IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 9, November 2014.
www.ijiset.com
ISSN 2348 – 7968

Enhancing Security Concerns in Cloud Computing Virtual Machines :(Case Study on Central Bank of Sudan)

Samah Sabir M. Hassan, Shadi M. S. Hilles

Faculty of Computer & Information Technology

Al-Madinah International University

Shah Alam, Malaysia

Abstract

This research clearly illustrates the importance of risk management and security awareness, especially with the lack of proper protection which makes detecting and preventing the leakage of information even harder. The study used a review of literature on the risks of virtualization, interviews and questionnaires with thirty three virtualization experts in Central Bank of Sudan (CBOS) and other organizations were used to create an overview of the most worrying risks. The results indicated that data management, external attacks, security training and awareness are the top three of the most worrisome risks of CBOS. These risks were discussed in detail along with the approaches taken to reduce these risks. Also a test in a similar environment was conducted in order to determine whether the approaches chosen actually reduced the risk or not. This study will be of great benefit to all organizations in Sudan and to CBOS in particular.

Keywords: *CBOS, Virtual Machine, Cloud Computing, Hypervisor, Risks, Virtualization*

1. Introduction

Virtualization has become one of the most attractive and widely used technologies today. The ability to share resources of a single physical machine between several isolated virtual machines (VM) enables more optimization in hardware utilization. Also virtual machine offer the ease of management and migration compared to its physical counterpart. However, adding another abstraction layer between hardware and software raises new security challenges.

1.1 Cloud Computing

(Mell & Grance, 2011) NIST states that Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

In today's global software markets every business needs to play a major role and respond faster to the changes that are happening in the software market based on customer demands and the growth opportunities. For this to occur we need have a flexible infrastructure that can be upgraded to the current changes in the market. Virtualization is a key element in cloud computing, because it is really an entry point to a much longer evolution that will lead to cloud computing thus changing technology architectures, management tools, operational processes, customer relationships, funding models and nearly everything along the way. The path from virtualization to cloud computing is achieved through five stages Server Virtualization, Distributed Virtualization, Private Cloud, Hybrid Cloud and Public Cloud (Figure 1) (Bittman, 2011).

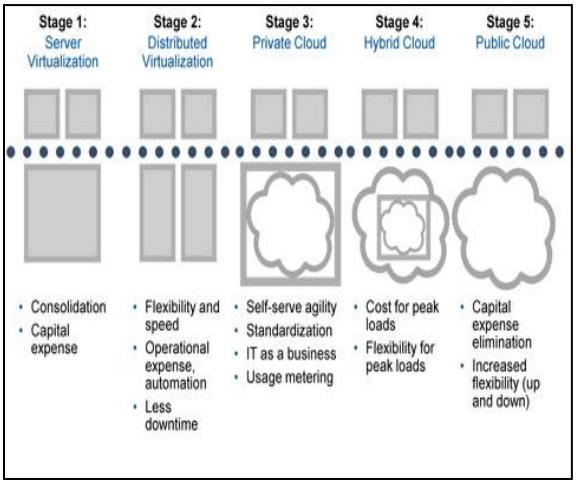

Figure 1: Gartner Road Map: From Virtualization to Cloud Computing

ISSN 2348 – 7968

Cloud computing consists three service models IaaS (Infrastructure as a Service), PaaS (Plat-form as a Service), SaaS (Software as a Service) and has three types which are Public, Private and Hybrid. The type of service received from service providers depends on the service model that has been chosen by the customer.

1.2 Benefits of Cloud computing

The Cloud as it is called by experts has many tremendous benefits these benefits are such as; economies of scale resulting in low-costs of IT infrastructure, low maintenance costs and low IT administration costs. Other benefits are, improved of performance as a result of having access to dynamic and scalable computing, memory and storage capabilities based on demand. Cloud computing also offers easier data monitoring, quick incident response, and low costs to undertake security measures. Easier group collaboration, universal access to computing resources and the removal for the need for specific devices or hardware in-house are also benefits that can be accrued from cloud computing (Shimba, 2010).

1.3 Limitations of Clouds

Due to the various benefits Clouds provide many organizations find it to be an attractive alternative to their current computing resources which depending on the size of the organization can be very costly and tedious to maintain. Unfortunately despite all the benefits of cloud computing there are enormous limitations and security risks that cannot be ignored and have made many organizations hesitant on whether to trust Cloud computing for to host their systems and data or not. What is important is to make customers aware of the risks of deploying Cloud computing.

1.4 Why do organizations avoid moving to the cloud?

We are in the middle of a technology hype cycle called cloud computing. According to the Gartner Group (Smith, 2013) we are at the peak of inflated expectations. Despite the media hyping cloud computing, there can still be tremendous benefit to many who adopt a cloud computing strategy. This benefit exists for industry, government and the general public alike.

