Why is the cloud useful and needed in the Dealership?

CSS410 Key Assignment

Instructor: Dr. Tonya Canada

By: Joshua Powell

20JAN2023

Table of Contents

Benefits and Risks of Cloud Computing

IaaS (Infrastructure as a Service):

This is a type of service that can provide the necessary storage and protection to the company without the need for an extensive amount of hardware in the physical shop. Iaas is detrimental in making sure that the company can keep the cost down and prevent overhead due to overcalculated growth costs. With Infrastructure as a service, the company can expand data storage and stay secure without having to expand the physical location and allow for the more rapid growth of data versus having to expand physical hardware then expanding data. Not to mention the overall maintenance cost of keeping the hardware at the physical location would be cut almost completely by having Iaas. One of the issues surrounding Iaas is that switching vendors can be daunting if looking to change due to contract concerns and so on. Iaas also is Internet Dependent, in that the service will only work as well as the internet platform that is being used (*What Is IaaS? Infrastructure as a Service | Microsoft Azure*, n.d.).

PaaS (Platform as a Service)

Platform as a Service is another good cloud service that can offer the company some benefits as far as performance, customers, and employees. Using a Platform as a

Service can help with the development and running of customer-based apps. Like using apps for customers to buy parts and to check up on the status of their vehicle while it is in the shop. This would be a great advantage for overall productivity and customer appreciation for the company and would set the company above the rest. This being such a big benefit, there are some drawbacks. One of these drawbacks is that with a service such as this, it is good to keep an eye on the contract for the service as it can be very easy to get caught up in what is known as a Lock-In. A Lock-In can cause a customer of the PaaS to get caught up using a language, interface, or program they no longer need (*What Is PaaS? Platform as a Service | Microsoft Azure*, n.d.).

SaaS (Software as a Service)

SaaS is also another cloud service that has many benefits to the company that can create a very sound cloud working system. One such SaaS system that we use is used to keep licenses up to date and running on the computers that the technician uses to diagnose the trucks and vehicles that are in the shop without the need for having several different licenses. With this type of service, the software can be updated without the need for the technician to worry about keeping the software up to date and be able to focus more on fixing the vehicles they have. This service unfortunately has some downfalls as well. One of those being latency compared to Client/Server apps. There is also Limited Customization as most SaaS offer little in customization. This can be countered with the fact that SaaS offers a great deal in flexibility in that anywhere the technician with an internet connection has access to such services no matter where they are (Smith, 2022).

Overall expectancy:

There are a lot of changes happening in the world of the cloud and basic computing. Just for details Artificial Intelligence and Quantum Computing bring about a new era

of computing and the cloud is part of that. This means that even though what I have mentioned is new and innovative it could soon be outdated due to new technological advancements. Having a flexible plan with these services and making sure that you can switch, and switch smoothly is adamant in the years to come as technology advances more and more. For making sure when you are using an IaaS that you make sure in the policy for the usage of it through the vendor that it will not vendor lock you and make it hard to switch, if need be, the same is for PaaS and SaaS as well. Another part to keep in mind is that when it comes to ensuring functionality and flexibility is that with cloud services you need to ensure that you have good internet service with decent bandwidth to allow for steady and reliable transmissions. This one thing alone could inherently hinder the company if not planned for and mitigated properly.

Current Strategies for Securing Cloud Computing Services

Effective access controls and techniques

When trying to make sure that cloud services are secure there can be a lot of skepticism as to whether or not the techniques being used are up to date and effective. There are a lot of good practices and techniques that will alleviate a lot of issues. The best ones are IP restrictions, Geo-Fencing, and Browser Restriction.

1. IP Restriction

This only allows those certain IP addresses associated with the company to access the cloud services. When restricting IP access, you can either restrict a single user, a subset of users, or a whole organization to an IP restriction policy. Customize mapping of users over one or more IP addresses. This would allow for the ability to make sure that any users are not doing things they shouldn't and would allow for ease of mind when employees are using the cloud services. This technique also does not need firewalls or local installation for it to work allowing for rapid adjustments by the IT department keeping those who would seek to act maliciously from gaining access. From these details, you can tell that this is an easy setup and can be used (*Access Control in Cloud Security – Restrict Unauthorized Access*, n.d.).

