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.

### 2.2. Virtualization technologies

The concept of virtualization originated in the 1960s when the costs of mainframes were very expensive. IBM divided a large UNIX mainframe into multiple logic instance to enable users to fully utilize a mainframe's calculation resources [63]. Each logic instance is essentially a virtual machine (VM) or a guest operating system (OS). As the OS or the hardware of the mainframe computer may have different compatibilities with VMs, a virtual machine monitor, called hypervisor, may be needed to serve as the interface between VMs and the physical hardware [29]. As shown in Fig. 1, each virtual machine has its own virtualized resources including I/O ports and DMA channels, and these VMs are capable of running on any OS through the hypervisor, as long as the hardware is supported by the OS [29]. In other words, the hypervisor is the key. In the example of VMware's solution, the hypervisor of VMware, called VMware Virtualization Layer, is capable of hosting multiple virtual machines with a shared CPU, memory, network driver and hard disk space. On the other hand, the hypervisor is inevitably having security vulnerability and is susceptible to hacker attacks, requiring a higher level of information security management [21].

Virtualization technologies have been increasingly adopted in recent years and researches are emerging in this subject field. Table 2 lists several related research topics. Specifically, in terms of information security, the study of Vaughan-Nichols [69] pointed out that virtualization creates certain challenges for organizations and suggested that organizations should look closely at their virtualization systems for different security issues. Hoesing [22] in his review of virtualization security assessment techniques further argued that the security risks of virtualization comprise those carried over from a physical server environment, those amplified with virtualization due to the speed and ease to deploy computing resources and those unique to the virtualization tools. Huang et al. [24] reviewed the known security impacts of virtualization on a network testbed and suggested that correct configurations, proper optimization, and conscientious connectivity management must be implemented to minimize such security impacts. Zissis and Lekkas [76] evaluated major virtualization security issues in cloud computing and proposed a trusted third party as the solution to provide end-to-end security services with the establishment of the necessary trust level between entities across the network.

On the other hand, virtualization also brings new schemes of information security. For example, Christodorescu et al. [11] proposed a cloud security monitoring system with the design of placing the monitoring system on a virtual machine and monitor the cloud system from the outside through virtual-machine introspection. Such introspection monitoring allows an assessor to perform the monitoring of a guest VM at any time in its life cycle without knowing the guest OS in advance and assessing to the OS source code, suitable for both Windows and Linux systems [11]. Li et al. [36] proposed CyberGuarder, a virtualization-based security assurance architecture for green cloud computing. CyberGuarder was designed to be carried on net software operating systems to provide three services: a virtual machine security service, a virtual network security service, and a policy-based trust management service, and the preliminary test of CyberGuarder showed promising results [36].

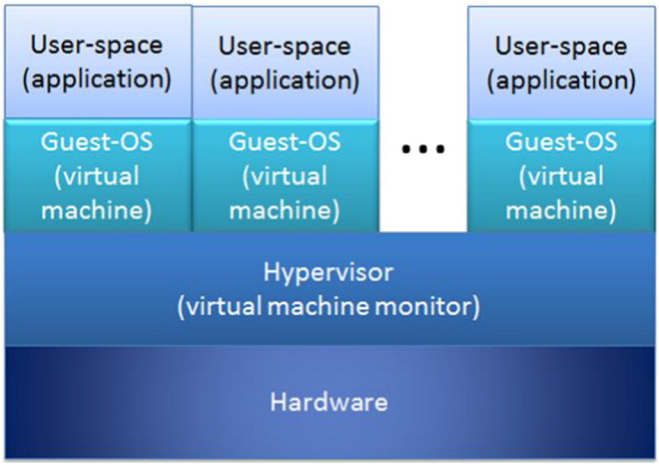


**Fig. 1.** Overview of virtualization environments. [29].

**Table 2**
Virtualization literature review.

| Server virtualization issues | Topic | Literatures |
|---|---|---|
| Server virtualization management tools | Virtual machine tuning: Setting up highly-efficient but also responsive virtual machines can be very difficult for system administrators. | [28,31] |
| Security monitoring and policy of server virtualization | Concerns regarding virtualization security. Cloud security through virtualization. Risk monitoring of virtualized servers: Virtualized systems do have their own security risks. The O.S., virtualization tools and the network all have their own share of risks. Security design for virtualized systems. Server virtualization guidelines: In an IT management plan, virtualized servers must follow the policy and rules. | [11,17,22,24,30,54,57,69,76] |
| Infrastructure and framework of server virtualization | Servers and virtualization: If virtualization is used to consolidate server usage, some infrastructure problems must be addressed. Network virtualization issues: Even if top-grade virtualization software and server hardware are used, networking bottlenecks and/or other technical glitches may bring down the system. | [10,44,68,74] |
| Backup and disaster recovery plans for virtualized systems | Backup and disaster recovery: Server virtualization requires planning of backup plans and disaster recovery. | [32,45] |
| Server virtualization plans and usage | Cloud computing: The cloud computing architecture demands much more server capacity and raw computing power. | [23,64,65] |
| Benefits of server virtualization | Server consolidation: Virtualization can reduce server costs. | [7,43] |