As a result, virtualization and virtualization security have gone through major transforms in the recent years. Virtualization and its unique architecture have many characteristics and advantages over traditional non-virtualized machines. However, these new characteristics create new vulnerabilities and possible attacks on a virtualized system. This has caused a widespread of concern regarding virtualization security. Since Cloud computing, is an umbrella term that encompasses virtualization. There are certain issues to address when adopting virtualization in any environment, there are additional security concerns that arise when using virtualization to support a cloud environment. Moving to the cloud from a virtual environment can be complicated because there are many risks which are associated with virtualization. Poor knowledge about the risks and a lack of good methods to mitigate these risks reduces the speed at which companies adopt cloud computing in the future (Chow, et al., 2009). Most likely the initial reaction of people would be to avoid moving to the cloud. This represents a general lack of understanding but at the same time can be a valid concern.

1.5 The need for virtualization

Almost every organization today depends on technology for running its business efficiently and effectively in one way or another. This dependency along with the rapid growth of the internet has lead organizations to incorporate virtualization in their data centers to fully utilize their hardware resources in order to achieve the required scalability, availability and performance. As organizations move toward virtualizing more of their servers and data center infrastructure, they need specialized protective technologies that match this environment.

There are several important security concerns that need to be addressed when considering the use of virtualization for cloud computing. These concerns are many but the major concerns are (Winkler, 2011):

a. There is a possibility of compromising the virtual machine (VM) hypervisor. If the hypervisor is vulnerable to exploit, it will become a primary target. At the scale of the cloud, such a risk would have broad impact if not otherwise mitigated. This requires an additional degree of network isolation and enhanced detection by security monitoring.
b. The nature of allocating and de-allocating resources such as local storage associated with VMs. During the deployment and operation of a VM, data is written to physical memory. If it's not cleared before those resources are reallocated to the next VM, there's a potential for exposure.

ISSN 2348 – 7968

c. The theoretical technique for limiting traffic flow between VMs would be to use segregation to gather and isolate different classes of VMs from each other. VMs could be traced to their owners throughout their lifecycle. They would only be collocated on physical servers with other VMs that meet those same requirements for colocation.
d. When considering the security issues with VMs, it's important to recognize that this technology is not new. Several products have undergone formal security evaluations and received certification. What this means in practical terms is that several VM technology vendors have taken pains to obtain independent and recognized security certification.

Moving to the cloud from a virtual environment comes with many risks. But how big are these risks? And how can they be mitigated? Companies that want to move a part of or maybe all of their environments into the cloud often have these questions, while they can be very hard to answer. Because of this organizations are hesitant to move their current virtual environment to the cloud. This hesitation is causing a great delay in the adoption of cloud services.

It can be concluded that the uncertainty about the risks of virtualization forms a barrier to cloud adoption. This barrier can be gradually removed by making organizations aware of what these risks are and using effective approaches to reduce the risks.

The study we present in this paper is primarily focused to determine what the virtualization security risks are when moving to the cloud from a virtual environment, how to evaluate these risks and which approaches can be used to reduce these risks. These approaches may be existing approaches which are available and can be applied or entirely new approaches may be found. Identifying which risks are the most important was achieved by using interviews and questionnaires with virtualization experts working in different organizations.

1.6 Virtualization and Cloud computing

Virtualization is a staple technology of cloud computing. IBM pioneered it in 1960s (Armbrust, 2009) to fully utilize their hardware resources with timesharing and multiprogramming techniques. These techniques led to the adaptation of virtualization. Virtualization is "the ability to run multiple *virtual* machines on a single piece of hardware. The hardware runs software which enables you to install multiple operating systems which are able to run simultaneously and independently, in their own secure environment, with minimal reduction in performance. Each virtual machine has its own virtual CPU, network interfaces, storage and operating system" (Oracle, 2009).These resources can be made available to the users on demand through the internet. Virtualization's unique architecture has many characteristics and advantages over traditional non-virtualized machines. However, with virtualization benefits comes the need for virtualization security (Garber, 2012)

Many solutions to the vulnerabilities of virtualization have been developed or are in the process of being developed. Most of the solutions target either the virtualization architecture itself or the infrastructure. Many of these solutions have already been utilized by some virtualization security companies in their products to combat the vulnerabilities that are present.

Enormous benefits can be gained from moving to cloud computing. That is why it is very important for organizations to be aware of current risks of their virtual systems and how to address them. Therefore, most of the previous work has focused on the challenges and risks of virtualization that may occur when moving to the cloud from a virtual environment and the approaches used to overcome them. It would also be an advantage to experiment and validate the use of approaches chosen to overcome a specific risk. In this, study a similar setup to that of CBOS which is built on VMware will be used to perform the validation test.

2. Previous work

Risks of Virtualization is a topic which has been discussed in many previous researches. For example (Studnia, Alata, Deswarte, Kaâniche, & Nicomette, 2012) discussed virtualization vulnerabilities such as Scaling, Transience, Software lifecycle, Diversity, Mobility, Identity, Data lifetime.

