Cloud Sentinel: Cloud Migration and Data Protection

Clarence V. Kimbrell Jr.

Old Dominion University

CYSE 494

Professor Akeyla Porcher

June 21st, 2023

Clarence V. Kimbrell Jr.

Cloud Sentinel: Cloud Migration and Data Protection

Cloud migration and data protection have been increasing in popularity in recent years due to the convenience they offer to companies, businesses, and individuals. They provide a larger storage capacity for information, addressing the limitations of on-site servers that can quickly reach storage capacity due to the vast data businesses produce in just a few days. According to professors Harjot Singh Dod and Rajeev Sharma from the University of Melbourne, business data can be collected from various sources such as customer transactions, sales records, website interactions, supply chain activities, and many more (Dod & Sharma, 2012). This information allows a business to gain a competitive advantage against its competitors.

Additionally, the wear and tear on the machines themselves exacerbate these challenges, which are crucial for businesses. On average, businesses should upgrade their server infrastructure every three to five years (Greenstein, 2020). For example, very large businesses often follow these guidelines, and in many cases, they upgrade more frequently to maintain the best infrastructure (Greenstein, 2020). Cloud Sentinel offers solutions to these problems, eliminating the need for businesses to constantly research data server upgrades and worry about storage limitations. Our migration service handles these issues while ensuring stored data protection. This service is accessible to anyone, including individuals, local businesses, and small companies.

Cloud migration and data protection are rapidly becoming essential assets for companies and businesses. It is evident that many smaller companies still lack an online presence; if they do, it does not meet the expected standard. Some of these companies may or may not have on-

site servers to collect and process data. By embracing cloud computing and implementing robust

data protection measures, businesses can free up space occupied by large technical machinery.

They will gain the capability to store vast amounts of data effortlessly, all while ensuring

comprehensive protection. In a little over a year from 2017 to 2018, it is estimated that 1.9

billion personal records and sensitive data were stolen in data breaches (Maurer & Hinck, 2020).

Cloud security is different from traditional cybersecurity because cloud security is networked,

concentrated, and shared (Maurer & Hinck, 2020). Since it relies on internet connectivity, it

comes with the added danger of potential threats that could take advantage of this (Maurer &

Hinck, 2020).

Cloud Sentinel acknowledges the significant increase in data breaches over the past few

years and the differences between cloud cybersecurity and normal cybersecurity. It emphasizes

the criticality of data protection following migration. Our company will remain vigilant and up to

date with the evolving cyber threat landscape. Cloud Sentinel proactively adapts our strategies to

combat emerging attacks and promptly implements the necessary changes. Security is our top

priority, and we continually strive to provide a secure environment for our client's valuable data.

Governments worldwide have established regulations that businesses must comply with

to operate within their respective regions. Cloud Sentinel is committed to adhering to these

regulations, safeguarding user data, and refraining from sharing it with other companies and

individuals. Unlike major corporations that profit from selling personal data, Cloud Sentinel

prioritizes security and maintains the utmost confidentiality. Many online users unknowingly

sign terms allowing their information, such as cookies, to be sold off to larger companies

(McGregor et al., 2013). These companies can have better estimates of demand and customer

preferences (McGregor et al., 2013). This information can benefit the major company in many ways but at the expense of user privacy.

The Problem and the Solution

At Cloud Sentential, their mission is to provide a seamless data migration service and a robust data protection product. But what exactly is the cloud? Cloud computing refers to the delivery of hardware, software, and storage services from a remote provider, eliminating the need for local sourcing and support (Rampp et al., 2012). The advantages of transitioning to the cloud include cost savings, time-saving for staff, and eliminating local system maintenance (Rampp et al., 2012). This is particularly beneficial for smaller companies that would otherwise need to hire server technicians for repairs, as the responsibility is shifted to the cloud migration company.

The potential of cloud computing is so significant that even the US Department of Defense is fully embracing it (Doubleday, 2019). In the twenty-first century, migrating to the cloud has become essential due to its practicality and user-friendliness. One of the key principles guiding our approach is understanding the risks associated with data protection. As stated by Mahmoud (2013), the world's productive and informational services have become heavily reliant on the internet, making them vulnerable to cyberattacks:

> Most of the world's productive, intangible, and informational services have come to exclusively rely on the Internet. This process began in the 1990s with the shift of mass communication to the Internet and the ever-growing demands on it in the fields of production, distribution, communications, and finance. Such a heavy reliance on the Internet makes the potential damage from cyberattacks even greater. (p. 1)

This aligns perfectly with the work of Cloud Sentential, as they recognize the critical importance

of adapting to and learning from past events and attacks to safeguard our data centers. By doing

so, they can enhance our preparedness and fortify our defenses against potential threats.

