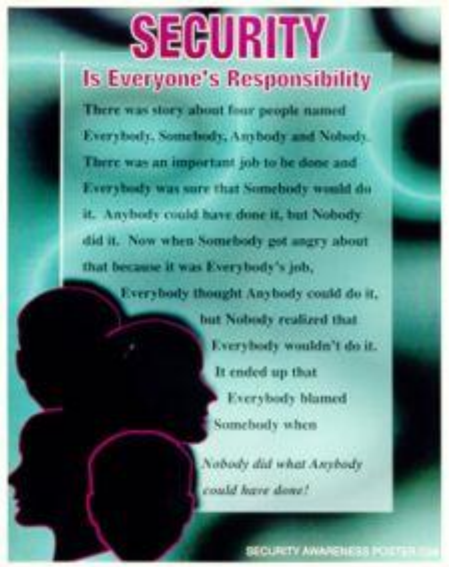
The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of gaining entry into the field. It offers many areas for specialization including Information Systems Auditing, Business Continuity Planning and Digital Forensics Science, to name a few.

This article presents a general overview of information security and its core concepts.

IT Security standards

- ISO/IEC 15443 A framework for IT security assurance (covering many methods, i.e. TCSEC, Common Criteria, ISO/IEC 17799)
    - ISO/IEC 15443-1: Overview and framework
    - ISO/IEC 15443-2: Assurance methods
    - [ISO/IEC 15443-3: Analysis of assurance methods (expected in 2007)]
- ISO/IEC 15408 refer also to Common Criteria
- ISO/IEC 17799:2005 Code of practice for information security management refer also to ISO/IEC 17799
- refer also to TCSEC Trusted Computer System Evaluation Criteria (Orange Book)

Information security



There was story about four people named Everybody, Somebody, Anybody and Nobody. There was an important job to be done and Everybody was sure that Somebody would do it. Anybody could have done it, but Nobody did it. Now when Somebody got angry about that because it was Everybody's job, Everybody thought Anybody could do it, but Nobody realized that Everybody wouldn't do it. It ended up that Everybody blamed Somebody when *Nobody did what Anybody could have done!*

Security is everyone's responsibility. Security awareness poster. U.S. Department of Commerce/Office of Security.

A brief history of Information Security

This write-up describes the earliest roots and key developments of what is now known as information security.

Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering. Persons desiring secure communications have used wax seals and other sealing devices since the early days of writing to signify the authenticity of documents, prevent tampering, and ensure confidentiality of correspondence.

Julius Caesar is credited with the invention of the Caesar cipher c50 B.C. to prevent his secret messages from being read should a message fall into the wrong hands.

World War II brought about much advancement in information security and may mark the beginning of information security as a professional field. WWII saw advancements in the physical protection of information with barricades and armed guards controlling access into information centers. It also saw the introduction of formalized classification of data based upon the sensitivity of the information and who could have access to the information. During WWII background checks were also conducted before granting clearance to classified information.

The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through a network generically called the Internet or World Wide Web.

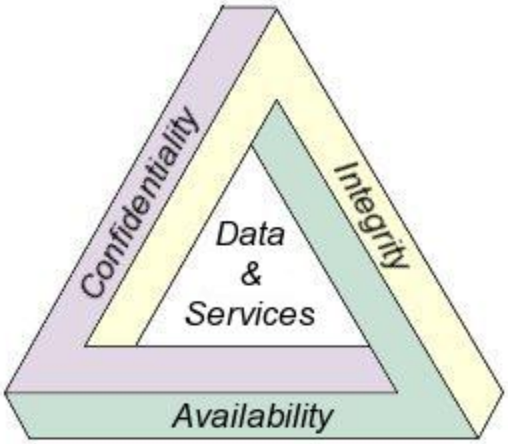
The rapid growth and wide spread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting these computers and the information they store, process and transmit. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations - all sharing the common goals of insuring the security and reliability of information systems.

Chapter 3

Basic principles of Information Security
Confidentiality, integrity, availability

For over twenty years information security has held that three key concepts form the core principles of information security: confidentiality, integrity and availability. These are known as the CIA Triad.

Confidentiality
It is virtually impossible to get a drivers license, rent an apartment, obtain medical care, or take out a loan without disclosing a great deal of very personal information about ourselves, such as our name, address, telephone number, date of birth, Social Security number, marital status, number of children, mother's maiden name, income, place of employment, medical history, etc. This is all very personal and private information, yet we are often required to provide such information in order to transact business. We generally take it on faith that the person, business, or institution to whom we disclose such personal information have taken measures to ensure that our information will be protected from unauthorized discloser, either accidental or intentional, and that our information will only be shared with other people, businesses or institutions who are authorized to have access to the information and who have a genuine need to know the information.



The CIA Triad.

Information that is considered to be confidential in nature must only be accessed, used, copied, or disclosed by persons who have been authorized to access, use, copy, or disclose the information, and then only when there is a genuine need to access, use, copy or disclose the information. A breach of confidentiality occurs when information that is considered to be confidential in nature has been, or may have been, accessed, used, copied, or disclosed to, or by, someone who was not authorized to have access to the information.

For example: permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it would be a breach of confidentiality if they were not authorized to have the information. If a laptop computer, which contains employment and benefit information about 100,000 employees, is stolen from a car (or is sold on eBay) could result in a breach of confidentiality because the information is now in the hands of someone who is not authorized to have it. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is a requisite for maintaining the privacy of the people whose personal information the organization holds.

Integrity

In information security, integrity means that data can not be created, changed, or deleted without authorization. It also means that data stored in one part of a database system is in agreement with other related data stored in another part of the database system (or another system). For example: a loss of integrity can occur when a database system is not properly shut down before maintenance is performed or the database server suddenly loses electrical power. A loss of integrity occurs when an employee accidentally, or with malicious intent, deletes important data files. A loss of integrity can occur if a computer virus is released onto the computer. A loss of integrity can occur when an on-line shopper is able to change the price of the product they are purchasing.

Availability

The concept of availability means that the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed. The opposite of availability is denial of service (DOS)

In 2002, Mr. Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. His alternative model includes confidentiality, possession or control, integrity, authenticity, availability, and utility. The merits of the Parkerian-hexad are a subject of debate amongst security professionals.

Risk management

A comprehensive treatment of the topic of risk management is beyond the scope of this article. We will however, provide a useful definition of risk management, outline a commonly used process for risk management, and define some basic terminology.

Breaching Organizational Security

A number of organizational security breaches can occur; some of these are amplified by the use of a database because of the integrated approach to data storage and retrieval. Some of these breaches and security issues include:

- Virus
- Unauthorized access (hacking)
- Industrial and/or individual sabotage
- Accidents by users (incompetence)

And in his analysis of some of the threats and risks to data, he mentioned the following:

Loss of access to your company data
Unproductive workforce
Viral infection
Theft of company secrets
Inadvertent law breaking

Security can be divided into a number of aspects:

(a) Prevention
(b) Detection
(c) Deterrence
(d) Recovery procedures
(e) Correction procedures
(f) Threat avoidance.

Crimes and instructions on automated information systems

Computer crime encompasses any unauthorized use of a computer system including software piracy or theft of system resources for personal use including computer processing time and network access time. It is also a crime to take any action intended to alter data programs or to damage or destroy data, software, or equipment. All these crimes are committed through intrusion, the forced and unauthorized entry into a system.

Computer crime through intrusion can occur in one of two ways, which is either by hackers break into a system to destroy the data or the network, or software viruses inserted into a system to destroy programs and data.

Software Piracy
Piracy is the act of making of illegal copies of copyright information, and software piracy is the making of illegal copies of software. This is one of the most serious issues in IT today because it is so widespread that it is responsible for an enormous loss of revenue to software originators.

Protections against Software Piracy
Software Copyright Protection: This is the legal protection of original works against unauthorized use, including duplication, provided the owner visibly displays a notice on the product. This method has been used for many yeas for the protection of books, magazines, music and other commercial original works, but today it also applies to computer software, database etc.

Copyright Protection: This is a software protection scheme that defeats attempts to copy a program or makes the copied software unreliable.

Software Site Licensing: This is an agreement under which a software purchaser pays a fee to the manufacturer to make a specified number of copies of a particular program.

Hackers

Hackers are people that attack/gain access into system/networks illegally to see what is there and mostly to destroy data for their profits, to be malicious or just because it is there. Hackers usually gain access to a system through a network, but sometimes they physically enter a computer or network facility.

Business people should always keep their intellectual property from the eyes of their competitors or hackers, because much of the data is very difficult and expensive to generate. Therefore if care is not taken loss or damages can put the individual out of business because networks are attack by morons. Consider what will happen when an enemy/hacker gains access to your network.

Network Security Measures Against Hackers

There are various ways and methods of protecting networks from dangers or hackers, and it is always very wise for not to rely on a single protection method and deploy them in layers designed so that an attacker has to defeat multiple defense mechanisms to perform a successful attack.

Below are some security measures that should be adhered to by all users of a network system:

Physical Access Control is the most basic level of security, but it is frequently forgotten. The most trivial way of stealing data or disrupting IT operations is to physically take or destroy pieces of equipment. Instead of spending more effort and resources securing your data against threats coming from the network, make sure to control physical access to critical servers and network infrastructure.

This involves the employing of security guards to monitor and guard the IT room/office so that nobody will have the direct access of stealing or damaging data or equipment and theft will not take place. Therefore the workplace should have tight security measure to prevent un-authorized people from invading the place. A padlock may be your most effective network security investment.

User authentication mechanisms are designed to uniquely identify users, assign their corresponding access rights to information, and track their activities. Workers should know that the security of the organization must not be compromised. User’s ID and passwords are the primary means of safeguarding organizational assets.

Authentication is usually performed by challenging the user to provide access keys (passwords, biometric information, tokens, ID cards, etc) and checking their access privileges against a RADIUS, LDAP or SLDAP database.

Data Encryption is the process of encoding data through a series of mathematical functions to prevent unauthorized parties from viewing or modifying it. It has the objective to protect the confidentiality and integrity of the information, even when the encrypted data is in transit over unsecured media such as the Internet.

Data encryption works so that only the recipient can decode the data using the decoding algorithm that is not necessarily secret and an encryption key that is secret.

Network Packet Filtering is performed at network level and can be performed at routers and gateways by analyzing headers of IP packets and allowing or denying forwarding based on source or destination address, protocol type, TCP port number, packet length, etc. This is useful to prevent access even before there is an attempt to authenticate or look at system data.

Firewalls are devices that perform packet filtering but look beyond the Internet Protocol headers and also analyze the packet payload for patterns to deny/allow user.

The use of Passwords on data or the entire computer system can act as a protection from unauthorized people. A password has to be keyed in to gain access to the data or computer system and this is made up of characters, numbers, or in an alphanumeric form and the password is issued only to people authorized to use the system and this should be changed frequently to keep the data secure.

