Group #7

May 5th, 2017

Abhinav J.

David Whitney

Shaina Sexton

Kyler O’Neal

Lane McGuire

CS394 Cloud Computing

**Abstract:**

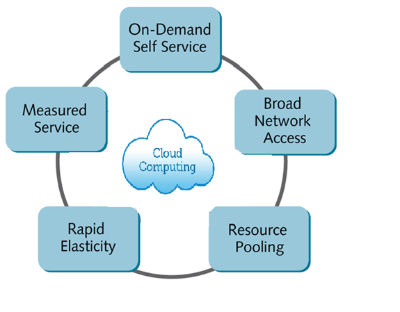
Cloud computing is one of the largest developments in recent years when it comes to information technology. With the low costs, easy accessibility, and ability to virtually store information, cloud computing is desirable for many individuals and organizations throughout the world. Although cloud computing has many advantages, this internet based service brings up concern when it comes to some aspects of information security. The migration objectives is displayed throughout this report by the implementation of the five R's: re-host, replace, refactor, rebuild, and revise. The various constraints that come with working with the cloud and possible solutions to these inconveniences will also be presented in this paper.

**Introduction:**

Cloud computing is a way of storing and accessing data and providing web services over the internet from another location. At a cheaper cost to the user, it provides the user with services that might not be available to them. There are many concerns about cloud computing such as privacy, loss of data, and being unable to access your data. The privacy of your information is a concern because companies that provide the service have access to all of the data of every user that stores information on their servers. Since there has been an increase in the number of people using the service, security has become a larger issue. There are few restrictions or laws that define what companies have to do with the user’s information which could mean that they can release information by accident or otherwise to anyone that they want. Finding a way to insure that your information is protected is essential for the future of cloud computing.

**Background:**

Cloud computing started out as an idea from the 1950s to help cut costs from owning a mainframe. Instead of buying a mainframe for each employee, they bought the one mainframe and then had the employees access that mainframe from terminals. The next step in creating the cloud was the concept of virtual machines. Using virtual machines made the cost cheaper to distribute and overall it is a required component of cloud computing. Cloud computing arose from previous evolutions like grid computing, utility computing, and SaaS. Cloud computing is a combination of these previous types. Cloud computing is a way of storing and accessing data over the internet from somewhere else, other than using your own computers resources. Cloud computing can be summed up into five unique features; on-demand self-service, global network access, resource sharing, rapid elasticity, and measure service. On-demand self-service means that the cloud computers themselves can facilitate their own resources effectively when needed without human control. Global network access means cloud computing services can be accessed anywhere with internet access at any time of the day. Resource sharing is a way to share data centers in other parts of the world which would allow for better connectivity for clients that live closer to certain cloud computing centers. Rapid elasticity, is what the use to be able to boost power to one consumer when needed more than others. Lastly, measured service is the cloud service provider’s way of tracking what the consumer has used so that they only pay for what they use.



**Cloud Computing in Simple Words:**

Cloud computing, in turn, refers to sharing resources, software, and information via a network, in this case the Internet. The information is stored on physical servers maintained and controlled by a cloud computing provider, such as Apple iCloud, Microsoft Azure, etc. As a user, you access your stored information on the cloud via the Internet.

By using cloud storage, you don’t have to store the information on your own hard drive. Instead, you can access it from any location and download it onto any device of your choice, including laptops, tablets, or smartphones. Moreover, you can also edit files, such as Word documents or PowerPoint presentations, simultaneously with other users, making it easier to work away from the office. There are several types of cloud computing services available to suit diverse needs. While some cater to individual users who want to store photos, documents, and videos, others are destined for companies that need extensive platforms to develop IT applications.

**Brief Description of Microsoft Cloud Provider: AZUR**E

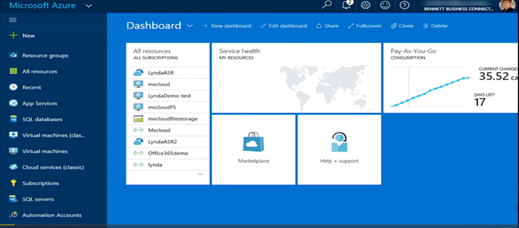
**What is Azure?**

Cloud solutions from Microsoft, it is present in 24 regions, has 21 online data centers and providing 67 different type of services. It is one of the top cloud provider in the world.

