LEGION

BROADBAND TELECOMMUNICATIONS NETWORK (PRIVATE) LIMITED

ANNUAL RISK ASSESSMENT REPORT 2022

IT19976686 - Jayasinghe D. A.
IT19974606 - Mahappukorala K. S.
IT19126166 - Kaluwewe K.M.G.V.O.
IT19969688 - Silva K.R.G.T.

Table of Contents

1.Executive Summary

A hybrid approach was used to conduct this risk assessment. The OCTAVE Allegro framework is a methodology for streamlining and optimizing the process of analyzing information security risks so that a company can get adequate results with a modest investment of time, personnel, and other restricted resources. This report includes a few corporate members, as well as the company's overall structure and assets, each of which has reserves within the corporation that must be protected (Table:01). Threat analysis (Threat Profile) includes critical assets and descriptions of each important asset, as well as security requirements (Table:02). A graph was given to assist the company in understanding the seriousness of the risks highlighted previously. Finally, an overview of the steps that must be taken to reduce threats to critical assets is provided.

This risk assessment identifies the following main issues and mitigation strategies.

Identified some key issues and recommendations.

I. Outdated Software
It has been discovered that certain software is out of date. Splunk 7.0.1 is an out-of-date piece of software that is prone to data leakage (CVE-2018-11409). It is strongly advised that you update your program to the most recent version.

II. Backup and Backup Storage
Club Loyalty member registration information and New User registration information are regularly saved to local storage servers. This makes it vulnerable to both unintended data loss and malicious attacks. As a result, it is advised that you use cloud storage for your backups.

III. Implementing new security features to IOS and Android “Club Loyalty” App
Security features used in “Club Loyalty” in both platforms are outdated and vulnerable to Cross Site Scripting (XSS) and weak authentication and authorization mechanisms can be detected. Therefore, it is good to inform the application development team about this issue.

IV. Implementing new Bring-Your-Own-Device (BYOD) policies
With the rapid addition of new employees and devices to the company network, as well as allowing employees to work from home, it is highly suggested that new BYOD policies be implemented, as well as new employee awareness programs concerning company data security regulations.

2.Introduction

LEGION is Sri Lanka's most popular and subscribed Quad-Play connection service. On the Colombo Stock Exchange, the corporation is one of the largest listed enterprises. LEGION has expanded its range beyond telecommunications to include a wide range of services and solutions that cater to a digital lifestyle. LEGION is an ISO 9001-certified firm that has been named Telecommunications and Internet Service Provider of the Year by Sri Lankan customers. High-speed fiber optic network, IPTV network throughout the island, training facilities, and a next-generation communications experience arcade are all part of the LEGION corporation. The headquarters of LEGION Broadband Networks (Private) Limited (LBN) are at No 257/17A, Duke Street, Colombo 07. There also is a next-generation telecommunications experience arcade which is located on Lotus Road, a densely populated residential neighborhood, where visitors may try out the latest 5G capabilities and more. Since the late 1990s, LEGION has been at the forefront of mobile industry innovation and digitalization in Sri Lanka. LEGION provides advanced mobile telephony and high-speed mobile broadband networks to 16.5 million Sri Lankans through 3G/3.5G, 4G/4.5G, and 5G networks. LEGION is the first telecommunications company in South Asia to deploy and manage a 5G network, demonstrating next-generation technologies that will move Sri Lanka forward.

There are various systems under the LEGION Broadband Network Company that assist provide a consistent service across the country. LEGION Marketing and Advertising System (LMAS), Subscriber Information Management System (SIMS), LEGION Broadband System (LBS), Base Station Management System (BSMS), Internet Service Providing System (ISPS), and Employee Management System are the systems in question (EMS).

2.1 Purpose

The risk management approach's goal is to assess LEGION Broadband Network Company's flaws and vulnerabilities. As well as recognizing potential risks and their expected fiscal impact on the organization, as well as ensuring the security of linked systems. The study is organized and presents both quantitative and qualitative risk assessment methodologies.