It is not advisable to use the name of the company or the owner's name or his/her family name as a password because many people might know this and others might try this to gain access to the data.

Restricted Access (privileges) to different data areas can be set up so that only authorized users can gain access to certain data. In this case all the users may be able to access the company's files, but access to certain data will be restricted to certain members, and this is done through the use of additional passwords or by setting up the system so that only certain terminals can gain access to certain data.

Back Ups: This is the act of duplicating files so that incase of any accident such as loss of original file, there will be copies/duplicates of the original, and if possible this duplicate will not be kept in the computer system alone or at workplaces but there should be more secured places to keep it.

Computer Viruses

A virus is defined as a small computer program that is capable of copying itself from one computer to another, thus emulating a biological virus that infects new hosts. Viruses are almost always written with malicious intent, and may inflict damage ranging from temporarily corrupting the screen display or slowing down the computer operation, through deleting certain files, up to erasing the entire hard disk content.

In certain cases intrusions occurs by way of software. According to Wikipedia, "A computer virus is a hidden program that alters, without the user's knowledge the way the computer operates or modifies the data and programs stored on the computer." It is said to be a virus because it reproduces itself, passing from one computer to another, or it can also enter a computer when a file to which it attaches itself is being transferred to a remote computer through a communication network and an infected disk or diskette will continue to spread the virus each time it is used. Other viruses take control of the operating system and stop it from functioning.

The most dangerous viruses do not act immediately after infection but often lie dormant for a long period until it is triggered by some event; such as reaching a particular date (Friday the 13th is popular) or running a certain program.

Writing a virus is technically demanding, so they are always written for the most popular brands of computer, where there exists a reasonable chance that they will replicate. Historically they have been mainly confined to IBM – compatibles Personal Computers and the Apple Macintosh.

The first virus was probably the 1987 Lehigh virus, followed by the more widely infectious stoned, Jerusalem and Cascade viruses, all of which infected PCs running MS-DOS. These early viruses disseminated themselves via a floppy disk, copying themselves into the Boot Sector of the hard disk of any computer that was booted from that floppy. Their spread was exacerbated by the people taking floppy disks to work to play games, and exchanging pirated software on floppies. Once software became too big for floppies, this class of virus almost died out, as they can not infect the read-only Compact Disk – Read Only Memory (CD-ROM). Now almost all viruses are disseminated via the Internet, either by the down-loading of files that they have infected, or hidden in an attachment to an Email.

There are three main categories of virus:

(a) File viruses
(b) Script or Macro viruses
(c) Boot Sector viruses.

Protections against viruses

Scanning: This is a method by which virus-checking programs such as Norton Anti-virus searches disks and memory for known viruses.

Interception: This is a virus checking program that monitors processing, seeking to spot virus program in action.

Digital signature encryption: These are published programs that are encoded with mathematical key, making it difficult for virus to attack data or programs.

Health hazards & safety precautions associated with computer workplaces

Having a proper workplace and ensuring that workers enjoy the benefits a good and accident-free workplace is a good motivation for employees. It is very clear that a healthy and happy worker is more productive to any business. The key to designing a proper workplace for the knowledge worker is flexibility.

Computer operators/users are also covered by the health and safety act 1974. Therefore to comply with this act, employers are required to make sure that their places of work are safe environments. Issues related to the use of computers include the regular checking of all electrical equipment to make sure that it is safe to use.

It is also the duty of employees to undertake safe working practices and they are required to:

(a) Report any hazards relating to computers immediately and this could include trailing computer leads, loose wiring etc.
(b) Avoid lifting heavy equipments unless the individual is trained to do so.
(c) Take breaks at regular intervals.
(d) Maintain good posture when sitting at terminals.

Chapter 4

Risk Management

The CISA Review Manual 2006 provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

There are two things in this definition that may need some clarification. First, the process of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). Vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man made or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called residual risk.

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

The ISO-17799:2005 Code of practice for information security management recommends the following be examined during a risk assessment: security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, and regulatory compliance.

In broad terms the risk management process consists of:

(a) Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, and other), and supplies.

(b) Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, and malicious acts originating from inside or outside the organization.

(c) Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.

(d) Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernable loss of productivity.

For any given risk, Executive Management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or out-sourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk. This is itself a potential risk.

Three types of controls
When Management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls.

1. Administrative controls are comprised of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed - the Payment Card Industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.
Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

2. Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.
An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read Email and surf the Web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change,

or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

3. Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

An important physical control that is frequently overlooked is the separation of duties. Separation of duties ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator - these roles and responsibilities must be separated from one another.

Security classification for information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

Common information security classification labels used by the business sector are: public, sensitive, private, confidential. Common information security classification labels used by government are: unclassified, sensitive but unclassified, confidential, secret, top secret.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.[3]

Access control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

Identification is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is Festus Ajibuwa." Such a person is making a claim of who he is. However, his claim may or may not be true. Before Festus Ajibuwa can be granted access to protected information it will be necessary to verify that the person claiming to be Festus Ajibuwa is really Festus Ajibuwa.

Authentication is the act of verifying a claim of identity. When Festus Ajibuwa goes into a bank to make a withdrawal, he tells the bank teller he is Festus Ajibuwa (a claim of identity). The bank teller asks to see a photo ID, so he hands the teller his driver’s license. The bank teller checks the license to make sure it has Festus Ajibuwa printed on it and compares the photograph on the license against the person claiming to be Festus Ajibuwa. If the photo and name match the person, then the teller has authenticated that Festus Ajibuwa is who he claimed to be.

There are three different types of information that can be used for authentication: something you know, something you have, or something you are. Examples of something you know include such things as a PIN number, a password, or your mother’s maiden name. Examples of something *you have* include a driver’s license or a magnetic swipe card. Something you are refers to biometrics. Examples of biometrics include palm prints, finger prints, voice prints and retina (eye) scans. Strong authentication requires providing information from two of the three different types of authentication information. For example, something you know plus something you have. This is called two-factor authentication.

On computer systems in use today, the Username is the most common form of identification and the Password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called authorization.

Authorization to access information and other computing services begins with administrative policies and procedures. The polices prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies.

Different computing systems are equipped with different kinds of access control mechanisms; some may offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The discretionary approach gives the creator or owner of the information resource the ability to control access to those resources. In the Mandatory access control approach, access is granted or denied bases upon the security classification assigned to the information resource.

Examples of common access control mechanisms in use today include Role-based access control available in many advanced Database Management Systems, simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS, and the simple access lists used in many firewalls and routers.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held accountable for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail.

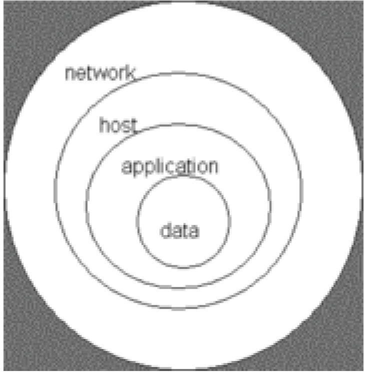
Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental discloser while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure application such as telnet and ftp are slowly being replaced with more secure applications such as SSH that use encrypted network communications. Wireless communications can be encrypted using the WPA protocol. Software applications such as GNUPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. PKI solutions address many of the problems that surround key management.

Defense in depth



Information security must protect information through out the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its life time, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defense in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the bases upon which to build a defense in depth strategy. With this approach, defense in depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense in depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people as the outer layer of the onion, and network security, host based security and applications security forming the inner layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense in depth strategy.

Chapter 5 - Analysis

Information security as a process

The terms reasonable and prudent person, due care and due diligence have been used in the fields of Finance, Securities, and Law for many years. In recent years these terms have found their way into the fields of computing and information security. U.S.A. Federal Sentencing Guidelines now make it possible to hold corporate officers liable for failing to exercise due care and due diligence in the management of their information systems.

In the business world, stockholders, customers, business partners and governments have the expectation that corporate officers will run the business in accordance with accepted business practices and in compliance with laws and other regulatory requirements. This is often described as the "reasonable and prudent person" rule. A prudent person takes due care to ensure that everything necessary is done to operate the business by sound business principles and in a legal ethical manner. A prudent person is also diligent (mindful, attentive, and ongoing) in their due care of the business.

In the field of Information Security, Harris offers the following definitions of due care and due diligence:

"Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees." And, [Due diligence are the] "continual activities that make sure the protection mechanisms are continually maintained and operational."

Attention should be made to two important points in these definitions. First, in due care, steps are taken to show - this means that the steps can be verified, measured, or even produce tangible artifacts. Second, in due diligence, there are continual activities - this means that people are actually doing things to monitor and maintain the protection mechanisms, and these activities are ongoing.

Change management

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made. It is not the objective of change management to prevent or hinder necessary changes from being implemented.

Any change to the information processing environment introduces an element of risk. Even apparently simple changes can have unexpected effects. One of Managements many responsibilities is the management of risk. Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented.

Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying new desktop computers are examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk to the processing environment and are not a normal everyday activity.

Change management is usually overseen by a Change Review Board comprised of representatives from key business areas, security, networking, systems administrators, Database administration, applications development, desktop support and the help desk. The tasks of the Change Review Board can be facilitated with the use of automated work flow application. The responsibility of the Change Review Board is to ensure the organizations documented change management procedures are followed. The change management process is as follows:

Requested: Anyone can request a change. The person making the change request may or may not be the same person that performs the analysis or implements the change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organization's business model and practices, and to determine the amount of resources needed to implement the change.

Approved: Management runs the business and controls the allocation of resources therefore; Management must approve requests for changes and assign a priority for every change. Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices. Management might also choose to reject a change request if the change requires more resources than can be allocated for the change.

Planned planning a change involves discovering the scope and impact of the proposed change; analyzing the complexity of the change; allocation of resources and, developing, testing and documenting an implementation plan.

Tested: Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment.

Scheduled: Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.

Communicated: Once a change has been scheduled it must be communicated. The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the Help Desk and users aware that a change is about to occur. Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.

Implemented: At the appointed date and time, the changes must be implemented. Part of the planning process was to develop an implementation plan, testing plan and, a back out plan. If the implementation of the change should fail or, the post implementation testing fails or, other "drop dead" criteria have been met, the back out plan should be implemented.

Documented: All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.

Post change review: The change review board should hold a post implementation review of changes. It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement.

Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment. Good change management procedures improve the over all quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication.

ISO/IEC 20000, Visible Ops and Information Technology Infrastructure Library all provide valuable guidance on implementing an efficient and effective change management program.

Laws and regulations governing Information Security

Below is a partial listing of European, United Kingdom, Canadian and USA governmental laws and regulations that have, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.

UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU members must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.

The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland, have drawn inspiration when subsequently drafting their own information security laws.

EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 g; 34 CFR Part 99) is a USA Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

Health Insurance Portability and Accountability Act (HIPAA) requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.

Gramm-Leach-Bliley Act of 1999(GLBA), also know as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.

Sarbanes-Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.

Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

State Security Breach Notification Laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.

