Enterprise Risk Management for the Implementation of Cloud Security

Sourav Mukherjee
Senior Database Administrator &
PhD student at University of the Cumberlands
Chicago, United States

Abstract
Cloud computing technology has evolved tremendously in the last few years as it provides several advantages for both organizations and individuals. But, simultaneously, numerous issues have arisen due to the massive development of cloud computing. Establishments often have raised concerns about the migration and operation of cloud computing due to the diminishing control over their outsourced resources and cloud computing is susceptible to risks. Accordingly, a cloud provider needs to accomplish the cloud computing landscape risks with the intention of identifying, assessing, and prioritizing the risks in order to lessen those risks, expand security, upsurge confidence in cloud services, and dismiss organizations’ concerns about using a cloud environment. Considering that a conservative risk management framework does not fit healthy with cloud computing due to the intricacy of its environment, research in this area has become extensive. The review will consider the extent of the involvement and participation of my organization in developing cloud computing and how the study of emerging threats and countermeasures helped achieve a sustainable ecosystem in my organization.

Keywords: Cloud Computing, Enterprise Risk Management, Encryption Methods, Patching, SCADA
Introduction

Risk management is one of the greatest important components in permitting an organization to attain its decisive vision. Through implementing appropriate risk management ethos and acquaintance, members of the organization will be talking the identical language, and they will influence common analytical aptitudes to classify and mitigate possible risks along with exploit opportunities in an opportune fashion. Therefore, Enterprise Risk Management (ERM) is necessary for the contentment of any organization’s goals and objectives. Comprehensive risk management authorizes not an only project, program managers, but also among the executives and units, departments, and sectors to accomplish timely and effective decision-making processes.

Literature Review

Throughout the implementation of an Enterprise Risk Management (ERM) application in an IT consulting firm, we have started with the end in mind and drove according to ERM success aspects in this organization to implement a sustainable Cloud Computing model for our valuable clients. We commissioned into the organization's risk awareness, we associated with the appropriate stakeholders, and we leveraged executive patronage towards the success of the project.

The participation of all parties in the organization had a foremost and significant impact on accomplishing the risk management procedure. This paper will articulate the importance of risk management in the modern IT world especially in the Cloud computing space which is heading in the market and creating a Billion Dollar marketplace through proper role
Enterprise Risk Management for the Implementation of Cloud Security

distribution. It will also highlight the importance of ERM, the necessary steps to succeed in such an endeavor, and the challenges that might also arise through compelling examples from a project carried out in a reputed IT consulting firm in the United States.

From what I’ve talked about so far, it has turned out to be very clear that enterprise risk management is not just about evading hazards and disasters. In fact, if the risk is intrinsic to any business, it’s essential to define which of them are adequate, which should be evaded at all costs and which are unavoidable and even accepted by an organization’s solid portfolio and strategy, because by assuming them, effectiveness can even be increased by a significant margin.

Let’s take a quick example. Imagine that a company is operating in a restaurant chain of business or selling office accessories. They are already running with outdated technology and resources but caters to a portfolio of customers satisfactorily. Now if the enterprise(s) decide to upgrade their internal process or software they might run into several challenges with risks and opportunities. This is the place where Enterprise Risk Management plays a vital role in managing the resources with proper measurement and utilization.

**Enterprise Risk Prevention Model Implementation**

Establishments typically face and are exposed to numerous types of risk such as policy, program, operational, functional, project, financial, human capital, technical, health, security, and political risks. The International Organization for Standardization (ISO) has defined risk as to the effect of uncertainty on objectives. Or else, the risk is articulated as a mixture of the significances of an event and the related probability of occurrence. Risk management is a systematic process for handling the risks or threats faced by an
Enterprise Risk Management for the Implementation of Cloud Security

organization with the intention of enabling it to identify the events that may result in unsuccessful or harmful consequences and to create the best course of accomplishment for classifying, measuring, sympathetic, acting on, and collaborating risk issues. Risk management enhances the value and offers many purposes to an organization. Some of these objectives are snowballing system security, defending and enhancing the organization’s assets, building knowledgeable decisions, and improving operational efficiency.