These vulnerabilities were addressed by (Garfinkel & Rosenblum, 2005) with the use of good policies. Even so attackers were still able to exploit flaws the system and perform an attack. Examples of these attacks are detecting a virtualized environment, identifying the hypervisor, breach in the isolation, accurate targeting of VMs in a cloud and virtual machine based rootkits. Each example was explained in detail and to avoid such attacks and improve

ISSN 2348 – 7968

security VM monitoring and isolation Enforcement were used.

(Zheng, 2011) On the other hand focused on risks related to attacks which may occur on the hypervisor such as attacks on hypervisor through host OS and attacks on hypervisor through guest OS.

These attacks are considered the most well-known vulnerabilities in virtualization and exploit mainly the architecture. There are other forms of risks which are related to characteristics and infrastructure of virtualization and they are; Virtual library check-out, Migration attack and Encryption attack.

(Sabahi, 2012) Discussed Virtual machine level attacks and Communication in virtualization and the attacks were DDoS attacks and Client to client attacks. The author described the risks in detail and to overcome these risks proposed virtualization architecture to secure the cloud.

A similar methodology approach was also used by Anton den Hoed in his research which aimed to find out which data privacy related risks are causing the most concerns and which technology based methods can be used to reduce these risks and had a positive contribution (Hoed, 2012).

Virtualization will continue to being widely implemented, however, the question is whether there's been adequate consideration for possible security threats. One reason may be because many security professionals are uninformed about the security risks of virtualization. On the other hand, those that are aware are challenged because they lack the authority to ensure that adequate measures are implemented at the IT infrastructure and operations level according (Mnovellino, 2013). Also most of the concentration of security of virtualization has been on external risks therefore much more consideration should also be done to internal risks.

3 Virtualization security risks

Our study was aimed at determining what the virtualization security risks are when moving to the cloud from a virtual environment, how to evaluate these risks and which approaches can be taken to reduce these risks based on a case of Central Bank of Sudan (CBOS). Therefore an overview of the risk of virtualization domain was required as a basis for the interviews and questionnaires before they could begin, thus leading to the answer of the first research question (What are the risks / challenges of virtualization?).

3.1 Challenges of virtualization

The latest security reports from PCI (PCI, 2011), SANS (Hietala, 2009) , Computer and Electronics Security Applications (Studnia, Alata, Deswarte, Kaâniche, & Nicomette, Survey of Security Problems in Cloud Computing Virtual Machines, 2012), MacAfee (Hau, 2007) , Beyond Trust (Trust, 2013) and Trend Micro (Reis, 2013) were used to provide the overview of the risk of virtualization which was used as a guidance in structuring the interviews and questionnaires. Before starting an interview the interviewees were presented with the overview of the risk of virtualization and they were asked to answer the questions. The interviews covered five administrators and operators from Central Bank of Sudan and consisted of twenty four questions. As for the questionnaires, they consisted of six personal questions and thirty nine technical questions. It covered thirty three experts from various organizations which ranged from commercial banks to specialized companies in this field were sent by email. Information gathered will be analyzed using SPSS in order to give us a clear view on what the most critical risks are as well as how aware and well prepared organizations are in dealing with these risks. Thus leading us to answer the second research question (What are the most critical risks of virtualization?).

3.2 Critical risks of virtualization

The number of times a risk was classified as one of the most important risks was based on the result of the interviews and questionnaires. Even though it was not discussed in this research, overall it was indicated that policies is a very important source of worries for most organizations.

When it comes to policies nothing changes significantly from the physical world. Current best practices are still relevant even though virtualization adds new components and considerations the basic security threats do not change. An example of this is provisioning accounts on the host. This should be handled with very carefully because providing a user with access to the host can be a potentially very powerful privilege over the guest. Therefore it is a good idea to link authentication to the host to existing identity management solutions such as Active Directory. It is always better for organizations to use the capabilities of their existing technologies to bring virtualization into the current infrastructure.

ISSN 2348 – 7968

Three different risks were chosen for further research based on the results of the interviews and questionnaires.

First data management and protection because the results indicate that it is a big problem with many uncertainties. It is important to consider the security of the virtual disk files because virtual disks are stored as files on the host, especially if deployed on mobile computers or in untrustworthy physical environments.

The second risk is external attacks. Some of these attacks have already been covered in previous chapters. There are many types of external attacks and all cannot be covered in this research. Therefore, in addition to those already stated in previous chapters only most recent possible security threats in virtualized environments that are emerging will be highlighted here. According to an article by (Mnovellino, 2013) there are possible security threats in virtualized environments that are emerging which are:

1. The first is called the Blue Pill. This occurs when a virtual machine masquerades as a hypervisor by installing itself on a host machine. As a result, resource allocations and interactions between virtual OS instances are controlled by the virtual machine acting as an imposter.
2. The second is called SubVirt, which is a VM rootkit that positions itself on the physical machine. It then monitors and records the activity of the VM. As a result, it disguises when the system is compromised and also may involve other threatening programs like spyware or keystroke loggers.
3. The third threat is Denial-of-Service. This is a virtual machine infrastructure attack that allows a single or multiple VMs to consume all of the resources that are contained within the host machine. Thus, these resources would not be available for other VMs.
4. The last threat is a Trojan. In this case, a hacker compromises the virtual machine manager, which allows them to control the applications and operating systems that are found on the machines, which is generally not addressed by antivirus software.

