Journal of Information Security and Applications 35 (2017) 128–137

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

# Information security risks management framework – A step towards mitigating security risks in university network

Chanchala Joshi [a,*], Umesh Kumar Singh [b]

[a] Institute of Computer Science, Vikram University Ujjain, M.P. India
[b] School of Engineering and Technology, Vikram University Ujjain, M.P. India

ARTICLE INFO

*Article history:*

*Keywords:*
Security risk
Security threats
University campus network
Vulnerability

ABSTRACT

Information is one of the most prominent assets for Universities and must be protected from security breach. This paper analyzed the security threats specifically evolve in University's network, and with consideration of these issues, proposed information security framework for University network environment. The proposed framework reduces the risk of security breach by supporting three phase activities; the first phase assesses the threats and vulnerabilities in order to identify the weak point in educational environment, the second phase focuses on the highest risk and create actionable remediation plan, the third phase of risk assessment model recognizes the vulnerability management compliance requirement in order to improve University's security position. The proposed framework is applied on Vikram University Ujjain India's, computing environment and the evaluation result showed the proposed framework enhances the security level of University campus network. This model can be used by risk analyst and security manager of University to perform reliable and repeatable risk analysis in realistic and affordable manner.



## 1. Introduction

With increasing development of Information Technology, computing and network applications have become an integral part of universities environment. Today's universities are on the forefront of technological advancement. The greater access to technology results in valuable learning environment, on the other hand can also results vulnerable computing environment with more security threats. University campuses are proving themselves to be some of the most technologically advanced places in the world by providing facilities like extensive Wi-Fi support, online learning using lecture capture software, digital library, classroom virtualization, web conferencing etc. All these advancement makes University's computing environment particularly vulnerable because in contrast to hacking targets like banks, college and university computing environments are often large open networks. Protecting open large university campus against constantly evolving threats and vulnerabilities presents major challenges. On the other hand, the open computing university environment also supports diverse users; mainly the three distinct types of users of university are students, faculty and administration. Each of the user accesses university computing environment with varying level of university resources. Therefore, University campus network must not only provide the secure access to users but also defend them from vulnerabilities and security breaches. In the large University campus network there is need of improving risk posture and security effectiveness. It requires identification of operationally critical threats, assessment of vulnerabilities for measurement of risk level by continuous network monitoring of University campus network. This paper proposes Quantitative Information Security Risk Assessment Model designed specifically for University computing environment, with the consideration of security dangers presents in large open campus network of University. The proposed model quantitatively measures the security risks by identifying potential threats and information processes within Universities network configuration. This model can be used by risk analyst and security manager of University to perform reliable and repeatable risk analysis in realistic and affordable manner.

## 2. Related work

There are various risk assessment models available, some of which are qualitative while others are quantitative in nature; having a common goal of estimating the overall risk value [1]. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), developed by CERT is a model for risk-based infosec strate-

* Corresponding author.
*E-mail addresses:* Chanchala.joshi@gmail.com (C. Joshi), umeshsingh@rediffmail.com (U.K. Singh).

http://dx.doi.org/10.1016/j.jisa.2017.06.006
2214-2126/

gic assessment and planning. OCTAVE defines assets as including people, hardware, software, information and systems. One of the major drawbacks of OCTAVATE is its complexity and it doesn't allow organizations to quantitatively model risk. In order to improve security organization system some standard principles are needed, Joshi et al. [2] analyzed the prominent taxonomies of attacks and vulnerability of computer system and network to improve vulnerability categorization and proposed novel approach towards Standardization of Network and Computer [3]. One another prominent risk assessment model is [4] FAIR (Factor Analysis of Information Risk), provides framework for understanding, analyzing and measuring information risk. FAIR is built to address security concern weaknesses. The framework allows organizations to standardize the risk, apply risk assessment, view in total organizational risk, defend risk determination using advanced analysis and understand how time and money will affect the organization's security profile. The main shortcoming of FAIR is the lack of information about methodology and examples of how the methodology is applied [5]. NIST RMF (National Institute of Standards and Technology's Risk Management Framework) covers a series of activities related to managing organizational risk [6]. TARA (Threat Agent Risk Assessment) is a risk assessment framework created by Intel that helps companies to manage risk by distilling the possible information about security attacks. The major drawback is to be prohibitively expensive and impractical to defend possible vulnerability. One of the primary tasks of risk assessment process is vulnerability scanning; Joshi et al. [7] evaluated the efficiency of web application vulnerability scanners by designing a vulnerable web application. This evaluation assists in choosing vulnerability scanner during first phase of proposed model.

