Cloud, IoT and Enterprise Security Assignment

Case Study Report

M.Tech. Software Systems

WILP

BITS, Pilani

Team Members:

Name	Mail ID
Vatsal Jain	2021MT12071@wilp.bits-pilani.ac.in
Vanshul Bajaj	2021MT12073@wilp.bits-pilani.ac.in
S Suhas	2021MT12353@wilp.bits-pilani.ac.in
Debanjona Nath	2021MT12389@wilp.bits-pilani.ac.in

Index

Context

BITS WILP (Work Integrated Learning Program) Division is aimed to provide opportunity to strive in highly technical career along with the ongoing professional career. BITS provides facility to attend classes and assessments online without having any need to visit the campus. Following are the key elements and provisions of BITS WILP Program:

- Learning material
- Facilities for practical work
- Enabling questions and discussions
- Assessments
- Student Support service

A blend of Lectures, simulations, Remote Labs and case studies are delivered by BITS faculties online. While this creates is a win-win scenario for industry professionals, it does require efforts to deal with several security issues which includes and are not limited to:

- Legal and Regulatory Compliance
- Internal and External Attacks
- Protection of confidentiality and privacy
- Any accidental damage to assets and system

WILP has in total 11 locations (1 Head Office, 3 Regional Offices, 7 Regional Campuses)

Head Office

Head office controls Central administration of Staff, students and central office systems

Regional Offices

3 regional offices hold student records, regional office system and payroll

Regional Campuses

7 regional campuses have IT Teaching laboratories, staff workstations and local office systems (file servers, printers)

Why is security important in this setup?

With the increase in data collection, the need of having to secure the same is on the rise as well. In the past years, there's been a surge in distance learning programs for working professionals to enable them to step up their intellect. BITS, being one of the most prestigious institutes in India as well as globally, offers WILP to encourage a continuous learning process which can be accessed remotely. However, the pandemic (COVID-19) has now transformed the whole learning experience by making the whole process online to be readily accessible from any device. With these changes being enforced, one can rightly assume that the cybersecurity landscape too has changed drastically. Students, faculty and staff alike, have the freedom to login via their personal devices and networks. Even though the this might be the new normal, the cyber threat landscape remains the same as to what we faced while being in our workplace if not more.

While one might think that the most crucial data to be secured are the lectures and modes of evaluating the students, one must keep in mind that confidential data such as employment details, official enterprise ids, mentor employment details, etc. are also to be secured from any cyber-attacks. Remote working has played a significant role in the rise of recent cyber-attacks and data leaks.

It is estimated that universities and colleges are still affected by incidents like Ransomware, where perpetrators block access to the data by encryption or other means and demand a ransom to be paid before they unlock the data. At times threats to leak the stolen data publicly over the dark web is made in order to gain more ransom.

Another vulnerability is the poor management of data and not maintaining proper data hygiene. While distant learning courses make use of 3rd party tools to enable collaboration between the students and faculty, one risk remains – poor data hygiene. The only way to prevent data breaches and leaks is by proper data management and the biggest threat is imposed when students send unencrypted emails and files containing confidential data back and forth via unencrypted emails or communication platforms.

While one cannot fortify an infrastructure to be 100% secure, one can try their level best to prevent from major damage by securing the systems and ensure proper methods are used while accessing and using the data.

Use Cases

BITS supplies the necessary materials (e.g. Course notes, videos etc.) and services (e.g. Lectures) to remote students using eLearn Portal (Taxila) and Impartus over the Public Multimedia Network as part of their WILP Program. Students can interact and submit work through same channel. Security considerations are determined by the sensitivity and nature of following identified information in the communication:

- Student Records
- Students Assignment and Examination Grades
- Payroll Information

This requires at least 3 levels of confidentiality:

1. Publicly available information (like brochure)
2. Information restricted to enrolled students only (like notes)
3. Information restricted to faculties or specific students (like grades, pay)

Along with confidentiality, it is necessary that one considers the availability as well as the integrity of data.

1. Course material, lectures, text material, virtual labs, online library server should be accessible to the staff, faculty and students whenever and wherever needed. (availability)
2. Educational data and metrics should remain and be maintained un-tampered and in its original condition (integrity)

Internal teams (IT Team, Network Team etc.), Faculties, Assistants and Students interact with WILP's system for their different requirements and through different channel. These are categorized into 3 major use cases to discuss the associated risk and security concerns, based on sensitivity of data, actions performed by the users, Security offered by communication channel and the trust on user.

Internal Users (IT Team, Network Team..)	Faculty, Staff and Teaching Assistants	Students, Assistants
•Access to Critical Systems and resources •Access through LAN	•Access to sensitive information •Access through VPN	•Access to limited required information •Access through Internet

1. IT Team, Network Team and other Internal Department Users are taken in the first use case.

   These users possess the highest trust and assess the most critical resources of the system. The trust gained by these users are induced from the where they come into the system and how to access the resource. In a brief,

   These include the internal users that have been hired by BITS management and have gone through the complete interview and background check process. These are categorized as Internal User' and security policies with respect to internal users apply to them.

   These users are authorized to access the critical infrastructure and data present in BITS system. Though the sensitivity of data at this level in highest but these users access the system from internal systems and components only. There are given access inside the office post physical authentication techniques.

   These users then access the systems through their unique credential which takes care of the Role Based Access Control and Least required privileges.

   The systems that are being used by the users are connected to the critical resources and data through LAN that offers the most security assurance and eliminates the major threat unlike the Public Media Channel.

