Int. J. Communications, Network and System Sciences, 2014, 7, 423-429
Published Online October 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.710043

Scientific Research

Virtualization Security, Strategy and Management

Simon Tran, Stuart Gold

University of Massachusetts, Boston, USA
Email: stran@cs.umb.edu, stugold@email.phoenix.edu

Received 29 July 2014; revised 22 August 2014; accepted 18 September 2014

Abstract

The purpose of this quantitative study was to determine the relationship between the security management framework of organizations and the security condition of the virtualized environment.

Keywords

Virtualization Technology, Virtual Machine Security Issues, Security Management Framework

1. Introduction

Information system managers continually improve the methods of managing an organization. In the age of technology, when the Internet is the primary source of communication and data exchange, a profound concern of all IT managers is protecting the environment from vulnerabilities. Computer hackers use public information to draw a complete picture of the organization to identify a point of exploitation (IBM, 2010). Attacks can come in any form, such as an e-mail or a web link to attractive documents. Known viruses seem to double every 18 months, and newly discovered vulnerabilities have increased by nearly 25% each year since 2000 (Hale & Brusil, 2007) [1]-[3].

The evolution of technology has reached the state that induced managers to think about reorganizing the technical infrastructure for better quality and lower operational costs. Data center consolidation has driven managers to look further into innovative technologies, and virtualization technology is an ideal selection for many organizations. Virtualization technology is the use of software to present the same hardware resource to multiple virtual servers. Virtual servers, also called guest operating systems (OS), recognize neither the modified state of the presented hardware nor its indirect access to hardware resources. Pragmatically, virtualization technology has opened a new path for computer hackers because IT infrastructure managers have not paid enough attention to the security of this newly emerged technology. In 2009, 63% of organizations did not have a plan to secure the

How to cite this paper: Tran, S. and Gold, S. (2014) Virtualization Security, Strategy and Management. *Int. J. Communications, Network and System Sciences*, **7**, 423-429. http://dx.doi.org/10.4236/ijcns.2014.710043

virtualized environment, and 21.2% planned to develop security in the coming three years (Barr, 2009) [4]-[6].

With new methods of deploying and managing servers in a virtual environment, managers could reduce technology expenses annually. The lengthy time required to build physical servers was replaced by an efficient process in which technical professionals could deploy virtual servers quickly. However, the dynamics of the environment made it difficult for IT managers to keep track of patch levels and security flaws (IBM, 2009). Unfortunately, guidelines for managers to keep up with protection are not readily available or well developed. Empirical analysis and academic research seemed to focus on a different aspect of virtualization technology: adopting virtualization technology for financial effectiveness and centralized management. The industry lacked valid research that recommended how managers should react in a virtualized environment: whether managers' knowledge is enough to manage the system, the management styles that prompt managers to take subjective actions in protecting the environment, and the insufficiency of corporate policy in auditing and verifying virtual environments.

This quantitative study was to learn the relationship between the security management framework of organizations and the security condition of the virtualized environment. The security condition was based on the implementation of security utilities or the application of technological configuration recommended by standardization guidelines, such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI DSS). The effectiveness of a management framework depended on IT managers' knowledge of virtualization, enthusiasm for promoting a highly secure environment, and willingness to accept changes proposed by subordinates.

2. Research Design

When a study is designed to explore a possible correlation without changing the investigated situation, descriptive quantitative research becomes the more appropriate approach. The quantitative approach addressed the research problem by requiring an explanation of the relationship among variables (Creswell, 2008) [7]-[9]. The variables in this study pertained to three different categories: the IT managers' knowledge in virtualization, the managers' confidence in operational decision-making, and the corporate security policy. In category 1, the variables were the number of years the managers have operated in the virtual environment, the level of managers' involvement in architectural design and planning, and managers' knowledge improvement plan as indicated by annual seminar or conference participation. Category 2 has such variables as the intention to obtain advice from subordinates or peers, persistence in making decisions, and the degree of accepting external comments ranged in percentages. The last category has such variables as the annual policy update, federal regulation updates, the level of coverage of virtualization technology in the policy, the frequency of security patch applications, and the coordination among teams for policy creation.