2. Geo-Fencing

This technique is used to ensure that data can only be accessed in certain areas local to the place that it deemed. This is a policy-based restriction and can provide a very decent amount of control over your data and where it is accessed to prevent unwanted access

from say a proxy server. This can be used on a single user, an organization unit, or the entire organization just like IP restrictions. Access control can be implemented in many ways and geo-fencing works well for keeping access to these services contained to only designated areas (*Access Control in Cloud Security – Restrict Unauthorized Access*, n.d.).

3. Browser Restriction

When it comes to browser restrictions it helps to keep end users from accessing confidential files and folders on any web browsers. Applicable to all trending web browsers such as Mozilla Firefox, Safari, Chrome, etc. This is organizational unit based granular control policies. This is also easy and has an automated rollout. The reason that browser restriction is such an important technique to implement is that not only can you have a piece of mind on the end-user side of things, but the employee should have the best access to applications as well. This will also decrease service calls to IT admin allowing them more time to focus on security measures and not be worried about employees' access to the cloud applications (*Access Control in Cloud Security – Restrict Unauthorized Access*, n.d.).

Securing Data at Rest (DAR)

For clarity data at rest means any data that is stored in any data warehouse or data lake and anything pertaining to data storage like hard drives and laptops. This is like most legacy systems, but with the new cloud services, they access them to get the data and store data. This can be very daunting to secure these areas if policies are not in place to protect the outside in and inside out. For instance, the access controls for a DAR are a little more extensive as there is a physical location. Securing data at rest is done by educating employees on the different types of personal information and making sure that those who need access to Personal information are the only ones who have access. The other part of Data at rest to secure is making sure that there

is adamant security surrounding the data warehouses and data lakes. One way to do this is by having a key card and a biometric scanner to prevent unwanted access. There is also a more conventional way of securing a data warehouse and that is security guards. The only issue with this would be the human element involved and there would need to be extensive training to make sure that the security guards are aware of the risks involved, along with what to look for with social engineering attacks by malicious actors. Another way I would protect your data at rest is also making sure that your employees are trained as well on social engineering attack schema so that those malicious actors looking to gain access might try to against your employees to use them as pawns to gain access. This is one of those risks that you cannot train employees for enough and there will need to be an extensive policy in place along with ways of enforcing that policy (*How to Secure Data at Rest*, 2022).

Data in Motion (DIM)

Data in motion is like it sounds and is any data that is in transit between data at rest locations. Like sending an email or text message that anyone sends between colleagues in the workplace. One of the best techniques to ensure the protection of data in transit is by ensuring that access to the data is controlled by restricting access by user role and only those who need access to that data are the only ones who should. The other vulnerability that data in motion faces is data hijacking also known as a “man in the middle attack”. These can pose serious risks to companies if they are ill-prepared and not ready for such risks. One way to mitigate such risks is to encrypt your data transmissions. This is best done through TLS and SSL. TSL provides a transport layer that acts as an encrypted tunnel between email servers or message transfers. SSL on the other hand uses public and private keys to encrypt private messages over the internet (Gillis & Fitzgibbons, 2021).

Cloud Security

Gaps in the Cloud

With cloud being a somewhat new innovative solution for companies today, it still has its draw backs. One being it is susceptible to what is known as a denial-of-service attack. Another issue within the cloud is data breaches. Now these can happen very easily but can also be prevented. One of the main sources of data breaches is human error which accounted for 23 percent of data breaches in 2022. One other security gap within the cloud is unlike and error is an insider threat according to Sobers (2022). This is someone who intentionally either leaks confidential information purposefully or actually hinders business operations purposefully from the inside. This would be employees or anyone allowed in and around the premises. The cloud is not 100 percent foolproof and with the rise in cyber-attacks in recent years due to a lot of people working from home, malicious actors have had a lot of surface attack areas compared to the past 5 years. This is only so you can see that there are threats to the cloud and that you must take the necessary precautions to protect the company, employees, and customers from those who would seek to do harm (Avey, 2022).

Sample Policy

Dealership

Company

Cloud Security

Policy

Prepared by:

Joshua Powell

Joshua.Powell74@student.ctuonline.edu

Updated: 3Jan2023

The main purpose of this Cloud Service Policy is to outline the guidelines and requirements for the dealership and ensure the protection of information and technology assets. This policy includes standard practices and methodologies that will help to mitigate risks and threats on the network or systems. This policy is going to lay out the role employees play when it comes to the assets as they pertain to the could services.