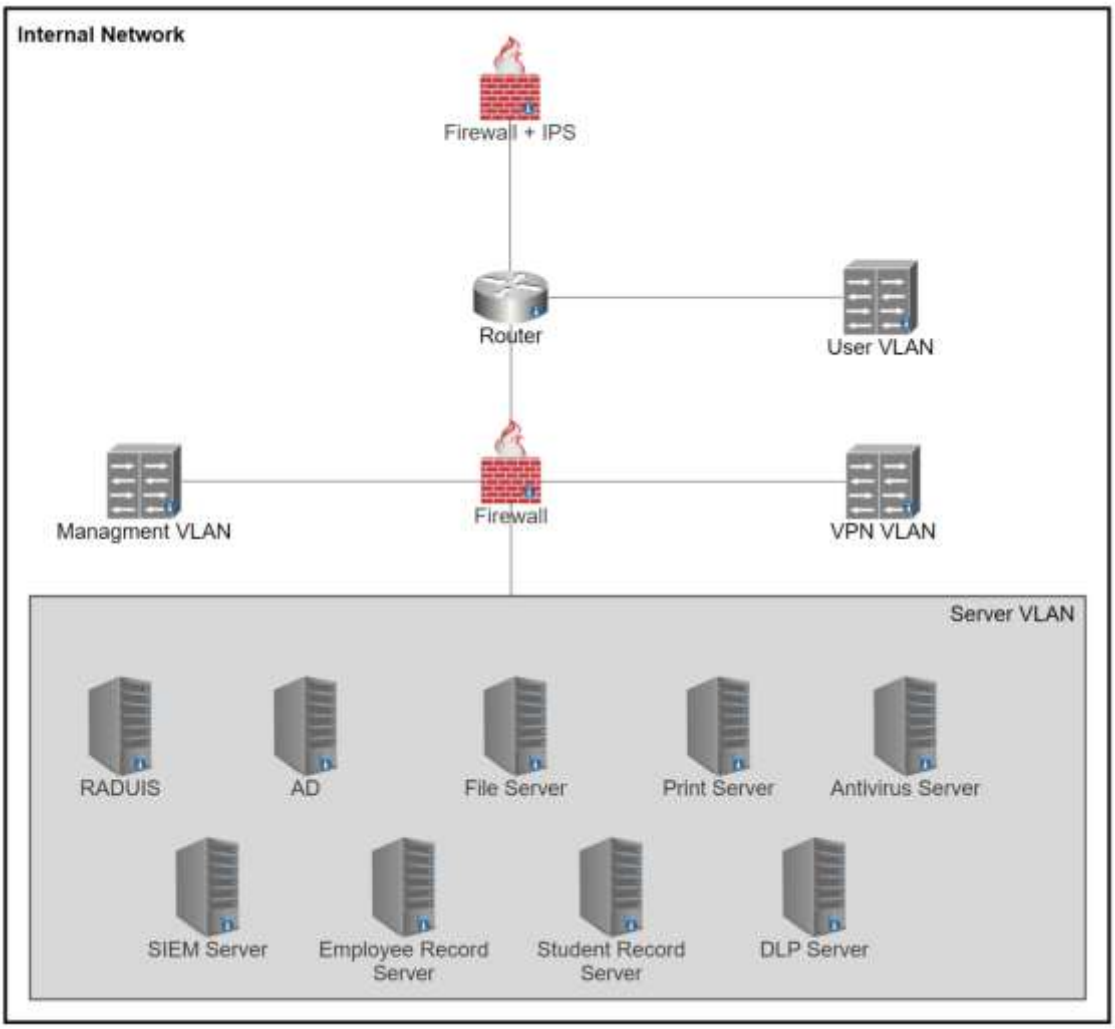

Fig 1.1: Internal User Network

Data Loss Prevention System is in place to prevent any leak of data to the outside world.

The physical and logical access of these users are terminated upon there termination and are stated well in associated policies and processes.

2. Faculties, Staff and assistant are considered in this second use case where the users are allowed to access the critical system, services and resources remotely. The resources access by these users are critical as they have access to the student's personal data and assessment records.

   These users access the system only through the domain systems provided by the University or through the Remote Desktop and Virtual Private Network.

Through the VPN, a secure tunnel is created between the user's system and the universities resources. The sensitivity level of data/resources and their integrity level requirement is high. But all interaction to data is logged and the users is responsible and accountable for any reads, updates and publish of data.

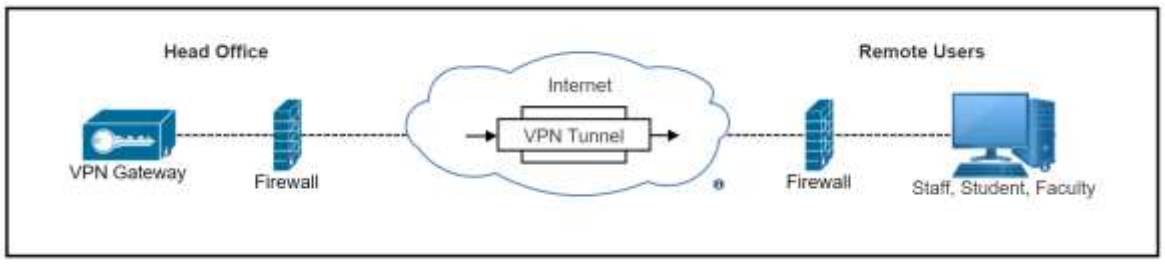

Fig 1.2: Communication between Head Office & Remote Users

The users access the system through their unique identification and after authentication only. Role based access control and authorization in maintained for authenticated users.

The users are required to follow best practices and recommendations for use through remote systems.

3. Students and some assistants are considered in the third use case, where users access the system through public channel which brings in most security concerns. The information accessed by the student is limited as required by their role and not business sensitive. Use cases relevant to Students are being assessed in detail to identify the associated risk and security issues.

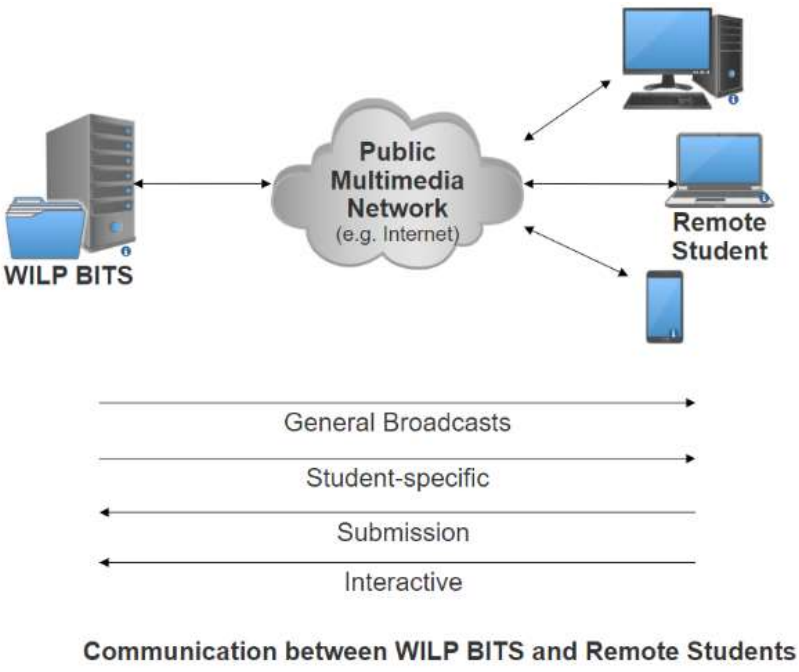

Fig 1.3: Communication between WILP & Remote Users

Student interaction lifecycle with WILP systems is in following stages:

Use cases with respect to each stage involves different security concerns which are stated below.

Enrolment

Remote students are identified is this stage who are then enrolled and access to allocated resources in enabled. Following are the consideration from security point of view.

Student is requested to furnish previous qualifications and other required document to enrol for WILP program. All the data with could personal information is kept safely in Student Records. Regulation and compliance related to privacy legislation is required.

Payments from the students are directed to payment gateways or other setups that supports for EMI. Card details are not stored by WILP division and Payment interaction page is made PCI/DSS compliant.

Authentication scheme for further communication and access is established here. Authentication, Authorization, Confidentiality and Non-repudiation is taken care of. User credentials are generated, shared and are required every time before accessing the system.