## 3. Research methods

This research studies the impacts of virtualization on information security. In the following sub-sections, the research design, questionnaire design, research subjects and sampling, and analysis method are described subsequently. In particular, the questionnaire design employs the Content Validity Ratio (CVR) analysis to extract important questionnaire items from ISO/IEC 27001 controls [34]. In this study, the items were reviewed by a panel of subject area experts (SAEs) who were

knowledgeable and experienced in the area of virtualization and information security.

### 3.1. Research design

The research framework is developed under ISO/IEC 27001 controls. Fig. 2 depicts the research framework of this study. Through an expert-panel's review with the use of CVR analysis, questionnaire items are extracted and independent/dependent variables are identified.

### 3.2. Research subjects and sampling

This study requires that subjects have a certain level of understanding of the virtualization information environment. The research subjects, sampling method and sampling workflow are described in detail in the following sub-sections.

#### 3.2.1. Research subjects

With such a technology-specific research topic, the subjects of this research are limited to IT professionals with an understanding of the virtualization information environment. Therefore, this study locates its suitable subject population in IT industry workers and IT professionals in enterprises.

#### 3.2.2. Sampling

Purposeful sampling, which selectively chooses survey respondents to provide an in-depth discussion about the issues of research focus, is employed by this study to extract information about the influence of virtualization on information security. Both web-based and paper-based questionnaires are distributed to selected subjects. Questions are provided at the beginning of the questionnaire to filter out those respondents having insufficient knowledge of virtualization. The distribution and collection of questionnaires were completed in a time period of about 6 weeks. A total of 133 valid web-based questionnaires were collected out of 400 email invitations. In addition, 17 valid paper-based questionnaires were collected from 20 distributed questionnaires. Consequently, the total number of valid questionnaires is 150.

### 3.3. Designing the measurement tools for this research

#### 3.3.1. The construction of the questionnaire

This research intends to study the impacts on information security by virtualization. The ISO/IEC 27001 standard is employed as the framework for information security management systems. As discussed earlier, it is a worldwide accepted evaluation and auditing tool for information security systems. Therefore, this study develops the research questionnaire based on the 133 controls of the ISO/IEC 27001 standard. To select the questionnaire items from the 133 controls, this study employs the Content Validity Ratio (CVR) analysis proposed by Lawshe [1,20,27,34] to evaluate the essentialness of each control to the research goal.

A 13-member expert panel was formed to conduct the CVR analysis. The experts are selected from senior IT professionals with at least 10 years of experiences. Each ISO/IEC 27001 control was evaluated and marked as either “required” or “not required” for the purpose of this study. The CVR value is then calculated as:

$$CVR = (n - N/2)/(N/2),$$

where n is the total number of experts answering a response of “required” or having the affirmative votes on a specific ISO/IEC 27001 control, and N is the number of experts. Following the recommendation of Lawshe [34], this study sets the lowest acceptable CVR value at 0.54. For this study, an ISO/IEC 27001 control having a CVR value exceeding 0.54 is considered highly relevant to the research topic and is thus adapted to become one of the questionnaire items. There are 32 qualified ISO/IEC 27001 controls which can be categorized to 5 dimensions: “Asset Management,” “Physical and Environmental Security,” “Communication and Operation Management,” “Access Control,” and “Information System Acquisition, Development and Maintenance.” To satisfy the dimension reliability, this study examined the internal consistency of the questionnaire items after checking the values of Cronbach's alpha with a number larger than 0.7. This study adapts these 32 controls to create the final research questionnaire (as listed in Table 3).

#### 3.3.2. Questionnaire contents

The questionnaire consists of three parts and they are (1) personal information — including the respondent's gender, age, educational