Mahmoud (2013) further emphasizes that cyberattacks have become low-cost yet powerful tools

capable of inflicting millions of dollars in damages. So, to allow businesses to operate without

fear of being under constant cyber threat, Cloud Sentinel will make data protection of utmost

importance.

      We will closely monitor emerging threats and make necessary changes promptly to

ensure the security of our customer's data. Next, we will conduct mandatory risk assessments.

According to Kaffenberger and Kopp, cyber risk is:

> The risk that a cyber event (attack(s) or another adverse event (s)) at an individual
>
> component of the infrastructure ecosystem will cause significant delay, denial,
>
> breakdown, disruption, or loss, such that services are impacted not only in the originating
>
> components, resulting in significant adverse effects to the health or safety of a company.
>
> (p. 5)

These assessments will be performed regularly, every few months, to identify any weaknesses or

vulnerabilities within our systems. Things that will be identified within Cloud Sentinel's risk

assessment but are not limited to are weak passwords, outdated software, and external risks.

After these regular assessments are conducted, the company can prioritize and allocate resources

to work on these areas. It can provide Cloud Sentinel with a priority list of the potential impact

and likelihood of an event occurring. Overall, this will bring down the risk factor of dealing with

customer data from the outside world. These risk assessments will work hand in hand with another part of risk assessment and that is incident response.

Businesses worldwide need to practice cyber incident response, and Cloud Sentinel is no different. The policymakers at Cloud Sentinel will develop a response framework before a disruptive cyber-attack occurs (Freakin, 2015). Although each response to different attacks will vary, the framework will ensure that Cloud Sentinel can swiftly consider its options. In the event of a cyber-attack on Cloud Sentential, their trained team of experts can quickly mitigate the situation. This will be partly due to risk assessment and incident response, enabling the team to navigate through the policy until it aligns with the corresponding attack. Cloud Sentinel will follow in the footsteps of other cloud migration and data protection services but will differentiate itself through its commitment to continuous improvement and advanced security measures to stay ahead of the curve.

Another aspect of the problem and solution that Cloud Sentinel will face is stakeholder confidence. By conducting regular risk assessments and updating incident response policies, Cloud Sentinel will demonstrate that it can be trusted and provide customer confidence in the service and protection it offers. The company aims to send a message to potential stakeholders, partners, and customers that their priority is to provide the best experience. Cedric E. Dawkins, an author of the Journal of Business Ethics, believes that to ensure stakeholder confidence, a business must focus on three things: dialogue, negotiation, and transparency. Cloud Sentinel will extensively work on all three aspects, and in recent years, the use of transparency has significantly increased (Dawkins, 2014). The company will disclose a lot of information to further enhance trust and transparency.

Cloud Sentinel will only authorize reputable figures from the customer's business to have access to their data at any time. Within the facility, they will employ a Terminal Access Controller Access Control Server, commonly referred to as TACACS+. This will allow for easy network device administration (Computer Security Update, 2022). With this approach, they can expect hundreds of customers to access their data simultaneously, providing our employees with a streamlined workflow that is not hindered by the authorization process for customers. All computers within Cloud Sentinel will be under TACACS+ monitoring (Computer Security Update, 2022). Enabling network device authentication and authorization to restrict access to authorized individuals at Cloud Sentinel and their customers (Computer Security Update, 2022). Authorized customers will need to complete a lengthy multi-step process to access the stored information. Our approach emphasizes a hands-off policy, and Cloud Sentinel employees will never search through the information stored in their service and product. This is important because, at Cloud Sentential, their top priority is to provide a service and product that prioritizes customer information and privacy.

Advanced encryption methods, such as multidimensional lattice point encryption, will be employed at Cloud Sentential. This encryption technique poses a challenge for most computers today, offering long-term protection for user information. Recognized by NIST as one of the four new quantum-resistant cryptographic algorithms, multidimensional lattice point encryption holds significant importance in the field (NIST, 2022). The process involves dimensional planes, where two points start at the same point and move in a direction, while a third point is located far from the original two. The third final point is obtained by combining the original points and directions using integer combinations (Alwen, 2018). In multidimensional lattice point encryption, computers are only given the vectors, not the dimensions, requiring them to determine the closest

point among all surrounding points to reach the final point (Alwen, 2018). Cloud Sentinel anticipates a significant increase in the number of dimensions, making decryption more challenging as time passes. This becomes particularly important in light of emerging threats like "store now and decrypt later" attacks and the potential rise of quantum computing (Ionescu, 2016). These attacks involve intercepting sensitive encrypted traffic or financial information with the hope of decrypting it easily in the future using a quantum computer. By proactively countering these threats, we can enhance security measures.