2.2 Risk Assessment Framework

To start with the risk assessment process, OCTAVE Allegro Risk Management Framework has been chosen. The OCTAVE Allegro framework is designed to examine risks with a stronger focus on information assets. The framework's "Top-to-Bottom" approach aids information security employees in analyzing important assets in a systematic manner. All instructions, worksheets, and quizzes are available in a collaborative environment in the OCTAVE Allegro Framework.

2.3 Scope of the Risk Assessment

The Information Security Risk Management team at LEGION Broadband Networks conducted this risk assessment to detect Confidentiality, Integrity, and Availability (CIA) violations and related hazards. In LEGION Networks, there are over 15 systems that interact together, but only 5 critical systems for the company are recognized and included in the risk assessment process. It is believed that CIA is preserved throughout the risk assessment process. (**Confidentiality** – Preventing unauthorized access to sensitive information; **Integrity** – Maintaining the consistency and correctness of data throughout its lifespan; **Availability** – Information is available to authorized parties when they request it.) A total of 300 LEGION Broadband Networks staff from various divisions took part in the risk assessment (Human Resources, Networking, Internet Services, Cyber Security, General IT, Financial and General Employees, Managers). Employees are chosen for the assessment procedure based on the fact that they span the whole geographical region and departments that the company owns (Including: Headquarters, server rooms, Critical data storing server rooms, Security division, Management division, Training facilities, Experience Arcade etc.). Questionnaires, interviews, identifying known issues in the systems and evaluating them, analyzing log data, and analyzing and assessing presently used and previously used security technologies are utilized as part of the information collection process, with advance notice to the personnel.

3.Approach of Risk Assessment

3.1 Participants of Risk Assessment

Position of the Participant	Participant Name
CEO	Dr. Avishka Perera
Main System Engineer	Mr. Thusil Vishawaka
Director Human Resources	Mrs. Nipuni kodithuvakku
Director of Innovations Team	Mr. Sampath Premadasa, Mrs. Thilijni Udawaththa
Financial Division Team	Mrs. Kaumini Kaushalya, Mr. Akila Pramod
Networking Team	Mr. Thisara Rajapaksha
Internet Service Providing Team	Mr. Kavindu Gunawardana
IPTV Service Team	Mrs. Rveen Kulathilaka
Telecommunications Team	Mr. Govindu Anjana
Director Cybersecurity	Mr. Duvindu Bethmage

4. Risk Assessment Criteria

4.1 Threat Probability/Likelihood Scale

Qualitative Analysis Parameters

below mentioned model is employed to decide the risks associated with systems of LEGION Broadband Networks.

Risk = Probability x Magnitude of Impact

Likelihood	Definition
High (1.0)	The threat source is exceptionally skilled at exploiting vulnerabilities and persuading people to do so. If the present safeguards are unsuccessful in preventing the hazard from reoccurring, or if the sent countermeasures are ineffective in preventing the hazard from recurring. Countermeasures must be taken quickly and effectively.
Medium (0.5)	The threat's originator is well-prepared to exploit the weakness and persuasive in doing so. Existing precautions are even required to prevent the issue from being manipulated indefinitely.
Low (0.1)	The threat source, on the other hand, is unable to properly exploit the weaknesses. For mitigation and restraint, the current security controls and countermeasures are sufficient.

4.2 Magnetic Impact

Impact Score	Definition
High (10)	A major event that has the potential to harm a person's reputation as well as their financial well-being, resulting in large customer and client base losses. Customer service disruptions, financial losses, critical asset losses, communication service disruptions, and internet service disruptions are all examples of customer service disruptions.
Medium (5)	A case with a medium risk is one that has the potential to have an impact but does not pose a systemic threat. Significant, but reasonable, impediment to market kinds or potentially significant data, resulting in insufficient operational efficiency and viability, leaving customers unhappy and disappointed. This will result in severe financial and resource shortfalls that can be remedied.
Low (1)	A low-rated case has little or no effect on the firm's corporate practices and prestige. Clients are dissatisfied due to a marginal decrease in efficacy and performance.