The researchers’ exertions are based on three separate viewpoints on Cloud Computing risk assessment. The primary proposed risk assessment frameworks can be expended only by a cloud computing consumer. It was recommended that in few instances risk should be transferred to the cloud provider or a reliable third party. However, these researchers disregard the fact that the cloud provider possesses and accomplishes the infrastructure of the cloud environment and cannot reveal their security models and actions to anyone who might be a malevolent user. In contrast, further researchers have projected risks should only be measured by the cloud provider, without taking into consideration the status of concerning the cloud consumers in the procedure since the cloud provider is the true owner of the data and the only party who knows the actual value of the resources in the cloud environment. Subsequently, some researchers believed in the position of relating the consumers in the risk assessment process. When and to what degree the consumers are engaged in this process was measured differently by the diverse proposed risk assessment frameworks.
Enterprise Risk Management for the Implementation of Cloud Security

Implementation of core concepts in projects

When it comes to the discussion of Cloud Security implementation through Enterprise Risk Management, the first thing which comes to the mind is the Security information and event management (SIEM) technique.

- **SIEM**: It’s an important tool primarily used in SOCs (Security Operations Center). They collect security-related events from diverse sources in enterprise networks, regularize the events to a common setup, store the regularized events for scientific analysis, and associate the events to classify spiteful activities in real-time. The SIEM system takes inputs from several security devices and sensors, with perimeter protection systems such as network firewalls and intrusion prevention systems, host sensors (IDSs and AVSs), applications (Web application firewalls and authentication systems), and network sensors.

  This technique is truly useful in our environment where the data is coming through different network sources and needs a solid mechanism to track and analyze the spiteful activities in a Realtime basis.

- **Encryption Methods**: A solid encryption method is required to be implied to the environment so that transactions happening through the wire can’t be challenged. Any delicate data being conducted within an enterprise or amid significant partners should be encoded. The traditional way of applying encryption is symmetric and embedded in hardware devices. When network transmission happens in an ad hoc means, the practical deliberation is that shared cryptography simply does not occur between organizations due to complication. This makes it hard to encrypt network traffic from coordinating things in advance. If an enterprise offers electronic
Enterprise Risk Management for the Implementation of Cloud Security

commerce services via the Internet, the use of generic encryption techniques such as Secure Sockets Layer (SSL) is used. It is also seamlessly fine to encrypt information numerous times if the supporting administrative tools are working properly.

- **Patching:** A distinct software lifecycle practice, timely processes for patching software and systems, separation of duty panels in system administration, threat management of all placid security information, security consciousness training for all system administrators, operational conformations for infrastructure management, and use of software security tools to safeguard proper integrity management. While cloud servers necessitate a similar level of maintenance and patching as on-premise solutions, users may be ignorant of cloud patching best practices, and cloud services may not issue patches on a consistent schedule. To efficiently patch your cloud-native infrastructure and remote workforces, and uphold compliance and security for your organization, following the below 3 key best practices for cloud patching are highly desirable.
  - Frequently Scanning for Vulnerabilities and Patches.
  - Use a monolithic Solution for Patching Across All the Providers
  - Maintain an Up-to-Date Inventory of Devices and Servers

Seeing the growing threats and a rapidly increasing attack surface, understrength and alert-weary organizations need additional efficient ways to remove their exposure to vulnerabilities.

In our working as well, we strictly consider patching as the crucial entity in protecting the cloud infrastructure.

- **Disaster Recovery Process:** Cloud disaster recovery Process (Cloud DR) is a backup and restore policy that includes storing and upholding copies of electronic
Enterprise Risk Management for the Implementation of Cloud Security

records in a cloud computing location as a security measure. Data needs to be restored quickly to get businesses up and running again. Nearly all data within a company is critical to its operations. Therefore, it is significant to protect this data and be ready when disaster strikes. Through the process of disaster recovery, security can decrease downtime and provide 24/7 access to business-critical data. Disaster recovery is an essential part of the security triangle: confidentiality, integrity, and availability of systems. Most businesses have learned a backup plan, i.e. when was the last time a full restore was essential? Cloud disaster recovery takes backup a step further by surrounding planning, process, integration, and testing. Considering that, we also have a strong DR strategy in place to ensure that in the event of any disaster the critical business application is up and running in a short span of time.

