Advances in Robotics & Automation

Keung, Adv Robot Autom 2013, 3:2
DOI: 10.4172/2168-9695.1000e118

Editorial Open Access

Information Security Controls

YAU Hon Keung*

Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong

Introduction

Bhaskar and Ahson [1] state that security controls are selected and applied based on a risk assessment of the information system. The risk assessment process identifies system threats and vulnerabilities, and controls are for mitigating risk and to reduce probability of loss. When management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls. Purcell [2] states that security controls are measures taken to safeguard an information system from the attacks against the confidentiality, integrity, and availability of the information system. There are two ways to categorize security controls. The first way is to put the security control into administrative, technical (also called logical), or physical control categories. In this taxonomy, the control category is based on their nature. The second way to categorize security controls is taxonomy according to the time that they act, relative to a security incident, they are directing, preventing and correcting.

Physical Security Controls

Physical security controls are means and devices to control physical access to sensitive information and to protect the availability of the information [2]. Schweitzer [3] states that those security elements necessary to ensure that unauthorized persons are excluded from physical spaces and assets where their presence represents a potential threat. All types of computers, computing devices and associated communications facilities must be considered as sensitive assets and spaces and be protected accordingly. Examples of physical security controls are physical access systems including guards and receptionists, door access controls, restricted areas, closed-circuit television (CCTV), automatic door controls and human traps, physical intrusion detection systems, and physical protection systems. Administrative and technical controls depend on proper physical security controls being in place.

Technical Security Controls

According to Bhaskar and Ahson [1], Technical security controls is also called logical controls, they refer to restriction of access to system. Schweitzer [3] said that logical security elements consist of those hardware and software features provided in a system that helps to ensure the integrity and security of data, programs and operating systems,

1. Hardware elements that segregate core and thus present overlap, accidental or intentional; Core clearing after job to prevent the following job seizing control, level of privileges that restrict access to the operating system programs, firmware programs that are not software- modifiable and similar elements.

2. Software elements that provide access management capabilities. These are the key security elements in a program to protect electronic information. An effective logical security system provides the means to identify, authenticate, authorize, or limit the authenticated user to certain previously stipulated actions, for each system user who may sign on or for each program that may be called on by the computer to process files with established value factors.

Administrative Security Controls

Administrative security controls (also called procedural controls) are primarily procedures and policies which put into place to define and guide employee actions in dealing with the organizations' sensitive information. They inform people on how the business is to be run and how day to day operations are to be conducted [2]. Laws and regulations created by government bodies are also a type of administrative control because they inform the business [3].

Administrative security controls in the form of a policy can be enforced with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

References

1. Bhaskar SM, Ahson SI (2008) Information Security: A practical Approach. Oxford: Alpha Science International Ltd.
2. 2.Purcell JE (2007) Security Control Types and Operational Security. Retrieved from World Wide Web.
3. Schweitzer JA (1990) Managing Information Security: Administrative, Electronics, and Legal measures to Protect Business Information. Boston: Butterworths.

***Corresponding author:** YAU Hon Keung , Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong, Tel: 9800 5418; E-mail: honkyau@cityu.edu.hk

Received January 29, 2014; **Accepted** January 31, 2014; **Published** February 3, 2014

Citation: YAU HK (2014) Information Security Controls. Adv Robot Autom 3: e118. doi: 10.4172/2168-9695.1000e118