When you use software as a service from Azure, all the essential work is done by the vendor which is Azure, than having your own data center with all the workload managed by yourself.

**What can you do with Azure?**

Azure is easy and intuitive to use and it is based on existing skill set. Follows existing best practices and has preconfigured templates. Azure provides us with common infrastructure services which are identity management, backup and recovery services and virtual machines.



**Identity protection:** It is Backbone of office 365,identity control to Saas applications. It has multifactor authentication and single sign on

**Disaster Recovery:** Top priority data backup and protects workload and virtual machines.

**Azure Virtual Machine:** It is fast**,** has pre-loaded templateswith licensing included. Virtual machines are scripted and is automated.

**Layering the foundation:**

Basic components include resource groups, virtual networks, and virtual storage

**Resource groups:** It contains all the resources**,** manages everything as one unit**.** Provides with control access and tags**.** Also gives an estimate usage billing.

**Virtual Networks:** Provides IP addressing and DNS service and VPN gateway

**Azure Storage:** It is durable, scalable and highly flexible meaning that the user can add or delete anywhere from any of the registered devices

*So, when laying the Azure foundation, the following step are followed initially:*

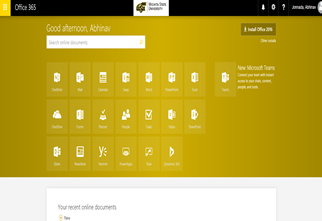
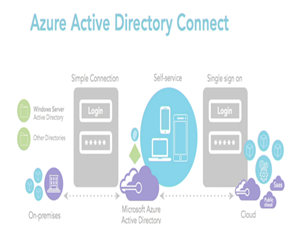
· *Build resource groups first*

· *Create IP addressing schemes*

· *VPN gateway and DNS resolution*

· *Create plans for the storage requirement*

**Azure Active Directory**



Azure Active Directory provides the function of single sign on, takes care of IT provided credentials, provides group access to certain applications and disables access to users or groups when not needed. Azure Active Directory controls the access panels, helps in multifactor authentication, branding, reporting and device management.

**Access planes:** It is a Web based portal, gives the of lists the Iaas applications i.e, storage, networking, etc. Provides the user with hints for passwords and usernames. Provides the functionality of self-service password rests. With such functionalities, the user becomes self-sufficient.

*(Fact: In a company, it costs up to 70$ to reset the password and most of the desk help calls are for password reset. In a way it keeps the cost down)*

**Multifactor authentication:**  It is basically another way to identify and access applications. Few of the multifactor authentication are IP based access, biometric access etc.

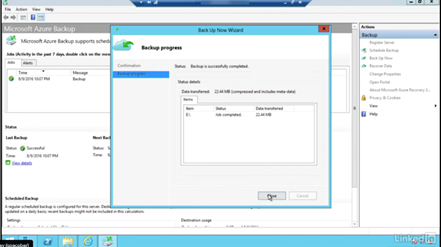
**Branding of the company:** Helps in providing branding of the company by adding logo, illustrations and provides the content in different languages.

**Reporting:** Notices and updates any suspicious activity, automatically blocks the users and the device when suspicious activity is noticed. Maintains activity logs of each and every user and devices registered on AAD.

**Device Management:** Can authenticate any device to AAD and automatically configures to company network**.** Takes care of disabling devices

**Disasters:**

**Azure Backup:** Encrypts the data and it requires a passphrase to access the backup**.** The backup is automatically compressed**.** The data backup on Azure can be backed for 99 years and it automatically maintains 6 copies of the data and it is easy to restore and auto scales the storage if more data is added in the future.

