Journal of Cases on Information Technology
Volume 20 • Issue 3 • July-September 2018

Developing an Information Security Risk Taxonomy and an Assessment Model using Fuzzy Petri Nets

Dhanya Pramod, Symbiosis Centre for Information Technology (SCIT), Symbiosis International (Deemed University), Pune, India

S. Vijayakumar Bharathi, Symbiosis Centre for Information Technology (SCIT), Symbiosis International (Deemed University), Pune, India

ABSTRACT

In the digital era, organization-wide information security risk assessment has gained importance because it can impact businesses in many ways. In this article, the authors propose a model to assess the information security risk using Fuzzy Petri Nets (FPN). Deeply rooted in the OCTAVE framework, this research presents a taxonomy of risk practice areas and risk factors. The authors apply the constituents of the taxonomy to risk assessment through a well-defined FPN model. The primary motive of the article is to extend the usability of FPNs to newer and less explored domains like audit and evaluation of information security risks. The unique contribution of this article is the definition and development of a comprehensive and measurable model of risk assessment and quantification. The model can also serve as a tool to capture the risk perception of the respondents for validating the criticality of risk and facilitate the top management to invest in information security control eco-system judiciously.

KEYWORDS

Business Continuity Planning, Database Security, Governance and Risk Compliance, NIST, OCTAVE, Operational, Privacy, Software Integrity, Strategy, Technical, Vulnerability Assessment

1. INTRODUCTION

The proliferation of the internet and the advancements in computing technology and communications has not only transformed the way organizations pursue the business, but also changed the lifestyle of individuals (Lee et al., 2016, Rothlin and McCann, 2016, Law et al., 2014, Kellermann and Jones, 2013). Though this has a positive impact on the information storage, transit, and processing, it has also lead to compromise of confidentiality, integrity, and availability of information (Mell et al., 2007, Ransbotham and Mitra, 2009, Hughes and Cybenko, 2013). In this view information security programs have been devised by organizations which focus on risk assessment and mitigation. There is a strategic approach to information protection and risk assessment. The strategic plan ensures synergy between organization's information, infrastructure protection goals with a well-planned execution

DOI: 10.4018/JCIT.2018070104

roadmap, (Pironti, 2010, Ahmad et al., 2014, Yaokumah and Brown, 2014, Peppard et al., 2014, Shimeall and Spring, 2013, Hu et al., 2012). These capabilities need to be included in IT strategy and should align with the business goals and the vision and mission of the organization (Havinga and Sessink, 2014). The information systems that handle the data need a design with security in mind, and security analysis and design practices have evolved. It is harmful to depend on a predetermined security measure entirely, and such an obvious security measure can be treated as a vulnerability (May et al., 2013). The motive of this paper is to explore, define and create a Fuzzy Petri-Nets (FPN) model for measuring information security risk perceptions. Such a model will address the organizational information security from strategy, operational and technical dimensions to efficiently identify and assess the criticality of risk. Firmly grounded on this understanding in the second section we present an extensive review of the previous works relating to information security risks and an inventory about the varied applications of Fuzzy Petri Nets (Zhou and Zain, 2016; Taj and Kumaravel, 2015a). The third section covers the rules of applying FPN rules to the information security risks and explains the model for validating the risk perception during any risk assessment process. The fourth and final section slates the future scope and summarizes the work.

2. LITERATURE REVIEW

This section contains two broad parts. Section 2.1 covers the existing literature relating to information security risks and present a taxonomy of risk and risk factors in the assessment model. Section 2.2 deliberates about the current applications of FPN and also bids for the use of FPN as a risk assessment model among other risk assessment models for information security (Macedo, and Da Silva, 2012).

2.1. Information System Security

Information technology revolution has transformed the way of doing business and increased the access to information. The ISO 27001 defines an Information Security Management System (ISMS) as a “systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process”. NIST 800-30 document developed by the National Institute of Standards and Technology defines risk as “a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization.” To minimize risks and maximize return on investments a security management program is essential (Stoll et al., 2013) and it further ensures legal compliance, goodwill, financial stature, a competitive edge which in turn leads to sustainable growth. It means that the organizations need to have a comprehensive management structure and systematic practices for information security (Chang et al. 2006). Though top management has a critical role in devising an information security programme to protect the information assets, their support is the most crucial issue in implementing and operationalizing the same. In addition to this, a comprehensive policy should be in place (Knapp 2009; Singh 2013), and top management should have interest and participation for continued improvement in information security programme (McFadzean, 2007). However, organizations still lack efficient Information security governance and stakeholder buy-in (Williams, 2001).

Information security governance is no more a technical issue, but a business issue (Kayworth and Whitten, 2010) and top management need to look at it from a business angle (Kwon 2012). Organizations need a holistic approach to business management with IT strategy and security strategy aligned to it (Soomro 2015; Baskerville et al., 2014). It primarily needs understanding the business goals of the organization and its risk profile, and accordingly, a better Information Security and risk management program can be implemented (Pironti 2010). Information Technology security strategy is a crosscutting concern for business planning (Pramod et al., 2013) with many intermediate points in business process execution. However, many organizations fail in having a security strategy aligned