4.3 Risk Calculated

	Impact		
Threat Likelihood	**Low Impact (1)**	**Medium Impact (5)**	**High Impact (10)**
High (1.0)	Low Risk (1.0 x 1 = 1.0)	Medium Risk (1.0 x 5 = 5.0)	High Risk (1.0 x 10 = 10)

Medium (0.5)	Low Risk (0.5 x 1 = 0.5)	Medium Risk (0.5 x 5 = 2.5)	High Risk (0.5 x 10 = 5)
Low (0.1)	Low Risk (0.1 x 1 = 0.1)	Medium Risk (0.1 x 5 = 0.5)	High Risk (0.1 x 10 = 1)
Risk Scale: [Low (0.1 to 1)] [Medium (>1 to 5)] [High (>5 to 10)]			

5.Critical Assets Identification

Critical Assets	Description	Container Specification	Security Requirements				Value
				H	M	L	
LEGION Broadband System (LBS)	This system primarily caters to 4G, 5G, and telecommunications (including voice, SMS, and MMS services), and it also controls all 4G and 5G capable devices linked to the network.	HP ProLiant DL380, 3TB RAM (24 x 128GB LRDIMM), 190TB Storage (12 LFF Drives), 2 x Intel C621 Platinum CPUs, HPE iLO 5.0 Remote Management CISCO Catalyst 9000 Series, with Windows Server 2019NT	Confidentiality	✓			Rs. 1,256,400
			Integrity		✓		
			Availability	✓			
Internet Service Providing System (ISPS)	Internet distribution (locally) and load balancing analysis, as well as a Gateway Management System	CISCO Catalyst 8500 Series Edge Platform Huawei AR160 Series FDD LTE 802.11 b/g/n FORTINET Gartner 2020 Enterprise series	Confidentiality	✓			Rs. 1,385,411
			Integrity			✓	
			Availability	✓			
Subscriber Information Management System (SIMS)	All the information related to subscribers are analyzing and managing is done by this system	ASUS Pro E800 G4, IntelR Xenon W-3200, 4 x NVIDIA Quadro RTX, 12TB ECC Memory, 10GbE LAN, 256GB RAM, Windows Server 2019NT	Confidentiality	✓			Rs. 1,240,400
			Integrity	✓			
			Availability	✓			
Base Station	This server manages information about	Dell Power Edge Rack Server, Intel Xenon E-	Confidentiality		✓		Rs.

Management System (BSMS)	base stations, BSS, MSC, as well as information about the handover process and dynamic information about subscribers.	2224 3.4GHz, 128GB RAM, 10TB Storage, 10GbE LAN x 4	Integrity			✓	850,600
			Availability	✓			
Employee Management System (EMS).	Information manages by Human Resource Department related to employees is stored and managed through this system	HP ProLiant ML310e Gen8, Intel Xenon E3-1200v2 (3.60 GHz), 64GB RAM, 1GbE LAN x 4, 4LFF 8TB Storage, 2 x PCIe 3.0 with Windows Server 2019	Confidentiality	✓			Rs. 440,500
			Integrity		✓		
			Availability			✓	

6.Threat Profile

Asset	Threat Analyze	Impact	Mitigation
LEGION Broadband System (LBS)	The major system for managing and providing voice calls, PSTN to VOIP transfers, SMS, 4G, LTE, and 5G services is the LEGION Broadband System (And all other telecommunication services). As a result, the LBS system is directly accessible to the general public, making it vulnerable to Man-In-The-Middle (MITM) attacks, DDoS assaults, SIP hacking, and DNS attacks. Because of the increased number of customers, the existing firewalls are insufficient. IDS/IPS systems are obsolete, and Packet-Filter Firewalls and Circuit-Level Firewalls are required to keep the system consistent.	LBS is the most critical system associated with the business. If the LBS is compromised by an any of the mentioned attacks, the business process of the company will be loss, and millions of LEGION customers will lose their connections completely due to unavailability of the connection. This will directly impact with the reputation, and availability of service of the company.	Installing FORTINET FortiGate4400f Firewalls Each cost Rs. 80,000/= Updating IDS/PS system to newest version, Cost of License Rs. 10,000/=
Before Mitigation		**After Mitigation**	
EF	47%	10%	
SLE	1,256,400 x 0.47 = Rs. 590,508/=	1,256,400 x 0.10 = Rs. 125,640/=	
ARO	0.40	0.30	
ALE	590,508 x 0.40 = Rs.236,203.20/=	125,640X 0.30 = Rs. 37,692/=	
Cost/Benefit	236,203.2 – 37,692 – (80,000 + 10,000) = Rs.108,511.20/=		