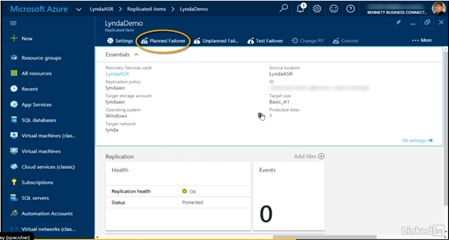


**Azure Site Recovery:** It contains the recent replica of workload which is 15 minutes last left. It is easy to recover and has the functionality of on premise virtual machine replication**.** Azure Site Recovery is based on planned, unplanned and test failover

· Planned failover: maintenance, weather it has no data loss but some lost time

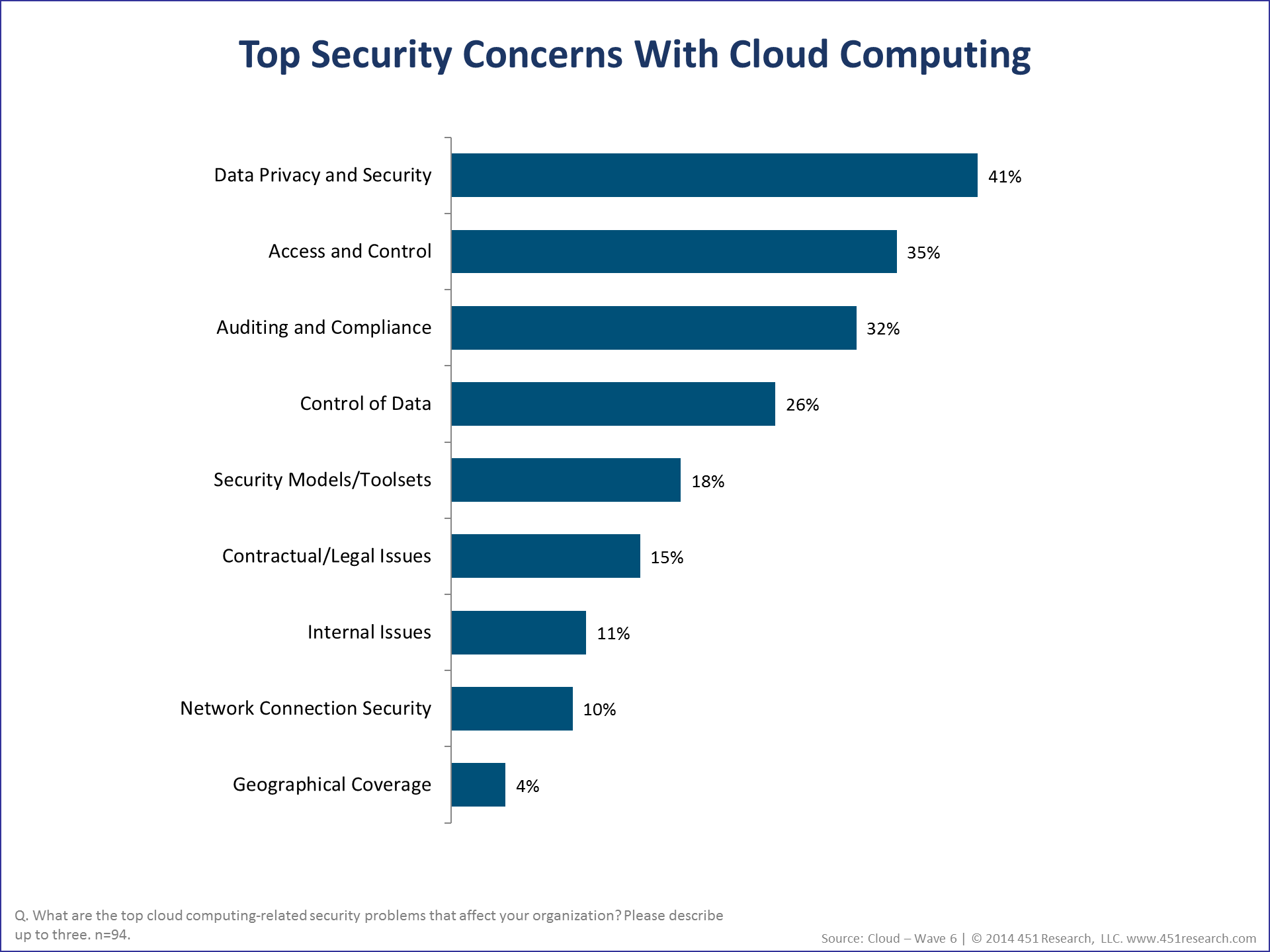
· Unplanned failover: Hardware failure, power outage and it has data loss