Scope

This policy applies to all business associates, part-time, and full-time employees, and other businesses that have dealings with the dealership who have access to its confidential data and the cloud. This is to include all computers, electronic devices, storage media, mobile devices, printers, and any other technological devices being used by the company for cloud services.

Policy Statement

IT Departments Responsibility

The IT department is to be responsible for the company's information security actions, maintenance, audit reports, and any other related procedures and actions pertaining to keeping cloud services up to date and running. Within the department, they will also make sure to adhere to local, state, national, and international regulations so the company can stay relevant and also make sure the company is not violating privacy laws.

New Employees

New Employees will be briefed on the existing cloud security template, methodologies, and standards by their managers during the new hire training process. This step is to further mitigate the risks within the company and educate new employees on what is expected of them.

Restrictions on Suspicious Websites

The IT department specialist will specify what websites to block and which ones to keep up with, along with where to access the cloud services and on what devices. This will be followed to ensure the safety and security of the company and its employee's data. Any violation of this will result in a warning and/or termination depending on the severity.

Download restrictions.

All Employees and subsidiaries are restricted from downloading or installing all unauthorized files or software onto any company-owned devices. Access to cloud services (i.e., email, files, company-owned data, and software) must only be accessed through the appropriate device (i.e., IP address) that the IT department has set up through the cloud services.

Monitoring of Communication

There will be no onsite cell phone communication monitoring. However, the IT department within the company will be monitoring and managing all tools of communication within the company, including social media and emails. This is mainly to ensure the safety and security of our company, employees, and customers.

Policy Violations

In the event of a policy infraction, witnesses, whether within or outside the company should submit a report specifying the infraction, the time and date it happened, and all who were involved and submit it to the IT Department. This way the IT department along with management can come up with the best course of action against those involved and to come up with a plan to mitigate this risk/threat from happening again.

Risk Assessment Strategies

When it comes to risks there are a lot, and you can get caught up securing one only to open another. That said I recommend that the company make sure that any and all employees have background checks done prior to being hired, along with a credit check to make sure the company want fall into an insider threat situation. Another thing to mention is making sure that employees are trained to pick up on changes in the behaviors of their colleagues and to report any behavior that could be discerning (i.e., aggressive behavior, big purchases, disconnection where they used to be outspoken, etc.) this way they can seek counseling and catch a possible insider threat before it happens. I would also recommend running systems checks on all cloud services to include that the services are performing properly and to make sure that they are not lagging due to a possible denial-of-service attack (Avey, 2022).

Business Impact Analysis

Cloud services are forever changing as we move forwards in the age of technology one cannot take for granted the advancements of using cloud technologies and advancements. With the introduction of cloud computing there have been some innovations into quantum computing that have aloud for bigger data analytics allowing for more data analysis on the time spent making key business decisions. This along with Paas, Saas, and Iaas can bring about great

change and with it concern about the security of the company. This can be a daunting task when unsure about the risks taken when applying these platforms to your systems. One thing to keep in mind is that with any innovation in technology, there has to be security measures put into place to help mitigate the risks involved with the new advancements. The biggest risk with all technology is the human element. Having a program in place to constantly train your employees is not the only risk to mitigate but is paramount in keeping your systems secure. For instance, one study done through Verizon in 2022 stated that 82% of breaches involved some sort of human element (Irwin, 2022). This alone can have things in shambles and allow for a lot of doubts and inconsistencies if not dealt with.

Securing Data at rest (DAR)

Something a company can do to secure its data at rest is use something like encryption. This will allow your employees to use the data in a secure manner, so as to keep them from accidentally allowing an outside malicious actor from getting access to the data.

Securing Data in Motion (DIM)

The other part is communication and with that comes a lot of concern with them emailing colleagues within the company, along with outside the company. If they are in fact emailing out of the domain there needs to be training on what data to send and what data not to send. This entails things like what the military uses to classify classified and unclassified data. Even unclassified data can be considered a threat depending on what it entails. Much like that, the company needs to classify data on its' importance and the best method for transferring that data from one party to another. This will be laid out in the risk management policy and enforced by the supervisors and managers (S. 2019). With an in-detail risk management policy and an understanding of the controls needed, the employee will understand that the risks go far beyond

the work place and that taking small steps to verify an email will go a long way in keeping the company secure from malicious actors.

