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

A Survey: Information Security and Information Privacy in Devices

Anil Kumar

Computer Science and Engineering, Noida International University, Greater Noida, G. B Nagar

Abstract: ***Information security is a feverish issue due to drastic increasing application of computer, internet and internet user and intrusions. Various IT security approaches have been invented on this aspect while among them Balanced (composition of Technical and Non-technical security issues) IT Security approach (BITS) is highly lucrative now-a-days due to its simplicity and effectiveness in the sector of Information security especially in Higher education. Two particular areas of interest may be user perceptions of privacy policies and opt-in/opt-out policies and procedures. Additionally, research related to individuals' concern for information privacy may be less problematic to study than organizational security issues. Research in this area is important because user concern for information privacy has the potential to affect the future of ecommerce.***

Keywords: Information security; information privacy

1. Introduction

Information technology security in higher education is the process of securing the higher education environment without disrupting the openness, accessibility, academic and intellectual freedom which is at the very heart of the higher education environment. It is one of the fundamental process towards the broader security because the further processing steps depends of what types of security breaches has been occurred and what strategies are in place to cope up with these. The history of information security begins with computer security. The need for computer security—that is, the need to secure physical locations, hardware, and software from threats— arose during World War II when the first mainframes, developed to aid computations for communication code breaking were put to use. Multiple levels of security were implemented to protect these mainframes and maintain the integrity of their data. Access to sensitive military locations, for example, was controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. The growing need to maintain national security eventually led to more complex and more technologically sophisticated computer security safeguards.

2. Key Information Security Concepts

- Access: A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers have illegal access to a system. Access controls regulate this ability.
- Asset: The organizational resource that is being protected. An asset can be logical, such as a Web site, information, or data; or an asset can be physical, such as a person, computer system, or other tangible object. Assets, and particularly information assets, are the focus of security efforts; they are what those efforts are attempting to protect.
- Attack: An intentional or unintentional act that can cause damage to or otherwise compromise information and/or the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone casually reading sensitive information not intended for his or her use is a passive attack. A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a fire in a building is an unintentional attack. A direct attack is a hacker using a personal computer to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems, for example, as part of a botnet (slang for robot network). This group of compromised computers, running software of the attacker's choosing, can operate autonomously or under the attacker's direct control to attack systems and steal user information or conduct distributed denial-of-service attacks. Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.
- Risk: The probability that something unwanted will happen. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk the organization is willing to accept.
- Subjects and objects: A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack—the target entity. A computer can be both the subject and object of an attack, when, for example, it is compromised by an attack (object), and is then used to attack other systems (subject).

3. Critical Characteristics of Information

The value of information comes from the characteristics it possesses. When a characteristic of information changes, the value of that information either increases, or, more commonly, decreases. Some characteristics affect information's value to users more than others do. This can depend on circumstances; for example, timeliness of information can be a critical factor, because information loses much or all of its value when it is delivered too late. Though information security professionals and end users share an understanding of the characteristics of information, tensions can arise when the need to secure the information from threats conflicts with the end users' need for unhindered access to the information.

1) Availability:-Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.
2) Accuracy:- Information has accuracy when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate.
3) Authenticity:-Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred. Consider for a moment some common assumptions about e-mail. When you receive e-mail, you assume that a specific individual or group created and transmitted the e-mail—you assume you know the origin of the e-mail.

4. ISO 27001:Information Security

ISO 27001 (formally known as *ISO/IEC 27001:2005*) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

ISO 27001 uses a topdown, risk-based approach and is technology-neutral. The specification defines a six-part planning process:
1) Define a security policy.
2) Define the scope of the ISMS.
3) Conduct a risk assessment.
4) Manage identified risks.
5) Select control objectives and controls to be implemented.
6) Prepare a statement of applicability

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organisation.

The 27001 standard does not mandate specific information security controls, but it provides a checklist of controls that should be considered in the accompanying code of practice, ISO/IEC 27002:2005. This second standard describes a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.

ISO 27002 contains 12 main sections:
1) Risk assessment
2) Security policy
3) Organization of information security
4) Asset management
5) Human resources security
6) Physical and environmental security
7) Communications and operations management
8) Access control
9) Information systems acquisition, development and maintenance
10) Information security incident management
11) Business continuity management
12) Compliance

Organizations are required to apply these controls appropriately in line with their specific risks. Third-party accredited certification is recommended for ISO 27001 conformances.
Other standards being developed in the 27000 family are:
1) 27003 – implementation guidance.
2) 27004 - an information security management measurement standard suggesting metrics to help improve the effectiveness of an ISMS.
3) 27005 – an information security risk management standard. (Published in 2008)
4) 27006 - a guide to the certification or registration process for accredited ISMS certification or registration bodies. (Published in 2007)
5) 27007 – ISMS auditing guideline.

References

[1] Bletchley Park—Home of the Enigma machine. Accessed 15 April 2010 from http:// churchwell.co.uk/bletchley-park-enigma.htm.
[2] Peter Salus. ―Net Insecurity: Then and Now (1969–1998).‖ Sane ’98 Online. 19 November 1998. Accessed 26 March 2007 from www.nluug.nl/events/sane98/aftermath/salus.html.
[3] Roberts, Larry. ―Program Plan for the ARPANET.‖Accessed 26 March 2007 from www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm.
[4] Roberts, Larry. ―Program Plan for the ARPANET.‖Accessed 8 February 2007 from www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm. Introduction to Information Security 35 © Cengage Learning. All rights reserved. No distribution allowed without express authorization.
[5] Schell, Roger R., Downey, Peter J., and Popek, Gerald J. Preliminary Notes on the Design of Secure Military Computer System. January 1973. File, MCI-73-1, ESD/ AFSC, Hanscom AFB, Bedford, MA 01731.
[6] Bisbey, Richard, Jr., and Hollingsworth, Dennis. Protection Analysis: Final Report. May 1978. Final report, ISI/SR-78-13, USC/Information Sciences Institute, Marina Del Rey, CA 90291.
[7] Basu, A., &Muylle, S. (2003). Authentication in E-Commerce. Communications of the ACM, 46(12)
[8] Burmester, M., &Desmedt, Y.G. (2004). Is Hierarchical Public-Key Certification the Next Target for Hackers? Communications of the ACM, 47(8)
[9] Cam-Winget, N., Housley, R., Wagner, D., & Walker, J. (2003).Security Flaws in 802.11 Data Link Protocols. Communications of the ACM, 46**(5),**