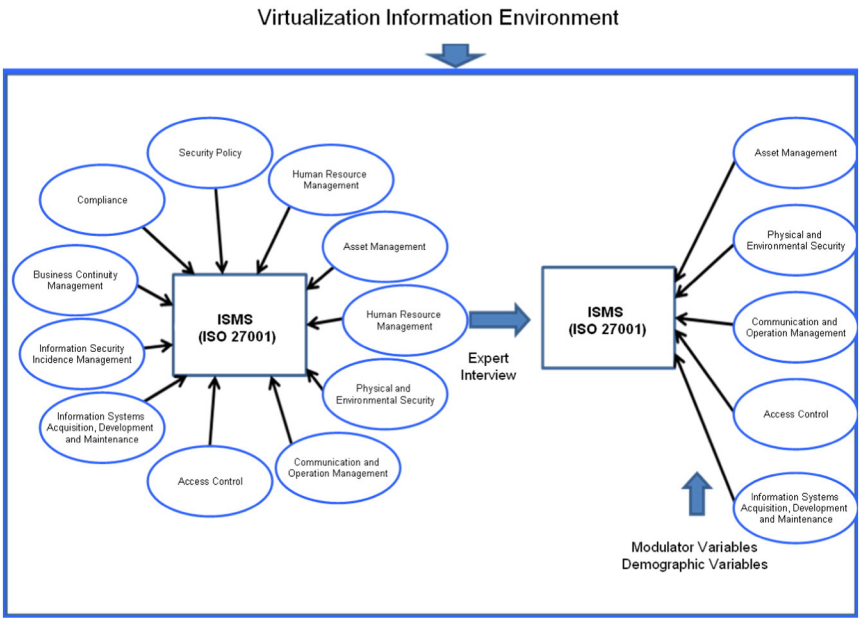


**Fig. 2.** Research framework.

background, job title, and time of employment in an IT-related field; (2) company information — including the industry sector, business type, company scale, and number of IT-related employees of the respondent's company, and (3) "The Survey of Information Security of the Virtualized Information Systems" — containing the questions adapted from the 32 qualified ISO/IEC 27001 controls regarding the virtualized information environment and information security. This study uses a 7-point Likert scale with values ranging from 1 to 7 to represent "Extremely Harmful", "Harmful", "Slightly Harmful", "Irrelevant", "Slightly Helpful", "Helpful" and "Extremely Helpful", respectively, in order to evaluate the respondent's opinion about the influence of virtualization on each questionnaire item. As each questionnaire item represents one of the 32 controls of ISO/IEC 27001, a high score means that the respondent believes that the implementation of virtualization information environment is helpful to information security, while a low score indicates that the respondent believes that the implementation of virtualization information environment may harm the resulting information security.

*3.3.3. Reliability test for the questionnaire*

After collecting the filled questionnaires, this study converted the data in valid samples to a format compatible with SPSS (The Statistical Package for the Social Sciences) and subsequently performed the reliability analysis using SPSS V18 for Windows. The Cronbach's alpha coefficient was used to evaluate the internal consistency of questionnaire items under the same category or dimension. For an exploratory research, questionnaire items are considered reliable only if the alpha value is equal to or larger than 0.7 [18,47]. The dimension "Asset Management" contains only one questionnaire item, not suitable for a reliability test and therefore it is not included in the questionnaire. The Cronbach's alpha coefficients for items in the other 4 dimensions ("Physical and Environmental Security," "Communication and Operation Management," "Access Control," "Information System Acquisition, Development and Maintenance") are all larger than 0.7 (see Table 3), and therefore the questionnaire items in this study are considered to be reliable.

**Table 3**
Summarization of reliability analysis.

| Dimensions | Questionnaire Item | Item # | Cronbach's alpha |
|---|---|---|---|
| Physical and Environmental Security | Equipment siting and protection | Q5 | 0.924 |
| | Cabling security | Q6 | |
| | Equipment maintenance | Q7 | |
| | Secure disposal or re-use of equipment | Q8 | |
| Communication and Operation Management | Separation of development, test, and operational facilities | Q9 | 0.952 |
| | Capacity management | Q10 | |
| | System acceptance | Q11 | |
| | Controls against malicious code | Q12 | |
| | Information backup | Q13 | |
| | Network controls | Q14 | |
| | Management of removable media | Q15 | |
| | Disposal of media | Q16 | |
| | Information handling procedures | Q17 | |
| | Security of system documentation | Q18 | |
| | Audit logging | Q19 | |
| | Monitoring system use | Q20 | |
| | Protection of log information | Q21 | |
| | Administrator and operator logs | Q22 | |
| | Fault logging | Q23 | |
| | Clock synchronization | Q24 | |
| Access Control | User registration | Q25 | 0.927 |
| | User password management | Q26 | |
| | Policy on use of network services | Q27 | |
| | Remote diagnostic and configuration port protection | Q28 | |
| | Network connection control | Q29 | |
| | Sensitive system isolation | Q30 | |
| | Teleworking | Q31 | |
| Information System Acquisition, Development and Maintenance | Control of operational software | Q32 | 0.913 |
| | Protection of system test data | Q33 | |
| | Technical review of applications after operating system changes | Q34 | |
| | Control of technical vulnerabilities | Q35 | |
| Asset Management | Acceptable use of assets | Not included in questionnaire | |

## 4. Data analysis

All collected data were analyzed using SPSS V18. The statistical analyses employed include reliability test, T-test, ANOVA, Scheffe's multiple comparison, and logistic regression analysis.