Personal Information Protection and Electronics Document Act (PIPEDA) An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

Sources of standards for Information Security
International Organization for Standardization (ISO) is a consortium of national standards institutes from 157 countries with a Central Secretariat in Geneva Switzerland that coordinates the system. The ISO is the world's largest developer of standards. The ISO-15443: "Information technology - Security techniques - A framework for IT security assurance", ISO-17799: "Information technology - Security techniques - Code of practice for information security

management", ISO-20000: "Information technology - Service management", and ISO-27001: "Information technology - Security techniques - Information security management systems" are of particular interest to information security professionals.

The USA National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. The NIST Computer Security Division develops standards, metrics, tests and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the USA Federal Information Processing Standardpublications (FIPS)].

The Internet Society (ISOC) is a professional membership society with more than 100 organizations and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The Information Security Forum is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It provides research into best practice and practice advice summarized in its biannual Standard of Good Practice, incorporating detail specifications across many areas.

Sources of standards for Information Security

International Organization for Standardization (ISO) is a consortium of national standards institutes from 157 countries with a Central Secretariat in Geneva Switzerland that coordinates the system. The ISO is the world's largest developer of standards. The ISO-15443: "Information technology - Security techniques - A framework for IT security assurance", ISO-17799: "Information technology - Security techniques - Code of practice for information security management", ISO-20000: "Information technology - Service management", and ISO-27001: "Information technology - Security techniques - Information security management systems" are of particular interest to information security professionals.

The USA National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. The NIST Computer Security Division develops standards, metrics, tests and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the USA Federal Information Processing Standard publications (FIPS)].

The Internet Society (ISOC) is a professional membership society with more than 100 organizations and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet

Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

Protecting privacy in information systems

Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use. There are several technologies to address privacy protection in enterprise IT systems. These fall into two categories: communication and enforcement.

Policy Communication

- P3P - The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.
  Policy Enforcement
- XACML - The eXtensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.
- EPAL - The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

North America

Data privacy is not highly legislated or regulated in the U.S.. In the United States, access to private data is culturally acceptable in many cases, such as credit reports for employment or housing purposes. Although partial regulations exist, for instance the Children's Online Privacy Protection Act and HIPAA, there is no all-encompassing law regulating the use of personal data. The culture of free speech in the U.S. may be a reason for the reluctance to trust the government to protect personal information. In the U.S. the first amendment protects free speech and in many instances privacy conflicts with this amendment. In many countries privacy has been used as a tool to suppress free speech.

The safe harbor arrangement was developed by the US Department of Commerce in order to provide a means for US companies to demonstrate compliance with European Commission directives and thus to simplify relations between them and European businesses.

The Supreme Court interpreted the Constitution to grant a right of privacy to individuals in Griswold v. Connecticut. Very few states, however, recognize an individual's right to privacy, a notable exception being California. An inalienable right to privacy is enshrined in the California Constitution's article 1, section 1, and the California legislature has enacted several pieces of legislation aimed at protecting this right. The California Online Privacy Protection Act (OPPA) of 2003 requires operators of commercial web sites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site and to comply with its policy.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) went into effect in relation to federally regulated organizations on 1 January 2001, and in relation to all other organizations on 1 January 2004. It brings Canada into compliance with the requirements of the European Commission's directive. For more information, visit the website of the Privacy Commissioner of Canada. The text of the Act may be found at [1].

Europe

The right to data privacy is heavily regulated and rigidly enforced in Europe. Article 8 of the European Convention on Human Rights (ECHR) provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence. According to the Court's case law the collection of information by officials of the state about an individual without his consent always falls within the scope of article 8. Thus, gathering information for the official census, recording fingerprints and photographs in a police register, collecting medical data or details of personal expenditures and implementing a system of personal identification have been judged to raise data privacy issues. Any state interference with a person's privacy is only acceptable for the Court if three conditions are fulfilled:

(1) The interference is in accordance with the law
(2) Pursues a legitimate goal and
(3) Is necessary in a democratic society.
.

The government isn't the only one who might pose a threat to data privacy, far from it. Other citizens and private companies most importantly, engage in far more threatening activities, especially since the automated processing of data became widespread. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was concluded within the Council of Europe in 1981. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did.

As all the member states of the European Union are also signatories of the European Convention on Human Rights and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the European Commission was concerned that diverging data protection legislation would emerge and impede the free flow of data within the EU zone. Therefore the European Commission decided to harmonize data protection regulation and proposed the Directive on the protection of personal data, which member states had to transpose into law by the end of 1998.

The directive contains a number of key principles which must be complied with. Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', 'holding' and 'disclosing'. For more details on these data principles, read the article about the directive on the protection of personal data or visit the EU data protection page.

All EU member-states adopted legislation pursuant this directive or adapted their existing laws. Each country also has its own supervisory authority to monitor the level of protection.

- In the United Kingdom the Data Protection Act 1984 was repealed by the Data Protection Act 1998. For details, visit U.K. data protection page or read the article about the Information Commissioner
- France adapted its existing law (law no. 78-17 of 6 January 1978 concerning information technology, files and civil liberties).
- In Germany both the federal government and the states enacted legislation.

Safe Harbor Program

The US Department of Commerce created the Safe Harbor certification program in response to the 1995 Directive on Data Protection (Directive 95/46/EC) of the European Commission. Directive 95/46/EC declares in Chapter IV Article 25 that personal data may only be transferred from the EU to countries which provide a level of privacy protection equivalent to that of the EU. This introduced a legal risk to organizations which transfer the personal data of European citizens to servers in the USA. Such organizations could be penalized under EU laws if the privacy protection of the USA were to be deemed weaker than that of the EU. The Safe Harbor program addresses this issue. Under this program, the European Commission agreed to forbid European citizens from suing US companies for transmitting personal data into the USA. ICT

Data remanence

Data remanence is the residual physical representation of data that have been in some way erased. After storage media are erased there may be some physical characteristics that allow data to be reconstructed. As early as 1960 the problem caused by the retentive properties of computer storage media was recognized. It was known that without the application of data removal procedures, inadvertent disclosure of sensitive information was possible should the storage media be released into an uncontrolled environment. Degaussing, overwriting, data encryption, and media destruction are some of the methods that have been employed to safeguard against disclosure of sensitive information. Over a period of time, certain practices have been accepted for the clearing and purging of storage media.

Data theft

Data theft is a growing problem primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices, since employees often spend a considerable amount of time developing contacts and confidential and copyrighted information for the company they work for they often feel they have some right to the information and are inclined to copy and/or delete part of it when they leave the company, or misuse it while they are still in employment.

While most organizations have implemented firewalls and intrusion-detection systems very few take into account the threat from the average employee that copies proprietary data for personal gain or use by another company. A common scenario is where a sales person makes a copy of the contact database for use in their next job. Typically this is a clear violation of their terms of employment.

The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices. Removable media devices are getting smaller with increased hard drive capacity, and activities such as podslurping are becoming more and more common. It is now possible to store 80 GB of data on a device that will fit in an employee's pocket, data that could contribute to the downfall of a business.

Types of data theft

Thumbsucking

Thumbsucking, similar to podslurping, is the intentional or unintentional use of a portable USB mass storage device, such as a USB flash drive (or "thumbdrive"), to illicitly download confidential data from a network endpoint.[1]

The moniker is derived from the act of downloading, or "sucking", data from a network endpoint onto a USB flash drive or similar storage device.

A USB flash drive was allegedly used to remove without authorization highly-classified documents about the design of U.S. nuclear weapons from a vault at Los Alamos.[2]

The threat of thumbsucking has been amplified for a number of reasons, including the following:

- The storage capacity of portable USB storage devices has increased.
- The cost of high-capacity portable USB storage devices has decreased.
- Networks have grown more dispersed, the number of remote network access points has increased and methods of network connection have expanded, increasing the number of vectors for network infiltration.

Database security

Database security is the system, processes, and procedures that protect a database from unintended activity. Unintended activity can be categorized as authenticated misuse, malicious attacks or inadvertent mistakes made by authorized individuals or processes. Database Security is also a specialty within the broader discipline of computer security.

Traditionally databases have been protected from external connections by firewalls or routers on the network perimeter with the database environment existing on the internal network opposed to being located within a demilitarized zone. Additional network security devices that detect and alert on malicious database protocol traffic include network intrusion detection systems along with host-based intrusion detection systems.

Database security is more critical as networks have become more open.

Databases provide many layers and types of information security including:

- Access control
- Auditing
- Authentication
- Encryption
- Integrity controls

Database security can begin with the process of creation and publishing of appropriate security standards for the database environment. The standards may include specific controls for the various relevant database platforms; a set of best practices that cross over the platforms; and linkages of the standards to higher level polices and governmental regulations.

An important procedure when evaluating database security is performing vulnerability assessments against the database. A vulnerability assessment attempts to find vulnerability holes that could be used to break into the database. Database administrators or information security administrators run vulnerability scans on databases to discover misconfiguration of controls within the layers mentioned above along with known vulnerabilities within the database software. The results of the scans should be used to harden the database in order to mitigate the threat of compromise by intruders.

A program of continual monitoring for compliance with database security standards is another important task for mission critical database environments. Two crucial aspects of database security compliance include patch management and the review and management of permissions (especially public) granted to objects within the database. Database objects may include table or other objects listed in the Table link. The permissions granted for SQL language commands on objects are considered in this process. One should note that compliance monitoring is similar to vulnerability assessment with the key difference that the results of vulnerability assessments generally drive the security standards that lead to the continuous monitoring program. Essentially, vulnerability assessment is a preliminary procedure to determine risk where a compliance program is the process of on-going risk assessment.

The compliance program should take into consideration any dependencies at the application software level as changes at the database level may have effects on the application software or the application server. In direct relation to this topic is that of application security.

Application level authentication and authorization mechanisms should be considered as an effective means of providing abstraction from the database layer. The primary benefit of abstraction is that of a single sign-on capability across multiple databases and database platforms. A Single sign-on system should store the database user's credentials (login id and password), and authenticate to the database on behalf of the user.

Another security layer of a more sophisticated nature includes the real-time monitoring of database protocol traffic (SQL) over the network. Analysis can be performed on the traffic for known exploits or network traffic baselines can be captured overtime to build a normal pattern used for detection of anomalous activity that could be indicative of intrusion. These systems can provide a comprehensive Database audit trail in addition to the intrusion detection (and potentially protection) mechanisms.

When a network level audit system is not feasible a native database audit program should be instituted. The native audit trails should be extracted on a regular basis and transferred to a designated security system where the database administrators do not have access. This ensures a certain level of segregation of duties that may provide evidence the native audit trails were not modified by authenticated administrators. Generally, the native audit trails of databases do not provide sufficient controls to enforce separation of duties; therefore, the network and/or kernel module level host based monitoring capabilities provides a higher degree of confidence for forensics and preservation of evidence.

After an incident occurs, the usage of Database Forensics can be employed to determine the scope.