- **Diversity Paradox of Cloud Computing:** As the level of diversity increases, the level of difficulty for an attack likewise increases. The global propagation of home PCs has augmented the danger of malware attacks. In modern computing, the closest thing we must do is making sure that the arrangement is virtualized, cloud-based computing. In such a setup, computing power and application intelligence change to a central complex of servers, reachable via light clients. The handheld mobile devices offer the corresponding of a desktop computer in such a cloud environment. Cloud computing would offer substantial security benefits by eliminating nondiverse desktops from the environment. This is most possibly true if the infrastructure subsidiary to the cloud applications is properly secured.
Enterprise Risk Management for the Implementation of Cloud Security

Having said that instead of maintaining the data is local storage we now adopt Windows 360 to store even the emails, documents and using OneNote all documents are now maintained in the cloud.

- **SPAM Protection**: Managers of commercial environments have also started to recognize that their computing endpoints cannot trust solely on the gateway or in-the-cloud processing. As such, the state of the practice in e-mail virus and spam defense includes a defense-in-depth disposition of filters to each laptop, netbook, personal computer, and server in the enterprise. The approach is even starting to find its way to the mobile handheld device, where the risk of viruses and spam is increasing where a given virus or spam e-mail sent from a malevolent source will have to find its way through at least two distinguished layers of filtering in order to scope its intended source. This cloud filtering arrangement found in most companies is suitable for organizations charged with national infrastructure. For the most critical applications, it is suggested that a depth method including both in-the-cloud and perimeter processing be employed.

  We use different SPAM control software which provides additional layers of security in the premise. The tools seamlessly scan the emails before being sent outside the home network to the outsiders to ensure that the mail does not contain any malicious virus program and the same stands good for incoming mails as well. Any incident is reported to the security and audit teams for immediate action.

- **SCADA (supervisory control and data acquisition)**: The purpose of these systems is to monitor and control operations remotely. They operate by transferring coded signals between the control center and the machinery that they are inspecting over. These systems can screen multiple sites even when spread over significant
Enterprise Risk Management for the Implementation of Cloud Security

distances, so they’re often used for most important industrial sites. SCADA devices do not diverge from critical systems in that these also necessitate redundancy, security, reduced costs, and uptime. Migrating SCADA devices to the cloud can solve critical issues connected to uptime and redundancy in industrial control systems (ICS) environments.

There exist two kinds of SCADA systems:

1. **On-Premise SCADA**: This is a traditional method. Since many years, on-premise SCADA systems were the most common and popular method. One of the major issues is that they necessitate an important investment before they can even be used, and it’s essential to build and continue a complicated infrastructure to allow them to function.

2. **Cloud SCADA Systems**: The Cloud SCADA systems is that these systems are operated over a cloud. Consequently, nearly all the physical infrastructure of the traditional systems can be avoided, and everything is effortlessly connected over a network.

**Benefits of Cloud-Based SCADA Systems**

Systems operating in a cloud are frequently become cheaper, easier, and more efficient, and SCADA systems are no exception. A cloud-based SCADA system can be set up much quicker, and one can often be functioning in a matter of hours (instead of months needed for a traditional system). Correspondingly, it costs a lot fewer than the traditional type. These will save us time and money over both the short and long term, and it lets for much more flexibility when anything needs to be updated or changed.
Enterprise Risk Management for the Implementation of Cloud Security

We also extensively used Cloud-Based SCADA solution as the overall cost of monitoring the solution is much more seamless and cost-effective.

The participation of consumers in the risk management process is significant as they are the only ones who distinguish the value of their assets.

- Consumer involvement should not be limited to the extent of dormancy and consumers should not be engaged in each step to the degree of complicating the process.

- Context establishment and risk identification are critical processes in risk management.

- The contribution of cloud consumers in the risk treatment process is important since they are part of the problem; therefore, they must be a part of the solution.

- It is desirable for the risk assessment process to be done for each of the provided services distinctly in order to grip conflicts in the consumers’ security requirements, due to the multi-tenancy feature of cloud computing.

Organization leaders not only need to understand the importance of risk management, the importance of its processes, and the importance of their involvement, but they also need to ensure its steadiness by defending a thorough but relatively simple framework. Once ERM is well implemented, it becomes a significant tool of timely decision-making towards diminishing negative risks and creating value for future opportunities.

In addition, both leaders and employees control risks. Employees of all stages need to be on the constant lookout for hazards related to their specific knowledge area; especially that
Enterprise Risk Management for the Implementation of Cloud Security

standpoint towards risk changes from one person to the other and a joint input will bring precious value.