Asset	Threat Analyze	Impact	Mitigation
Internet Service Providing System (ISPS)	ISPS manages internet distribution (locally), IPTV connections, Fiber Optics Network, and ADSL connections. This system's load balancing is also critical. ISPS is vulnerable to DoS/DDoS, XSS, SQLI, and Path traversal, among other things.	ISPS is directly connected to all internet and internet-related services, and Legions an Internet Service Provider for the majority of Sri Lanka's biggest IT firms. As a result, every assault on this system has a direct influence on connected or client firms; as a result, attacks on ISPS will harm the company's reputation, and losing internet across the country and experiencing major downtime will have a negative impact on the company's financial situation.	Updating Microsoft Server 2019 and patching security to newest possible version, updating firmware of CISCO and Huawei routers usedRs.25,000/=.Recruiting an employee for internet operations and threat detection center. Rs 50,000/=

	Before Mitigation	After Mitigation
EF	62%	30%
SLE	1,385,411 x 0.62 = 858,954.82/=	1,385,411 x 0.30 = Rs. 415,623.30/=
ARO	0.40	0.35
ALE	858,954.82 x 0.40 = Rs. 343,581.92	415,623.30 x 0.35 = Rs.145,468.05/=
Cost/Benefit	343,581.92 - 145,468.05 – (50,000 + 25,000) = Rs.123,113.87/=	

Asset	Threat Analyze	Impact	Mitigation
Subscriber Information Management System (SIMS)	There are millions of LEGION Networks subscribers whose information is stored in the Subscriber Information Management System (SIMS). This is also a critical asset of the LEGION. The SIMS is a database, hence attacks such as SQL injections, privilege abuse, denial-of-service attacks, and other forms of exploiting vulnerable systems are all possible. The power interruptions might have an impact on the system's availability. The backup power plans and systems are inadequate to sustain the continuity.	Security flaws have been left unpatched in the system's software. Full system failure may occur from this. Detection and prevention measures, such as IDS/IPS, are insufficient. Inexperienced staff, as well as premeditated assaults on the database, may be responsible for the attacks. Furthermore, since the system cannot withstand power outages lasting longer than two hours, this has a significant impact on the system's accessibility. If an attack occurs, the whole system will be wiped clean	The Oracle Database was upgraded to version 19c. Rs.10,000/= Installing a power backup system that will provide electricity for more than 12 hours. 30,000/= rupees Using Amazon Web Services (AWS) Cloud Storage as a Disaster Recovery Plan Rs 60,000/=

Before Mitigation		After Mitigation
EF	60%	22%
SLE	850,600 x 0.60 = Rs. 510,360/=	850,600 x 0.22 = Rs. 187,132/=
ARO	0.67	0.47
ALE	510,360 x 0.67 = Rs. 341,941.20/=	187,132 x 0.47 = Rs. 87,952.04/=
Cost/Benefit	341,941.20 – 87,952.04 – (60,000 + 15,000) = Rs. 178,989.16 /=	

Asset	Threat Analyze	Impact	Mitigation
Base Station Management System (BSMS)	Information related Base Stations, BSS, MSC and information related to hand over process and dynamic information of subscribers are managed by this server. Due to inexperienced employees' physical damages can happen to the physical connecting components of the base stations. Due to lack of authentication systems attackers can introduce fake base stations to attract nearby UEs and launch attacks on the UEs that are attached. Information processing databases are vulnerable to privilege escalation attacks.	Extra permissions are beyond the reach of attacks. Rouge Base stations attracts and track users. Eavesdropping on users can damage the confidentiality of clients. SMS Spoofing attacks can cause huge destruction on OTP codes. Those attacks intensifying the security threats, after backdooring attackers can launch attacks without requiring any privilege, attackers can trace user locations.	Implementing a false base station identification system Rs.60,000/= Conducting awareness programs for employees working at base station premises Rs. 15,000/=