A Database Security program should include the regular review of permissions granted to individually owned accounts and accounts used by automated processes. The accounts used by automated processes should have appropriate controls around password storage such as sufficient encryption and access controls to reduce the risk of compromise. For individual accounts, a two-factor authentication system should be considered in a database environment where the risk is commensurate with the expenditure for such an authentication system.

In conjunction with a sound Database Security program, an appropriate disaster recovery program should exist to ensure that service is not interrupted during a security incident or any other incident that results in an outage of the primary database environment. An example is that of replication for the primary databases to sites located in different geographical regions.

Data and Computer Security – A case study of Carnegie Mellon University
(Confidentiality of Administrative Data)
Policy Statement

Access to data residing in administrative systems and applications at Carnegie Mellon University is to be granted only to those individuals who must, in the course of exercising their responsibilities, use the specific information. Access to administrative data will be granted to university employees only. With special permission, a student may access data if the data pertains to that student or if that student is also an employee of the university. Individuals outside the university can be authorized access to university data only if that authorization is granted by an Executive Officer of the university.

Access and update capabilities/restrictions will apply to all administrative data, data stored on the Administrative Computing and Information Services (ACIS) computers and on mini-computers and micro-computers across campus. Security measures apply to administrative systems developed and/or maintained by university departments or outside vendors.

This policy only covers administrative aspects of academic and research units.

Reason for Policy

Carnegie Mellon University maintains data which are essential to performing university business. These data are to be viewed as valued resources over which the university has both rights and obligations to manage, secure, protect, and control. This policy secures and protects data defined as administrative data stored in and accessible by university-owned computing systems and accessible by university employees in their official university capacities. In addition, this policy addresses the broader data issues of the rights and responsibilities of authorized persons in the handling, as well as the security and protection, of university data.

Who Does This Policy Apply To?

- Employees
- Alumnae(i)
- Students with special permission

- Trustees
- Authorized persons with interests in:
  - University Finances
  - Education/Instruction
  - Research
  - University Facilities
  - Employee Data
  - Student/Alumni Data

Security Administration

Ownership of Administrative Data

In order to control access and update capabilities, an individual residing in the user area responsible for the specific application will be designated as the Data Owner. This individual performs in a supervisory or managerial capacity and is responsible for the data residing in the designated system. The responsibilities of the Data Owner are to:

- Ensure proper operating controls over the application in order to maintain a secure processing environment;
- Ensure accuracy and quality of data residing in application;
- Approve all requests for access to and update capability for the specific application;
- Ensure system issues impacting the quality of data within the system are properly reported and adequately resolved.

On an annual basis, the Data Owner and the Data Security Officer will review the current set of access and update capabilities granted to each individual on the system in order to ensure that no changes are necessary.

Stewardship of Administrative Data

In addition to the Data Owner, others will process and handle data in the course of the administrative cycle. They too will be responsible for the security of the data. These individuals and divisions include:

Data Security Officer

The Data Security Officer is responsible for all systems-related security issues associated with a particular application. A Data Security Officer will be appointed by the Assistant Vice President, ACIS, for each application and will act as the contact person for establishing, altering or deleting computer user ids and determining data access needs within a system.

Administrative Computing and Information Services (ACIS)

Administrative Computing and Information Services is responsible for the design, programming and maintenance of administrative applications. In designing or updating systems, Administrative Computing and Information Services must be aware of any security impacts of such designs and ensure that proper security control is programmed into each application to provide a secure computing environment and adequate protection of data. The Data Security Officer must convey application-specific security needs to the Assistant Vice President, ACIS.

Computing Systems

Computing Services maintains and operates the equipment upon which most central server administrative applications reside. It is the responsibility of Computing Services to ensure adequate physical security over such equipment, restrict equipment access to authorized personnel only, and adequately assure that output containing confidential information is properly safeguarded. Responsibilities also include maintenance of operating system-level security specific to the computing equipment under their jurisdiction.

Administrative Computing Security Committee

The Administrative Computing Security Committee is responsible for the maintenance of a secure administrative processing environment at Carnegie Mellon. The committee formulates overall policy, addresses issues impacting computer security, and reviews situations involving violations of computer security policy.

Data Accessibility

Because different types of data require different levels of security, data is classified into four categories: Public Information, Campus-Wide Information, Restricted Information - Moderately Sensitive, and Restricted Information - Highly Sensitive. Each category is explained below. For detailed examples of accessibility by data type, see the Appendix, Table 2.

Public Information is available or distributed to the general public either regularly or upon request.

Computing Security Procedures

Establishing Minimum Security Measures

Operating Systems

Operating Systems used for administrative computing will provide for, at a minimum, the following security features:

- Discretionary access controls, where individual users can be included/excluded from accessing files and other objects or from achieving certain forms of access (READ, WRITE, EXECUTE, DELETE, CONTROL).
- Prevention of disk scavenging (obtaining disk space that contains another user's data).
- Notification to the data owner/computer operator/data security officer of security breaches (unauthorized attempts to access certain files or the system). Maintenance of an audit record of security events, as well as authorized or unauthorized files access.
- Ability to audit changes to user id files and mounts/dismounts of disks and tapes.
- Ability for idle terminals logged into applications to be disconnected after a 15-minute period.
- An encryption system to provide a high level of security for sensitive data transmission files.
- Login features such as
    - Automatic disconnection on multiple login failures
    - Break-in detection and disabling user ids for a period of time after detection
    - Automatic id expiration - Access restrictions based on user id, time of day and day of week
    - Control over dial-up or network access to restricted data and systems

Database Management Systems

Database management software used in administrative application development will have the following features:

- Ability to designate the database "private" or "public"
- Access capabilities which can be restricted at the table and field levels

- Access capabilities which can be restricted based on user, time of day, day of week
- Audit trails/journals which record important system activity
- Control checkpoints

Applications

Applications developed in-house or purchased from a third party will be examined to determine:

- Security features used by the software (such as secondary passwords, captive user ids, etc.)
- Security enhancements or improvements needed to meet acceptable security levels.
- Interaction with other systems and related security implications.

The Data Security Officer and Administrative Computing and Information Services should examine application-level security on a system-by-system basis. Because of the complex interaction with other applications, the operating system, the underlying databases, as well as the needs of the user community and the nature of the data, there are many intervening factors which preclude an overall policy for application-level security. The security features of any new software will always be considered a priority in the selection and development of such software.

Network

Interactive access to applications occurs in many ways, e.g.:

- Terminal attachment to systems via a local area network
- Direct attachment to the serial lines
- Internet or web-based access

Terminals attached via networks are susceptible to monitoring and their passwords are insecure. Any local area network must be physically secure and is the responsibility of each person authorized to access administrative information to ensure the physical security of the local area network on which they operate. The login process should transmit only encrypted passwords across the network. Unauthorized persons shall not be permitted to access portions of the networks being used for transmitting university administrative data.

Periodic review and correction of network security weaknesses are undertaken jointly by the Administrative Computing and Information Services (ACIS) Department and the Data Communications Department of the Division of Computing Services. All weaknesses and security breaches will be reviewed by the Assistant Vice President, ACIS.

Establishing Backup and Recovery Procedures

Backup and recovery procedures must be developed and maintained for all administrative computing systems and data. The following requirements must be met:

- Provisions for regular backup of data residing on the system.
- Storage of backup media at a location remote from the processing center.
- Approved Disaster Recovery Plan written and implemented to cover situations in which hardware and/or software cannot run in its normal environment.

The Data Security Officer should periodically review backup and recovery procedures to ensure their continued applicability.

Protecting and Managing Passwords

Passwords are a critical component to any computer security program. To properly control passwords and maintain their integrity, the guidelines below will be followed:

- Passwords will automatically expire every 90 days, or more frequently in cases of user ids with access to very sensitive data.
- Users must never give out their personal password to anyone; sharing of passwords is a violation of this policy.
- As part of the educational process, the Data Security Officer will provide users with guidelines for selecting and changing their passwords.
- A password monitoring program will run weekly to check for insecure passwords. For example, the program would check to see if the user's first, last or middle name, user id, or other common words like "system," are used as passwords. If a user is found to have an insecure password, the program will notify them to change it. If the password has not been changed within one week, the user will again be notified, and the Data Security Officer will also be notified.

Generic user ids will not exist, except as the source for the production, maintenance, and development of application systems. In cases where many people log in under a single user id, audit trails and system statistics become ineffective in assigning responsibility.

Appropriate operating system security alarms will be activated, and available auditing tools will be in use.

Managing Systems for Employee Turnover

When an employee terminates employment with a department or the university, follow the guidelines below.

- Immediately change or remove the passwords for those user ids to which an employee leaving the university has had access or update capabilities. This standard practice serves to protect the employee in the event of any problems and the university systems against possible tampering. Monitoring such user ids is primarily the responsibility of user area management, with assistance from the Data Owner and the Data Security Officer.
- When an employee's termination is processed by the Human Resource Information System, the Computer Billing System will automatically receive notification. Upon receiving this notification, the user id will be suspended, and the Data Security Officer will be alerted so that any necessary files may be retrieved and the user id is deleted. Reinstatement will require the same level of authorization as establishing a new user id.

User Security Procedures

Requesting Authorization for Administrative Data Access Capabilities

If you wish to gain access to administrative data, follow the steps below:

1. Complete a Request for Data Access form. Make sure that you and your immediate supervisor have signed the form. This form certifies that access to the specific application or data sets is related to the completion of your work responsibilities.
2. Send the form to the Data Owner who reviews the form and evaluates the request with respect to the data that will be made available.

If your request is approved by the Data Owner

1. The Data Owner signs the form as evidence of approval.
2. The form is forwarded to the Data Security Officer.

3. The Data Security Officer reviews the form and ensures that the action to be taken will not breach data security from a systems perspective. The Data Security Officer is also responsible for identifying the most appropriate method of granting your request.

4. Upon approving the request, the Data Security Officer will initiate the proper action through either the Accounts Coordinator or Administrative Computing and Information Services to physically set up your user id on the specific system and/or application.

5. Once this process has been completed, you will receive a new user id and password, along with the original request form and any necessary instructions.

If your request is denied by the Data Owner or the Data Security Officer

1. The form will be returned to you with an explanation of the reason(s) for rejection.
2. If you have been denied access, you may appeal to the Administrative Computing Security Committee for review. The judgment of the committee is final in all cases.

Requesting Access to Restricted Information

1. Requests for access to restricted information for a department or a division must be authorized by the applicable department head and dean/division head.
2. Requests for access to information for multiple divisions or university-wide must be signed by the provost or appropriate vice president. Authorization is to be granted to employees who have job responsibilities requiring the information requested.
3. State whether you require one-time access or continual access.

