Open Access Library Journal
2023, Volume 10, ****
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Cloud Computing Security, Protecting University Information

Anita C. Eluwa

Department of Computer Science, Cybersecurity St. Mary's University, San Antonio, Texas, USA
Email: eluwa.anita@yahoo.com

How to cite this paper: Author 1, Author 2 and Author 3 (2023) Paper Title. *Open Access Library Journal*, **10**: ****.
https://doi.org/10.4236/***.2023.*****

Received: **** **, ***
Accepted: **** **, ***
Published: **** **, ***

Abstract

Cybersecurity is the study of protecting information and systems. One of the most secure ways of protecting information online is through cloud services when used appropriately. In St. Mary's university, cloud computing adaption has rapidly grown and evolved over the years. However, the protection and safety of students and staff's information is still unsteady, which prompted the evaluation and survey of this research. In this paper, a risk analysis is performed on one of the university's cloud portal (canvas) to identify and mitigate potential security vulnerabilities found in the portal. Once the vulnerabilities have been identified, the university's existing controls, risks, likelihood, and impact levels are then mapped to a risk register. Suggested and reliable security controls according to NIST SP 800-53A are then implemented to mitigate these vulnerabilities. The last phase of the analysis, risk monitoring is implemented using the NIST 800-39 risk monitoring plan.

Subject Areas

Cloud Computing, Information Management, Information and Communication: Security, Privacy, and Trust, Online Social Network Computing, Technology

Keywords

Privacy, Cloud Computing, Cybersecurity, Higher Education, NIST, Risk Framework

1. Introduction

NIST (National Institute of Standards and Technology) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Protecting student, faculty, and instructional information is a requirement that is a primary responsibility of any university or institution. There are multiple ways to accomplish these security measures though restricting access to information that has potentially damaging consequences for the university. Traditionally, all the information was maintained on campus and only selected individuals within the faculty would be assigned specific responsibilities to control the organization's information. The requirements to secure the classroom, student records, and course material mainly relied on physical restrictions to mitigate risk. The costs and convenience of transitioning the university to be available online is resulting in new accessibility and continued improvements for students, though the risks associated with online education need to be regulated and minimized by the university to avoid security and privacy issues. Irrespective of the fact that cloud computing is a young concept and there are still some loops that need to be covered, its functionalities and benefits outweigh its drawbacks. One of its benefits is that it is budget friendly. Moving the IT services to the cloud will cut costs for the institution in terms of maintenance and purchasing of infrastructures. Complexity can also be reduced with cloud computing by assisting the IT administrators with challenges that involves managing both the software and hardware networks and the burden of these issues can be drastically reduced. The adoption of cloud computing permits significant savings in supportive technologies, such as the massive air conditioning that is typically installed in university in-house server rooms to maintain a required level of temperature [2].

In the course of this paper, we will look at some case studies and related works on how different higher educational institutions analyzed the different risks associated with cloud computing security in their various universities and organizations.

Related Works

There has been some surveys and analysis on the security assurances in cloud computing. This paper highlights the three different types of cloud services and their different functionalities. They also narrowed their research to the application of cloud computing in higher education as well as identifying some of the limitations the institutions face during implementation. They identified security, performance and availability, Integration with In-House IT and Customizability as some of the concerns faced during adoption. Another related concern, which pertains to an earlier point about information security, is how to apply specific law requirements for data preservation and protection, such as the HIPAA requirements for Electronic Medical Records (EMRs) data in case of a university hospital research project [2]. They however suggest that if a transition is being made, it needs to be done carefully to ensure that the NIST standards are established, and the transition is smooth. Also, the institution should consider requesting for a government funding to explore a nationwide cloud computing and proper adoption.

Ardagna *et al.* described a cloud security taxonomy that consists of three main categories and is based on the *when*, *where*, *what*, and *how* approach. They analyzed three main security categories of contributions: the vulnerabilities of the attacks, the security techniques used to protect the information and the assurances used to verify that the security techniques have been implemented appropriately. Then they addressed the use of encryption, signature, access control, authentication, trusted computing, IDP/IPS as possible techniques to increase cloud security. They however conclude that any cloud security measures provided should embrace both introspection by cloud providers and outrospection by cloud customers.