Study

Students and faculties both access the system in this stage and are considered as End Users for Study stage. End Users are actively engaged in this stage and interacts with the system frequently for consumption of course material, assignment s, quizzes, examinations, grading etc. Following are the identified consideration in this stage:

End-users should only be able to view and retrieve the information that is relevant to them. Access to unauthorized information shall be prevented. Role based access control in introduced into the security framework to tackle with security concerns.

Systems shall be available to end users as and when required. Non-Repudiation and Integrity of any submissions done by the end user shall be maintained

Secure communication channel shall be maintained for lecture/tutorial sessions. Any unauthorized users shall not be able to communicate/access the resources.

Dissemination of grades shall be confidential to individual students and concerned parties.

End Users interaction and global statistics to be monitored, captured and maintained in the system. Information to be kept confidential and published selectively.

Submitted original work shall be verifiable and kept confidential. (eg. Research work)

Completion

With regards to completion of module following security scenarios shall be considered.

Access to future information shall be restricted, and requires the completion of current stage to move forward.

Proof of submission shall be provided and access to modify shall be restricted.

Access to previously held modules shall be allowed to restrict if required.

What kind of attacks are anticipated?

Cyber Attacks in the education sector seem to be gaining year-on year as one can note that the instances of breaches in universities and schools have been widely reported lately. This can result in immense damage in the form of financial loss or even worse, student safety/data being compromised. It is very important for a university such as BITS, Pilani to evaluate the risk and understand what data is vulnerable to unauthorized access. Let us look at some of the most prominent cyber-attacks and how BITS security architecture and its controls are in place to prevent them. Following are the risk scenarios at a high level which the organization is expected to face during the course of operations and should be taken care of with utmost urgency.

- **DDoS Attacks**- Distributed Denial of Service are a very common type of attack which the cyber criminals tend to make use of. The main motive of the attacker is to disrupt the institute's network and thereby, having a negative effect on productivity. In DdoS attack, the attacker overwhelms the target or its infrastructure with a flood of Internet traffic. Hence, regular traffic is prevented from arriving at its destination.
    - BITS has deployed Akamai's WAF solution which comes with a 'Bot Manager Premier' which analyses traffic and has advanced bot detection techniques using AI models for user behavior analysis, browser fingerprinting.
- **Injection Attacks**- these kinds of attacks occur when the attacker inserts malicious payloads/code into the server using SQL, commands forcing the server to deliver protected information.
    - BITS uses Kona Site Defender (Akamai WAF) which has a set of predefined WAF Rules to prevent SQL Injection, Command Injections and all the other injections. Additionally, it has enhancements where admin can add Custom Rules to prevent any advanced injection attacks. The application also undergoes penetration testing both internally and from external vendors bi-annually.
- **Phishing**- one of the most common types of attack. It relies solely on the victim's own vulnerabilities, mostly the emotions and ignorance. It is the practice of sending fraudulent communication that appears to come from a reputable source. Most of the phishing attempts occur via email.
    - Currently, BITS uses Fortinet's antivirus solution which included phishing prevention solutions which included powerful antispam techniques and impersonation detection. Additionally, educating the students and employees receive annual training regarding identification of phishing mails.
- **Privilege escalation**- this happens when a malicious user exploits a bug or design flaw to gain elevated access to resources that should ideally be unavailable to them. There are two types of escalations possible – horizontal and vertical. It is very hard to detect privilege escalation attacks especially if a rogue user who might have access to legitimate system compromises the security.

    - BITS ensures that all data that is sent from server to client is tamper proof using a digital certificate. Additionally, all critical data is kept on the server side and data sent to client is always encrypted.
- **Password Attacks**: It is one of the most common type personal data breaches. It is when a hacker tries to steal the user's password. There are multiple ways to implement a password attack based on the design of the system. Some of the most common methods include brute force attacks, spear phishing, dictionary attacks and credential stuffing.
    - Lately, BITS has implemented Open Athens SSO authentication which reduces the attack surface of an attack largely. This ensures that the user needs to login once each day and use only one set of credentials. It uniquely identifies the user and ensures compliance and the information provided by SSO is encrypted and transmitted across the network.

Security Architecture

Security Architecture has been prepared for each of the office with following considerations:

- Responsibilities of office
- Services provided by office
- Data held at each office

The identified security issues are being addressed by the designed security framework and following architecture. The architecture has been designed with a combination of established and enhanced security technologies.

Head Office

Head Office contains most of the critical infrastructure including RADIUS server, Active Directory, DLP Server, SIEM correlation server, personnel records amongst others. Since the crown jewels are within the Head Office network, they need to be protected sufficiently. For that reason, there are a total of 3 Next Generation Firewalls and VLAN (Virtual Local Area Network) segregation to ensure that access to the server VLAN (crown jewels) is restricted and only role based.

Further, there is a external Demilitarized Zone (eDMZ) which hosts the web server and ensures that the BITS website is accessible to users from the internet. The web server resides behind a load balancer to ensure that latency issues are taken care of. Internal Demilitarized Zone (iDMZ) resides on the other interface of the perimeter firewall, and hosts servers supporting the web server (DB server, Application server, Mail server and FTP server).

Head Office is connected to regional office and regional campus using a dedicated and secure MPLS link.