Requesting Authorization for Administrative Data Update Capabilities

Sometimes when you request authorization to access data, you may also want to request the ability to update data within an administrative application. The responsibility for approving such capabilities rests solely with the Data Owner. In general, such update capabilities are to be limited to individuals working in the organizational area(s) supported by the specific application or system, e.g. only Payroll Office and Benefits Office staff members may update data within the Human Resource Information System. It is important to emphasize that data update capabilities will be limited to those who require the capabilities to successfully meet their job responsibilities.

The Data Security Officer ensures that update capabilities are made available only to authorized users and that data not authorized for update will be satisfactorily protected.

When new applications are being developed or significant changes are being made to existing systems, general guidelines will be established to define who should have data update capabilities.

Distributing Administrative Information

Just as care must be exercised in granting access or update capabilities to administrative data/systems, such care must also be extended to the distribution of administrative information generated by the university's administrative systems.

The Data Owner is responsible for determining:

- Which data within administrative systems are appropriate for distribution.

- The audience for distribution.
- The methods and timing of distribution.

The Data Owner must ensure that:

- The information distributed is in compliance with any regulatory requirement (e.g., Buckley amendment) or university policy (e.g., employee salaries are not made available to the public).
- The distribution methods or non-system data storage (i.e., paper or diskettes) provide adequate security over the information contained on the particular media.

The Data Security Officer provides assistance in coordinating security measures over data distribution with Computing Systems and Administrative Computing and Information Services personnel.

Maintaining Confidentiality of Restricted Data

In the course of accessing data or information, you might access restricted information within the particular database. It is the responsibility of the Data Owner to ensure that all individuals with access to restricted data are aware of the confidential nature of the information and the limitations, in terms of disclosure, that apply.

- When accessing restricted information, you are responsible for maintaining its confidentiality. The granting of a user id and password assumes that you will maintain confidentiality over appropriate information without exception.
- The release of restricted data without the express approval of the Data Owner or outside the guidelines established for such data will not be tolerated.
- Unauthorized release of restricted information will result in appropriate disciplinary action, including possible dismissal. All matters involving university employees will be reviewed with the assistant vice president for human resources and/or the provost. Matters involving students will be reviewed with the dean of student affairs. Matters involving individuals not affiliated with the university will be reviewed with the university attorney.

Reporting Data Security Breaches

If you are aware of possible breaches in administrative data/computer security, you are strongly encouraged to report such occurrences to the Assistant Vice President, ACIS. Such reports will be held in strict confidence and promptly investigated by the committee. Likewise, Data Owners and Data Security Officers are responsible for reporting security breaches identified during the course of their responsibilities to the Administrative Computing Security Committee.

Upon notification of possible security breaches, the Administrative Computing Security Committee will investigate all facts related to the situation and recommend appropriate disciplinary action to university management. All matters involving university employees will be reviewed with the assistant vice president for human resources and/or the provost. Matters involving students will be reviewed with the dean of student affairs. Matters involving individuals not affiliated with the university will be reviewed with the university attorney.

Enforcing Penalties for Unauthorized Data Access or Disclosure (Unfortunately this body has not been set up here in Gambia)

All individuals with responsibility over or access to administrative data at Carnegie Mellon are expected to follow the policies and procedures in this document and to exercise discretion with regard to such information. Any university employee, student or non-university individual with access to administrative data who engages in unauthorized use, disclosure, alteration or destruction of data in violation of this policy will be subject to appropriate disciplinary action, including possible dismissal and/or legal action. The following steps will be taken:

1. Upon the identification of a potential breach of security or a misuse of information, the Administrative Computing Security Committee will meet to review the specific situation.
2. The Committee will present a recommendation to university management for action. All matters involving university employees will be reviewed with the assistant vice president of human resources and/or the provost. Matters involving students will be reviewed with the dean of student affairs. Matters involving individuals not affiliated with the university will be reviewed with the university attorney.

Responsibilities

The following shows the responsibilities each party has in connection with this policy.

You (individual requesting access)

- Complete Request for Data Access form.
- Get required signatures for form.
- Use system, application and data responsibly.
- Maintain data confidentiality of restricted data.
- Report incidents of possible security breaches.

Administrative Computing Security Committee

- Reports to the Administrative Computing and Information Services Executive Steering Committee.
- Ensures maintenance of a secure processing environment.
- Recommends university policy regarding administrative data and computer security.
- Addresses issues impacting computer security.
- Reviews situations involving violations of computer security policy.

Administrative Computing and Information Services

- Designs, programs, tests, and/or maintains administrative applications.
- Analyzes security impacts of programs.
- Ensures that proper control is built within a system to provide a secure computing environment and to protect data.

Assistant Vice president, ACIS

- Appoints and/or approves Data Security Officers.

Computing Systems

- Operates the equipment on which most of the administrative applications reside.
- Ensures adequate physical security over the equipment.
- Ensures proper processing of administrative applications within user-established timetables.
- Assures that output containing restricted information is properly safeguarded.

- Maintains security at operating system level specific to the various types of machinery.

Data Owner

- Determines what data are appropriate for distribution and update.
- Ensures proper operating controls over the application to maintain a secure processing environment.
- Ensures accuracy and quality of data residing in application.
- Approves all requests for access to and update capability for the specific application.
- Ensures system issues impacting the quality of data within the system are properly reported and adequately resolved.
- Reviews annually, in conjunction with the Data Security Officer, the current set of access capabilities granted to all individuals on the system to ensure that the status is current and accurate and that no changes are necessary.

Data Security Officer

- Evaluates and controls all system access.
- Acts as contact person for the establishment, alteration or deletion of computer user ids and data access needs within a system.
- Evaluates and resolves all systems-related security issues for a particular application.
- Provides guidelines for system security, e.g., changing passwords.
- Reviews annually, in conjunction with Data Owner, the current set of access capabilities granted to all individuals on the system.

Department Head/Supervisor

- Communicates specific security needs to Administrative Computing and Information Services.
- Communicates employee terminations and status changes immediately to Data Security Officer to ensure proper deletion/revision of user ids, access and update capabilities to administrative applications.

Chapter 6

Conclusion

All organizations require information for planning, controlling, recording transactions, performance measurement and decision-making. And such Information whether internal or external must be kept properly and well protected from intruders, hackers and unauthorized individuals.

Organizations across the globe in every industry sector are under increasing pressure and scrutiny to maintain the security and integrity of their data. Companies are faced with an enormous liability if sensitive, business critical, or confidential information gets into the wrong hands.

The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of gaining entry into the field. It offers many areas for specialization including Information Systems Auditing, Business Continuity Planning and Digital Forensics Science, to name a few.

Although information security has traditionally been the responsibility of IT departments, some companies have made it a business issue as well as a technological one. Companies are now adding strategic, operational, and organizational safeguards to the technological measures they currently employ to protect corporate information. But most companies continue to view information security as a technological problem calling for technological solutions even though technology managers concede that today’s networks cannot be made impenetrable and that new security technologies have a short life span as hackers quickly devise ways around them. Delegating security to technologists also ignores fundamental questions that only business managers can answer. Not all of a company’s varied information assets have equal value, for instance; some require more attention than others. One on-line retailer, Egghead.com, lost 25 percent of its stock market value in December 2000, when hackers struck its customer information systems and gained access to 3.7 million credit card numbers. Egghead, of course, had security systems in place and claimed that no data were actually stolen, but it lacked the kind of coordinated organizational response necessary to convince customers and shareholders that their sensitive data were actually secure.

Information security means the appropriate protection of information, systems, services and data communications by administrative, technical and other measures both in ordinary and exceptional circumstances. The confidentiality, integrity and availability of information is protected against threats and damage caused by faults in hardware and software, natural events and willful, negligent or accidental events.

The central concepts of information security have the following meanings: Confidentiality: information and systems are accessible only to those authorized to use them. Third parties are not given a possibility to alter or destroy information nor to process it otherwise.

Integrity: information and systems are reliable, correct and up-to-date and they have not been altered nor can they be altered in an uncontrolled way as a result of hardware or software faults, natural events or human activities.

Availability: information and services in the systems are accessible to those entitled to use them within a response time determined in advance. The information has not been destroyed nor can it be destroyed as a result of faults, events or other operations.

Other general requirements of information security include the verification of the parties and the non-repudiation of a transaction, which are especially important when it must be possible to identify the users of the system for example for interactive electronic communications or remote work. (Authentication means reliable identification of the parties (person or system)). (Non-repudiation means subsequent legally binding proof of what has happened).
Non-repudiation ensures that the other party cannot deny its actions afterwards.

The operations of public administration are extremely dependent on data and information technology. Information society development, internationalization, networking and the transfer of operations and services to data networks further enhance their significance. Information security is the means to ensure the management of important information and the continuity of operations. Information security is also important because public administration processes a lot of important information, such as personal data, financial information and documents of various organizations. Some of the information has to be kept secret or it is sensitive or otherwise confidential. Information to be kept secret means documents and information provided secret by the law. Secrecy is governed by the Act on the Openness of Government Activities, the Personal Data Act and other special Acts. Certain documents of the authorities to be kept secret are governed by a security classification. Therefore it is important that the information does not, willfully or otherwise, end up in the hands of unauthorized parties.

In addition, public administration involves a lot of information that is not to be kept secret but which is public in nature, but we must ensure that also this information is correct, unaltered and accessible and processed according to the law.

Sensitive Data Protection

Data Encryption

Approximately $20 billion per year is spent on IT security by enterprises worldwide; however, costly breaches such as devastating thefts of sensitive data continue to occur. In large part, the expanding loss of sensitive data can be attributed to security efforts mainly concentrating on network security rather than data privacy.

Until recently, the industry has seen network security primarily in terms of the defenses deployed against external threats. However such security infrastructure is beginning to struggle to keep up with the evolution of organizational working behaviors and advancing privacy of information threats.

Common data security problems faced by government and industry include:

- Perimeter security, consisting of firewalls, intrusion detection systems (IDS) and anti virus measures, form the 'Front Line' of tools used to create a trusted network. Such security infrastructure provides little protection for data at the asset level against the risk of a savvy hacker breaking through the firewall into the organizations network and gaining access to unprotected data.

- The loss of a laptop computer equates to the enterprise having to deal with more than just the cost of the device. Reputable industry analysts such as Gartner and IDC estimate the loss of a laptop computer, on average, costs the organization around US $35,000 in lost sensitive data.
- Recent analysis by numerous high profile industry research organizations (Gartner, IDC) have identified internal staff pose 80% of the threat to organizations confidential information, with external threats constituting 20%. The increased work practice of saving data centrally on file servers and databases, multi-site network connected workstations and laptops, outsourced storage providers, plus the growing use of mobile data storage media, has escalated internal digital asset security risks
- The encryption of data files stored on network file servers and workstations often impose restrictions on user access and can reduce employee productivity.