Referring to Table 4, the major distributions of the demographic information may include the following information. In specific, (1) most participants of the questionnaire are male (82.7%); (2) the ages of the participants range mainly from 31 to 40 (71.3%); (3) most of the participants have a college degree or higher (72.7%); (4) more than half of the participants majored in computer science or related disciplines (59.4%); (5) only 19.3% of the participants have professional certificates in virtualization and information security, while some other participants have Microsoft certificates (33.3%) and some have no professional certificates (36.7%); (6) two major groups of participants' job positions are either enterprise IT staff (34.7%) or IT engineers working in the IT industry (34.7%); (7) most of the participants have been working in IT-related fields for 5 years or more (72.0%); (8) more than half of the participants work less than 5 years in their current job positions (50.7%) and (9) most of the participants' employers are in the IT industry (62.7%).

Table 5 lists the average score and standard deviation of the answers to questionnaire items in each of the four ISO/IEC 27001 dimensions: "Physical and Environmental Security," "Communication and Operation Management," "Access Control" and "Information System Acquisition, Development and Maintenance." As all four dimensions have a frequency distribution approaching or exceeding 5, it is clear that virtualization can indeed benefit information security from the participants' views.

Table 6 summarizes the results of one-way ANOVA and Scheffe's Test for the differences in responses of participants with different job titles and from different industry sectors. The results of ANOVA F-test reveal that except for "Access Control," there is significantly conceived influence on information security from virtualization. In specific, Scheffe's Test provides more detailed results within each job position

**Table 4**
Brief summary of participants' demographic distribution.

| Question | Major distribution | Frequency | Percentage (%) |
|---|---|---|---|
| Gender | Male | 124 | 82.7 |
| Age | 31–35 years old | 66 | 44.0 |
| | 36–40 years old | 41 | 27.3 |
| Education degree | University | 64 | 42.7 |
| | Graduate school + | 45 | 30.0 |
| Education background | IT-related | 89 | 59.4 |
| Specialized certificates | Microsoft Professional Certificate | 50 | 33.3 |
| Job position | IT staff (enterprise) | 52 | 34.7 |
| | IT professionals (IT industry) | 52 | 34.7 |
| Time spent in IT-related professions | 5–10 years | 56 | 37.3 |
| | 10 years + | 52 | 34.7 |
| Time spent in current position | 1–3 year old | 40 | 26.7 |
| | 3–5 year old | 36 | 24.0 |
| Industry sector of your company | Information industry | 94 | 62.7 |
| The scale of your company | More than 500 employees | 53 | 35.3 |
| Number of employees in your company's IT department | More than 10 employees | 79 | 52.7 |

**Table 5**
Score distribution for the four ISO/IEC dimensions.

| Dimension | Average score of frequency distribution | Standard deviation of frequency distribution |
|---|---|---|
| Physical and Environmental Security | 5.382 | 1.2753 |
| Communication and Operation Management | 4.876 | 1.0918 |
| Access Control | 4.885 | 1.1640 |
| Information System Acquisition, Development and Maintenance | 5.060 | 1.2739 |

**Table 7**
Results of logistic regression analysis.

| | Beta coefficient | S.E. | Wald | df | Significance level |
|---|---|---|---|---|---|
| Intercept | −1.602 | 1.436 | 1.243 | 1 | .265 |
| Physical and Environmental Security | 0.118 | 0.288 | 0.167 | 1 | .683 |
| Communication and Operation Management | 1.537 | 0.724 | 4.512 | 1 | 0.034* |
| Access Control | −0.504 | 0.509 | 0.983 | 1 | .322 |
| Information System Acquisition, Development and Maintenance | −0.873 | 0.564 | 2.396 | 1 | .122 |

and industry and these information are that (1) in the dimension of "Communication and Operation Management," only engineers in the IT Industry consider virtualization has a significant influence on information security; (2) in "Access Control," both enterprise IT managers and IT industry engineers conceive a significant influence on information security on virtualization; (3) in "Physical and Environmental Security," the electronics, IT, and automobile industries believe that virtualization has a significant influence on information security; and (4) only the IT and automobile industries consider that virtualization has a significant influence on information security.

To reflect the perceptual differences among the different experience levels, we employed a new dependent variable by splitting "Time Spent in IT Related Professions" into two values (5–10 years versus more than 10 years) and used ISO/IEC dimensions as the independent variables. The logistic regression is thus executed in this study (as shown in Table 7). The independent variables are the four dimension in this study (i.e., "Physical and Environmental Security," "Communication and Operation Management," "Access Control" and "Information System Acquisition, Development and Maintenance"), and the dependent variable is the "Time Spent in IT Related Professions". The analysis result of logistic regression showed that "Communication and Operation Management" is the most critical determinant in this study.