To address potential issues, Cloud Sentinel will be prepared for all scenarios, including regular data backups. In the event of a natural disaster, the cloud migration and data protection service will remain operational in a separate location. According to Wing S. Chow and Wai On Ha (2009), authors of "Determinants of the critical success factor of disaster recovery planning for information systems",

> Disaster recovery consists of two measurement items, which are the external, off-site backup processing sites for disaster recovery planning. This critical success factor suggests that an external backup processing site should be established so that information systems operations/services would still be functional if a disaster were to strike at a local office. (p. 268)

By following this approach, Cloud Sentinel ensures data availability and security, minimizing the impact of potential data loss or corruption. Additionally, Cloud Sentinel will promptly monitor and respond to security events, including monitoring stored data to detect any potential data loss. This proactive approach ensures that no data is compromised when off-site backups are used.

Clarence V. Kimbrell Jr.

One barrier that we expect is smaller businesses' uncertainty about privacy when it comes to our product and service. Entrusting extremely sensitive data to a third-party company overall may not sound safe. But Cloud Sentinel can assure that the information stored is and will be. This can be achieved by using the "best, fastest, and most up-to-date computer equipment to handle massive amounts of data. Customers will also expect that cloud providers have the best hardware and software because data demand will continue to increase." (Sipes, 2011). The quote provided by James L. Sipes is at the forefront of Cloud Sentinel's business model and value proposition.

Another barrier we expect to encounter is dealing with the migration of older systems. This process will require more time and cooperation from the businesses seeking an upgrade. Legacy systems can present various issues, such as data format and compatibility problems. Cloud Sentinel will utilize cutting-edge technology for storing and migrating information. The data format may need to be modified to ensure a smooth and successful migration between systems. This process will be done using a holistic methodology, which has shown significant success in the past (Zhao & Zhou, 2015). In their article titled "Strategies and Methods for Cloud Migration," Zhao and Zhou explain the concept of a holistic methodology as follows:

> The migration of legacy systems to the cloud should be divided into reasonable types, the Cloud providers and legacy systems should be classified, too. Then, according to a specific kind of legacy system, the selection of Cloud providers, the migration type to be applied, and the required adaption for the migration should be made. (p. 6)

To facilitate this process, Cloud Sentinel can utilize software programs like Blu Age (Zhao & Zhou, 2015). This program aims to extract legacy architecture into product information

management and transform it into a model-driven architecture. By transforming older

technologies into newer, more modern forms, Cloud Sentinel can effectively meet the needs and

expectations of its customers and long-standing businesses.

As mentioned earlier, regulatory and compliance requirements for specific regions could

pose a barrier to overcome. Different geographical locations may have different regulations in

place regarding data protection and privacy, which must be met to comply with industry

standards in those areas. Researching and understanding these regulations could present a

potential barrier to cloud migration and data protection. Some of these standards and

compliances that Cloud Sentinel will have to enforce are as follows ISO/IEC 27000 which is a

security guideline that is filled with many different standards that need to be met (Yimam &

Fernandez, 2016). Then ISO/IEC 27002 which is the transfer of data from the end user,

privileged user, network, application, and information (Yimam & Fernandez, 2016).

The last barrier that Cloud Sentinel will have to face is competition. There are many other

cloud migration and data protection companies. Cloud Sentinel will differentiate itself from

others by offering personalized and tailored solutions, demonstrating advanced security

measures, and investing in marketing and branding. Cloud Sentinel will provide customized

solutions that address the specific requirements of individual customers. As mentioned earlier,

transparency will be a key aspect, where Cloud Sentinel will discuss the advanced security

measures implemented within the company. This includes showcasing the technologies and

measures used to safeguard customers' data, such as encryption methods, detection systems, and

compliance with industry standards and regulations. These efforts aim to demonstrate Cloud

Sentinel's commitment to data privacy and security. Also, Cloud Sentinel will focus on

developing a strong brand identity and engaging in targeted marketing strategies. This will

increase the company's visibility and attract potential customers. Cloud Sentinel will establish an online presence, participate in industry events, and actively engage in social media activities.