Common sensitive data related risks imposed on organizations include (to mention a few):

- Loss of corporate strategy secrets and R&D information for instance, can cost an organization first mover advantage.
- The exposure of personal information of customers and employees can violate civil and criminal privacy laws in many regions of the globe. Such legislated acts include Gramm-Leach-Bliley Act, The Australian Federal Privacy Act 1998, the European Data Protection Directive, plus others.
- The risk to a company's public image is heightened by the ease of which internal and external threats can access sensitive company information.
- Financial penalties and damage to an organization's public image if authenticity of financial information is compromised, as governed by corporate accounting regulations such as Sarbanes Oxley section 404.
- The vulnerability of sensitive information stored within an Application Service Provider (ASP) external data storage facility. This includes the risks of who can gain access, plus the susceptibility of data traffic traversing the non-secure Internet between the outsourced external server and the client device within the organization.

Data encryption delivers the ultimate level of defense to assist protection against the above, and many other threats.

Hackers and data thieves, whom are savvy enough to penetrate the strongest levels of perimeter security, still face the ultimate challenge of deciphering the encryption algorithm to unlock the encrypted data. This additional layer of defense, utilizing industry proven encryption algorithms to protect asset level data at rest, is virtually impossible to break.

Disk encryption encrypts the entire hard drive of a laptop, workstation and server, to protect against disclosure of its information in the case of theft, accidental loss, or disposal of the hardware device.

File Encryption with cryptographically endorsed access control, encrypts files and folders of confidential information within network connected servers, workstations and laptops. Access rights to encrypted files and folders can be easily managed for individuals and groups within the organization. This ensures that sensitive electronic information remains confidential against both internal and external threats of loss, theft and unauthorized exposure. Only those identities with authenticated access have the ability to read, write and modify the applicable files. As encryption and decryption is undertaken on the client, data files traveling the LAN and unprotected WAN (e.g. between outsourced external servers or remote users), are secured against the threat of unauthorized exposure.

Portable media encryption enables secure, encrypted transfer and storage of confidential data files on unprotected mediums (local, portable and on the network) that are difficult to defend by conventional network mechanisms employed within perimeter security. This includes data transferred via a portable USB drive, burnt to a CD or DVD, via email, plus any other of today's or tomorrow's file mobility technology.

Each of the Eracom Technologies data encryption products, ProtectDrive, ProtectFile and ProtectPack, are a robust solution for the protection of electronic information where confidentiality is imperative. When used in combination, this range of data encryption products can provide a heightened level of security. The 'Protect' family of data encryption products is designed specifically for medium to large organizations to uniquely address the industry needs for data integrity, confidentiality and controlled availability.

Solutions

ATM/EFTPOS Transactions

ATM and EFTPOS applications have grown enormously, with rapid acceptance and adoption by users of the magnetic stripe card and more recently the smart card. As more transactions take place over unsecured networks, there is a huge exposure and increasing threat of disclosure of PINs and fraudulent transactions.

Magnetic stripe card standards have evolved from single DES based systems to triple DES based systems to increase the strength of the cryptography to prevent possible attacks. There is also an increasing need to introduce smart card based systems such as EMV to replace magnetic stripe cards.

The use of hardware security modules (HSMs) in ATM and EFTPOS network environments is a widely accepted industrial practice and is mandated by major institutions such as Visa and MasterCard.

Eracom Technologies' HSM product family provides cryptographic services for ATM and EFTPOS applications. The cryptography used by these systems protects transactions and authenticates terminals and other nodes to protect PINs as they travel across global networks for verification by the issuing institutions.

Eracom' Technologies' HSMs fully support the requirements for EFTPOS processing for magnetic stripe card with DES and Triple DES. They also support EMV smart card transactions.

Card Management

To meet the increasing regulatory requirements for stronger user authentication for electronic transactions, major financial bodies have adopted smart card systems. With this increasing use of smart card technologies by financial institutions and large organizations, there is a growing need for centralized and secure management capability to maintain large volumes of cards.

The main functions of card management systems are:

- Card personalization such as private user information, secret / private keys and public certificates
- Certificate generation for injection into smart cards

The requirements for such systems include:

- High availability – no tolerance to stoppage of automated card processing equipment
- High speed or throughput of key generation
- High security

To achieve this it is necessary to integrate card management systems with hardware security modules (HSMs) to deliver the required level of security and performance. As a pioneer and leader in cryptographic technologies, Eracom Technologies' HSMs have been certified to FIPS 140-1 Level 3 to ensure the highest level of security for these functions.

PKCS#11/Cryptoki

Public Key Cryptography Standard (PKCS) is a suite of specifications developed by RSA Security in conjunction with system developers worldwide for the purpose of accelerating the deployment of public key cryptography.

PKCS#11 (also known as Cryptoki) is the specification for the cryptographic token interface standard. It defines a technology independent programming interface for cryptographic applications such as smart cards, PIN authentication and validation, certificate generation and management, and for the support of emerging crypto services.

Eracom Technologies has been actively involved in the definition, development and implementation of PKCS#11 (Cryptoki) standard by participating in standards committees and promoting its adoption in government, banking & financial institutions, defense and other major IT security sectors.

Eracom Technologies Solution

Eracom Technologies' ProtectToolkit C is the industry leading implementation and product category of PKCS#11 (Cryptoki) specifications. ProtectToolkit C provides an open interface to work with various application providers. It is supported by the following Eracom Technologies' Hardware Security Modules (HSMs):

- ProtectHost Orange
- ProtectServer Gold

- ProtectServer Orange

JCA/JCE

Java Cryptography Architecture (JCA) is defined by Sun Microsystems to introduce a core API of the Java programming language. This security API framework is designed to allow developers to incorporate both low-level and high-level security functionality into their program.

Java Cryptography Extension (JCE) extends the JCA API to include APIs for encryption, key exchange and Message Authentication Code (MAC). Therefore, JCA/JCE provides a complete, platform-independent cryptography API.

Solution

ProtectToolkit J is a flexible, performance-optimized, full-strength software crypto toolkit for all popular computing platforms. Eracom Technologies' Hardware Security Modules (HSMs), including ProtectHost Orange, ProtectServer Orange, ProtectServer Gold and ProtectServer Blue, perform cryptographic functions in a physically and logically secure, accelerated and high-speed processing environment.

Microsoft CryptoAPI

CryptoAPI is Microsoft’s application programming interface that enables application developers to add authentication, encoding and encryption to Windows-based applications.

The strength of a cryptosystem is dependent on the storage and management of the keys. Only hardware security modules such as Eracom Technologies' ProtectHost and ProtectServer family products can afford a much higher level of security owing to the built-in tamper-response feature, scalability, random number generation ability, and the highest assurance. In particular, ProtectToolkit M supports the processing-intense RSA public key algorithms for 4,096 bits.

Solution

ProtectToolkit M is Eracom Technologies' implementation of a Microsoft Cryptographic Service Provider (CSP). It allows a Windows-based application to call the Microsoft Cryptographic API (CAPI), to make use of the secure key storage and high speed cryptographic processing capabilities provided by Eracom Technologies’ HSM family of products including:

- ProtectHost Orange
- ProtectServer Gold
- ProtectServer Orange

Common data security problems faced by government and industry include:

- Perimeter security, consisting of firewalls, intrusion detection systems (IDS) and anti virus measures, form the 'Front Line' of tools used to create a trusted network. Such security infrastructure provides little protection for data at the asset level against the risk of a savvy hacker breaking through the firewall into the organizations network and gaining access to unprotected data.
- The loss of a laptop computer equates to the enterprise having to deal with more than just the cost of the device. Reputable industry analysts such as Gartner and IDC estimate the loss of a laptop computer, on average, costs the organization around US $35,000 in lost sensitive data.
- Recent analysis by numerous high profile industry research organizations (Gartner, IDC) have identified internal staff pose 80% of the threat to organizations confidential information, with external threats constituting 20%. The increased work practice of saving data centrally on file servers and databases, multi-site network connected workstations and laptops, outsourced storage providers, plus the growing use of mobile data storage media, has escalated internal digital asset security risks
- The encryption of data files stored on network file servers and workstations often impose restrictions on user access and can reduce employee productivity.

Common sensitive data related risks imposed on organizations include (to mention a few):

- Loss of corporate strategy secrets and R&D information for instance, can cost an organization first mover advantage.
- The exposure of personal information of customers and employees can violate civil and criminal privacy laws in many regions of the globe. Such legislated acts include Gramm-Leach-Bliley Act, The Australian Federal Privacy Act 1998, the European Data Protection Directive, plus others.
- The risk to a company’s public image is heightened by the ease of which internal and external threats can access sensitive company information.
- Financial penalties and damage to an organization’s public image if authenticity of financial information is compromised, as governed by corporate accounting regulations such as Sarbanes Oxley section 404.
- The vulnerability of sensitive information stored within an Application Service Provider (ASP) external data storage facility. This includes the risks of who can gain access, plus the susceptibility of data traffic traversing the non-secure Internet between the outsourced external server and the client device within the organization.

Data encryption delivers the ultimate level of defense to assist protection against the above, and many other threats.

Hackers and data thieves, whom are savvy enough to penetrate the strongest levels of perimeter security, still face the ultimate challenge of deciphering the encryption algorithm to unlock the encrypted data. This additional layer of defense, utilizing industry proven encryption algorithms to protect asset level data at rest, is virtually impossible to break.

Disk encryption, delivered by Eracom Technologies ProtectDrive, encrypts the entire hard drive of a laptop, workstation and server, to protect against disclosure of its information in the case of theft, accidental loss, or disposal of the hardware device.

File Encryption with cryptographically endorsed access control, delivered by Eracom Technologies ProtectFile, encrypts files and folders of confidential information within network connected servers, workstations and laptops. Access rights to encrypted files and folders can be easily managed for individuals and groups within the organization. This ensures that sensitive electronic information remains confidential against both internal and external threats of loss, theft and unauthorized exposure. Only those identities with authenticated access have the ability to read, write and modify the applicable files. As encryption and decryption is undertaken on the client, data files traveling the LAN and unprotected WAN (e.g. between outsourced external servers or remote users), are secured against the threat of unauthorized exposure.

Portable media encryption, delivered by ProtectPack, enables secure, encrypted transfer and storage of confidential data files on unprotected mediums (local, portable and on the network) that are difficult to defend by conventional network mechanisms employed within perimeter security. This includes data transferred via a portable USB drive, burnt to a CD or DVD, via email, plus any other of today’s or tomorrow’s file mobility technology.

Each of the Eracom Technologies data encryption products, ProtectDrive, ProtectFile and ProtectPack, are a robust solution for the protection of electronic information where confidentiality is imperative. When used in combination, this range of data encryption products can provide a heightened level of security. The ‘Protect’ family of data encryption products is designed specifically for medium to large organizations to uniquely address the industry needs for data integrity, confidentiality and controlled availability.

The University of Texas at Austin Responds to Data Theft

As one of the world’s largest academic institutions, The University of Texas at Austin maintains and uses vast information resources, including personal information collected from students, alumni, faculty and staff, vendors and others with whom we do business. It has long been the university’s policy and practice to treat personal information with the utmost care and diligence. In April 2006, a deliberate theft of data from the McCombs School of Business served to highlight the necessity of this commitment. It also underscored the ubiquity, severity and sophistication of today’s threats to information security.