The organization should be conscious of its ability to avoid, lessen, transfer, and accept negative risks as well as an exploit, enhance, and share positive risks, provided all of this is allied with the strategic objectives of the organization.

The types of risks such as security, integrity, availability, and performance are the same with systems in the cloud as they are with non-cloud technology solutions. An organization’s level of risk and risk profile may be changed in most cases if cloud solutions are adopted largely depending on how and for what determination the cloud solutions are used. This is due to the upsurge or reduction in likelihood and impact regarding the risk events.

Discussion

Cloud computing is a new paradigm shift in the technology industry which will continue to rise and develop in the next few years. The rate at which the enterprises migrating to a cloud-based environment is snowballing daily due to its high degree of returns. The foremost cloud computing recompenses which benefit organizations are high scalability and flexibility in organizational resources so as to meet peak time demand, excellent dependability and availability in that resources can be retrieved from anywhere and at whatever time, and there is no upfront cost involved while installing and managing the software and hardware infrastructure. On the other hand, cloud computing also has brought many risks to organizations since they outsource IT resources which make services completely managed and delivered by a third party. Thus, such organizations might lose control over how they secure their environment and they might be concerned with privacy and security as the new
Enterprise Risk Management for the Implementation of Cloud Security

technology is a major source of new vulnerabilities in these areas. Therefore, it is significant to find several controls which will work collected to decrease the risks, deliver layered security, upsurge confidence in cloud services, and dismiss the fear of using a cloud computing environment. Risk management is one of the cloud computing environments that panels which purposes to assess and achieve risks related to cloud computing and to avert those risks from impacting business goals.

Conclusion and Future Study

Assurance of virtuous corporate governance could be achieved through the implementation of regular measurement, reporting, and communication of risk management routine. For proper governance of risk, an ERM committee needs to be maintained who will monitor and evaluate the risk management framework and performance which includes compliance with the required standards and will report back to the board and the head of the IT Infrastructure. The team will guarantee that the essential resources are available and that policies are adhered to.

In conclusion, ERM can offer exceptional value if it is well planned and applied properly. It is not only a team effort but also a planned effort and not a random one. It desires to be based on strong risk culture, and it needs the sponsorship of the executives in the company or institution. In addition, the combination of risk information needs to be performed according to clear rules that everyone would understand and abide by. Above and beyond, streamlining the complex can save loyalty to risk in the company in the long run.

Reference
Enterprise Risk Management for the Implementation of Cloud Security

[1] Amoroso, E. (2012). Cyber-attacks: protecting national infrastructure. Elsevier.
ISBN: 978-0123918550

[2] Boukhari, M. (2013). Enterprise risk management application implementation case study. Paper presented at PMI® Global Congress 2013—EMEA, Istanbul, Turkey. Newtown Square, PA: Project Management Institute.

[3] Hillson, D. (2012). How much risk is too much risk? Understanding risk appetite. PMI Global Congress 2012, Marseille, France.

[4] Jonas, V. (2011). Portfolio risk management: Aligning projects with business objectives to deliver value. PMI Global Congress 2011, Dublin Ireland.

[5] A. Apostu, F. Puican, G. Ularu, G. Suciu, and G. Todoran, “Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud,” Recent Advances in Applied Computer Science and Digital Services, 2013.

[6] Cloud SCADA vs Traditional SCADA. Retrieved from https://petrocloud.com/uncategorized/cloud-scada-vs-traditional-scada/

[7] Mukherjee, S. (2019). Popular SQL Server Database Encryption Choices. arXiv preprint arXiv:1901.03179.

[8] Mukherjee, S. (2019). Benefits of AWS in Modern Cloud. arXiv preprint arXiv:1903.03219.

[9] Mukherjee, S. (2019). How IT allows E-Participation in Policy-Making Process. arXiv preprint arXiv:1903.00831.

[10] Mukherjee, S. (2019). How Stakeholder Engagement Affects IT Projects. International
Enterprise Risk Management for the Implementation of Cloud Security

Journal of Innovative Research in Science, Engineering and Technology, 8(3).

[11] Chakraborty, Moonmoon & Excellence, Operations. (2019). Supply Chain & Inventory Management. 10.6084/m9.figshare.7824107.