The third risk chosen for further research is security training and awareness. When it comes to security most organizations focus significant attention is focused on technology at the expense of the people. It is extremely important that people are properly trained about any new technology and its importance in order to be able to understand and plan for any change in process that may be brought about by the new technology.

4 The existing approaches which can be used to reduce this risk

Since this study is based on a case study for CBOS. The focus is on the risks that were specified by CBOS technical staff which are data management, training and awareness and external attacks.

4.1 Interviews and Questionnaires: The most important risks

The risk analysis documents of ENISA and PCI as well as latest security reports from SANS ,Computer and Electronics Security Applications ,MacAfee, Beyond trust and TrendMicro resulted in an overview of the most important risks of virtualization. However, it is not possible to cover all these risks in this thesis. Therefore, in order to determine which risks have the highest priority interviews and questionnaires with over thirty experts from eleven different organizations were used. These interviews and questionnaires were prepared using the overview of the top risks prepared earlier.

4.2 Interviews

Before an interview the interviewee received a document with an overview of the top risks formed from the three different analysis (Table 1) and instructions on how to access the risk analysis documents if required. During the interview many questions were asked but the two main questions were: “In your opinion and based on your experience what are the most well-known virtualization risks?” and the second question is “According to your previous answer number what the three most important risks are (1) being most important? Interviewees were given the possibility to introduce risks which were not on the list. For interviews only CBOS administrators were interviewed since this research is based on case study for CBOS.

Table 1- The top risks of virtualization according to MacAfee, SANS and Gartner

Gartner (Gartner, 2010)	SANS (Hietala, 2009)	MacAfee (Hau, 2007)

ISSN 2348 – 7968

Information Security Isn't Initially Involved in the Virtualization Projects	Misconfiguration of virtual hosting platform	Change control
A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads	Separation of duties	Asset tracking and management
The Lack of Visibility and Controls on Internal Virtual Networks Created for VM-to-VM Communications Blinds Existing Security Policy Enforcement Mechanisms	Failure of integration into life cycle management	Patch management
Workloads of Different Trust Levels Are Consolidated Onto a Single Physical Server Without Sufficient Separation	Security awareness	Contingency Planning
Adequate Controls on Administrative Access to the Hypervisor/VMM Layer and to Administrative Tools Are Lacking	Lack of tools and policies	
There Is a Potential Loss of Separation of Duties for Network and Security Controls	VM sprawl	
	Lack of open ecosystem	
	Failure of policy coordination	
	Failure to consider hidden costs	

During the interviews no new risks were introduced to the list but all interviewees agreed that the most important risks according to their environment are data management, external attacks and lack of proper training & awareness.

4.3 Questionnaires

The information obtained after analyzing the data using SPSS indicated the following:

- 65% of the participant's ages were 25-35 years of age; Most of them held a bachelor degree and 75% had more than five years' experience.
- The most widely used technology by most of the organizations was VMware Vsphere (Figure 2). About 38% of them have 25-100 hypervisors and more than 100 virtual guests.
- More than half of the participants agreed that they regularly use security tools as a part of their administration and the most widely used tools were antivirus and security scanners (Figure 3).
- Most of the organizations used SAN as a shared storage and 60% indicated that their current security components are virtual aware (Figure 4). About half of them had virtual environments that met regulatory compliance and 80% had well trained administrators and operators which is a good indication on the awareness on the importance of virtualization security.
- Most of the participants believed that the most well-known risks are related to mostly patching and data management (Figure 5) and this was due to the fact that about 30% didn't patch regularly (Figure 6), while 35% didn't even know how often they need to perform security scans on virtual machines (Figure 7).
- Many of the participants also indicated that they monitored their VMs using virtualization monitoring software, their inward-facing and outward-facing VMs placed on the same physical servers but their dormant VMs are not scanned regularly for known vulnerabilities (Figure 8). This was an indication of poor data management which is considered a big risk but on the other hand most organizations handled the data associated with retired VMs properly, backup their VMs and have a backup policy.
- According to the information gathered by interviews and questionnaires, data management and protection was classified as one of the top risks of virtualization (Figure 9).

It is important to consider the security of the virtual disk files because virtual disks are stored as files on the host, especially if deployed on mobile computers or in untrustworthy physical environments. However, the security measure implemented by each organization differs from one to another depending on size and business type. Some perform specific

ISSN 2348 – 7968

audits and implement best practices while others do not.

Another risk which has been mentioned frequently and may occur as the result of improper data management and protection is external attacks.

Virtual systems and networks are subject to the same attacks and vulnerabilities that exist in a physical infrastructure. For example if a vulnerable application from a physical environment is moved to a virtual environment it will still have those same flaws and vulnerabilities.