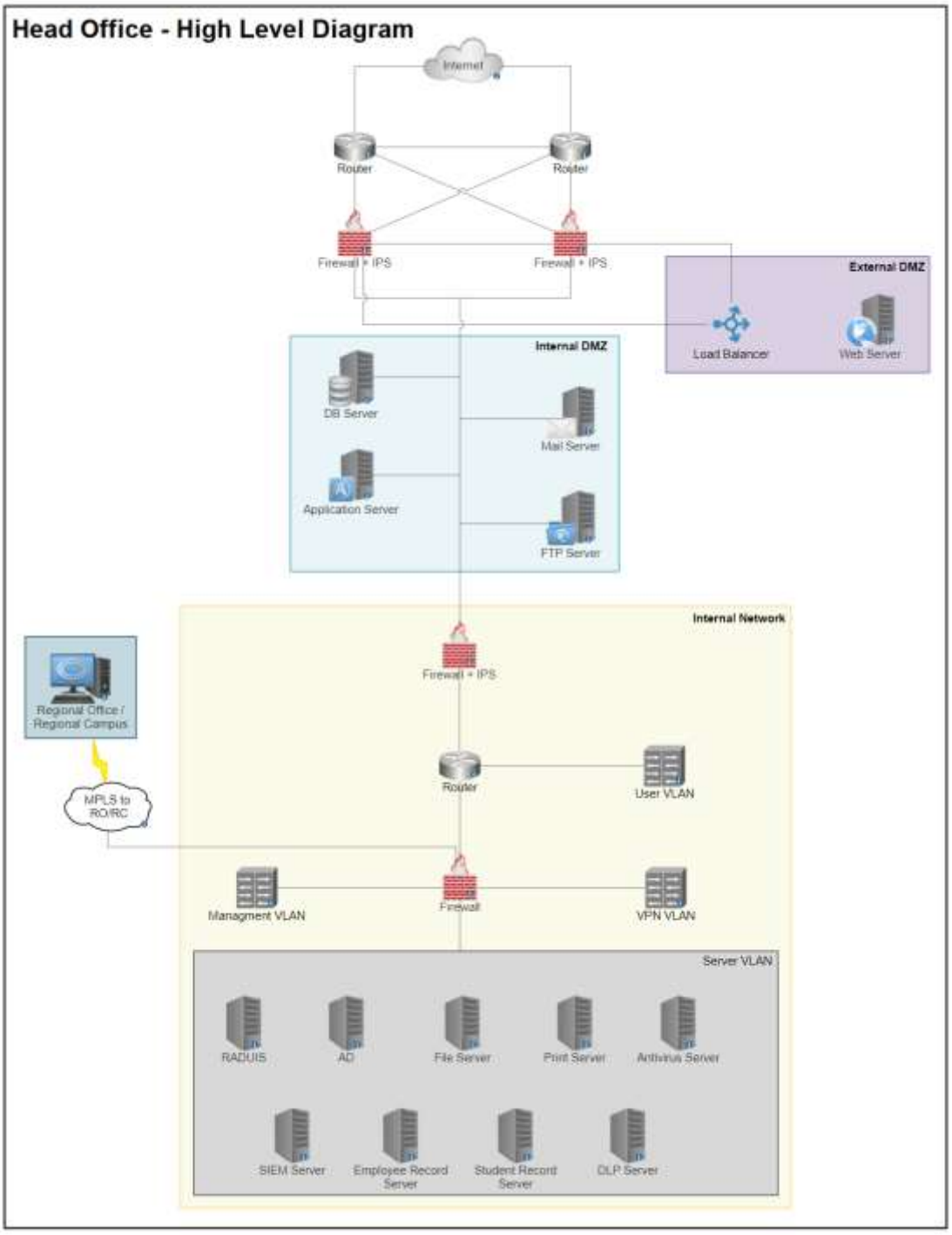

Fig 2.1: High level diagram of Head Office

Head Office is one of the most critical infrastructures to the BITs system. One must give equal importance to security and redundancy at the same time to ensure the infrastructure is always secure and up and running. The system is supported by two ISP providers (Jio and ACT) which work with 5Ghz and 2.4 GHz bandwidth of internet. This ensures that there is connectivity throughout. Cisco Router is used to route traffic from ISP which is then

monitored and filtered by the next gen firewall by Fortinet. Mesh topology is followed at this phase where the routers and the firewall are connected with each other.

Our infrastructure has an internal and external DMZ. The external DMZ ensures that all traffic that is going to the end user via the web server is monitored via WAF. We have also implemented a Akamai Application Load Balancer Cloudlet which is a multi-layered global server load balancer purpose-built to solve hybrid/multi-cloud application delivery and traffic management challenges. Akamai's Kona Site Defender is the WAF solution that has been placed in front of the Web Server. Kona Site Defender, is one in a suite of security products that also includes DDoS protection, bot management, and an API gateway. Kona Web Application Firewall provides always-on and highly scalable protection against web application attacks including SQL injections, cross-site scripting and remote file inclusion – while keeping application performance high. The Load balancer and WAF in turn leverages the advantages of the globally distributed Akamai Intelligent platform (Akamai CDN) and delivers end users the authorized data without any hassle. The internal DMZ consists of business-critical servers including Mail Server (Google), FTP server, DB server (My SQL) and the application server.

The internal network is supported by a Dell DMZ switch which is connected to a Fortinet IPS/Firewall which then routes traffic to different VLANs. For the user VLAN, the Akamai WAF is again in position to prevent various attacks. Fortinet firewall is in place for Management VLAN.

Since data stored in BITs is very critical and there needs to a disaster recovery plan, there is a Disaster Protection or a primary site that is in place behind the management VLAN. It also ensures that static data is presented to the end user in case the server is down instead of displaying any server errors.

The server VLAN is managed by DELL EMC VxRail which integrates everything in a hybrid fashion. The Server VLAN consists of all the critical server which includes File Sever, SIEM server, DLP Server, Replication server, Antivirus server, Print server, RADIUS, ERP Server, Employee Record server and finally, the student record server.

Lastly, a secure MPLS link is connected from the head office to the regional office regional campus.