## 5. Discussion

This study intends to understand the impacts of virtualization onto the information security. Through the examination of the 32 controls selected from ISO/IEC 27001, the specific dimensions of information security that are identified to be influenced by the implementation of virtualization, with some variations existing across the participants' demographic backgrounds. The four proposed research questions and hence research contributions are addressed below.

(1) Question 1 relates to the viewpoint of Physical and Environmental Security and is proposed to see whether the implementation of virtualization in an enterprise significantly affects information security. The answer is positive for electronics, IT, and automobile industries, but negative for the banking industry. Information security is one of the greatest concerns in the banking industry and high-level information security measures are always used for all banking operations. It can be understood that no significant differences in information security can be found before and after the implementation of virtualization if the implementation is conducted under the same high-level information security measures.

(2) Question 2 is associated with the viewpoint of communications and operations management, and proposed to see whether the implementation of virtualization in an enterprise significantly affects information security. Results suggest that practitioners working in the IT industry in particular conceive the influence of virtualization on information security. One possible justification is that virtualization provides an isolated information environment for software development and testing. Another reason may be that the fast backup and recovery enabled in the virtualized environment allows practitioners to perform modifications and improvements to information systems in a timely manner.

(3) Question 3 is proposed from the viewpoint of Access Control, and it is designed to check whether the implementation of virtualization in an enterprise significantly affects information security. The obtained findings indicate that virtualization has influences on information security regarding Access Control in IT and automobile industries. In fact, referring to Fig. 1, virtual machines on the hypervisor are well-isolated and this feature does enable good access control.

(4) Question 4 concerns from the viewpoint of Information System Acquisition, Development and Maintenance and is proposed to locate whether the implementation of virtualization in an enterprise significantly affects information security. However, results show that no significant influences exist for all surveyed industries.

**Table 6**
ANONA and Scheffe test results.

| Variable name | Physical and Environmental Security | | Communication and Operation Management | | Access Control | | Information System Acquisition, Development and Maintenance | |
|---|---|---|---|---|---|---|---|---|
| | F | Scheffe | F | Scheffe | F | Scheffe | F | Scheffe |
| IT staff (Enterprise) | 3.415* | No significant differences | 3.101* | No significant differences | 2.228 | No significant differences | 2.738* | No significant differences |
| IT manager (Enterprise) | | No significant differences | | No significant differences | | significant differences | | No significant differences |
| Engineer (IT industry) | | No significant differences | | significant differences | | significant differences | | No significant differences |
| Manager (IT industry) | | No significant differences | | No significant differences | | No significant differences | | No significant differences |
| IT personnel (IT industry) | | No significant differences | | significant differences | | No significant differences | | No significant differences |
| Electronics industry | 4.357** | Significant differences | 3.111* | No significant differences | 3.41* | No significant differences | 3.41* | No significant differences |
| IT industry | | Significant differences | | No significant differences | | Significant differences | | No significant differences |
| Automobile industry | | Significant differences | | No significant differences | | Significant differences | | No significant differences |
| Bank and securities industry | | No significant differences | | No significant differences | | No significant differences | | No significant differences |
| Other | | Significant differences | | No significant differences | | No significant differences | | No significant differences |

* $P < 0.05$.
** $P < 0.01$.

Results of data analysis also show that IT professionals in different job positions conceive differently in the influence of virtualization on information security. Such differences may be caused by the different practical experiences related to different job functions/tasks.

## 6. Conclusion

This research studies the influence of virtualized information environment on information security. The results of the analysis have shown that the implementation of virtualization in enterprises may prove to be particularly beneficial to information security. Scheffe's Test reveals that for the electronics, IT and automobile industries, the implementation of the virtualization information environment indeed has a significant influence on information security in the aspect of "Physical and Environmental Security." For the IT and automobile industries, virtualization also has a significant influence on information security in the aspect of "Access Control." The IT industry professionals and enterprise IT managers conceive a significant influence from virtualization on information security in the aspect of "Communication and Operation Management." As for the "Information System Acquisition, Development and Maintenance" dimension, the introduction of virtualization technologies however, does not significantly affect information security.

For the implications and contributions of this study, this study provides new approaches of investigating the influence of virtualization on information security. The combination of a questionnaire based on ISO/IEC 27001 and the viewpoints from IT practitioners lead to new aspects for future academic researches in the subject areas of virtualization and information security. For IT practitioners and enterprises, the information about different influences of virtualization on information security in different dimensions across different industries may provide some useful information security guidelines for the IT practitioners in the consideration, adoption and/or implementation of virtualization.