Kalaiprasath *et al.* conducted a comprehensive study to review the potential threats faced by cloud consumers and determined the compliance models and security controls that should be in place to manage the risk [3]. They identified a couple of security standards and security controls that have been implemented by various cloud providers. They then developed an ontology to capture the concepts of these security threats and compliance controls. This ontology was implemented into an application built using php, html, ajax web technology and MySQL. The application is used by cloud consumers to determine the compliance policies and cloud security. This research provided a broad overview on the vulnerabilities of security in the cloud, but the ontology however does not eradicate the issues of security in the cloud as the ontology does not match some cloud providers.

Another research paper discusses the concept of "cloud" computing, some of the issues it tries to address, related research topics, and a "cloud" implementation available today [4]. It mentions a technology called the Virtual Computing Laboratory (VCL) that is managed through a web portal or an API where students and lecturers have easy access to laboratory works in an institution. It is a virtualized technology but has some required functionalities that are missing in a cloud framework. The addition of these features is however still under construction.

We have viewed different related works in cloud computing for different organizations and for higher education institution. We have been able to compare how these different organizations propose different security analysis and solution regarding the issue with cloud computing security. The process for St. Mary's university will now be analyzed and evaluated in the next chapter.

2. University Regulatory Bodies

St. Mary's university is committed to long term strategies. These are the goals that promote a culture of excellence, foster formation of faith at St. Mary's and throughout the southwest. Also prepares students for professional lives as ethical leaders in Texas, the nation, and the world. To innovate and change, and steward wisely, allocate resources strategically, and increase financial and capital funding.

During the research process, the policies that the university uses to protect information and the bodies that ensure the adherence of these laws were identified.

The Executive council is responsible for overseeing and authorizing the annual information service policy reviews. The governance body is made up of various stakeholders and these stakeholders are designated different roles and functions as shown below.

2.1. Vice President of Information Services or Chief Information Officer (CIO)

The CIO oversees all security management of the university's assets.

2.2. Information Security Committee

The Information Security Committee ensures that the CIA triad (Confidentiality, Integration and Availability) is safeguarded and ensures that all policies are adhered to.

2.3. Information Services Advisory Committee

This committee is currently still in process and has not been set up or assigned functions yet.

2.4. Enterprise Risk Management Committee (ERM)

The ERM is chaired by the vice president and finance. The functionality of this committee is to analyze and identify potential risks impact on the university and ensures that these risks are mitigated or avoided.

There are also general governed bodies that all higher education institution uses for information security policies and procedures. Please see below.

2.5. Executive Council

This council advises the president on internal and external matters concerning the universities.

2.6. Academic Council

This Council considers and advises the provost and vice president for academic affairs on academic matters and programs.

2.7. Faculty Senate

The Senate meets regularly during the Fall and spring semesters and all appointees with full-time or pro-rata faculty status may attend.

2.8. Student Government Association (SGA)

The Student Government Association (SGA) is the recognized student governing body at St. Mary's University. Its Constitution and By Laws are found in the

Student Handbook of St. Mary's University.

The above bodies explained are the different committees that the university has created to ensure that the information and data of the university is protected. Furthermore, the computer science department is making recommendations for security measures which are then taken into consideration by the Information Security Committee.

3. Present Problems

There are several redundant policies that needs to be updated or taken out from the policy documentation if need be. When these laws are not updated regularly, potential vulnerabilities in the system will not be identified on time. With the canvas portal where zoom recordings are saved on the cloud, these videos and audios are made available to both the students and tutors for future references. However, if there is a legal issue in a class, where a student or instructor were to press charges, the zoom recordings would then become evidence to such case. The university does not have any control or policy over these recordings. As well as how it is being outsourced to zoom. This also points to the security issue of the canvas portal. Due to the easy availability of the cloud recordings and access to the portal, an unauthorized user can gain access to the cloud service and the university then faces a risk of confidential information being exposed to the public. Student records can also be easily tampered with and modified. We will however perform a risk analysis to view the potential vulnerabilities of these threats and weigh the impact level.

4. Risk Analysis on the University's Cloud Portal (Canvas)

As mentioned earlier, one of the current cloud media that is used by St. Mary's University is called Canvas. The school's mail server is also integrated into the portal. On canvas, a student or tutor is assigned a username and prompted to create a secure password with a two-factor authentication. The authentication can either be through the user's email address or the user's mobile number. This then grants access to the portal. This access is unique as it contains personal information of the user. Zoom is also implemented in canvas. Virtual lectures are taken via zoom and the cloud recordings are saved in the cloud of canvas. Student grades and course information are also saved on the portal.

