International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Information Security

Asif Husain

Abstract: ***According to one common view, information security comes down to technical measures. Given better access control policy models, formal proofs of crypto-graphic protocols, approved firewalls, better ways of detecting intrusions and malicious code, and better tools for system evaluation and assurance, the problems can be solved. In this note, we put forward a contrary view: information insecurity is at least as much due to perverse incentives. Many of the problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons***

Keywords: Information Security

1. Introduction

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. 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.

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.

2. History

This article will not attempt to provide a comprehensive history of the field of information security, rather it will suffice to describe 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.

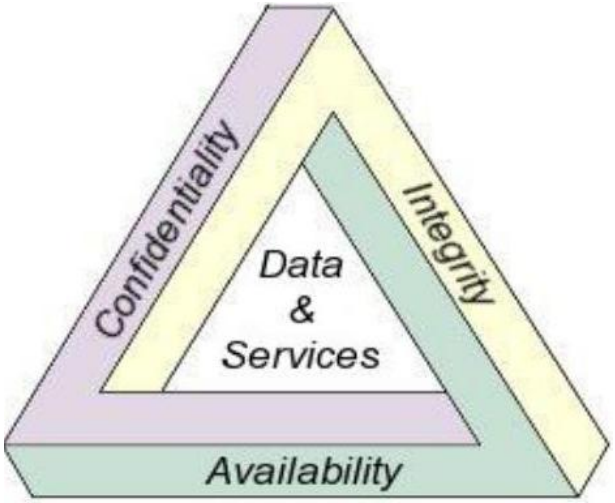
The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small 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.

3. Basic Principles

Key Concepts
For over twenty years information security has held that confidentiality, integrity and availability (known as the CIA Triad) are the core principles of information security.

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 disclosure, 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



Information that is considered to be confidential in nature must only be accessed, used, copied, or disclosed by persons who have been authorized to do so, and only when there is a genuine need to do so. 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 necessary (but not sufficient) 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.

Authenticity
In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine (i.e. they have not been forged or fabricated.).Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

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.

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). A **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.

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.

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**, **Restricted**,

Confidential, **Secret**, **Top Secret** and their non-English equivalents.

Access Control
Access to protected information must be restricted to people who are authorized to access the information. This requires that mechanisms be in place to control the access to protected information. 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 John Doe."* they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe.

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

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.

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 provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and 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.

Fast growing area

Information Security has become one the fastest growing areas in the information technology industry. This is borne by the fact that previously secure organizations are widening the borders of their environments to conduct business over the Internet. This strategy while encouraging growth in business can and has led to information security incidents where adequate security measures have not been implemented.

Internet related security incidents occur due to organizations implementing business-related functions over the Internet without placing proper security or indeed not being aware of the security risks that accompany conducting business over the Internet. One must also note that security incidents also occur within organizations and as such many insider security breaches have happened due to lax internal security and /or organizations having the wrong notion that all members of staff are performing their functions in an authorized manner.

4. Future

Looking into 2008, the information security agenda for executives continues to evolve. The complexities of what to protect and when, overlaid with requirements of regulation and compliance, create the need for a new type of information security executive--one with business savvy, sound risk fundamentals and holistic technical understanding. These skills, coupled with a strong strategy, will be necessary for organizations to achieve their 2008 information security goals.

The number one item on the 2008 information security agenda is data protection. The practice of protecting the confidentiality, integrity and availability of data is not new--passwords, encryption and data classification structures have been around for years. What has changed is the type of data that's now considered valuable. From the external attacker perspective, intellectual property and insider information was once the most sought-after data asset. Now, the data currency of choice is identity--e-mail addresses, social security numbers and credit card information. Corporate espionage is still a significant threat, but the new underground deals in volume, where success is being measured in thousands and millions of identities.

5. Conclusion

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 or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review.

References

[1] Introduction to Computer by V.Rajaraman.
[2] Internet techonology & web design (choice publications).
[3] Computer Networks by Tanenbaum.
[4] Computer Networks by frozen.
[5] http://www.wikipedia.com