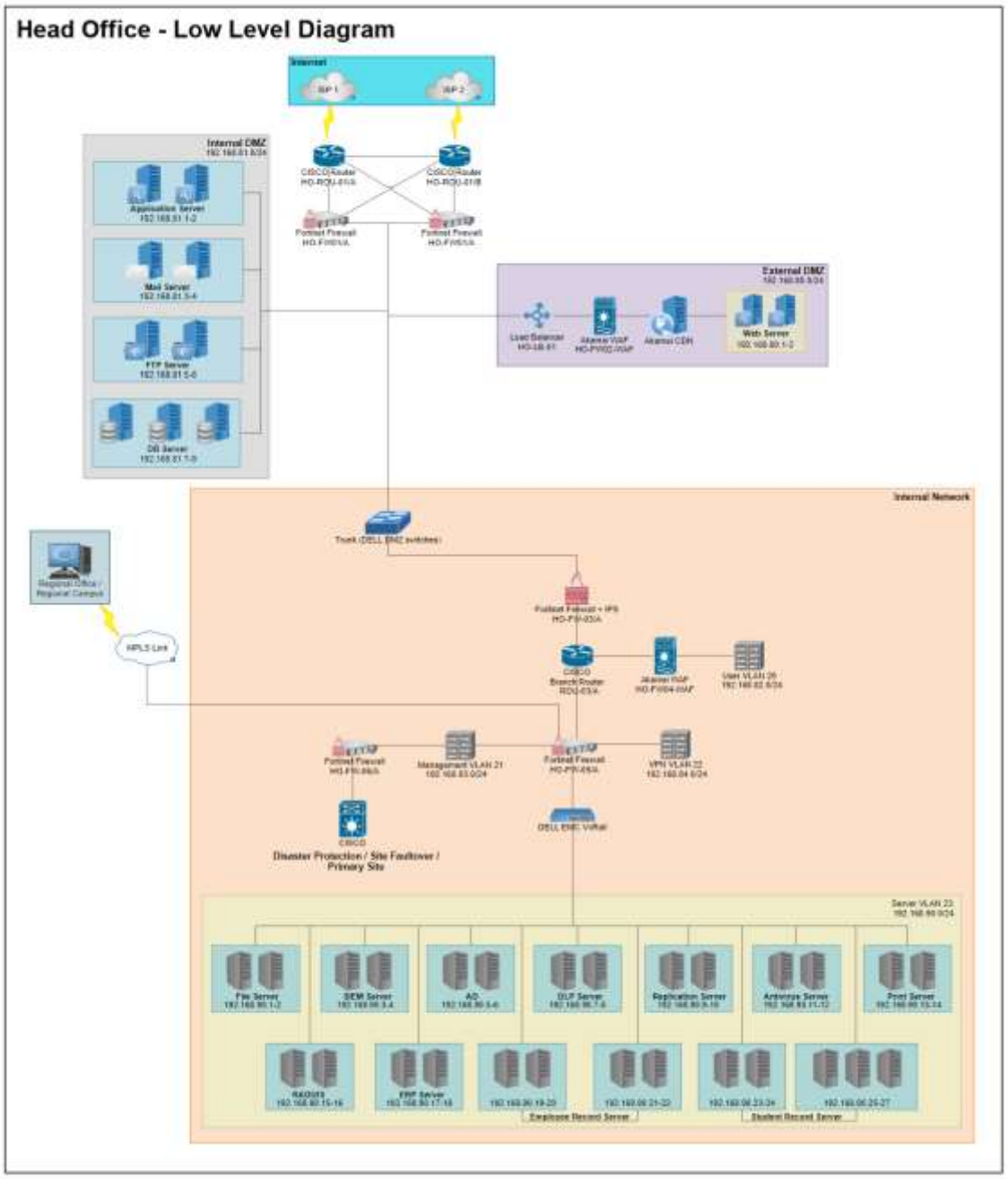

Fig 2.2: Low level diagram of Head Office

Regional Office

Regional Office is spread across locations and provides access to employees across offices to access student records and process applications and other student related information. The network has a perimeter firewall and a router which segregates server VLAN, user VLAN and payroll VLAN.

Payroll, user and server VLAN are segregated to ensure no unauthorized access takes place on the payroll data or student records. Routers use ACL to create the logical segregation.

There is an MPLS link to ensure dedicated and secure connectivity to head office and regional campus.

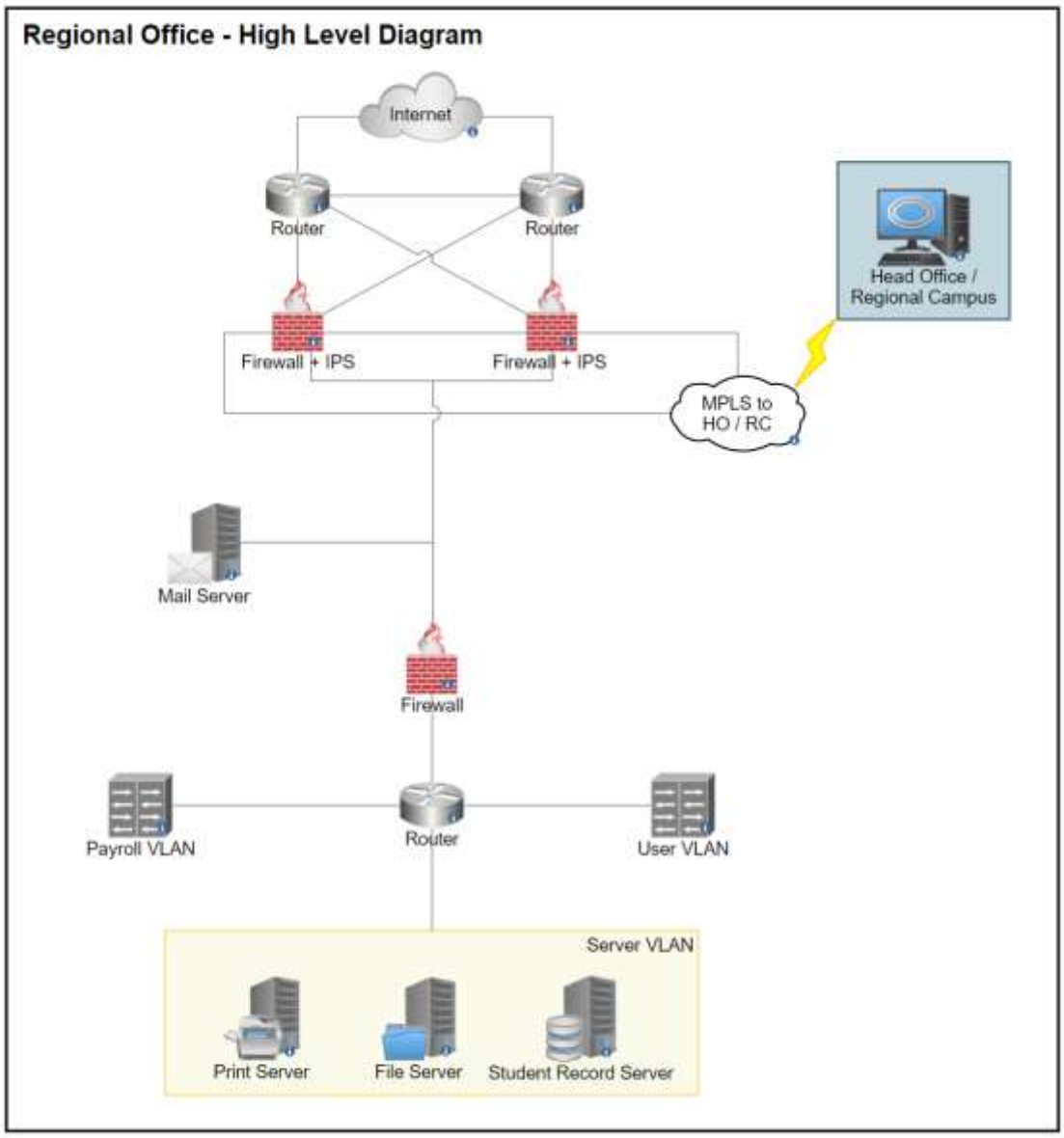

Fig 3.1: High level diagram of Regional Office

Regional Office LLD- Multiple regional offices are present across various locations. Major use case of the regional office is to access the student records and process applications. The system is supported by two ISP providers (Jio and ACT) which work with 5GHz and 2.4 GHz bandwidth of internet. This ensures that there is connectivity throughout. Cisco Router is used to route traffic from ISP which is then monitored and filtered by the next gen firewall by Fortinet. Mesh topology is followed at this phase where the routers and the firewall are connected with each other.

A secure MPLS link connects the regional office with the head office. Additionally, a mail server(Google) is in place ensure proper usage of the mail services. The Cisco branch router links the traffic to the various VLANs. One such VLAN is the User VLAN which is secured by the Akamai WAF(Kona Site Defender). The other VLAN connected to the router is the Payroll VLAN which consists of all the financial data. The Server VLAN is the most critical VLAN which is integrated with the Dell EMC VxRail which consists of the File Server, Student Record Server, Replication Server for back-ups and lastly, Print Server.