Despite these aforementioned findings, this study may have some limitations. Both the content validity and reliability aspects of the study were limited by a small sample size. Only 13 experts participated in the first round of the validity study, which precluded the strict use of the CVR to establish a statistical significance. Moderate attrition also occurred in the reliability phase of this study. A larger sample size for both phases I and II would have improved the strength or our validity and helped to mitigate the attrition in phase II. After the large empirical data collected, some advanced statistical analysis methods (e.g., Structural Equation Modeling) can be employed to assess the model stability, and apply/examine the proposed model/measurement items to the different relevant information security environments.

The following are some suggestions that may be helpful to future researchers.

(1) While this research adopted ISO 27001 as the auditing standard, other information security standards, such as COBIT and ITIL, may also be used to accomplish the purpose of this study. Choosing or comparing with a different standard may provide additional insights about the influence of virtualization on information security.
(2) With virtualization technologies becoming more matured and widely-accepted, more samples shall be collected to incorporate other industries to improve data reliability and validity. By doing so, some detailed or additional suggestions/findings may be provided to businesses that are planning to adopt or implement virtualization.
(3) Exploratory and confirmatory factor analyses should be evaluated in the near future for having a better understanding of the measurement scales proposed in this study. Future research may be needed to discern whether these key factors are attributable to the divergent IT/IS experts and users.

## References


[1] D. Ary, L. Jacobs, A. Razavieh, Introduction to Research in Education, 7th Ed Wadsworth Publishing, New York, NY, 2005.
[2] M. Bogicevic, I. Milenkovic, D. Simic, Identity management—a survey, Innovative Management and Firm Performance: An Interdisciplinary Approach and Cases2014. (370).
[3] A. Calder, Implementing Information Security Based on ISO 27001/ISO 27002, Van Haren Publishing, Zaltbommel, NL, 2012.
[4] T. Carlson, Understanding ISO 27001. Available at http://www.orangeparachute.com/documents/Understanding_ISO_27001.pdf 2005.
[5] M. Carpenter, Integrated security risk management solution is a key to protecting government networks, Homel. Def. J. 5 (1) (2007) 40–41.
[6] E. Casey, G.J. Stellatos, The impact of full disk encryption on digital forensics, ACM SIGOPS Oper. Syst. Rev. 42 (3) (2008) 93–98.
[7] Q. Chen, R. Xin, Optimizing enterprise IT infrastructure through virtual server consolidation, Proc. 2005 Inf. Sci. IT Educ. Joint Conf., 19, 2005 (2009).
[8] R.M. Chen, K.T. Hsieh, Effective allied network security system based on designed scheme with conditional legitimate probability against distributed network attacks and intrusions, Int. J. Commun. Syst. 25 (5) (2012) 672–688.
[9] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B.F. Machado, A. Forget, R. Biddle, The MVP Web-based Authentication Framework. Financial Cryptography and Data Security (pp. 16–24), Springer, Berlin, DE, 2012.
[10] N.M. Chowdhury, R. Boutaba, A survey of network virtualization, Comput. Netw. 54 (5) (2010) 862–876.
[11] M. Christodorescu, R. Sailer, D.L. Schales, D. Sgandurra, D. Zamboni, Cloud security is not (just) virtualization security: a short paper, Proc. 2009 ACM Wkshp. Cloud Comput. Secur 2009, pp. 97–102.
