Computer Standards & Interfaces 42 (2015) 1–8

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Effects of virtualization on information security

Shing-Han Li [a,1], David C. Yen [b,2], Shih-Chih Chen [c,3], Patrick S. Chen [d,4], Wen-Hui Lu [d,5], Chien-Chuan Cho [d,*]

[a] Department of Accounting Information, National Taipei University of Business, 321, Sec.1, Chi-Nan Rd., Taipei 100, Taiwan
[b] School of Economics and Business, SUNY College at Oneonta, 226 Netzer Administration Bldg., Oneonta, NY, United States
[c] Department of Accounting Information, Southern Taiwan University of Science and Technology, No. 1, Nan-Tai Street, Yungkang Dist., Tainan City 710, Taiwan
[d] Department of Information Management, Tatung University, 40 ChungShan North Road, 3rd Section, Taipei 104, Taiwan

ARTICLE INFO

Article history:
Received 6 June 2014
Received in revised form 23 March 2015
Accepted 23 March 2015
Available online 1 April 2015

Keywords:
Virtualization
Information security
ISO 27001
Information security management
Information technology

ABSTRACT

Virtualization provides the essential assistance to save energy & resources and also simplify the required information management. However, the information security issues have increasingly become a serious concern. This study investigates the post-virtualization business security landscape related to system security. A questionnaire is developed based on 133 control management principles of ISO/IEC 27001 standard and a sampling technique is employed to collect responses from IT professionals with an understanding of virtualization information environment. The obtained findings suggest that virtualization may be beneficial to certain industrial sectors in handling the issues of information security.

1. Introduction

Cloud computing is one of the critical topics in the IT domain in the 21st century. After years of rigorous and enthusiastic discussion, cloud computing has gradually evolved from concept introduction to application development and consequently become one of the promising fields in which enterprises and the IT industry start to invest massively. The features of cloud computing technology may include super-large scale, dynamic scalability and on-demand deployment and in which virtualization plays an important role. In addition, enterprises began to realize the importance of virtualization and invest heavily in its implementation [37]. According to a recent ESG's 2011 IT Spending Intentions Survey, more than 60% of surveyed organizations will increase their spending on virtualization software in 2011 [15].

Apparently, the IT industry has already started to accept virtualization. The question — "how does/can virtualization benefit business?" is still an important one to be answered. Among the potential benefits, virtualization helps to centralize and integrate IT resources. Centralized data storage makes data easier to back up, prevents redundancy, and improves control. It also facilitates a better compliance to IT regulations and management. Secondly, virtualization helps to reduce the number of servers, and by doing so, it tends to reduce the usage of power and cooling facilities. The reduced number of servers and power usage can not only relieve the pressure of efficiency IT management, but also conform to the pervasive trend toward global green energy. With these aforementioned benefits, there are however many issues to be addressed and resolved regarding the implementation and/or adoption of virtualization. Namely, one of the most important issues may be the security concerns regarding virtual machines and virtualized environments. Recent researches and/or studies revealed both challenging and beneficial aspects of virtualization regarding information security [11,22,54,69]. Further, it is highly suggested that security measures shall be implemented and adopted as businesses move toward virtualization [42,66]. The implementation of security measures, however, requires specific regulations to support, audit and monitor. The ISO/IEC 27001 Standard [26] is currently one of the most widely accepted information security standards and therefore is highly suitable to serve as one guideline for the implementation and evaluation of different information security measures of virtualized systems.

This study focuses on the impacts of a virtualized information environment on information security. A business may be exposed to threats and problems that occurred due to mismanagement and/or compromised security measures. To fully understand the influence of virtualization on information security, a questionnaire is designed

* Corresponding author. Tel.: +886 9 33002536.
E-mail addresses: shli@ntub.edu.tw (S.-H. Li), David.Yen@oneonta.edu (D.C. Yen), scchendr@mail.stust.edu.tw (S.-C. Chen), chenps@ttu.edu.tw (P.S. Chen), d9906007@ms.ttu.edu.tw (W.-H. Lu), chinch.uancho@gmail.com (C.-C. Cho).
[1] Tel.: +886 2 23226571 (office); fax: +886 2 23226369.
[2] Tel.: +1 3820 607 436 3458; fax: +607 436 2543.
[3] Tel.: +886 6 253 3131.
[4] Tel.: +886 2 25925252 ext.3609.
[5] Tel.: +886 2 25925252 ext.3610.

http://dx.doi.org/10.1016/j.csi.2015.03.001
0920-5489/

based on ISO/IEC 27001 to collect responses from IT practitioners with experiences in the area of virtualization either in the specific enterprises or in the IT service industry. A combination of the ISO/IEC 27001-based questionnaire and viewpoints gathered from IT practitioners in fact provides a new direction for addressing and examining the issues of virtualization and information security. Results of the questionnaire survey are intended to reveal the post-virtualization business security landscape from the aspect of system security. In summary, this study would like to address the following research questions.