· Test failover: Simulates what happens when there is a failover. Environment and is not affected and no down time.



**Concerns with Cloud Computing:**

Although cloud computing has made a major breakthrough in the way data is stored, shared, and accessed, there are some concerns that come with internet based computing services. The most vital issue that comes with the implementation of cloud computing is the safety aspect. There are many insufficient factors that portray the cloud as being unsecure when it comes to the protection of data. Because of this, some may believe that this system is an inadequate way of handling information. The process of outsourcing data with the use of cloud computing allows access of personal information to third party providers. By doing so, the user is compelled to trusting the provider with their data. Another concern of security comes from the fear of cyberattacks. Dealing with the access of data through the use of the internet allows for the target of information. By putting data on an internet susceptible system, the user is risking the theft, destruction, and alteration of their data. From small businesses to large corporations, hackers have their reasons for wanting to target these cloud users. Small companies are easier to breach, while big businesses allow for larger payouts. No matter what the type of business the user is, they are increasing their risks of being hacked by using cloud services. Along with hackers and malware, cloud services are also attacked by insider threats. Because there are now multiple people who have access to the data, a user now has to worry about not only the vendor's staff, but the corporation's own staff targeting their information. A downfall in the cloud provider can affect every user making them all more susceptible to being targets. Another concern of users is the accessibility of their data by the U.S. government. A ruling was made by the U.S. judicial system stating that "any data stored in the U.S. vendor's data center, regardless of location, was [available to the government] with the right warrant." By allowing information to be publicly accessed and maintained by a third party vendor, the government is allowed entrance under the Patriot Act. The interpretation of what "safe" is varies from cloud to cloud. The different cloud providers each seem to have their own definition of what safe is and how they implement their protection regulations. Because a lack of cloud standardization, there is no evident guideline that cloud providers should follow in order to create an undivided principle between clouds. Since cloud providers are not all built the same, there is no "rule of thumb" for how safety protocols are utilized. When using a cloud service you ae putting your data in the hands of the vendor, along with the internet service provider, ISP. Without internet access, cloud computing cannot be sufficiently used. No ISP can promise uptime at all hours of the day, therefore the cloud provider also cannot guarantee 100% uptime.