[12] S. De Haes, W. Van Grembergen, R.S. Debreceny, COBIT 5 and enterprise governance of information technology: building blocks and research opportunities, J. Inf. Syst. 27 (1) (2013) 307–324.
[13] M. Egele, T. Scholte, E. Kirda, C. Kruegel, A survey on automated dynamic malware-analysis techniques and tools, ACM Comput. Surv. (CSUR) 44 (2) (2012) 6.
[14] B. Elisa, S. Ravi, Database security—concepts, approaches, and challenges, IEEE Trans. Dependable Secur. Comput. 2 (1) (2005) 2–19.
[15] Enterprise Strategy Group, ESG Research Brief: 2011 Virtualization Software Spending Trends. Available at http://www.enterprisestrategygroup.com/2011/02/esg-research-brief-2011- virtualization-software-spending-trends/ 2011.
[16] D.G. Feng, M. Zhang, Y. Zhang, Z. Xu, Study on cloud computing security, J. Softw. 22 (1) (2011) 71–83.
[17] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv. 9 (2) (2011) 50–57.
[18] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, Multivariate Data Analysis: A Global Perspective, 7th Ed. Pearson Prentice Hall, Upper Saddle River, NJ, 2010.
[19] D.A. Haworth, L.R. Pietron, Sarbanes–Oxley: achieving compliance by starting with ISO 17799, Inf. Syst. Manag. 23 (1) (2006) 73–87.
[20] S.N. Haynes, D.C.S. Richard, E.S. Kubany, Content validity in psychological assessment: a functional approach to concepts and methods, Psychol. Assess. 7 (3) (1995) 238–247.
[21] K.J. Higgins, VMs create potential risks. Available at http://www.darkreading.com/security/security-management/208804369/index.html 2007.
[22] M.T. Hoesing, Virtualization security assessment, Inf. Secur. J.: Glob. Perspect. 18 (3) (2009) 124–130.
[23] C.T. Hsieh, Strategies for successfully implementing a virtualization project: a case with VMware, Commun. IIMA 8 (3) (2014) 1.
[24] Y.L. Huang, B. Chen, M.W. Shih, C.Y. Lai, Security impacts of virtualization on a network testbed, Proc. SERE 2012 2012, pp. 71–77.
[25] S. Iizuka, K. Ogawa, S. Nakajima, Factors affecting user reassurance when handling information in a public work environment, Int. J. Hum. Comput. Interact. 23 (1–2) (2007) 163–183.
[26] International Organization for Standardization, ISO/IEC 27001: 2005. Available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103 2005.
[27] B. Johnson, L. Christensen, Educational Research: Quantitative, Qualitative, and Mixed Approaches, 2nd ed. Pearson, New York, NY, 2004.
[28] T.A. Johnson, Server virtualization: information security considerations, Information Security Management Handbook, 6 2012, p. 101.
[29] T. Jones, Discover the Linux Kernel Virtual Machine. Available at: http://www-128.ibm.com/developerworks/linux/library/l-linux-kvm/ 2007.
[30] M. Kallahalla, M. Uysal, D. Swaminathan, E. Nigel, C.I. Dalton, F. Gittler, SoftUDC: a software-based data center for utility computing, IEEE Comput. Soc. 37 (11) (2004) 38–46.
[31] G. Khanna, Y. Beaty, G. Kar, A. Kochut, Application performance management in virtualized server environments, Proc. 10th IEEE/IFIP Netw. Oper. Manage. Symp 2006, pp. 373–381.
[32] M.A. Khoshkholghi, A. Abdullah, R. Latip, S. Subramaniam, M. Othman, Disaster recovery in cloud computing: a survey, Comput. Inf. Sci. 7 (4) (2014) 39.
[33] G. Kovacich, ISSO career development, Comput. Secur. 16 (6) (1997) 455–468.
[34] C.H. Lawshe, A quantitative approach to content validity, Pers. Psychol. 28 (4) (1975) 563–575.
[35] G. Lawton, Virus wars: fewer attacks, new threats, Computer 35 (12) (2002) 22–24.
[36] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, K.P. Lam, CyberGuarder: a virtualization security assurance architecture for green cloud computing, Futur. Gener. Comput. Syst. 28 (2012) 379–390.
[37] Q. Li, C. Yang, Development trends of MIS based on cloud computing environment, 2010 Int. Symp. Inf. Sci. Eng. (ISISE) 2010, pp. 145–148.