Related Material

At Cloud Sentential, the company is based on a wide variety of subjects. One of these subjects is sociology, which involves the study of human societies, their interactions, and the processes that shape them (Form & Faris, 2023). Within sociology, there is a theory called actor-network theory. Huang and Hsieh (2010) describe it as "the way actors form alliances, involve other actors, and utilize non-human actors to strengthen their alliances and protect their interests" (p. 2). It is important to highlight the four essential components of this theory: problematization, interessement, enrollment, and mobilization (Huang and Hsieh, 2010). While most of these terms are familiar in the business context, one term may be less commonly known. It is a French word that is occasionally used in English, and Huang and Hsieh (2010) define it as "the focal actors convincing other actors that the interests defined by the focal actors align well with their interests."

By adopting the lens of actor-network theory, businesses can comprehend how companies create value through networks and align their interests with their services (Huang and Hsieh, 2010). Understanding business values and approaching them as human societies can foster better mutually beneficial relationships. This involves identifying shared problems, and interests, demonstrating involvement in the new relationship, and ensuring partnership stability (Huang and Hsieh, 2010). These concepts align with sociology and are relevant to Cloud Sentinel's services and products, particularly in terms of potential future partnerships and relationships with other companies.

Another concept that will be utilized at Cloud Sentinel is interdisciplinary research. Many successful businesses worldwide take an interdisciplinary approach to solving problems, creating new products, or improving their overall business environment. According to Moti Nissani's article "Fruits, Salads, and Smoothies: A Working Definition of Interdisciplinarity,

> Interdisciplinarity involves bringing together distinctive components of two or more disciplines. Typically applies to four realms: knowledge, research, education, and theory. Interdisciplinary research combines distinctive components of two or more disciplines in the search or creation of new knowledge, operational procedures, or artistic expressions. (p. 121)

This approach aligns perfectly with the research and development team at Cloud Sentential. By adopting an interdisciplinary research approach, engineers can benefit from diverse perspectives and backgrounds to create optimal solutions for new ideas and products. For example, by integrating computer science, cryptography, and business background knowledge, Cloud Sentinel can develop user-friendly, well-protected, and effectively marketed solutions. Furthermore, Cloud Sentinel can leverage interdisciplinary research to create new operational procedures that integrate aspects of security, legal considerations, and organizational management (Nissani, 1995).

Overall, interdisciplinary research serves as a valuable tool for Cloud Sentinel to harness the expertise and insights from various disciplines, resulting in innovative and well-rounded approaches to address complex challenges and meet the needs of their customers. Without this type of approach, Cloud Sentinel would be left in the dark, narrowed in on one viewpoint, with zero insights from other existing sources.

Effectiveness and Success

Several factors will contribute to the success of the cloud migration and data protection business. One of the most significant factors is customer satisfaction, which serves as a strong indicator of our success. Customer satisfaction is linked to customer loyalty, so building a strong satisfaction level can increase customer loyalty (Singh, 2006). Satisfied customers are more likely to share their positive business experiences with others (Singh, 2006). To ensure customer satisfaction, we will conduct surveys and regularly seek feedback about the services and products we provide. This feedback will provide valuable insights for testimonials, retention rates, and referrals. Cloud Sentinel will utilize this information to make informed decisions and maintain a high level of satisfaction among both customers and employees.

Another important indicator of success is business growth. A growing customer base indicates that more people are choosing our products and services over our competitors. This growth demonstrates the effectiveness and value of Cloud Sentinel offerings. Additionally, having a positive online reputation is crucial for success. Online opinions about our business hold considerable weight and can significantly influence potential customers. According to Vartiak (2015), "A proper online reputation management strategy is beneficial for every organization. Recommendations for organizations are to monitor their online presence and manage it properly, so they can gain more customers and, of course, higher profit" (p. 270). Building and maintaining a good online reputation will enhance Cloud Sentinel's credibility and attract more customers.

Furthermore, collaborations and partnerships with other companies serve as indicators of success. These collaborations demonstrate that other companies trust Cloud Sentinel and find

value in working with us, establishing mutually beneficial relationships that contribute to our overall success. By focusing on customer satisfaction, fostering business growth, cultivating a positive online reputation, and establishing strategic collaborations, Cloud Sentinel can gauge and achieve success in its cloud migration and data protection business.