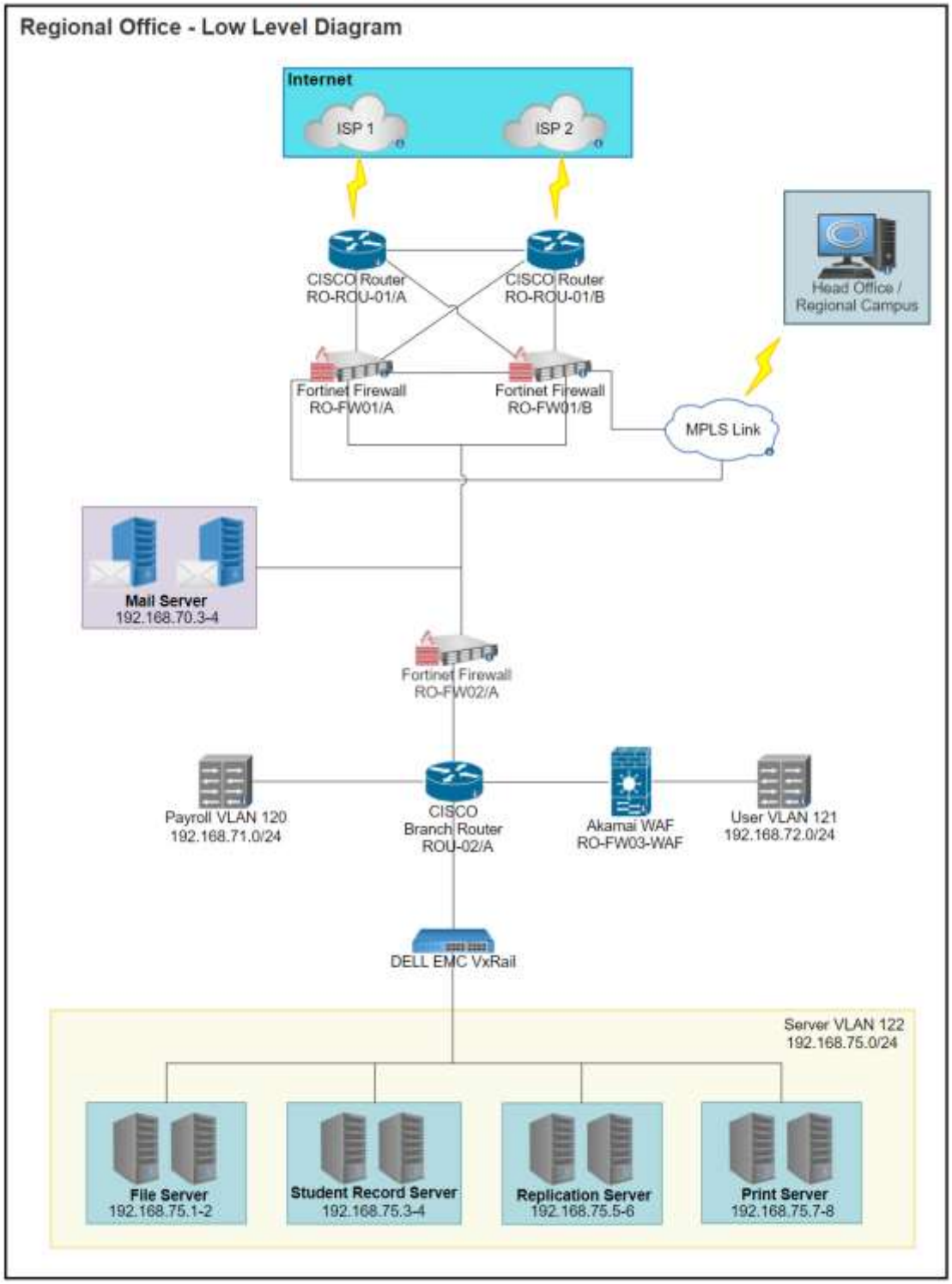

Fig 3.2: Low level diagram of Regional Office

Regional Campus

Regional campus is that part of the network where we see heavy traffic from most of the internal users. This is the region where faculties access network to take classes and students refer to books and periodicals stored on file servers. Labs are hosted on a separate VLAN which cater to a variety of hands-on practice opportunities to the students. Servers have been placed in a separate VLAN to ensure segregation and reduce chances of unauthorized access.

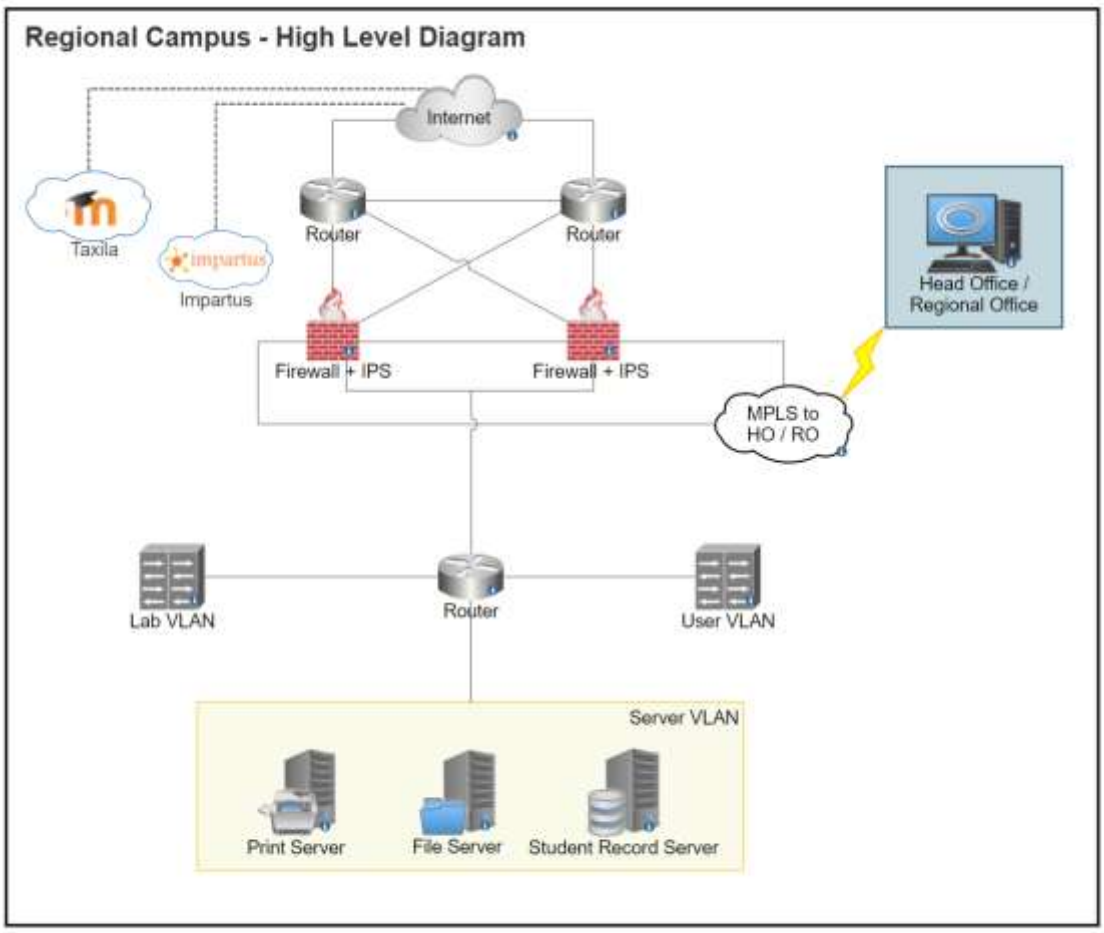

Fig 4.1: High level diagram of Regional Campus

Low Level Diagram for Regional Campus is more or less same as that of the Regional Office.