Security training and awareness is a risk which must be dealt with carefully. Unlike malware and viruses which are external threats and can be reduce by use of technology. Lack of proper security training and awareness is considered as an internal threat. When it comes to security implementations customers usually focus most of their attention on technology at the expense of the people. Therefore, it is extremely important that people are properly trained about any new technology and its importance in order to be able to understand and plan for any change in process that may be brought about by the new technology.

5 Results

The below figures are the output of SPSS which gave a clear indication of what the most critical risks of virtualization are in CBOS.

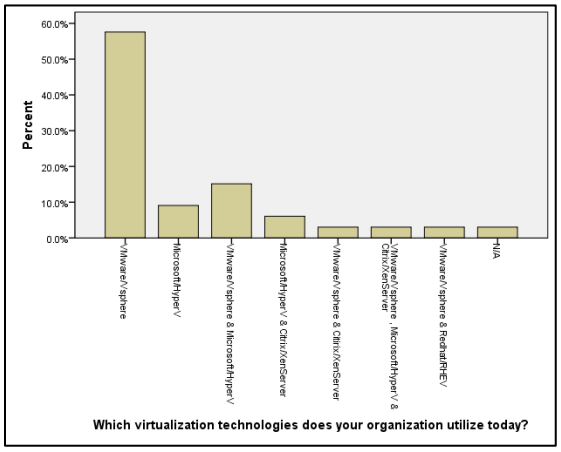

Figure **2**: Virtualization technologies used

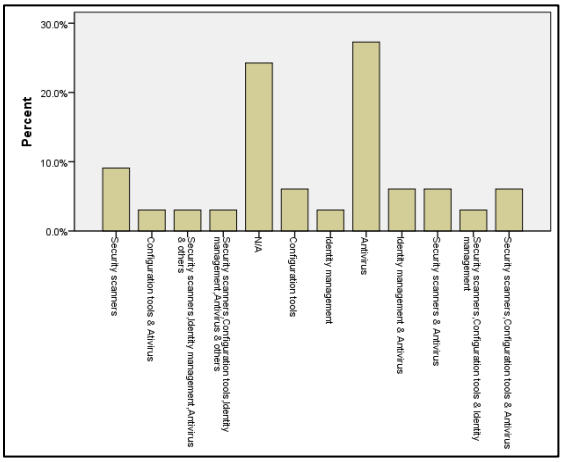

Figure **3**: Most widely used tools

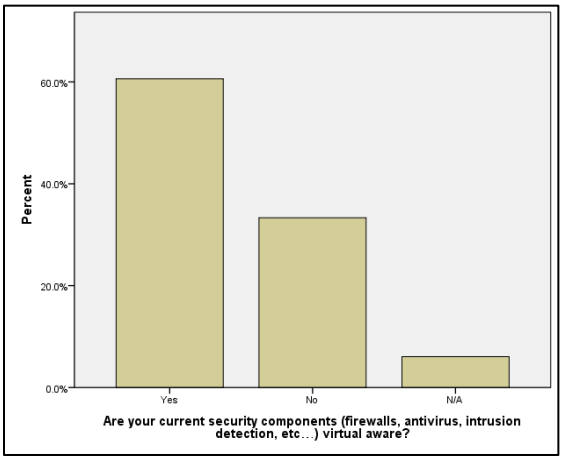

Figure 4: Are security components virtual aware?

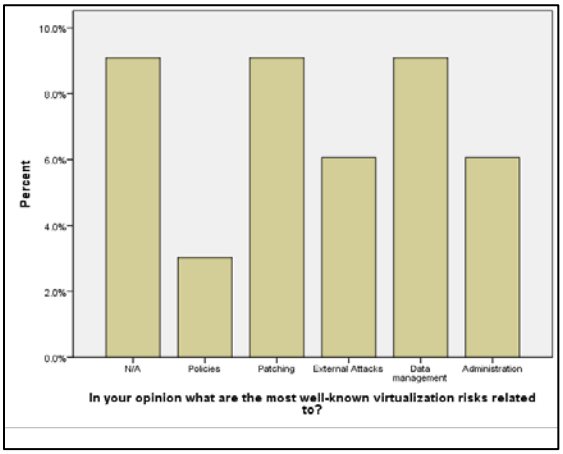

Figure 5: Most well-known risks

ISSN 2348 – 7968

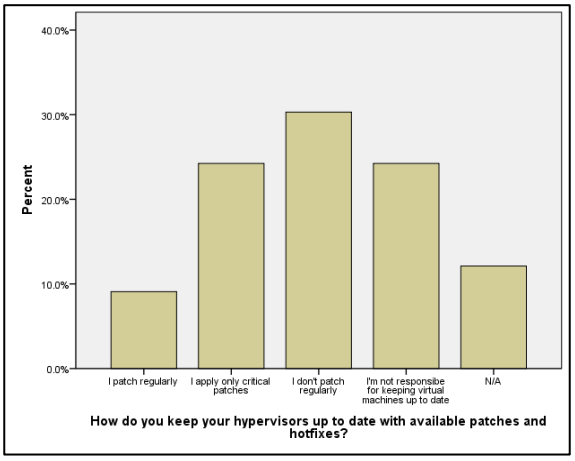

Figure 6: Do you patch hypervisors?