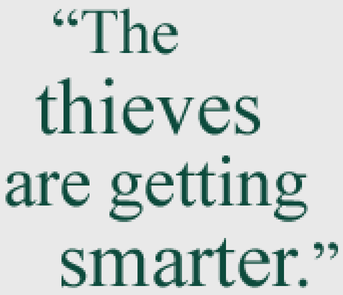
d Alert Update

u believe your personal information has been compromised you may place a fraud alert with ational credit bureaus, good for 90 days. The alert may be renewed indefinitely.

by-step instructions can be found at the Fraud Alert, Data Theft and Identity Theft Resources

McCombs Help Center page addresses many subjects regarding the data theft, as well as ions involving credit and credit protection.

oley Interview



oley, cofounder of the nonprofit Identity Theft Resource Center, discusses the growing em of data theft and identity theft in America.

Interview - wmv

Interview - QuickTime

Since the data theft in April, 2006, the University focused its work on three areas relating to the data theft and the issue of data security in general:

Security: Ways we are improving security measures to ensure this never happens again.
Remediation: Steps being taken to lessen the exposure of Social Security numbers in our systems.
Protection: Resources and tips for responding to identity theft concerns.

Security

We carefully examined all of our existing security systems. A full security audit was conducted by the UT Information Security Office. In addition, we called in independent consultants and major IT firms to do a comprehensive evaluation of our systems and applications.

Specific security steps were implemented to eliminate vulnerabilities. We cannot comment in detail on the steps taken, as it would not be in the interest of ongoing security, but we can tell you that we took definitive steps to secure the safety of information on our server. This includes removing all Social

Security numbers from the McCombs server, and disabling several administrative programs containing personal information.

We cooperated with law enforcement authorities. Cyber Crimes Unit investigators from Texas Attorney General Greg Abbott's office investigated the data theft at McCombs, in coordination with the Federal Bureau of Investigation and the UT Police Department. Internet security and data theft are obviously enormous global problems, and any institution with a substantial database is at risk. Data theft is a serious crime. While we still do not know who committed this crime, it is apparent from the evidence that this was a dedicated, highly skilled attack carried out by someone who knew exactly what they were doing. We do not know the motivations for the theft.

We added security resources. McCombs has significant resources dedicated to computer system functionality and security, and we added additional security expertise and technical capability to ensure that we can fully implement the recommendations highlighted by our security audits.

Remediation

McCombs has made changes in compliance with the University's remediation plan. We have disabled several administrative programs, and removed all Social Security numbers from the McCombs server.

The University has an active remediation effort campus-wide. The University has spent tens of thousands of work hours and millions of dollars upgrading our databases to eliminate sensitive data where possible. At an institution the size of UT Austin, with more than 150 separate business units, it's an enormous task. But this is being taken very seriously, under direction of the Information Security Office.

Protection

UT Austin communicated with nearly 200,000 individuals regarding the theft. This includes 45,000 e-mails, followed by 80,000 letters to those with SSN's compromised. Tens of thousands of all-clear e-mails and letters were sent, followed by an additional 60,000-plus letters to those with non-sensitive information compromised. The University far exceeded the legal notification requirements, and made an attempt to contact everyone for whom we have a valid address or e-mail.

Our call center and response teams handled thousands of inquiries. Our data theft call center handled over 9,000 calls from concerned individuals, and our on-site response team followed up with approximately 6,000 personal calls or e-mails, answering specific questions and gathering updated contact information.

Identity protection resources have been shared. This site provides valuable information to help protect against identity theft, including step-by-step instructions on filing a free 90-day fraud alert. In addition, we provide links to both government resources and commercial programs for credit protection and monitoring.

We will report any evidence of identity theft. To date, the University has not seen any patterns of identity theft resulting from the data theft at McCombs. It has been estimated there are over 50 million data thefts every year, so naturally it would be difficult to link a specific incident of identity theft to this particular crime. However, we are taking any report of suspicious activity seriously, and are turning that information over to authorities investigating this crime.

Is your company keeping information secure?

Most companies keep sensitive personal information in their files and on their computers—names, Social Security numbers, account data—that identifies customers or employees. You'll need information like that to fill orders, meet payroll, or perform other necessary business functions. But if sensitive data falls into the wrong hands, it can lead to fraud or identity theft.

Safeguarding sensitive data is just plain good business. Are you taking steps to protect personal information? A sound data security plan is built on five key principles:

Take stock. Know what personal information you have in your files and on your computers.
Scale down. Keep only what you need for your business.
Lock it. Protect the information you keep.
Pitch it. Properly dispose of what you no longer need.
Plan ahead. Create a plan to respond to security incidents.

Information Security Plan for Organizations

Purpose
The purpose of the Information Technology Division (ITD) Data Security Plan is to ensure that steps to safeguard data information use, storage and transmission are established.

1. All access to computer servers/networks must be controlled through the use of accounts/passwords or other ITD approved means.

2. Physical access to key areas such as computer server rooms and storage
areas must be restricted to necessary personnel only. These areas are to be
locked at all times.

3. To protect data information from hackers and other forms of sabotage, the following will be implemented:

A. Firewall(s)

B. Anti-virus software and regular updates.
1. Servers
2. Microcomputers

C. Backups
1. Regular backups - full, incremental, etc.
2. Provide onsite and offsite storage of backups.

4. Monitoring by ITD staff of the computer servers and networks for any activity such as hacking, theft of information, unauthorized access to systems and files, or any activity that violates the integrity or interferes with the normal operation of the organization's computer system or the work of another user.

5. The implementation of the Organization's data information disaster recovery/contingency plan ensures adequate continuation of data information.

The plan should be:

A. Updated regularly.

B. Tested regularly.

6. All Organizations' personnel must adhere to the "CSU" Computer and Information Code of Conduct Policy.

7. All violations will be logged and modifications made to prevent future violations.

8. Periodic assessment of firewalls, anti-virus software, and other security software and devices by ITD. Recommendations for improvement must be given to the Chief Information Officer of such organization.

9. Periodic assessment of all security violations and corrective actions taken.

10. All policies, plans, and rules must be made public and available for viewing for all

users of data information. Examples include but are not limited to the Web, paper copies in computer laboratories and offices.

Below is an Information Security Policy for Universities as an example of organizations that deal with both human and material resources:

Information Security Policy

Introduction

Storage of university data on computers and transfer across the network eases use and expands our functionality. Commensurate with that expansion is the need for the appropriate security measures. Security is not distinct from the functionality.

The Information Security Policy (Policy) recognizes that not all communities within the University are the same and that data are used differently by various units within the University. The principles of academic freedom and free exchange of ideas apply to this policy, and this policy is not intended to limit or restrict those principles. These policies apply to all units within the University.

Each unit within the University should apply this policy to meet their information security needs. The Policy is written to incorporate current technological advances. The technology installed at some units may limit immediate compliance with the Policy. Instances of non-compliance must be reviewed and approved by the chief information officer or the equivalent officer(s).

Throughout the document the term must and should are used carefully. "Musts" are not negotiable; "shoulds" are goals for the university. The terms data and information are used interchangeably in the document.

The terms system and network administrator are used in this document. These terms are generic and pertain to any person who performs those duties, not just those with that title or primary job duty. Many students, faculty and staff member are the system administrators for their own machines.

Purpose of this Policy

By information security we mean protection of the University's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction

The purpose of the information security policy is:

- To establish a University-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks and computer systems.

- To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

Responsibility

The chair of the University Technology Management Team (UTMT) is responsible for implementing the policy. UTMT, chaired by the Vice President for Administration, is a coordinating group comprised of chief information officers from the three campuses, the university administration, and the hospital.

UTMT must see to it that:

- The information security policy is updated on a regular basis and published as appropriate.
- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Each unit appoints a person to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

Members of UTMT are each responsible for establishing procedures to implement these policies within their areas of responsibility, and for monitoring compliance.

General Policy

Required Policies

- The University will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the University’s data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Recommended Practices

- Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual, network administrator, system administrator, data custodian, and users.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by the University in accordance with University and campus disciplinary policies, procedures, and codes of conduct.

Data Classification Policy

It is essential that all University data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. We have specified three classes below:

High Risk: Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

Confidential: Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public: Information that may be freely disseminated

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.

- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- No University-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- High risk data must be encrypted during transmission over insecure channels.
- Confidential data should be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Access Control Policy

- Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
- Where possible and financially feasible, more than one person must have full rights to any university owned server storing or transmitting high risk data. The campuses and University Administration (UA) must have a standard policy that applies to user access rights. This will suffice for most instances. Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems should be achieved by individual and unique logins, and should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
- As stated in the current campus policies on appropriate and acceptable use, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. When limited access to university-related documents or files is required specifically and solely for the proper operation of University units and where available technical alternatives are not feasible, exceptions are allowed under an articulated unit policy that is available to all affected unit personnel. Each such policy must be reviewed by the unit executive officer and submitted to the CIO for approval. All users must secure their username or account, password, and system access from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong password- the definition of which will be established and documented by UTMT after consultation with the community. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by UTMT.
- Passwords must not be placed in emails unless they have been encrypted.
- Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all University authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the University’s network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.
- Activities performed as administrator or superuser must be logged where it is feasible to do so.

- Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.

Virus Prevention Policy

- The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion Detection Policy

- Intruder detection must be implemented on all servers and workstations containing data classified as high risk.
- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Internet Security Policy

- All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk.
- All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data is classified confidential.

System Security Policy

- All systems connected to the Internet should have a vendor supported version of the operating system installed.
- All systems connected to the Internet must be current with security patches.
- System integrity checks of host and server systems housing high risk University data should be performed.

Acceptable Use Policy

Each Campus and UA must have a policy on appropriate and acceptable use that includes these requirements:

- University computer resources must be used in a manner that complies with University policies and State and Federal laws and regulations. It is against University policy to install or run software requiring a license on any University computer without a valid license.
- Use of the University's computing and networking infrastructure by University employees unrelated to their University positions must be limited in both time and resources and must not interfere in any way with University functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.
- Uses that interfere with the proper functioning or the ability of others to make use of the University's networks, computer systems, applications and data resources are not permitted.
- Use of University computer resources for personal profit is not permitted except as addressed under other University policies.
- Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations. Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Auditors or security officers in the performance of their duties may also use them. They must not be used to monitor or track any individual's network activity except under special authorization as defined by campus policy that protects the privacy of information in electronic form.

Exceptions

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use which do not comply, but near-term future systems will, and are planned for;
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, units must develop a written explanation of the compliance issue and a plan for coming into compliance with the University's Information Security Policy in a reasonable amount of time. Explanations and plans must be submitted to the campus CIO or the equivalent officer(s).