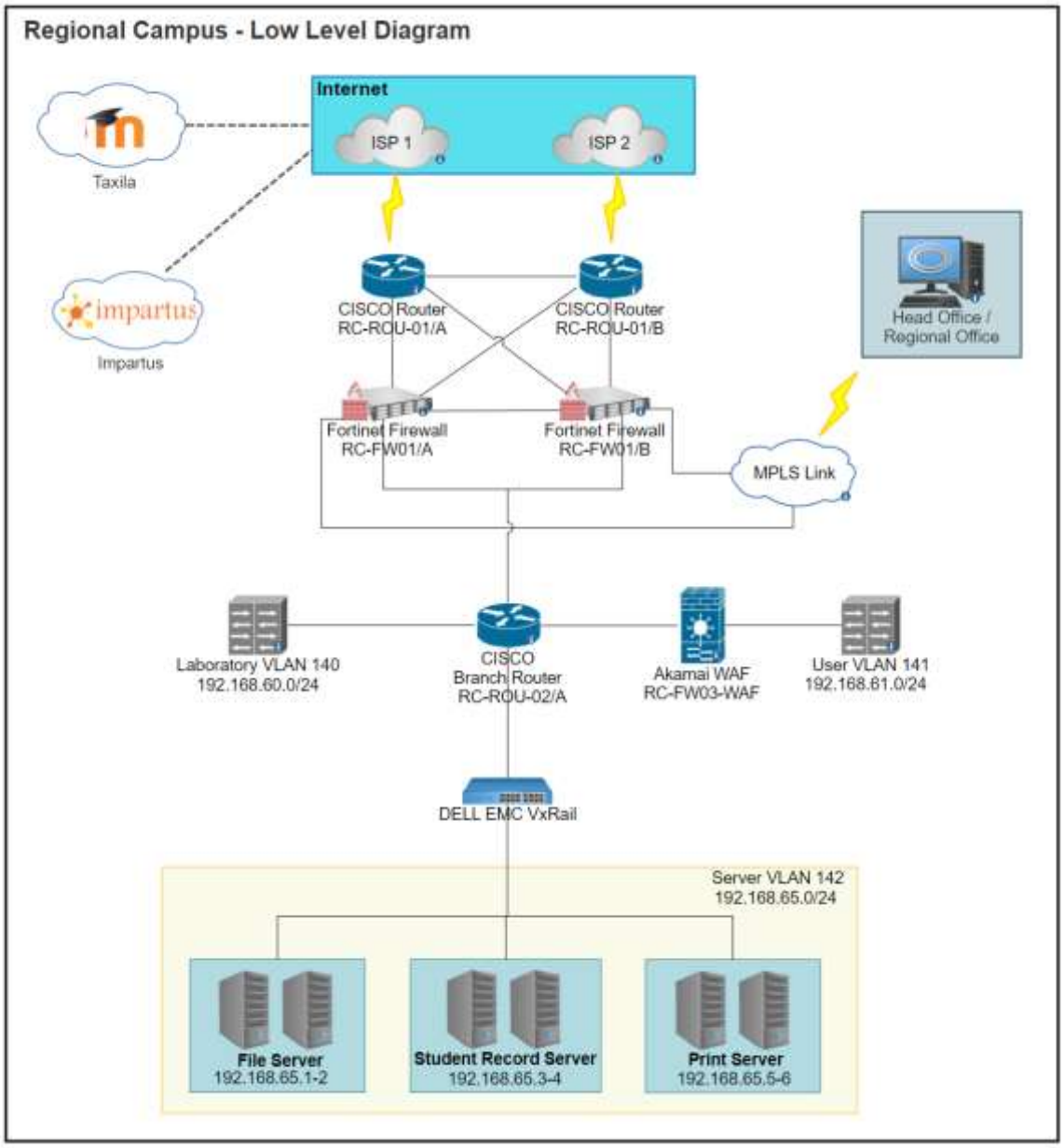

Fig 4.2: Low level diagram of Regional Campus

Applicable Laws and Regulation

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) aims at giving, users residing in California, more control over how businesses collect and use their personal information. This is intended to enhance the user's privacy rights which includes –

- The right to know about the personal information a business collects about them and how it is used and shared.
- The right to delete personal information collected from them (with few exceptions)
- The right to opt-out of the sale of their personal information
- The right to non-discrimination for exercising their CCPA rights

Personal information as defined by CCPA is, information that can (directly or indirectly) identify, relate, describe, reasonably associate, or reasonably link to a particular consumer or household, such as personal IDs, online IDs, Internet Protocol addresses, email address, account name, social security number, driver's license number, license number, passport number geo-location fata, biometrics, purchase history, or another similar identifier.

Information which are publicly available from federal, state, or local government records, such as professional licenses and public real estate/property records are not considered as personal information which in turn is not covered under CCPA.

The CCPA requires business privacy policies to include information on consumer's privacy rights and how to exercise them (the right to know, the right to delete, the right to opt-out & the right to non-discrimination)

As the Work-Integrated Learning Programme (WILP) by BITS Pilani offers its courses to all students without any location barrier, the CCPA will be applied for students and staff who are residing in California.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) primarily aims to enhance an individual's control and rights over their personal data and simplify the regulatory environment for international business. The GDPR is a regulation in the European Union (EU) Law on data protection and privacy in the EU and the European Economic Area (EEA) which also addresses the transfer of personal data outside the EU and EEA. As the GDPR is a regulation, not a directive, it is directly binding and applicable, and provides flexibility for certain aspects of the regulation to be adjusted by individual member states.

The GDPR provides various rights to the data subject, such as – transparency, right of access, right to be forgotten for rectification and erasure of data, right to object and automate decisions.

Key differences between CCPA and GDPR include the scope and territorial reach of each, definitions related to protected information, levels of specificity, and an opt-out right for sales of personal information. CCPA differs in definition of personal information from GDPR as in

some cases the CCPA only considers data that was provided by a consumer. The GDPR does not make that distinction and covers all personal data regardless of source. In the event of sensitive personal information, this does not apply if the information was manifestly made public by the data subject themselves, following the exception under Art.9(2, e). As such, the definition in GDPR is much broader than defined in the CCPA.
GDPR will be applied to any student or faculty residing in any country which is under the EU. An organization's physical location doesn't exempt it from GDPR applicability.