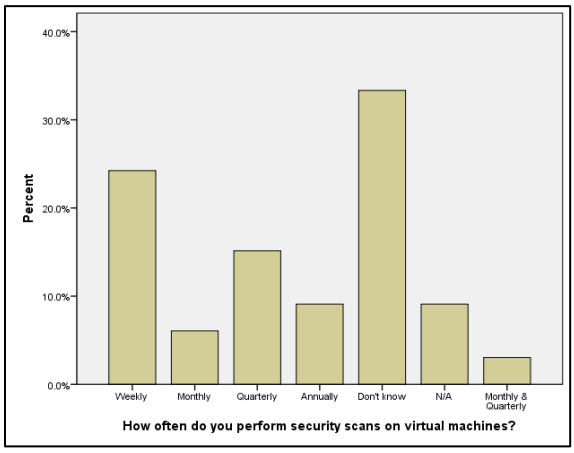

Figure 7: How often do you scan VMs?

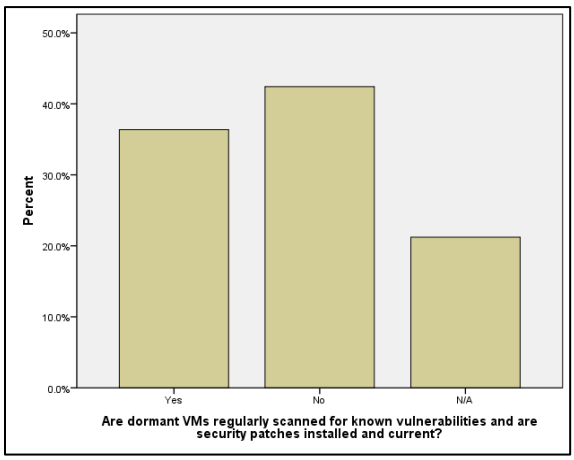

Figure 8: Are dormant VMs scanned?

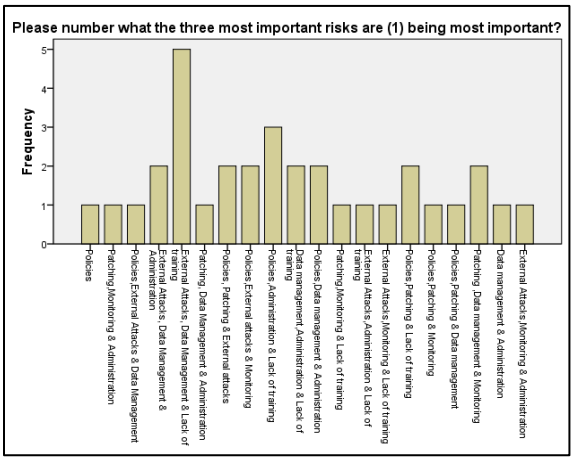

Figure 9: Three most important risks

After the three most important risks which were Data management, External attacks and lack of security awareness and training were identified. Existing approaches were found and used to reduce these risks.

5.1 Approach to resolving Data management risk

CBOS consists of an environment which uses a SAN storage system and proper backup software which is used to back up there application data. There is no backup for the virtual machines which is considered as a major risk.

In order to reduce this risk, appropriate backup software to backup and restore the virtual machines. The software chosen as method to reduce this risk was Veeam Backup. This conclusion was reached after thorough research and according to 2013 virtual Server survey (Wendt, 2013) which consisted of a comparison between three software applications which are Veeam, Appsure and Netbackup (Table 2). The chosen software was not tested on the actual environment but on a production environment that was setup specifically for this study.

Table 2- Comparison between Symantec, Veeam and Dell

Product	Overall Score	Backup Technology	Manage ment	Restore	Support
Symantec NetBackup 7.5	83.00	40.50	24.50	10.00	8.00
Veeam Backup & Replication 6.5	55.00	28.00	16.00	8.00	3.00
Dell AppAssure 5.2	47.50	20.50	14.00	9.00	4.00

ISSN 2348 – 7968

Overall Scores Rankings	
Recommended	41.59 – 46.00
Excellent	69.38 – 81.27
Good	57.46 – 69.37
Basic	39.50 – 57.45

Backup Technology Scores Rankings	
Recommended	81.28 – 87.50
Excellent	34.69 – 41.58
Good	27.78 – 34.68
Basic	13.50 – 27.77

According to Gartner report 2014 (Figure 10) and based on user reviews, if the software solution will be implemented in a complete virtual environment with no physical servers then Veeam would be the best option. If the environment is mixed with both physical and virtual servers and a single backup solution is required then Appsure would be a more appropriate choice. More details regarding Veeam can be found in http://www.veeam.com and Appsure can be found in http://software.dell.com.

Figure 10: Magic quadrant for enterprise backup software and integrated appliances

Whether CBOS decide to use Vaeem backup software or not it is recommended that they follow the top 10 best practices of backup Replication for VMware and Hyper-V (Davis, 2011).