Data collection performed over the Internet, also called a web-based survey, was the first choice in this study. Survey Monkey was the selected website to create the survey and collect data from personal e-mail. The Likert-type scale survey was the primary research instrument used in the data collection process. The 5-point scale provided participants flexibility in choosing answers and offered an accurate assessment of beliefs or opinions (**Appendix**).

3. Data Finding and Analysis

For every research question, it was critical to summarize the information about the variables. This study used the measure of central tendency, standard deviation, correlation coefficient, and regression analysis in computations. The analysis in this research used the mean to compute the average, computing the mean by dividing the sum of all scores by the number of scores (**Figure 1**).

The standard deviation provided a comprehensive computation based on the spread, dispersion, or variability around the center (Neuman, 2006). Standard deviation is the measurement of distance between all scores and the mean. **Figure 2** provides the formula used in standard deviation computation.

The correlation coefficient calculation determines any relationship between variables: virtual infrastructure security and leaders' knowledge, security policy, and IT managers' belief in individual operational decision-making regarding virtualization technology. A regression analysis takes the study a little further, measuring the level of association between chosen variables. Using regression analysis, one can predict a dependent variable (Y) when he or she knows the value of the independent variable (X) (Vogt, 2007) [10]-[12] (**Figure 3**).

	Question 1	Question 2	Question 3	Question 4
MQ_x	$(P_1+P_2+P_n)/N$	$(P_1+P_2+P_n)/N$	$(P_1+P_2+P_n)/N$	$(P_1+P_2+P_n)/N$
MVR1	(MQ1 + MQ2 + MQ3 + MQ4) / 4			

Figure 1. Computation of the mean.

x = score of the question

$\bar{x}$ = mean

Σ = Sum

N = Number of cases

$$\text{Standard deviation} = \sqrt{\frac{\Sigma(x-\bar{x})^2}{N-1}}$$

Figure 2. Standard deviation formular.

x_1 Value	x_2 Value	x_3 Value	x_4 Value	y Value	Predicted Value
3	2	3		3	3
2	1	4		2	2
4	1	5		2	2
3	5	4		2	2

y = a + b(x1) + c(x2) + d(x3) + e(x4)

y = 4.2727 + 0.36364x1 + -0.090909x2 + -0.72727x3

Figure 3. Multiple regression calculator.

In this research, there were three variables X associated with the change of the variable Y. X1, X2, and X3 were the IT managers' knowledge, confidence in decision-making process, and the corporate security policy. In other words, the growth or reduction of the security condition of the virtualized environment may be proportional to the growth or reduction of the value of the associated variables. The measure of central tendency and standard deviation revealed the trend of thoughts in each research question. The correlation coefficient reflected how much two variables go together (Neuman, 2006) [13]-[18].

- Research Question 1: The Relationship between Virtual Infrastructure Security and Mid-level IT Managers' Knowledge of Virtualization Technology (**Figure 4**).
- Research Question 2: The Relationship between Virtual Infrastructure Security and Mid-level IT Managers' Confidence Level (**Figure 5**).
- Research Question 3: The Relationship between Virtual Infrastructure Security and Corporate Security Policy (**Figure 6**).
- The Criterion, Participant's Current Technical Environment (**Figure 7**).

4. Discussion of the Research Findings

1) Mid-level IT managers' knowledge of virtualization technology: The mean score of the question about how managers updated knowledge was 3.83, and the mean score of the question about how managers tested applications in the virtualized environment was 3.76. This indicated a preference for bypassing formal training and professional recommendations in learning the technology and in operating the virtualized environment. It is not definitive that formal training can help IT managers rectify all security issues in the virtualized environment, but it would provide learners deeper knowledge about the technology and some of the best approaches to resolve known issues the vendor has not fixed in the product. The value of training is also reflected in the discovered correlation between training and the criterion, the current security condition of the organization. The computed correlation coefficient between the mean value of the predictor and the mean of the criterion was 0.14, and it

	Measure of Central Tendency	Standard Deviation	Correlation Coefficient between the question's average value and criterion
Question 1	2.22	1.07	-0.04
Question 2	3.83	0.95	0.25
Question 3	3.76	0.94	0.15
Question 4	2.18	0.96	-0.13
All Questions (Research Q1)	3.00	0.39	0.14

Figure 4. Research Question 1.