What is Needed

One of the first steps that Cloud Sentinel will take early on is the creation of an extensive roadmap to guide its journey. This roadmap will encompass vital information, including short-term and long-term goals, the company's vision, marketing strategy, pricing models, and competitive analysis. Developing a comprehensive business plan of this nature will establish a solid foundation and steer Cloud Sentinel in the desired direction. In their journal article titled "A Checklist for Writing Your Business Plan," Rathod and Mohamedbhai delve into the intricacies of business plans (2016).

> A business plan provides an estimate of your start-up costs and revenue. It can help assess important things like whether you will need financing or how long it might be until you make any money. Some lenders will not consider a loan or other financing without reviewing your plan and others generally look more favorably on applicants who have one (p. 16).

This underscores the importance of Cloud Sentinel creating a comprehensive plan to secure financial support and showcase the company's vision and start-up expenses. In addition to the business plan, Cloud Sentinel will focus on developing effective marketing strategies during its early stages of development. This will ensure a consistent marketing style and approach. The strategies will include capturing the audience's attention quickly, addressing them directly,

creating a memorable impact, establishing trust and confidence rapidly, and employing targeted segmentation.

Furthermore, Cloud Sentinel will leverage various advertising channels, allowing flexibility in the duration of advertisements while effectively conveying the intended message. By prioritizing the creation of a business plan and implementing strategic marketing initiatives, Cloud Sentinel can establish a strong foundation, attract potential investors, and effectively communicate its value proposition to target customers.

The second step that will be taken early on in Cloud Sentinel's lifetime is to plan the infrastructure and technology needed to bring the company to life. To create a successful cloud migration and data protection company, many crucial elements need to be set up and ready from the start. Data centers will serve as the lifeline of Cloud Sentential, housing the infrastructure that is essential for the company's survival. According to Munn (2023), data centers and servers can be considered a "nexus." This is where Cloud Sentinel will store the vast amount of data from its customers. Many large businesses and corporations have turned to the Nordic Countries to locate their data centers, as highlighted by Doyle (2022). The natural cold weather in this region makes it an attractive choice. Larger data centers generate significant heat from thousands of servers and computers operating simultaneously. Therefore, companies have been investing in the area to reduce cooling costs (Doyle, 2022). These data centers employ a ventilation system with open-air ducts that remove the warmer air generated by the infrastructure and bring in cold air from the outside (Doyle, 2022). This approach utilizes an unlimited renewable resource to cool the data centers, resulting in cost savings and environmental friendliness. Cloud Sentinel aims to follow in the footsteps of these companies by creating an environmentally friendly and

cost-efficient workplace. As part of the planning process, Cloud Sentinel will search for a location that aligns with these goals.

Lessons Learned

While conducting research for this project, I have gained valuable insights into creating a business. One of the key lessons I learned was the importance of developing an effective strategy for evaluating an innovation. In this case, the innovation is a cloud migration service, which was conceived early on by Group D due to our collective cybersecurity backgrounds. It made sense for us to create something we were all well-versed in. However, when it came to the business startup aspect, we lacked experience. By reading numerous journal articles and online opinions, it became evident that building a project or business based on evidence was crucial. This involved developing a comprehensive plan that encompassed an executive summary, general company overview, industry analysis, financial plan, and marketing strategies (Rathod & Mohamedbhai, 2016, p.17). Given the substantial costs associated with a startup, meticulous planning in every aspect alleviated potential budgetary challenges down the line.

Secondly, I learned the importance of translating academic information about an entrepreneurial endeavor through multiple perspectives. During my research for this paper, I came across articles tailored to specific disciplines. By extracting information from these diverse sources and utilizing my understanding of entrepreneurship and interdisciplinary approaches, I was able to effectively describe the innovation behind Cloud Sentential. This enabled me to comprehensively address every aspect of starting a potential business. The knowledge and experience gained from this process will increase the likelihood of success if I decide to pursue the creation of a business or project driven by evidence, research, and confidence.

References

Alwen, J. (2020, August 15). What is lattice-based Cryptography & why you should care? Medium. https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717

Chow, W.S. and On Ha, W. (2009), "Determinants of the critical success factor of disaster recovery planning for information systems", Information Management & Computer Security, Vol. 17 No. 3, pp. 248-275.

