Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 314 – 322

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

The Impact Assessment of IT Infrastructure on Information Security: A Survey Report

Ankur Kumar Shrivastava

Research Scolar Sai Nath University,Ranchi,Jharkhand 834001,India

Abstract

Information technology infrastructure trigger unending concern for IT players accountable for information security. Sensitive organization information can be easily acquired and lost. The community dearth of self-confidence in information technology (IT) infrastructure is not purely about security of worth, but also about faith in the information group. Integrity, privacy and vulnerability security fears are the important cause web user is not confident over the web. Proposes to investigate the integrity, privacy and vulnerability security fears of IT user in order to establish a consensus among them. Uses data from 127 contributors to come to a decision that the following major concerns (in the descending of importance) exist: integrity, privacy, security and fears, unauthorized access, data leaked, impersonation and forged identity and e-mail safety. The objective of the survey was to collect statistics to quantify the influence of Information technology infrastructure on organization information security.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Risk assessment; Threat evaluation; Risk gauge: Quantitative; Qualitative; Privacy; Integrity; Vulnerability.

1. Introduction

The establishments in the private and public segments rely on information classifications to positively carry out their duties and commercial roles. Information technology infrastructure can include very distinct units varying from financial, office networks, and personnel systems to very specialized systems. IT infrastructure are question to risky hazards that can have negative effects on organizational processes, organizational assets, other organizations, individuals, and the Nation by utilizing both unknown and known vulnerabilities to compromise the integrity,

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.062

confidentiality, or availability of the information being managed, collected, or communicated by those systems. Risks to information and information systems can include persistent attacks, environmental disruptions, and man/machine errors and result in great damage to the national and economic security interests. Hence, it is essential that managers and leaders at all stages identify their duties and are held responsible for handling information security risk that is, the hazard associated with the process and use of information systems that support the processes and business functions of their organizations. Threat is a degree of the extent to which an entity is vulnerable by a potential incident or event, and is typically a function of: (i) the unfavorable effects that would arise if the situation or event occurs; and (ii) the probability of existence. Information security threats are those threats that arise from the loss of confidentiality, integrity, availability of information/information systems and expose the potential unfavorable impacts to organizational assets, organizational functions, individuals, other organizations, and the Nation. A risk measurement is the process of identifying, prioritizing, and evaluating information security risks. Evaluating information security danger requires the watchful examination of threat and vulnerability information to determine the extent to which situations or events could unfavorably impact an organization and the likelihood that such situations or events will occur. Any assessment of risk includes: (i) an precise risk model, outlining key terms and measureable risk factors and the associations among the factors; (ii) an evaluation approach, indicating the extent of values those risk factors can assume during the evaluations; and (iii) an evaluation approach, specifying how values of those threat factors are functionally merged to evaluate risk. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk features are also used extensively in risk communications to focus the numerous features of problem domains that powerfully affect the intensities of risk in particular circumstances, situations, or contexts. Some of the risk factors include, for example, impact, threat, vulnerability, likelihood, and predisposing condition. Risk factors can be further decomposed into more detailed characteristics. A risk assessment methodology is a process for risk assessment, together with a risk model, assessment approach, and analysis approach. Risk evaluation practices are defined by organizations and are a factor of the risk management approach developed during the risk-framing step of the risk management procedure. Organizations can use a single risk evaluation procedure or can employ multiple risk evaluation procedures, with the selection of a specific practice depending on: (i) the criticality and sensitivity of the organization's core duties and business tasks including the supportive mission/business processes and information systems; (ii) the maturity of the organization's mission/business procedures; (iii) the stage of information systems in the SDLC. By making explicit the risk model, the assessment approach, and the analysis approach used, and requiring as part of the assessment process, a basis for the evaluated values of threat factors, organizations can increase the duplicability and reappearance of their threat evaluations.

1.1. Security Risk Models

This describes the crucial terms used in risk evaluations involving the factors of the risk to be evaluated and the associations among those factors. These explanations are vital for corporations to document previous of managing risk evaluations because the evaluations depend upon significant properties of threats, vulnerabilities, and other risk factors to well determine the risks. Figure 1. (a) Explains a pattern of a risk model for severe threats including the key risk factors related with the model and the association among the features. All of the risk factors is defined in larger detail underneath and used in the process of risk evaluation. A threat is an event with the potential to negatively impact organizational resources and processes, individuals, other organizations, or the Nation through information system via unlawful access, devastation, admission, or information modification, and/or denial of service. There are two sides to threat cogitated in this paper: (i) threat causes; and (ii) threat incidents. A threat cause is a play-actor with the intent and method targeted at the exploitation of vulnerability or a state and method that may unintentionally exploit vulnerability. In common, types of threat causes include: (i) adverse cyber/physical attacks; (ii) humanoid mistakes of exclusion or instruction; (iii) structural failures of organization-controlled resources; and (iv) natural and man-made adversities, mishaps, and flops beyond the control of the organization. A threat incident is an incident or condition initiated or caused by a threat cause that has the potential for causing adverse impact. The tactics, techniques, for cyber attacks typically characterizes threat events and procedures employed by adversaries. Risk models can provide useful differences between threat causes and threat incidents. Various taxonomies of threat causes have been established. A typical classification of threat causes uses the type of adverse impacts as an