	Measure of Central Tendency	Standard Deviation	Correlation Coefficient between the question's average value and criterion
Question 5	2.39	0.84	-0.07
Question 6	2.23	0.89	-0.01
Question 7	2.39	1.02	-0.14
Question 8	3.64	1.09	0.21
All Questions (Research Q2)	2.66	0.54	0.01

Figure 5. Research Question 2.

	Measure of Central Tendency	Standard Deviation	Correlation Coefficient between the question's average value and criterion
Question 9	2.33	1.08	-0.05
Question 10	2.20	0.96	-0.04
Question 11	2.17	0.93	-0.02
Question 12	2.28	1.02	-0.05
All Questions (Research Q3)	2.25	0.75	-0.05

Figure 6. Research Question 3.

	Measure of Central Tendency	Standard Deviation
Question 13	2.86	1.31
Question 14	2.88	1.22
Question 15	3.00	1.29
Question 16	3.43	1.05
Question 17	2.68	1.32
All Questions (Criterion)	2.97	1.26

Figure 7. The Criterion.

showed that when the managers' knowledge shifted from hands-on training to formal training, there were signs of improvement in the infrastructure security

2) Mid-level IT managers' confidence level: When IT managers were asked if he or she would assess the risks of a system upgrade and make technical decisions individually prior to checking with the team, the measure of central tendency of 3.64 indicated that the majority had attempted to do so. However, this habit caused managers to create negative effects on the infrastructure security. The correlation coefficient of 0.21 between the question and the criterion, the current security condition of the organization, indicated that the managers' independence in risk assessment caused a negative effect on the infrastructure security.

From time to time, managers thought of asking for advice from subordinates before making technical decisions, but a large number of the participants (32%) did not think it was a necessity in every scenario. Similarly, managers were willing to ask for input from other teams, but still a high percentage of IT managers (26%) did so only sometimes. Practically speaking, one may attribute the degradation of infrastructure security to the lack of communication between managers and system administrators; however, the correlation coefficient of negative

0.07 showed the lack of relationship between the two factors.

3) Corporate security policy: The majority of participants affirmed the existence of such policies, and the measure of central tendency of all questions was at the optimum part of the ranking: 2.23, 2.20, 2.17, and 2.28. Summing up all questions in the section for the mean value of the corporate policy, the final value was on the optimum section of the scale: 2.25. This implied the effectiveness of the corporate policy staying compliant with security requirements for virtualization technology. The negative value of the correlation coefficient denied a relationship between the corporate policy and virtual infrastructure security. Therefore, managers may review the corporate policy for improvement, but should not expect better security conditions for the virtualized environment through the act of policy-making.

4) The security condition of the corporate virtual infrastructure: The last part of the survey was to collect information about the security condition of the corporate virtual infrastructure. If the IT managers' knowledge of virtualization technology, confidence in the decision-making process, and the corporate security policy represented the predictor variables in the study, the security condition of the corporate virtual infrastructure represented the criterion variable. The criterion consisted of five questions for the following data:

- The last time participants applied patches to the guest OS.
- The last time participants applied patches to the hypervisor.
- The last time participants updated the antivirus software.
- The type of security certificate used in the hypervisor.
- The last time participants scanned the end-user network for desktop virtualization products.

Summing up all five questions in the section, the measure of central tendency resulted in 2.97, a high score of near-at-risk or at-risk condition. The SD of 1.26 may shift the answer to more than 1 unit, but it still showed the security condition of the virtualized environment was not at the optimal level in a large number of participating companies.