Dawkins, C. E. (2014). The Principle of Good Faith: Toward Substantive Stakeholder Engagement. Journal of Business Ethics, 121(2), 283–295. http://www.jstor.org/stable/42921381

Dod, H. S., & Sharma, R. (2012). Competing with Business Analytics: Research in progress. In D. N. Hart & S. D. Gregor (Eds.), Information Systems Foundations: Theory Building in Information Systems (pp. 239–250). ANU Press. http://www.jstor.org/stable/j.ctt24h30p.15

Doubleday, J. (2019). Pentagon details plan to 'aggressively' embrace cloud computing. Inside the Pentagon, 35(6), 1, 12–13. https://www.jstor.org/stable/26586060

Doyle, S. (2022, December 12). Is Iceland the coolest location for Data Centres?. RSS. https://eandt.theiet.org/content/articles/2022/12/is-iceland-the-coolest-location-for-data-centres/

Feakin, T. (2015). Developing a Proportionate Response to a Cyber Incident. Council on Foreign Relations. http://www.jstor.org/stable/resrep05657

Form, W., and Faris, Robert E.L. (2023, May 16). sociology. Encyclopedia Britannica.

https://www.britannica.com/topic/sociology

Greenstein, S. (2020). The Basic Economics of Internet Infrastructure. The Journal of Economic

Perspectives, 34(2), 192–214. https://www.jstor.org/stable/26913190 Competition and

server data

Huang, C., & Hsieh, C. (2010). Sociology view on cloud computing value: Actor-network theory

perspective. In Proceedings 1st Conference on Cloud Computing GRIDs and

Virtualization, Lisbon, Portugal (pp. 145-149).

Ionescu, A. M. (2016). Nanotechnology and Global Security. Connections, 15(2), 31–47.

http://www.jstor.org/stable/26326438

Kaffenberger, L., & Kopp, E. (2019). Properties of Cyber Risk. In Cyber Risk Scenarios, the

Financial System, and Systemic Risk Assessment (pp. 2–7). Carnegie Endowment for

International Peace. http://www.jstor.org/stable/resrep20985.7

Mahmoud, K. W. (2013). Cyber Attacks: The Electronic Battlefield. Arab Center for Research &

Policy Studies. http://www.jstor.org/stable/resrep12651

Maurer, T., & Hinck, G. (2020). Cloud Security. In Cloud Security: A Primer for Policymakers

(pp. 22–37). Carnegie Endowment for International Peace.

http://www.jstor.org/stable/resrep25787.9

McGregor, V. K., Calderón, S. H., & Tonelli, R. D. (2013). Big Data and Consumer Financial

Information. Business Law Today, 1–4.

http://www.jstor.org/stable/businesslawtoday.2013.11.05

Munn, L. (2023). Introduction. In Technical Territories: Data, Subjects, and Spaces in

Infrastructural Asia (pp. 3–12). University of Michigan Press.

http://www.jstor.org/stable/10.3998/mpub.12584902.5

Nissani, M. (1995). Fruits, Salads, and Smoothies: A Working Definition of Interdisciplinarity.

The Journal of Educational Thought (JET) / Revue de La Pensée Éducative, 29(2), 121–

128. http://www.jstor.org/stable/23767672

NIST announces the first four quantum-resistant cryptographic algorithms. NIST. (2022, July 7).

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-

resistant-cryptographic-algorithms

PORTNOX UNVEILS THE FIRST CLOUD-NATIVE TACACS+ SOLUTION. (2022).

Computer Security Update, 23(7), 3–4. https://www.jstor.org/stable/48673655

Rampp, C., Clarke, J., & Burkholder, B. (2012). Moving Your Library to the Cloud. In B. R.

Bernhardt, L. H. Hinds, & K. P. Strauch (Eds.), Something's Gotta Give: Charleston

Conference Proceedings, 2011 (pp. 494–496). Purdue University Press.

https://doi.org/10.2307/j.ctt6wq4sf.88

RATHOD, S. H., & MOHAMEDBHAI, Q. (2016). A Checklist for Writing Your Business Plan.

Family Advocate, 38(3), 16–17. http://www.jstor.org/stable/24628863

Singh, H., 2006. The importance of customer satisfaction in relation to customer loyalty and

retention. Academy of Marketing Science, 60(193-225), p.46.

SIPES, J. L. (2011). CLOUD CONTROL. Landscape Architecture, 101(5), 62–68.

http://www.jstor.org/stable/44795619

Vartiak, L. (2015). Benefits of online reputation management for organizations operating in

various industries. TRANSCOM 2015, (pp. 270-276).

Yimam, D., Fernandez, E.B. A survey of compliance issues in cloud computing. J Internet Serv

Appl 7, 5 (2016). https://doi.org/10.1186/s13174-016-0046-8

Zhao, JF., Zhou, JT. Strategies and Methods for Cloud Migration. Int. J. Autom. Comput. 11,

143–152 (2014). https://doi.org/10.1007/s11633-014-0776-7