June 14, 2004: Approved by Senate of Urbana-Champaign Campus

Date Revised: July 22, 2004
Date Issued: April 8, 2003
Issued by: Office of the Chief Information Officer
Approved by: Office of the Provost and Vice Chancellor for Academic Affairs
Use of University Premises, Facilities and Computing Infrastructure: Section VIII/1.2

Increased security implications of the 1998 Data Protection Act

Scope And Security Principles
At the heart of the legislation is a set of eight principles. Good information security practice is implied in all eight, but explicitly in Principle 7, which relates to the prevention of unauthorized or unlawful processing, and of accidental loss or damage to data. It requires that organizational as well as technical means be used to protect personal information. It also requires that a security regime must be technologically up to date. All organizations have to comply with the eight principles.

Records

The 1998 Data Protection Act applies to computerized records, as well as to certain manual records involving personal information.

Notification
If you register under the Data Protection Act 1998, you will be asked to fill in a security statement to help the Information Commissioner decide whether you are likely to satisfy the requirements of Principle 7 of the Act. 04 ISO/IEC 17799 is the international standard for information security management. It provides best practice across a wide range of business requirements.
Its companion standard, BS 7799 Part 2, specifies an Information Security Management System (ISMS). This can help your business International and British Standards on Information

Security Management develop, implement and maintain effective information security – it is effectively a framework for following the best practice in ISO/IEC 17799. ISO/IEC 17799 and BS 7799 apply to all information regardless of where it is located and processed, or how it is stored.

The standards outline a number of key principles:

- The use of risk assessment – identifying and evaluating risks, and specifying appropriate security controls to help minimize loss or damage associated with these risks

- Periodic reviews of security and controls – this accounts for any changes that have taken place in your business, as well as identifying new threats and vulnerabilities

- Taking steps to implement information security – some are essential from a legislative point of view (such as data protection, privacy of personal information and safeguarding organizational
records) whilst others are best practice recommendations (such as business continuity management, and information security awareness and training).

To implement an ISMS, you will need to follow four steps:

Step 1: Design the ISMS
At this stage, you would determine your policy and objectives regarding information security, assess your security risks, evaluate various ways of handling these risks, and select controls from the ISO/IEC 17799 standard that reduce risks. Remember to compare the cost of risk control against the value of the information and other risks to your business.

Step 2: Implement the ISMS
Put the selected controls in place to manage risks. This would involve setting up procedures and instructions for staff, raising awareness through training, assigning roles and responsibilities, and implementing any new systems.

Step 3: Monitor and review the ISMS
This will help you ensure that the ISMS continues to manage the risks to your business data. This includes monitoring how effective the controls are in reducing the risks, reassessing the risks taking account of any changes to the business, and reviewing policies and procedures.
Step 4: Improve the ISMS Maintain your system by improving existing controls, as well as putting into practice new controls.

Traditional approaches to data security simply don't mitigate today's data risk. Over the years, companies have invested millions in perimeter defense systems and application security systems but despite these necessary technologies there remains a gap in data security. This gap is created by a lack of visibility into and understanding of what users are actually doing with critical data.

I believe that Information and people are probably the most important business assets in any organization. The 1998 Data Protection Act came into force on 1 March 2000 and means one is obliged to ensure that information held about people is adequately protected. The Data Protection Act concerns personal data, i.e. information about living, identifiable individuals ('data subjects') and details important principles for the security of such information.

Businesses have to be open about their use of personal data, and follow sound and proper practices in how they treat it. By implementing good information security practice, businesses are better equipped to keep their information accurate and up to date. They can also ensure it is accessed by the right people, and in a secured way. If the security of a business' information is compromised, it can cost such business a great deal – financially and in terms of reputation.

References

Allen, Julia H. (2001). The CERT Guide to System and Network Security Practices. Boston, MA: Addison-Wesley.

BTEC (2005). Higher National in Computing. Pearson Custom Publishing: UK.

Colin Ritchie (2004). Relational Databases Principles. Thomson: London

David Brown (1997). Object-Oriented Analysis. John Wiley & Sons Inc.: USA.

Dr. Dobb's Journal (2000). Java.

Godoy, Max B. (2004). A Segurança da Informação e Sua Importância para o Sucesso das Organizações - Information Security and this Importance for de Organizations Success. Rio de Janeiro, Brazil: Kirios Graf. and Editors - RJ Brazil.

Howard Anderson, Sharon Yull, & Bruce Hellingsworth (2004). Higher National Computing. Elsevier: Oxford.

IMIS Journal (1998). IT Security – Formulating a policy.

Krutz, Ronald L.; Russell Dean Vines (2003). The CISSP Prep Guide, Gold Edition, Indianapolis, IN: Wiley.

Layton, Timothy P. (2007). *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach publications.

McNab, Chris (2004). *Network Security Assessment*. Sebastopol, CA: O'Reilly.

Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Boca Raton, FL: Auerbach publications.

Peltier, Thomas R. (2002). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Boca Raton, FL: Auerbach publications.

Terence Driscoll and Bob Dolden (1997). Computer Studies and Information Technology. Macmillan education Ltd: London and Oxford.

White, Gregory (2003). *All-in-one Security+ Certification Exam Guide*. Emeryville, CA: McGraw-Hill/Osborne. 0-07-222633-1.

Wikipedia

www.google.com

Appendices

Data security: is the means of ensuring that data is kept safe from corruption and that access to it is suitably controlled. Thus data security helps to ensure privacy. It also helps in protecting personal data. In the UK, the Data Protection Act is used to ensure that personal data is accessible to those whom it concerns, and provides redress to individuals if there are inaccuracies. This is particularly important to ensure individuals are treated fairly, for example for credit checking purposes. The Data Protection Act states that only individuals and companies with legitimate and lawful reasons can process personal information and cannot be shared.

The International Standard ISO/IEC 17799 covers data security under the topic of information security, and one of its cardinal principles is that all stored information, i.e. data, should be owned so that it is clear whose responsibility it is to protect and control access to that data.

Data corruption refers to errors in computer data that occur during transmission or retrieval, introducing unintended changes to the original data. Computer storage and transmission systems use a number of measures to provide data integrity, the lack of errors.

Data corruption during transmission has a variety of causes. Interruption of data transmission causes information loss. Environmental conditions can interfere with data transmission, especially when dealing with wireless transmission methods. Heavy clouds can block satellite transmissions. Wireless networks are susceptible to interference from devices such as microwave ovens.

Data loss during storage has two broad causes: hardware and software failure. Head crashes and general wear and tear of media fall into the former category, while software failure typically occurs due to bugs in the code.

When data corruption behaves as a Poisson process, where each bit of data has an independently low probability of being changed, data corruption can generally be detected by the use of checksums, and can often be corrected by the use of error correcting codes.

If an uncorrectable data corruption is detected, procedures such as automatic retransmission or restoration from backups can be applied. RAID disk arrays, store and evaluate parity bits for data across a set of hard disks and can reconstruct corrupted data upon of the failure of a single disk.

If appropriate mechanisms are employed to detect and remedy data corruption, data integrity can be maintained. This is particularly important in banking, where an undetected error can drastically affect an account balance, and in the use of encrypted or compressed data, where a small error can make an extensive dataset unusable.

Data privacy

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data.

Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. The most common sources of data privacy issues are:

(a) Health information
(b) Criminal justice
(c) Financial information
(d) Genetic information
(e) Location information

The challenge in data privacy is to share data while protecting personally identifiable information. Consider the example of health data which are collected from hospitals in a district; it is standard practice to share this only in the aggregate. The idea of sharing the data in the aggregate is to ensure that only non-identifiable data are shared.

The legal protection of the right to privacy in general and of data privacy in particular varies greatly around the world.

The Universal Declaration of Human Rights states in its article 12 that:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Glossary of Terms

Information Security Guidelines

An Information Security Guidelines is a suggested action or recommendation to address an area of the Information Security Policy. A security guideline is not a mandatory action, and no disciplinary action should result from non adoption. However, Information Security Guidelines are considered Best Practice and should be implemented whenever possible.

A guideline typically uses works like "should" or "may" in the definition. Guidelines are usually written for a particular environment and are used to help guide users' actions. For example, "all successful logins should be logged and monitored." A guideline may apply to management, administrators, end users, or a specific group within the organization.

Information Security Guidelines will usually supplement the Procedures Manuals with their adoption encouraged and promoted rather than enforced.

Information Security Incident

An Information Security incident is an event which appears to be a breach of the organization’s Information Security safeguards. It is important to respond calmly and to follow a logical procedure, first to prevent the breach from continuing, if possible, and second, to inform the appropriate person(s) within the organization; this usually includes the appointed Security Officer.

N.B. Where a member of staff fails to observe Information Security procedures; this is not, of itself, an Information Security incident. However, depending on the risk of the incident, disciplinary and/or improved procedures may be required.

Information Security Plan

The Information Security plan complements the IT Plan in so far as it documents, budgets and resources the upgrades to hardware, software, training and procedures, in relation to Information Security.

The driving force behind the Information Security Plan will be the Security Officer with the executive sponsor likely to be the Chief Information Officer, or the Chief Executive Officer / Managing Director.

Information Security Policy

Information Security Policy is an organizational document usually ratified by senior management and distributed throughout an organization to anyone with access rights to the organization’s IT systems or information resources.

The Information Security Policy aims to reduce the risk of, and minimize the effect (or cost) of, security incidents. It establishes the ground rules under which the organization should operate its information systems. The formation of the Information Security Policy will be driven by many factors, a key one of which is risk. How much risk is the organization willing and able to take?

The individual Information Security Policies should each be observed by personnel and contractors alike. Some policies will be observed only by persons with a specific job function, e.g. the System Administrator; other Policies will be complied with by all members of staff.

Compliance with the organization's Information Security Policy should be an incorporated with both the Terms and Conditions of Employment and also their Job Description.

Information Security Risk Assessment

An Information Security Risk Assessment is an initiative which identifies:-

1. the nature and value of the Information Assets or Business Assets
2. the threats against those assets, both internal and external
3. the likelihood of those threats occurring
4. the impact upon the organization.

Risk is defined as a danger, possibility of loss or injury; and the degree of probability of such loss. Before introducing Information Security safeguards, you must be aware of the dangers to which you are exposed, the risks and likelihood of such events taking place, and the estimated impact upon your organization were each to actually occur.

In order to determine the overall level of Information Security safeguards required, you should consider performing a comprehensive Information Security Risk Assessment.

Information Systems

The computer systems and information sources used by an organization to support its day to day operations.

Information User

An Information User is the person responsible for viewing / amending / updating the content of the information assets. This can be any user of the information in the inventory created by the Information Owner.

Information Warfare / Infowar

Also Cyberwar and Netwar. Infowar is the use of information and information systems as weapons in a conflict in which the information and information systems themselves are the targets.

Infowar has been divided into three classes;-

1. Individual Privacy
2. Industrial and Economic Espionage
3. Global information warfare, i.e. Nation State versus Nation State.

Most organizations will not need to be concerned over classes I and III, but clearly Class II is relevant to any organization wishing to protect its confidential information.