International standard for information security (ISO/IEC 27001)
ISO/IEC 27001 is an international standard which defines how information security can be managed which was originally published jointly by the International Organization of Standardization (ISO) & International Electrotechnical Commission (IEC). It mostly focuses on requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – aiming to help organizations make the information assets they hold more secure.
ISO/IEC 27001 requires that management:

- Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities, and their impacts
- Designs and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
- Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

Payment Card Industry Data Security Standard (PCI DSS)
The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle payment cards from the major card schemes. PCI compliance is mandated by most credit card companies to help ensure the security of the transactions in the payment industry. This mainly focuses on increasing the controls around the cardholder data to reduce credit card fraud by creating an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process, and transmit cardholder data.
As students enrolling in WILP are given the opportunity to pay their fees via credit card, it is mandatory for BITS to be PCI DSS compliant, even if it is not handling the collection, processing, and storage of the protected cardholder data directly.

Cost Benefit Analysis

Cost Benefit Analysis is a systematic process to calculate and compare benefits and costs of a system, project or a policy and figure out if the investment is a worthy one or not. Cyber Crime is one of the most dominant ways of crime which is currently evolving rapidly as the Internet expands as its associated risks are increasingly becoming global. To stay protected against these threats requires all the users to be aware of the threats and improve their security best practices.

Cyber-security has associated costs and threats such as Hacking, Cracking, Cyber-Terrorism, Cyber -Grooming, Cyber-Pornography, Cyber-Stalking, Phishing, Piracy, Malware attack, and so on. The constantly evolving nature of threats and vulnerabilities not only affects individual firms and their customers, but collectively the threats pose a persistent economic and national security challenge. Sharing responsibility to protect cyber security across all relevant sectors is becoming ever more important. Computing devices are highly and increasingly interconnected, which means security deficiencies in a limited number of systems can be exploited to launch cyber intrusions or attacks on other systems.

Tangible costs or direct costs are costs such as involve financial losses and loss of assets. This represents the monetary value of all services, hardware, software and other resources expended in providing cyber security systems. In this work, the types of tangible cost evaluated are outlined as follows.

i. Average purchase cost of hardware device before cyber-attack.

ii. Average repair cost of hardware damage after cyber-attack.

iii. Average cost of software damage after cyberattacks.

iv. Average cost of software solutions before attack.

v. Average cost of software update after cyber-attack.

vi. Average cost of hardware maintenance.

vii. Average cost of software maintenance.

viii. Average cost of labor (local technical expert or expatriate).

ix. Average cost of Research & information gathering.

Intangible/ Indirect Cost of Cyber Security Additional labor (wasted labor), downtime and business interruptions can be described as intangible cost incurred especially when there are cyber security breaches. Intangible costs should factor into investment decisions. he types of intangible cost evaluated are outlined as follows.

i. The effort or need for reactive labor after being proactive.

ii. Number of resources (labor) required to respond quickly after a cyber-attack.

iii. Rate of data loss after cyber-attack.

iv. Average user/ customer convenience for respective choice of strategy used against cyber-attack.

v. Potential damage through cyber-attack to reputation.

vi. Rate of business interruption during a cyber-attack.

When coming to BITS Pilani's security architecture analysis, one can notice that there are multiple firewalls, WAFs, antivirus and other servers in place. The value of the data is huge. It is not only about the loss of the data but also about the opportunity or business lost in case the information systems are not accessible by legitimate users or down for processing.

Let's discuss the single loss expectancy (SLE). It contains information about the potential loss when a threat occurs (expressed in monetary values). It is calculated as follows: SLE = AV x EF, where EF is exposure factor. Exposure factor describes the loss that will happen to the asset as a result of the threat (expressed as percentage value).

Assuming,

- Public facing website which attracts business (new students) is down for 5 days in a year, apart from scheduled maintenance (ARO = 5).
- Single Loss Expectancy or the loss expected with one unscheduled downtime is $ 0.5 Million
- Annual Loss Expectancy is ARO multiplied by SLE, which in this case is $ 2.5 Million (5 x $ 0.5 Million)

Now to have a redundant server (web server) and to ensure high availability, the expense for having an on-premise server up and running costs $ 0.1 Million (including cost of maintenance, administration and electricity).

Which means by spending $ 0.1 Million, we are saving $ 2.4 Million (Expected Loss – Cost of safeguard)

Similarly, let us assume,

- Ransomware attack occurs once in 5 years and cripples AD and Domain Controller, making the services in accessible (ARO = 0.2)
- Single Loss Expectancy or the loss expected with one Ransomware attack is $ 1 Million
- Annual Loss Expectancy is ARO multiplied by SLE, which in this case is $ 0.2 Million (0.2 x $ 1 Million)

Now to have EDR (Endpoint Detection and Response) capability to protect against ransomware, annual expenditure would be approximately $ 0.6 Million (3000 managed devices including Labs, all BITS owned machines @ $ 150 per endpoint annually plus the administration cost).

This means, if the organization decides to go ahead with this solution, they would be spending $ 0.6 Million to save an asset/risk of $ 0.2 Million. Simply put, you would not want to buy a safe worth $ 200 to save a $ 20 bill!

Overall, the cost of security over time precedes the overall system failure estimated cost over a period of time as mentioned in the below:

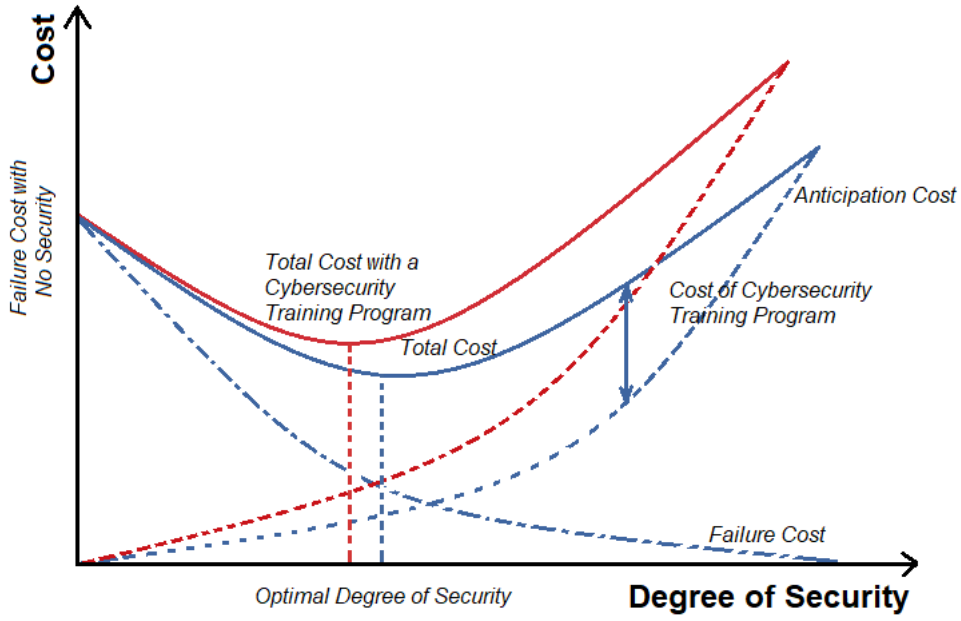

Fig 5: Cost vs. Degree of Security (Source: Emerald Insight)