(1) From the viewpoint of Physical and Environmental Security, does the implementation of virtualization in an enterprise significantly affect the resulting information security?
(2) From the viewpoint of communications and operations management, does the implementation of virtualization in an enterprise significantly affect the resulting information security?
(3) From the viewpoint of Access Control, does the implementation of virtualization in an enterprise significantly affect the resulting information security?
(4) From the viewpoint of Information System Acquisition, Development and Maintenance, does the implementation of virtualization in an enterprise significantly affect the resulting information security?

This study consists of six parts. Section 1 introduces the background and the scope of this study. The next section reviews the relevant literatures related to information security and virtualization. Section 3 describes the research methodology including sampling and questionnaire design. Sections 4 and 5 provide the statistical analyses of the surveyed results and the discussion of the research questions, accordingly. Finally, the last section summarizes the findings, discusses the contributions of this study and provides some future research directions.

2. Literature review

This study investigates the impact of virtualization on information security. This literature review section is mainly composed of two subsections and they are the information security part and virtualization part. The former one introduces the current state of information security researches and ISO/IEC 27001 standard while the latter reviews these studies regarding virtualization and related technologies.

2.1. Information Security Management System (ISMS)

Issues regarding information security have been covered on the rise in recent years, and this fact leads to the development of researches related to various aspects of information security. Table 1 lists researches related to information security, categorized by different information security issues. Some of the studies are also related to virtualization. Because of the relevancy of these aforementioned two subjects, a suitable assessment tool may be required to evaluate how virtualization affects information security. The ISO/IEC 27001 is one of the most widely accepted auditing standards for assessing information security, and therefore it is appropriate to be used and adapted by this study to assess the effects of virtualization on information security.

The ISO/IEC 27000 series of standards published by the International Standard Organization (ISO) and International Electrotechnical Commission (IEC) are the standards dedicated to information security. Specifically, the ISO/IEC 27001 standard (Information technology–Security techniques–Information security management systems–Requirements) provides the important definition and requirements of an Information Security Management System (ISMS) [77]. Originally evolved from the BS 7799 standard of the British Standards Institution (BSI), the current version of ISO/IEC 27001 is ISO/IEC 27001:2005 [4].

Table 1
Information security issue review.

Information security issue	Topic	Literature
Business network security	Network security tools, software and products: To enhance internet and intranet security, security tools, products and/or software may be used.	[8,49,53,61]
	User's trust and perceived security in online environment.	[25,59,60]
	Virtual Private Network (VPN): Online resources can be remotely accessed via the VPN.	[10,75]
Business data protection	Hard disk- and file-level encryption: Using encryption tools and/or software to encrypt disks and/or files may keep data from unauthorized access in the case of a leak.	[6,39]
	Information leakage prevention: Building an information leakage monitoring system may uncover and/or prevent hostile eavesdropping.	[5,70]
	Database security control: The encryption of data and auditing of database access may reduce the likelihood of security breach.	[14,62]
Enterprise personnel identification and access control	Personnel identification management: It is suggested to establish an identification and password management policy.	[46,67]
	User authentication service: Methods such as single sign-on or smart card authentication may be implemented.	[2,38]
	Web site user authentication: It is suggested that the systems only allow authorized user to access contents and use single sign-on to prevent threats from hacking.	[9,55]
Security auditing, implementation and standards	ISO 27001: It includes auditing standards, guidelines and implementation.	[3,19]
	COBIT: It focuses on the IT processes.	[12,56]
Security of applications and platforms	O.S. security: A reasonably secure O.S. for PCs and servers is vital to security.	[72,73]
	Risk management: The management and examination of weaknesses is required.	[48,52]
	Cloud security; virtualization security	[11,16,54,58]
	Security concerns and assessment regarding virtualization.	[22,41,69]
Threats to information security	Malware includes viruses, Trojan horses, spyware, computer worms, rootkits and adware.	[13,35,40]
	Hacking tools and tricks: Hackers are always developing new tools, ways and technologies of attack.	[33,51]
	Application-level attacks: Many hackers now have turned from O.S.-level attacks to buffer-overflow and cross-site scripting attacks.	[50,71]

The ISO/IEC 27001 standard follows the PDCA cycle (Plan, Do, Check and Act) and includes 11 Control Areas. Namely these areas include (1) Security policy, (2) Organization of information security, (3) Asset management, (4) Human resources security, (5) Physical and Environmental Security, (6) Communications and operations management, (7) Access Control, Information systems acquisition, (8) Development and Maintenance, (9) Information security incident management, (10) Business continuity management, and (11) Compliance [4,77]. This standard is the evaluation and auditing foundation for creating, implementing and maintaining ISMS. A number of certification bodies around the world are accredited by national standard bodies to audit the compliance with ISO/IEC 27001 and issue certificates to participating organizations.