4.1. Categorize Information and Information Systems

In this chapter, we have analyzed the vulnerabilities of this portal and measured the possible impacts of these potential threats to the university. The first step in achieving this is to identify the key assets and map them to various Information Types from NIST SP 800-60 to their different security categories along with their CIA triad impact level. This is achieved using the below expression.

$$\begin{aligned}&\text{Security Category Information Type}\\&=\left\{(\text{confidentiality},\text{impact}),(\text{integrity},\text{impact}),(\text{availability},\text{impact})\right\}\end{aligned}$$

Table 1 shows the key assets mapped to the appropriate information types and their various CIA triad impact levels.

4.1.1. User Login Information

The first key asset is the user login information. This asset was mapped to the information type personal identity and authentication. The confidentiality impact level is moderate because the login credentials of the user is of high importance and needs to be protected and always encrypted. Any breach of this information can have a serious impact on the user and the university. The integrity is moderate because student's records and grades are displayed on the portal and any form of unauthorized modification of data will lead to inaccurate data and distort the effective evaluation of student records. The availability is low because the unavailability of the user's information will have a less serious or severe impact on the university.

4.1.2. Backup Storage

The backup storage is mapped to the continuity of operations. The confidentiality level is moderate because if there is an unauthorized access of the records, it will have a serious effect on the university as all the student's records will be at risk. The integrity is low because modification of the stored information will have a less serious adverse effect on the university. The availability is moderate because the backup data is created to ensure that there is a copy of the user's information in case of a catastrophic event.

4.1.3. Cloud Service

This asset is mapped to the services acquisition information type. The cloud web server that the portal is hosted on must remain private with proper encryption. Failure to protect the server from being penetrated by hackers will result in a serious adverse impact on the university. Hence, confidentiality is moderate. The integrity is low because any adjustment or modification of the web server will have a less serious impact. The availability is moderate because without the cloud server, the portal cannot be hosted. So, it is expected to be always available.

Table 1. Key assets mapped to information types.

Key Assets	Information Type (NIST SP 800-60)	Confidentiality Impact level	Integrity Impact level	Availability Impact level
User login information and records	Personal Identity and Authentication	moderate	moderate	low
Backup storage	Continuity of operations	moderate	low	moderate
Cloud service	Services Acquisition	moderate	low	moderate
Internet Service provider	System and Network Monitoring	low	low	moderate
Policies and Procedures	Policy and guidance development	low	low	moderate

4.1.4. Internet Service Provider

Any service that is carried out on the cloud must be connected to the internet and frequently monitored. The confidentiality level here is low because unauthorized access to the provider will not require the university operation to shut down. The integrity level is low because the result of an unauthorized modification of the service provider will have a less serious effect on the institution. The availability is moderate because without the internet being available, virtual meetings, classes etc. will not function and this may lead to a serious effect on the university's operations.

4.1.5. Policies and Procedures

We have outlined the university's policies and bodies that governs these laws in section two (2) and these policies needs to be guided and always implemented. Hence, the availability is moderate. The confidentiality and integrity are low because any breach of such will not have a serious or severe impact on the daily operations of the institution.

4.2. Security Controls

Using the NIST SP 800-53, we analyzed the risks, likelihood and consequence level of the current existing security controls the university has attempted to in minimizing these threats or vulnerabilities. This is shown in **Table 2** below.

The risk register maps the threats and existing security controls to the likelihood, consequence and level of risks occurrence and impact level. This table gives us a better understanding on the possible threats that the university is facing with the canvas portal and provides a rough idea on the damage that these threats will cause to the school in the case of an attack.

With this, the institution can propose a plan on how to either improve the current existing controls or eradicate them completely, and implement new security controls which takes us to the next phase of this analysis.

Table 2. Risk register.

Key Assets	Threats	Existing Controls	Likelihood	Consequence	Level of Risk
User login information and records	Unauthorized access of passwords and username	Encryption of passwords	Possible	Moderate	Medium
Backup storage	Corruption, loss of information	Firewalls, Encryption	Possible	Moderate	Medium
Cloud service	Attacks affecting the system	Firewalls, Encryption	Possible	Moderate	Medium
Internet Service provider	Attacks affecting the system.	Firewalls, Encryption	Possible	Minor	Medium
Policies and Procedures	Unauthorized modification of information	Annual reviews and check ins	Rare	Insignificant	Low

4.3. Implement and Access Security Controls

In the previous phase, we have analyzed the existing security controls, identified the potential threats and the impact of these threats. In this phase, we assessed these controls and implemented them using the NIST SP 800-53A (**Table 3**).