5. Summary

The findings indicated that IT managers tended to use hands-on experience to gain knowledge. Using this approach, IT managers could dive into work immediately and learn from failures. However, the data analysis showed that the managers' chosen method of updating knowledge exacerbated the security condition of the virtualized environment. There were several reasons that prevented IT managers from having formal training, but it came to the point that managers needed to plan for formal training if the managers wanted to be more effective at work. For IT managers, the knowledge would open a gate to different positions and help make sound technical decisions. If managers could capitalize on the knowledge of subordinates and colleagues from different teams, technical decisions would become more effective. Several technologists contributing efforts toward one specific topic would help the team cover any possible missing points. The findings in the survey proved that when IT managers tended to make decisions individually, the security condition of the virtual infrastructure was exacerbated.

The results of this study let IT managers recognize the quality of information system leadership. Much past research has provided managers a broader view of the security condition, but there has been a limited amount of research focused on how managers operate the environment, especially those managers using virtualization technology. Many managers apply leadership styles used in managing the physical environment to the virtualized environment. Theoretically, OSs run independently, and invaders must find ways to attack servers differently. Virtualization technology allows multiple OSs to run on the same underlying hardware. This opens an opportunity for invaders to exploit one virtual server and gain access to the rest. Updating the corporate security policy is one way to maintain the level of security. Managers must know the criticality of the policy and stay compliant. Otherwise, security policies just stay on paper, and the virtualized environment is still the target of attacks.

IT managers need to improve technical and management skills continuously. It managers also need to look for better ways to obtain training and knowledge. Persisting in the traditional method of self-training possibly puts managers in the opposite direction. Some managers decide to rely on subordinates for technical decisions and avoid making mistakes that can exacerbate the virtualized environment. This approach deterministically splits job responsibilities, managers' focus on management, and technologists' focus on technical configuration. To determine if this is a good approach for IT managers in this fast-paced industry, a future study will be helpful.

The collected data, the statistical analysis, and deliberate thought in recommendations may provide IT managers a possible path for management strategies; however, this study does not address the only problems for organizations that use virtualization technology. It will be indispensable to have more research about security conditions if executive managers decide to virtualize the end-user workstations and to virtualize the demilitarized zone and any OSs that interface with the public Internet. This study assumed the virtualized environment was for server platforms. Virtualizing end users' workstations or servers in demilitarized zone will create an ambiguous area in support and management. Should server IT managers own the environment from the support and security perspective? Alternatively, should that environment be shared, and how would it be shared? Such questions require much more research in the field.

References

[1] Neiger, G., Santoni, A., Leung, F. and Rodgers, D. (2006) Intel Virtualization Technology: Hardware Support for Efficient Processor Virtualization. *Intel Technology Journal*, **10**, 167. http://dx.doi.org/10.1535/itj

[2] Neuman, L.W. (2006) Social Research Methods: Qualitative and Quantitative Approaches. 6th Editon, Allyn and Bacon, Boston.

[3] Nikhil, B. (2009) Performance Evaluation of Intel EPT Hardware Assist. VMware, Inc., California. http://www.vmware.com

[4] Nikitasha, P., Jyotiprakash, S., Subasish, M. and Prasanna, P.S. (2011) A Security Framework for Virtualization Based Computing Environment. *International Journal of Engineering Science and Technology*, **3**, 6423-6429. http://www.techrepublic.com/research-library

[5] Park, Y.R. and Sharma, S. (2009) Providing Service Using a Virtualization Infrastructure. *Journal of Service Science*, **2**, 17-22. http://search.proquest.com/docview/195627357?accountid=35812

[6] Payne, B.D. (2010) Improving Host-Based Computer Security Using Secure Active Monitoring and Memory Analysis. Georgia Institute of Technology, Atlanta. http://www.bryanpayne.org/

[7] Peng, Q. and Yu, C. (2007) Enhanced Integrated Manufacturing Systems in an Immersive Virtual Environment. *Proceedings of the Institution of Mechanical Engineers*, **221**, 477-487. http://search.proquest.com/docview/195146511?accountid=35812 http://dx.doi.org/10.1243/09544054JEM453

[8] Perkins, G.H. (2004) Will Libraries' Web-Based Survey Methods Replace Existing Nonelectronic Survey Methods. *Information Technology and Libraries*, **23**, 123-126.