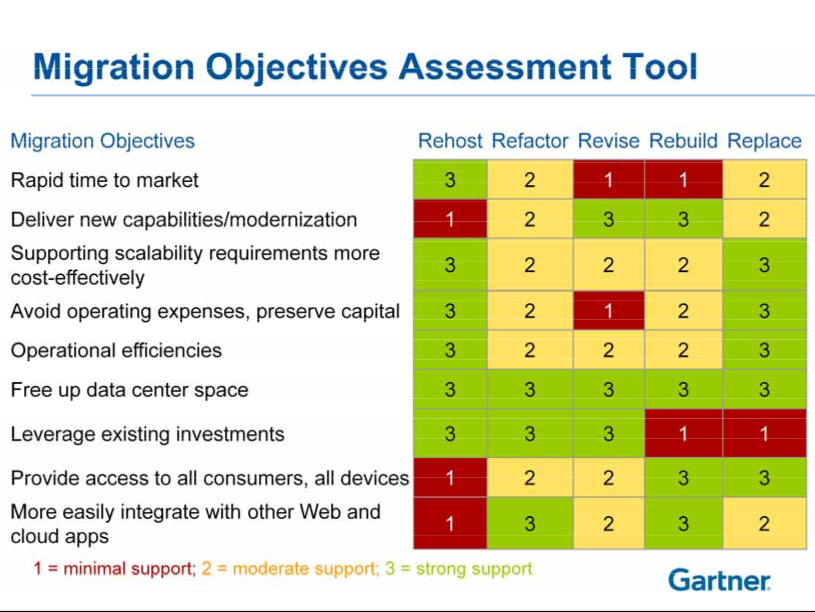
**Solutions to Common Concerns:**

To build trust in cloud computing’s security of user data there should be some solutions to the problems that have been presented so far. One of the major problems that has been mentioned is that of how cloud service providers and third parties use clients’ data. Vic (J.R.) Winkler says that “Depending on the type of cloud provider with whom you contract, you’ll have to consider if your data is going to be mined by the supplier or others. The use of your data may occur unbeknownst to you or by virtue of a configuration error on the provider’s part. Based on the sensitivity of your data, you may wish to ensure your contract prohibits or at least limits the access the cloud provider has to use this data (“Cloud Computing: Data Privacy in the Cloud”).” When it comes to preventing data breaches both the cloud provider and the client need to exercise preventative and reactive measures against breaches. Cloud providers, according to Aliah D. Wright, need to encrypt the data in transit and at rest, have good password configurability, encrypt the passwords, support IP address based access control (IP restrictions), support two-factor authentication, support full system auditing, and subject their setup to third-party vulnerability scanning and penetration testing annually (How to Prevent Data Breaches). Organizations also need to follow many techniques. Fahmida Y. Rashid says “Data breaches and other attacks frequently result from lax authentication, weak passwords, and poor key or certificate management. Organizations often struggle with identity management as they try to allocate permissions appropriate to the user’s job role. More important, they sometimes forget to remove user access when a job function changes or a user leaves the organization…Many developers make the mistake of embedding credentials and cryptographic keys in source code and leaving them in public-facing repositories such as GitHub. Keys need to be appropriately protected, and a well-secured public key infrastructure is necessary, the Cloud Security Alliance said. They also need to be rotated periodically to make it harder for attackers to use keys they’ve obtained without authorization. (The dirty dozen: 12 cloud security threats)”. Data loss is another problem that can result from a data breach. Again, Fahmida Y. Rashid offers advice here by telling us that “Cloud providers recommend distributing data and applications across multiple zones for added protection. Adequate data backup measures are essential, as well as adhering to best practices in business continuity and disaster recovery. Daily data backup and off-site storage remain important with cloud environments. The burden of preventing data loss is not all on the cloud service provider. If a customer encrypts data before uploading it to the cloud, then that customer must be careful to protect the encryption key. Once the key is lost, so is the data (The dirty dozen: 12 cloud security threats).” There also needs to be a solution for when a cloud provider goes bankrupt or has internet or power issues. Brandon Butler says that “At the most basic level, preparing for your cloud provider to go out of business should start before you even actually use the cloud, says Ahmar Abbas, vice president of global services for DISYS, an IT consultancy. DISYS helps companies create a cloud strategy, and one of the first things to plan before going into the cloud is how to get the data out, at any time. “It all goes back to how businesses historically plan for disaster recovery,” says Abbas. Typically DISYS will work with customers to classify the applications and data that are being placed in the public cloud and rank them based on criticality to the business. High-value data and applications that are mission critical need the highest levels of availability and are treated differently from low-value data that an organization can live without for a certain period of time. If a business is running a core enterprise app in the cloud that is crucial to the company’s daily operations, it should have a live copy of that app in another location, be it another cloud provider or on the company’s own premises, Abbas says. For testing materials perhaps there backup once a month, or maybe even not at all (Cloud's worst-case scenario: What to do if your provider goes belly up).” There is also the problem of a lack of standardization in cloud computing, but there are many organizations that are at work to set some up. These include the Institute of Electrical and Electronics Engineers, the IT Process Institute, the National Institute of Standards and Technology, and the Cloud Security Alliance.