5.2 Approach to resolving External attacks risk

External attacks are one of the biggest risks that face any organization especially financial ones. According to CBOS environment the most major risks which may result in external attacks are lack of VM patching and use of security tools. The current virtual environment is running on VMware version 4.1 and has been never been patched. For this particular situation the best option is to upgrade to version 5.5.

Regarding the security tools none have been used and the current security infrastructure is not virtual aware and needs to be replaced with new equipment that is virtual aware. This is not any easy process and may take time. Currently to reduce this risk it is recommended to use Retina virtual security scanner.

This decision was reached after extensive research and study of user reviews and surveys and vulnerability tool assessments by Gartner (Kavanagh, 2013), SC magazine (Stephenson, 2013) and InfoSec (Bakar, 2014). Both Nexpose and Retina were installed and tested in a testing environment prepared for this study. Based on this test Retina was recommended for CBOS.

5.3 Approach to resolving Security awareness risk

CBOS has invested thousands to build and secure its current IT infrastructure. Its true investment on technical training has been made but unfortunately when it comes to security this is not enough.

After a few interviews with CBOS users it was found that their knowledge of the importance of security was weak. Also using social engineering we were able to obtain some confidential information such as passwords and use accounts. Therefore there is an enormous need to work on security awareness for CBOS users. In this attempt a presentation of the importance of security and how they can be a part of the awareness program was conducted for managers in coordination with CBOS IT staff which was complete success. Also visual aid using screens located in different parts of the building was used to show tips and reminders of the importance of security. Also tips and hints were used on the intranet of the organization.

6. Conclusions

Virtualization technologies can bring many interesting new features such as optimized use of hardware resources, eased restoration and machine migration but they also introduce new means to perform attacks. These attacks may either be directed against virtualized systems or leverage some features related to virtualization in order to take over a system. Therefore, especially if a system is shared between many users, as is the case in cloud

ISSN 2348 – 7968

computing, strong security of virtual machines is crucial to protect their data and gain the customer's trust. In the above sections we initially describe the basic features of clouds and then covered virtualization in more detail beginning from its history, types, characteristics, benefits and ending with its limitations.

The research on security issues in virtualization is very active today, following a great diversity of possibilities, going from ways to secure popular systems like Xen, KVM or VMware are solutions, to creating new models such as the microkernel-based virtualization. However, even if these solutions are satisfying security-wise, one should still consider the possible issues of their large-scale deployment. Indeed, additional control procedures will cause a decrease in efficiency. Therefore it is important to find the right balance between performance and security according to their needs, keeping in mind that the usage of virtualization technology effectively can lead to efficient usage of cloud computing in the future.

The risks that are covered in this thesis are data management, external risks, security training and awareness. Out of the three risks in my opinion lack of proper security training and awareness seems to be the most critical. The introduction of technology in the banking sector began to flourish in year 2000 when CBOS implemented its first network and since then has been expanding rapidly. Today almost the entire banking sector is completely dependent on technology. All this concentration on the implementation of technology has come at the expense of security.

The lack of proper protection and the increase of Bring your own device (BYOD) a concept which refers to employees bringing personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications such as email, which makes detecting and preventing the leakage of information even harder. Therefore moving to the cloud from the current virtual environment means that your data is also moved to a location where there is no direct control over it. Therefore additional risks will be added to those already present in the current environment.

Acknowledgement

The research process is by no mean an isolated activity and I am grateful to all those who helped me in completing my research work. First and foremost I would like to thank my father Dr. Sabir Mohamed Hassan for his endless support and encouragement throughout the years. Also I would like to thank Dr. Shadi Hilles, my supervisor, for his valuable input, guidance and timely support. Thank you for never saying no to any of my enquiries.

I am much obliged to my friends, Mohamed Mahmoud Abkam and Elrasheed Babikir for extensive proof-reading of my thesis draft and guiding me in regards to my grammatical errors. They deserve my deepest gratitude for being so kind and helpful. I would like to thank all the interview and questionnaire participants who kindly shared their views, ideas and knowledge with me. Without their support, I would have never been able to achieve the outcome I did with this research work.

References

Armbrust, M. e. (2009). Above the Clouds : A Berkeley View of Cloud Computing. *Science*.

Bakar, R. A. (2014, April). *Vulnerability scanner product reviews*. Retrieved from Infosec: http://www.royabubakar.com/blog/2014/04/29/vulnerability-scanner-product-reviews/

Bittman, T. J. (2011, March). *The Road Map From Virtualization to Cloud Computing*. Retrieved from Easystreet.com: http://easystreet.com/wp-content/uploads/2012/12/Gartner_The-Road-Map-From-Virtualization-to-Cloud-Computing-G00210845_English.pdf?bcsi_scan_b895edbe82a47962=0&bcsi_scan_filename=Gartner_The-Road-Map-From-Virtualization-to-Cloud-Computing-G00210845_Englis

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., et al. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 85-90.