[12] Mukherjee, Sourav. "Overview of the Importance of Corporate Security in business." Available at SSRN 3415960 (2019).

[13] Mukherjee, Sourav. "How Stakeholder Engagement Affects IT Projects." International Journal of Innovative Research in Science, Engineering and Technology 8.3 (2019).

[14] Chakraborty, M. (2019). Fog Computing Vs. Cloud Computing. arXiv preprint arXiv:1904.04026.

[15] Mukherjee, Sourav. "SQL Server Development Best Practices." International Journal of Innovative Research in Computer and Communication Engineering 10 (2019).

[16] Mukherjee, S. (2019). Indexes in Microsoft SQL Server. arXiv preprint arXiv:1903.08334.

[17] Chakraborty, Moonmoon. (2019). Planning, Control Systems and Lean Operations in Information Technology. 10.6084/m9.figshare.7886138.

[18] Chakraborty, Moonmoon. (2019). Managing Risk, Recovery & Project Management. 10.6084/m9.figshare.7886141.

[19] Chakraborty, Moonmoon. (2019). OPERATION IMPROVEMENTS & QUALITY MANAGEMENT IN HEALTHCARE Operation Improvements & Quality Management in Healthcare. 10.6084/m9.figshare.7886144.
Enterprise Risk Management for the Implementation of Cloud Security

[20] Mukherjee, Sourav. "The battle between NoSQL Databases and RDBMS." Available at SSRN 3393986 (2019).

[21] Mukherjee, Sourav, Cloud-based Security Solutions (June 24, 2019). Available at SSRN: https://ssrn.com/abstract=3408882 or http://dx.doi.org/10.2139/ssrn.3408882

[22] Mukherjee, Sourav, Information Governance for the Implementation of Cloud Computing (June 17, 2019). Available at SSRN: https://ssrn.com/abstract=3405102 or http://dx.doi.org/10.2139/ssrn.3405102

[23] Mukherjee, Sourav, Predictive Analytics and Predictive Modeling in Healthcare (June 1, 2019). Available at SSRN: https://ssrn.com/abstract=3403900 or http://dx.doi.org/10.2139/ssrn.3403900

[24] Mukherjee, Sourav. "Decision-Making with Technology." Available at SSRN 3393984 (2019).

[25] Mukherjee, S. Cyber warfare and Implications.

[26] Mukherjee, Sourav. "The battle between NoSQL Databases and RDBMS." Available at SSRN 3393986 (2019).

[27] Mukherjee, Sourav, Cloud-based Security Solutions (June 24, 2019). Available at SSRN: https://ssrn.com/abstract=3408882 or http://dx.doi.org/10.2139/ssrn.3408882

[28] Mukherjee, Sourav, Information Governance for the Implementation of Cloud Computing (June 17, 2019). Available at SSRN: https://ssrn.com/abstract=3405102 or http://dx.doi.org/10.2139/ssrn.3405102
[29] Mukherjee, Sourav, Predictive Analytics and Predictive Modeling in Healthcare (June 1, 2019). Available at SSRN: https://ssrn.com/abstract=3403900 or http://dx.doi.org/10.2139/ssrn.3403900

[30] Mukherjee, Sourav. "Decision-Making with Technology." Available at SSRN 3393984 (2019).

AUTHOR’S PROFILE

Sourav Mukherjee is a Senior Database Administrator and Data Architect based out of Chicago. He has more than 12 years of experience working with Microsoft SQL Server Database Platform. His work focusses in Microsoft SQL Server started with SQL Server 2000. Being a consultant architect, he has worked with different Chicago based clients. He has helped many companies in designing and maintaining their high availability solutions, developing and designing appropriate security models and providing query tuning guidelines to improve the overall SQL Server health, performance and simplifying the automation needs. He is passionate about SQL Server Database and the related community and contributing to articles in different SQL Server Public sites and Forums helping the community members. He holds a bachelor's degree in Computer Science & Engineering followed by a master's degree in Project Management. Currently pursuing Ph.D. In Information Technology from the University of the Cumberlands. His areas of research interest include RDBMS, distributed database, Cloud Security, AI and Machine Learning. He is an MCT (Microsoft Certified Trainer) since 2017 and holds other premier certifications such as MCP, MCTS, MCDBA, MCITP, TOGAF, Prince2, Certified Scrum Master and ITIL.