There are numerous risk assessment models; however, there is no mechanism to assist organizations in determining which model is the best to be employed within an organization; also these models considered the security challenges identified in hacking target organizations like banks. Although security risk assessment is crucial for these organizations but these organizations have secure and close network environment. On the other hand, higher educational institutions like Universities where information security risk assessment is major and high priority job are having large and open computing environment. The next section describes the typical scenario of University network environment comprises of diverse small network.

## 3. University campus network setup

Fig. 1 shows an ideal, large and open, University campus network setup, comprises of diverse small networks. With the rapid development of technology, universities strive to develop a convenient and valuable learning environment through IT technologies. University large computing environment includes diverse network devices, various software applications and many servers.

## 4. Proposed quantitative information security risk assessment model

The main objective behind designing a security risk assessment framework is, "security controls should be selected based on real risks to an organization's assets and operations". Numerous of security risks assessment models are available but University computing environment is differ from other organizations as it is large, open and consists of several small diverse network with various users. Selecting risk assessment model without analysis, results in implementation of security controls in the wrong places, wasting of resources and leaving an organization vulnerable to unanticipated threats. The proposed risk assessment model initially analyses what is to be assessed, who needs to be involved and the criteria for quantifying, qualifying, and comparing severity of risks. The assessment results must be documented properly. The goal of proposed framework is to measure risk level quantitatively that will allow higher educational institutes to understand security risks. The proposed model is based on the most popular risk frameworks in use today, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), developed at Carnegie Mellon University. The proposed framework performs three phase activities to make standard model more absolute, and provides a practical approach which can be used in real educational environment.

Fig. 2 shows the abstract three phase view of the proposed model:

The goal of proposed model is to reduce risks of security breach, this means understanding the cause that makes system vulnerable. The first phase focuses on knowing weak points, even in constantly changing and challenging University's environment. Then the second phase concentrates on understanding which areas are having the highest risks, based on reliable and granular real risk scoring. The proposed framework uses Common Vulnerability Scoring System (CVSS) [8] to validate which vulnerability can be actively exploited. The third phase pivot along the creation of actionable remediation plan over with University environment's unique factor to and finally generate powerful reporting to track recursive risk measurement activities. The central of the proposed risk assessment framework is an objective of assessing University's campus network, recursive mechanism that collects input regarding vulnerabilities and threats and produces quantitative risk level that can be measured and treated. General steps for the proposed framework are: identifying assets and stakeholders, understanding security requirements, assessing vulnerabilities, analyzing the effectiveness of controls, evaluation of risks by estimating frequency and impact of exploit, designing remediation plans and finally drive decisions using powerful reporting. Fig. 3 shows the proposed framework for Quantitative Information Security Risk Assessment:

### 4.1. Assets and stakeholders identification

The risk assessment techniques require to clearly specifying the assets. This step of proposed model defines the boundaries and contents of the asset to be assessed. In proposed framework information is taken as an asset.

### 4.2. Understanding security requirements

In this step, along with the resources and the information that constitute the system, the boundaries of the IT system will be identified. This step defines the scope of the risk assessment effort and provides information essential to defining the risk. The input for this step is information about hardware, software, data and information, network connections and system interfaces; and the output is a document that describes system mission, system boundary, system functions and information about criticality and sensitivity of data.

### 4.3. Threats and vulnerabilities identification

In this step, threat scenarios are created by listing the most common combinations of attack paths, attack goals and attack actor (attackers or hackers), that might lead to the compromise an asset.

### 4.4. Analysis of effectiveness of controls

In this step of assessment technical controls like authentication and authorization, intrusion detection, network filtering and routing, and encryption are considered and a document is prepared as