Davis, D. (2011, November). *Top 10 Best Practices of Backup and Replication for VMware and Hyper-V*. Retrieved from informationweek: http://www.informationweek.com/whitepaper/Hardware/Virtualization-Hardware/top-10-best-practices-of-backup-and-replication-fo-wp1321629893?articleID=191703853

ISSN 2348 – 7968

Garber, L. (2012). The Challenges of Securing the Environment.

Garfinkel, T., & Rosenblum, M. (2005). When Virtual is Harder than Real: Security Challenges in Virtual Machine. *Proceedings of the 10th conference on Hot Topics in Operating Systems-Volume 10*, p. 20.

Hau, W. A. (2007). *Virtualization and Risk – Key Security Considerations for your Enterprise Architecture.* Retrieved from MCafee: http://www.mcafee.com/uk/resources/white-papers/foundstone/wp-virtualization-and-risk.pdf

Hietala, J. D. (2009, August). *Top Virtualization Security Mistakes (and How to Avoid Them).* Retrieved from SANS: http://www.sans.org/reading-room/analysts_program/McAfee_Catbird_Virtualization_Jul09.pdf

Hoed, A. d. (2012, October). *Technology Based Methods to Reduce The Risks of Cloud Computing.* Retrieved from Leiden Institute of Advanced Computer Science: http://www.liacs.nl/assets/Masterscripties/2012-12AntonDenHoed.pdf?bcsi_scan_b895edbe82a47962=0&bcsi_scan_filename=2012-12AntonDenHoed.pdf

Kavanagh, K. M. (2013, September). *MarketScope for Vulnerability Assessment.* Retrieved from Gartner: https://www.gartner.com/doc/2586218/marketscope-vulnerability-assessment

Mell, P., & Grance, T. (2011, September). *The NIST Definition of Cloud Computing.* Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Mnovellino, C. a. (2013). *Virtualization: awareness and security threats*. Retrieved from MIT Geospatial Data Center Media: http://cybersecurity.mit.edu/2013/09/virtualization-awareness-and-security-threats/

Oracle. (2009). *Oracle VM Server User's Guide.* Retrieved from Oracle: http://docs.oracle.com/cd/E11081_01/doc/doc.21/e10898/intro.htm

PCI. (2011, June). *Information Supplement: PCI DSS Virtualization Guidelines.* Retrieved from PCI: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

Reis, D. (2013). *Cloud & Virtualization Security for Dummies.* Hoboken, New Jersey: John Wiley & Sons.

Sabahi, F. (2012). Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. *International Journal of Machine Learning and Computing*.

Shimba, F. (2010, September). *Cloud Computing:Strategies for Cloud Computing Adoption.* Retrieved from Dublin Institute of Technology: http://arrow.dit.ie/scschcomdis/1

Smith, D. M. (2013, May). *Hype Cycle for Cloud Computing, 2013*. Retrieved from Gartner: https://www.gartner.com/doc/2573318/hype-cycle-cloud-computing-

Stephenson, P. (2013, February). *Vulnerability assessment tools.* Retrieved from SC magazine: http://www.scmagazine.com/vulnerability-assessment-tools/grouptest/278/

Studnia, I., Alata, E., Deswarte, Y., Kaâniche, M., & Nicomette, V. (2012). Survey of Security Problems in Cloud Computing Virtual Machines. *Cloud and security:threat or opportunity*.

Trust, B. (2013, May). *Survey Results: Virtual Insecurity.* Retrieved from Beyond Trust: http://img.en25.com/Web/eEyeDigitalSecurityInc/%7B81b03119-b2ea-42e6-9924-13b20d8412fd%7D_BEYONDTRUST_Virtual_Insecurity_Survey_Results.pdf

Wendt, J. M. (2013). *2013 Virtual Server Backup Software Buyer's Guide.* Retrieved from DCIG: http://webdocs.commvault.com/assets/dcig-2013-virtual-server-backup-software-buyers-guide-analyst-report.pdf?dl=1

Winkler, V. (2011, December). *Cloud Computing: Virtual Cloud Security Concerns*. Retrieved from TechNet Magazine: http://technet.microsoft.com/en-us/magazine/hh641415.aspx

ISSN 2348 – 7968

Zheng, M. (2011). *Virtualization Security in Data Centers and Clouds.* Retrieved from www.cse.wustl.edu: http://www.cse.wustl.edu/~jain/cse571-11/ftp/virtual/index.html

Biographical Details

SAMAH SABIR M. HASSAN holds a BSc (honors) in Information Technology from Future University. Samah started her career in 1999 at Central Bank of Sudan (CBOS) as a network engineer and worked her way up. Currently she is the Head of Operating Systems and Internet Section at CBOS. She has worked in an array of fields including networking, security, operating systems, email, virtualization and storage. She also worked as a project manager for many of CBOS's most important projects. Samah enjoys traveling, learning, reading and listening to music.

SHADI M S HILLES, hold PhD of Computer System and Networks 2006 from Vinnytsia International Technical University, currently working as an Assistant Prof. and head of computer science dept. since 2010, in Al-Madinah International University. Interesting area for research image coding, semantic web programming, cloud computing, pattern recognition and neural network.