[38] T.E. Lindquist, K.A. Gary, H.E. Koehnemann, H. Naccache, Component framework for web-based learning environments, Front. Educ. Conf. 2 (1999) 23–28.
[39] W. Liu, Software protection with encryption and verification, Software Engineering and Knowledge Engineering: Theory and Practice, Springer, Berlin, DE, 2012. 131–138.
[40] P.Y. Logan, S.W. Logan, Bitten by a bug: a case study in malware infection, J. Inf. Syst. Educ. 14 (3) (2003) 301–305.
[41] F. Lombardi, R. Di Pietro, Secure virtualization for cloud computing, J. Netw. Comput. Appl. 34 (4) (2011) 1113–1122.
[42] R.M. Magalhaes, Security and virtualization. Available at: http://www.windowsecurity.com/articles/Security-Virtualization.html 2008.
[43] D. Marshall, Top 10 benefits of server virtualization, InfoWorld 2 (11) (2011).
[44] A. Menon, A.L. Cox, W. Zwaenepoel, Optimizing network virtualization in Xen, Proc. USENIX Annual Tech. Conf 2006, pp. 15–28.
[45] I. Mevag, Towards Automatic Management and Live Migration of Virtual MachinesMaster thesis University of Oslo, Norway, 2007.
[46] Personnel system identifies commendable actions and problematic trends, in: L. Miller, R. Pierce (Eds.),TechBeat Dated: Winter 2013 2013, p. 14.
[47] J.C. Nunnally, I.H. Bernstein, Psychometric Theory, 3rd Ed. McGraw-Hill, New York, NY, 1994.
[48] M. Nyanchama, Enterprise vulnerability management and its role in information security management, Inf. Secur. J.: A Glob. Perspect. 14 (3) (2005) 29–56.
[49] R. Oppliger, Internet security: firewalls and beyond, Commun. ACM 40 (5) (1997) 92–102.
[50] J. Park, B. Noh, Web attack detection: classifying parameter information according to dynamic web page, Int. J. Web Serv. Pract. 2 (1–2) (2006) 68–74.
[51] J. Pauli, The Basics of Web Hacking: Tools and Techniques to Attack the Web, Elsevier, Amsterdam, NL, 2013.
[52] C.L. Pritchard, Risk Management: Concepts and Guidance, 4th Ed. ESI International, Arlington, VA, 2010.
[53] Y. Qi, B. Yang, B. Xu, J. Li, Towards system-level optimization for high performance unified threat management, Int. Conf. Netw. Serv. (INCS) 7 (2007).
[54] E. Ray, E. Schultz, Virtualization security, Proc. 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, 2009.
[55] K. Renauda, Quantifying the quality of web authentication mechanisms: a usability perspective, J. Web Eng. 3 (2) (2004) 95–123.
[56] G. Ridley, J. Young, P. Carroll, COBIT and its utilization: a framework from the literature, Proc. 37th Annu. Hawaii Int. Conf. Syst. Sci., 8, 2004.
[57] F. Sabahi, Virtualization-level security in cloud computing, Proc. IEEE 3rd International Conference on Communication Software and Networks (ICCSN) 2011, pp. 250–254.
[58] D. Shackleford, Virtualization Security: Protecting Virtualized Environments, John Wiley & Sons, New York, NY, 2012.
[59] D.H. Shin, The dynamic user activities in massive multiplayer online role-playing games, Int. J Human–Comput. Interact. 26 (4) (2010) 317–344.
[60] D.H. Shin, Y.J. Shin, Consumers' trust in virtual mall shopping: the role of social presence and perceived security, Int. J Human–Comput. Interact. 27 (5) (2011) 450–475.
[61] H. Shiravi, A. Shiravi, A.A. Ghorbani, A survey of visualization systems for network security, IEEE Trans. Vis. Comput. Graph. 18 (8) (2012) 1313–1329.
[62] E. Shmueli, R. Vaisenberg, Y. Elovici, C. Glezer, Database encryption: an overview of contemporary challenges and design considerations, ACM SIGMOD Rec. 38 (3) (2010) 29–34.
[63] A. Singh, An introduction to virtualization. Available at: http://www.kernelthread.com/publications/virtualization/ 2004.
[64] A. Singh, M. Korupolu, D. Mohapatra, Server-storage virtualization: integration and load balancing in data centers, Conf. High Perform. Netw. Comput, 2008.
[65] J.C. Song, J.W. Ryu, B.J. Moon, H.K. Jung, Strategy for adopting server virtualization in the public sector, J. Inf. Commun. Converg. Eng. 10 (1) (2012) 61–65.
[66] Symantec, Information security trends forecast. Available at http://protectyoursecrets.symantec.com/zh/tw/about/news/release/article.jsp?prid=20090202_02 2009.
[67] C.W. Thompson, D.R. Thompson, Identity management, IEEE Internet Comput. 11 (3) (2007) 82–85.
[68] H.N. Van, F.D. Tran, J.M. Menaud, Performance and power management for cloud infrastructures, Proc. IEEE 3rd International Conference on Cloud Computing 2010, pp. 329–336.
[69] S.J. Vaughan-Nichols, Virtualization sparks security concerns, Computer 41 (8) (2008) 13–15.
[70] Q. Wang, W. Wu, Y. Gu, The application of Lucene in information leakage monitoring and querying system, IEEE 2010 2nd International Conference on Information Engineering and Computer Science (ICIECS 2010, pp. 1–4.
[71] X. Wang, J. Luo, M. Yang, Z. Ling, A potential HTTP-based application-level attack against Tor, Futur. Gener. Comput. Syst. 27 (1) (2011) 67–77.
[72] T. Yokoyama, M. Hanaoka, M. Shimamura, K. Kono, Simplifying security policy descriptions for internet servers in secure operating systems, Proc. 2009 ACM Symp. Appl. Comput 2009, pp. 326–333.
[73] G.U.I. Yong-Hong, Study and Applications of Operation System Security Baseline. (Available at http://en.cnki.com.cn/Article_en/CJFDTOTAL-DZJC201110009.htm) Computer Security, 2011–102011.
[74] O. Yoshihiko, Y. Tetsu, Server virtualization technology and its latest trends, Fujitsu Sci. Tech. J. 44 (1) (2008) 46–52.
[75] I.X. Zhang, Economic consequences of the Sarbanes–Oxley Act of 2002, J. Account. Econ. 44 (2) (2007) 74–115.
[76] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Futur. Gener. Comput. Syst. 28 (2012) 583–592.
[77] ISO 27001, "Information Technology, Security Techniques, Information Security Management Systems, Requirements,", International Organization for Standardization ISO, Geneve, 2005.