**Migration:**

Your first option is to re-host your application. This is the simplest of the five R’s and most of your data, code, frameworks, and languages are transferred over just the same as it was on your application. “Re-host implies redeployment of the application to a different hardware environment.” In re-host, the provider will begin handling the hardware that your application runs on, so that you don’t have to. This works very well with systems where code modifications cannot be done. The next option is replacing your application. In replacing you application, you will lose an existing application(s) and use existing commercial software from the provider company. All parts of the application will be managed by the provider and all that comes from you is transforming your existing data to match the standards of the provider’s software. Refactor is another option for migrating you application to a cloud system. When you refactor, you are only required to manage your app data/configuration and the source code of your application. All the languages, frameworks, and hardware are managed by the provider and most of the data and code are updated in the process. Refactor usually implies using a web application to replace your application. This could mean that a few changes would need to be made to your code during the refactor but everything else could be reused. Rebuild is a much more time consuming option. It involves discarding the code for the existing application and recreating it on the provider’s platform. While this could take a significant amount of time, all of the app data, source code, languages, and frameworks would be the newest and most efficient versions and there would be no risk of compatibility issues with the provider’s platform. The final option of the five R’s is revise. Revise is a hybrid option that includes modifying or adding to your existing code so that it will support modern requirements. After that has been done, re-host or refactor would be used to move to the cloud. A major disadvantage to revise is that it will be a large development project with a lot of upfront expenses and can take quite a lot of time to fully implement.

There are a lot of factors to think about when deciding to move your application or website to a cloud server. It comes down to costs, time to get up and running again, and how much of your application will need to be rewritten. The chart below sums up where each method is stronger or more convenient as opposed to areas where the method requires a larger time or money commitment.



**Conclusion:**

Cloud computing has grown in usage due to its five powerful features: on-demand self-service, global network access, resource sharing, rapid elasticity, and measure service. It is important to understand some of the technical aspects of how cloud computing works, for example AZURE. Additionally, understanding common concerns such as security and data loss and the solutions to these problems are important, as well as how to migrate to a cloud cleanly using the five R's. We hope this paper has shed some light on topics to think about before getting started with cloud computing.

Works Cited

<https://gartnerinfo.com/futureofit2011/MEX38L_A2%20mex38l_a2.pdf>

Bothwick, Neil. "Data Privacy: How Safe Is Your Data in the Cloud?" *TechRadar*. TechRadar

Pro IT Insights for Business, 03 Aug. 2013. Web. 02 May 2017.

Butler, Brandon. “Cloud's worst-case scenario: What to do if your provider goes belly up.”

Network World. IDG Communications, Inc., 2 Jun. 2014. Web. 2 May 2017.

*Planning a Microsoft Cloud Solution*. Dir. Sharon Bennett. N.d. *Lynda*. Web. 02 May

2017.

Rashid, Fahmida. “The dirty dozen: 12 cloud security threats.” InfoWorld. IDG

Communications, Inc., 11 Mar. 2016. Web. 26 Apr. 2017.

"What Is Cloud Computing?" *Cloud Computing News*. N.p., 04 Aug. 2016. Web. 02 May 2017.

Winkler, Vic. “Cloud Computing: Data Privacy in the Cloud.” TechNet Magazine. Elsevier and

Microsoft, Aug. 2012. Web. 26 Apr. 2017.

Wright, Aliah. “How to Prevent Data Breaches.” Society for Human Resource Management, 28

Sep. 2015. Web. 26 Apr. 2017

Contributions

Gathered Group – Abhinav J.

Abstract – Shaina Sexton

Introduction – David Whitney, Kyler O'Neal, Shaina Sexton, Lane McGuire, Abhinav J.

Background – Kyler O'Neal

AZURE Details – Abhinav J.

Concerns with Cloud Computing – Shaina Sexton

Security Solutions – David Whitney

Cloud Migration – Lane McGuire

Conclusion – David Whitney, Kyler O'Neal, Lane McGuire, Abhinav.J

Paper Structure/Error fixes – Lane McGuire, Kyler O'Neal, David Whitney, Shaina Sexton, Abhinav J.

Works Cited Format – Shaina Sexton