[9] Petter, S., Delone, W. and McLean, E. (2008) Measuring Information Systems Success: Models, Dimensions, Measures, and Interrelationships. *European Journal of Information Systems*, **17**, 236-263. http://www.palgrave-journals.com http://dx.doi.org/10.1057/ejis.2008.15

[10] Pozgaj, Z. and Strahonja, J. (2008) It Service Management Based on Itil Methodology. 965-978. http://search.proquest.com/docview/217738441?accountid=35812

[11] Prism MicroSystems (2010) 2010 State of Virtualization Security Survey. http://www.prismmicrosys.com/documents/VirtualizationSecuritySurvey2010.pdf

[12] Reichman, A. (2009) Rethinking Storage for Server Virtualization Environments. *TechTarget*. http://searchservervirtualization.techtarget.com

[13] Rosnow, R.L. and Rosenthal, R. (2008) Beginning Behavioral Research: A Conceptual Primer. 6th Edition, Pearson Prentice Hall, Upper Saddle River.

[14] RSA List Service (2012) Fortune 1000 Company List. http://www.rsalistsinc.com

[15] Samoilenko, S. (2008) Information Systems Fitness and Risk in IS Development: Insights and Implications from Chaos and Complex Systems Theories. *Information Systems Frontiers*, **10**, 281-292. http://dx.doi.org/10.1007/s10796-008-9078-3

[16] Sandifer, C. (2008) The Economics of Virtualization. University of South Carolina, Columbia. http://search.proquest.com

[17] Scadden, R., Bogdany, R., Clifford, J., Pearthree, H. and Locke, R. (2008) Resilient Hosting in a Continuously Available Virtualized Environment. *IBM Systems Journal*, **47**, 535-548. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5386523 http://dx.doi.org/10.1147/SJ.2008.5386523

[18] Seiler, S. and Pfister, A.C. (2009) Why Did I Do This: Understanding Leadership Behavior through a Dynamic Five-Factor Model of Leadership? *Journal of Leadership Studies*, **3**, 41-52. http://dx.doi.org/10.1002/jls.20122

Appendix: Virtual Infrastructure Management Questionnaire

Part 1: Manager's knowledge in virtualization technology

- You spend at least 30 minutes per week to update your knowledge in information security written specifically for virtualization technology, and the reading material can be but is not limited to being from vendors, online journals, or books.
- To understand virtualization technology, you would rather experiment by hands-on interaction, not by attending training classes.
- You perform a self-test about the performance and operability of your new applications in the virtualized environment before you involve the vendors for their recommendation.
- You see a necessity to change the security configuration of your physical environment for potential risks introduced by virtualization technology.

Part 2: Manager's confidence in operational decision-making

- How often do you ask for advice from subordinates before making decisions about infrastructure or application changes?
- Do you see a necessity to have other technical teams review the changes you plan to make to the system?
- Do you need to cross-check the company's policies and regulations every time you make application or infrastructure changes?
- When assessing the risks of system upgrades or changes with executive managers, you can decide by yourself prior to checking with your team.

Part 3: Corporate security policy

- Your corporate policy has a separate section that indicates the requirements for virtualization security.
- Your corporate policy has instructions and procedures to scan the corporate network for virtualization products installed and operated by end-users such as VMware Workstation or Microsoft Virtual PC.
- Besides restricting access by User ID, your corporate policy limits access to the hypervisor (such as the management console) to certain stations or network segments.
- Your corporate policy enforces the centralizing of all hypervisors' logs to one system outside of the virtualized environment.

Part 4: Your environment

- The last time you applied patches to your guest OS was more than 30 days ago.
- The last time you applied patches to your hypervisor was more than 30 days ago.
- The antivirus software in your guest OS was updated more than 7 days ago.
- You are using self-signed certificate on your hypervisor.
- The last time you scanned your end-user network for any desktop virtualization platforms such as VMware Workstation or Microsoft Virtual PC was more than 30 days ago.