Principles and Practice

Impact of Laws

One law that will impact the overall process of the organization when it comes to using cloud services is conducting federal inspections on class 8 vehicles. These have to be kept on file and having this in a cloud service will help cut back on paper work but it also can make things interesting when the department of transportation needs to see these files. The

law covering this is covered under the 49 CFR 396.17, 396.21. This is no little matter to mess around with and all organizations that handle the class 8 side of things need to be aware of these standards (*The Motor Carrier Safety Planner*, n.d.).

There is also the law 2013 South Carolina Code of Laws Title 59 - Education CHAPTER 67 - TRANSPORTATION OF PUPILS; SCHOOL BUSES SECTION 59-67-270. Inspection of buses. Which governs the inspection of school buses in the state of South Carolina that entails much like the 49cfr for class 8 vehicles, but buses fall under a completely different standard and should be adhered to. When it comes to buses the company will make sure that they keep documentation of the employees training and the inspections on buses. If this is not adhered to they will need to make sure that they keep the correct documentation and checks within the cloud so if DOT needs access to them they can get documentation without any issues. This is adamant in ensuring that the company stays up to standard (*2013 South Carolina Code of Laws :: Title 59 - Education :: CHAPTER 67 - TRANSPORTATION OF PUPILS; SCHOOL BUSES :: SECTION 59-67-270. Inspection of Buses.*, n.d.).

Frameworks

One framework that the company would benefit from ensuring a successful transition into the cloud services it is called “Cloud Security Alliance Controls Matrix” which is a foundational grouping of security controls, created by the cloud security alliance, which will provide a basic guideline for the company to allow for a more secure framework of cloud services. This way there want be a loss off data, like say DOT inspections and bus inspections.

There is another framework that will assist the company in providing the best services. This is called FedRAMP this design framework is a must for those that are dealing with the

federal government. So the fact that the company is doing federal DOT inspections, this standard must be followed to ensure the most secure cloud services for Employees, customers, and the federal government when they need access to DOT inspections (Knowles, 2022).

References

1. *What is IaaS? Infrastructure as a Service | Microsoft Azure*. (n.d.). https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas/
2. *What is PaaS? Platform as a Service | Microsoft Azure*. (n.d.). https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-paas/
3. Smith, M. (2022, April 27). *What is Platform as a Service? PaaS examples + SaaS vs PaaS vs IaaS*. Zendesk. https://www.zendesk.nl/blog/what-is-paas/#georedirect

4. *Access Control In Cloud Security – Restrict Unauthorized Access*. (n.d.). CloudCodes. https://www.cloudcodes.com/solutions/access-control-for-cloud-security.html
5. *How to Secure Data at Rest*. (2022, March 9). https://www.teradata.com/Trends/Data-Management/Data-at-Rest
6. Gillis, A. S., & Fitzgibbons, L. (2021, November 30). *data in motion*. WhatIs.com. https://www.techtarget.com/whatis/definition/data-in-motion
7. Sobers, R. (2022, June 22). *89 Must-Know Data Breach Statistics [2022]*. https://www.varonis.com/blog/data-breach-statistics
8. Avey, C. (2022, October 17). *7 Key Cybersecurity Threats to Cloud Computing*. Cloud Academy. https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/
9. Irwin, L. (2022, July 1). *Human Error is Responsible for 82% of Data Breaches*. GRC eLearning Blog. https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches
10. S. (2019, June 12). *SOAR Platform Buyer's Guide*. Swimlane. https://swimlane.com/resources/soar-buyers-guide?utm_source=bing
11. *The Motor Carrier Safety Planner*. (n.d.). https://csa.fmcsa.dot.gov/safetyplanner/MyFiles/SubSections.aspx?ch=22&sec=65&sub=148
12. *2013 South Carolina Code of Laws :: Title 59 - Education :: CHAPTER 67 - TRANSPORTATION OF PUPILS; SCHOOL BUSES :: SECTION 59-67-270. Inspection of buses.* (n.d.). Justia Law. https://law.justia.com/codes/south-carolina/2013/title-59/chapter-67/section-59-67-270

13. Knowles, M. (2022, March 24). *Cloud Compliance Frameworks: What You Need to Know*. Hyperproof. https://hyperproof.io/resource/cloud-compliance-frameworks/

14.