4.4. Authorize: Preparing the Information System for Use

When the outlined security controls have been accessed and implemented, the authorizing officer now examines the output of these security controls and determines whether the risks are acceptable. As mentioned in section two (2) of this paper, there is a committee at St. Mary's university called the Enterprise Risk Management Committee (ERM). This committee is chaired by the vice president and will be responsible for the risk analysis and when this assessment is done, the Office of the president examines and approves it then the Chief of staff of the president authorizes these releases if they have been accepted.

4.5. Risk Monitoring

The last phase of this analysis is the risk monitoring. Risk monitoring refers to an organization's framework for staying aware of its current risk exposure, including the implemented risk management system and other activities that inform the organization's risk decisions. Key risk indicators (KRI) are created to identify how much risk can be tolerated in the organization. The purpose of risk monitoring is to address how risk will be monitored. This includes verifying compliance with the risk response decisions by ensuring that the organization implements the risk response measures (and any information security requirements), determines the ongoing effectiveness of risk response measures, and identifies any changes that would impact the risk posture [5].

Table 3. Security control implementation.

Key Assets	Implement Security Controls (NIST SP 800-53A)	Access Security Controls (NIST SP 800-53)
User login information and records	AC-2 Account management. PE-access control	Security Awareness
Backup storage	AC-1 Access control policy. PE-access control	Security Awareness, Access Enforcement
Cloud service	AC-8 System use notification. PE-access control	Security Awareness, Access Enforcement
Internet Service provider	AC-8 System use notification. PE-access control	Security Awareness, Access Enforcement
Policies and Procedures	AT-1 Security awareness and training policy and procedures	Security Awareness Training

Risk monitoring activities at the various levels of the university will be coordinated and communicated. This can include sharing risk analysis results that would have an organization-wide impact to risk responses being planned or implemented. The university also considers the tools and technologies that will be needed to facilitate monitoring and the frequency necessary for effectively monitoring risks, including the changes that would impact responses to risks. The goal of this phase is to continuously monitor the implemented controls for the system and its environment. Looking out for changes or signs of attack. If any vulnerability is found, the controls will be reassessed and updated controls implemented. An integrated organization wide monitoring program is implemented using the NIST 800-39 risk monitoring.

5. Recommendation

Before the risk analysis and assessment, we identified all the policies that St. Mary's university uses to protect IT services. We also identified the different bodies responsible for handling different operations. Most of these policies were found to be redundant and not in full effect. We suggest that these policies are thoroughly reviewed, and the redundant ones eradicated. After our analysis for the canvas portal, we identified potential weaknesses to the system. It is recommended that the risk evaluation results using the NIST risk management framework are mapped together with the updated policies to increase the security of the portal as well as other services of the institution.

6. Conclusion

Cloud computing is young and growing rapidly. Its scalability, flexibility, reduced cost, and service-oriented architecture are all but a few of the benefits that the cloud service offers to the higher education institution and any organization at large. In this paper, we have identified the present security problems that St. Mary's university faces and related research topics on the issues with cloud security. We also provided a risk analysis on the security vulnerabilities on one of the cloud services that the institution currently uses, canvas. We then measured the impact levels of the effects that these threats can cause and provided possible recommendations to help curb and mitigate these effects in the university.

Acknowledgements

I would like to thank my professor for giving me the opportunity to thoroughly understand and implement the NIST framework standards for risk management and for the feedback on the draft that helped with the improvement of this paper.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Mell, P. and Tim, G. (2011) The NIST Definition of Cloud Computing. Special Publication 800-145. https://doi.org/10.6028/NIST.SP.800-145

[2] Tout, S., William, S. and L.G, (2009) Cloud Computing and Its Security in Higher Education. *Proceedings of ISECON,* **26**, No. 2314.

[3] Kalaiprasath, R., Elankavi, R. and Udayakumar, R. (2017) Cloud Security and Compliance—A Semantic Approach in End-to-End Security. *International Journal on Smart Sensing & Intelligent Systems,* **10**, 482-494. https://doi.org/10.21307/ijssis-2017-265

[4] Mladen, V.A. (2008) Cloud Computing-Issues, Research and Implementations. *Journal of Computing and Information Technology,* **16**, 235-246. https://doi.org/10.2498/cit.1001391

[5] Metheny, M. (2017) Chapter 7—Comparison of Federal and International Security Certification Standards. In: *Federal Cloud Computing* (*Second Edition*), The Definitive Guide for Cloud Service Providers, 211-237. https://doi.org/10.1016/B978-0-12-809710-6.00007-X