Before Mitigation		After Mitigation
EF	60%	22%
SLE	850,600 x 0.60 = Rs. 510,360/=	850,600 x 0.22 = Rs. 187,132/=
ARO	0.67	0.47
ALE	510,360 x 0.67 = Rs. 341,941.20/=	187,132 x 0.47 = Rs. 87,952.04/=
Cost/Benefit	341,941.20 – 87,952.04 – (60,000 + 15,000) = Rs. 178,989.16 /=	

Asset	Threat Analyze	Impact	Mitigation
Employee Management System (EMS)	EMS – Employee Management System is associated with the HR department. Employee recruitment and on-boarding, payment management etc. are handled through this system. As security threats risk management team identified Data breaches, DoS, Crypto-jacking, Insecure APIs and Legislation compliance. Those attacks are results of vulnerable databases and connected other software and systems.	Exploiting those vulnerabilities is uncomplicated therefore in few steps attackers can access the system. Attackers can leak data of employees to public and can demand for a ransom. Family information of employees are also included in the database records. This will encourage attackers to perform crime actions. Employees will lose their impressions and confidentiality towards the company. If the case was spread to the community LEGION will lose their subscribers.	Introducing comprehensive security strategies for instance regularly updating the database and security of the database Rs.20,000/= Using an enterprise level data encrypting software to encrypt he sensitive data. Rs 12,000/=

	Before Mitigation	After Mitigation
EF	55%	19%
SLE	440,500 x 0.55 = Rs. 242,275/=	440,500 x 0.19 = Rs. 83,695 /=
ARO	0.60	0.50
ALE	242,275 x 0.60 = Rs. 145,365/=	83,695 x 0.50 = Rs. 41,487.50/=
Cost/Benefit	145,365 – 41,487 – (20,000 + 12,000) = Rs. 71,878 /=	

7.Summary and Recommendations

The Risk Assessment was conducted with the help of 300 volunteers, and the LEGION Broadband Network (Private) Limited has 15 known systems. Five important systems have been selected within the 15-system risk assessment team. This paper explains the dangers of five different systems. The five most significant systems linked with LEGION are the LEGION Broadband System (**LBS**), Internet Service Providing System (**ISPS**), Subscriber Information Management System (**SIMS**), Base Station Management System (**BSMS**), and Employee Management System (**EMS**). We've found a number of threats that might jeopardize the systems' Confidentiality, Integrity, and Availability. We've detailed all of the risks to the systems, as well as response plans for those systems, in the Threat Profile section. Under mitigation, the reaction strategy as well as the EF, SLE, ARO, and ALE values before and after mitigation are presented.

The most useful solution for business continuity is the LEGION Broadband System (LBS). As a precaution against current attacks, the team recommends installing Fortinet FortiGate 4400f firewalls at each end connection point. Furthermore, by upgrading the IDS/IPS system to the most recent version, LEGION can minimize attacks.

The Internet Service Providing System is responsible for the distribution of internet and internet-based services (ISPS). This system has a significant influence on the business process's continuity as a major business content. As a mitigation approach for the detected risks, we suggested that Microsoft Server 2019 be updated and patched. In addition, the team recommended that two people be hired for internet operations and a threat detection center.

The Subscriber Information Management System (SIMS) holds all of the information regarding LEGION Broadband Network's 15 million customers. As a result, all three must be maintained: secrecy, integrity, and availability. The Oracle Database version should be upgraded to 19c, according to the team. As a mitigating approach, the team suggests keeping an AWS Cloud storage as a disaster recovery plan.

Implementing a fake base station identification system and performing awareness seminars for staff working at base station premises are advised for the Base Station Management System (BSMS). This system manages and processes all of the information linked to Base Stations, BSSs, and MSCs. This system is linked to a number of radio signaling devices, and it is responsible for all communication radio signals, which are carried out by radio antennas.

The HR department is linked to the Employee Management System. This system handles employee recruiting, onboarding, and payment. It is suggested that thorough security techniques be used for database updates and database security. It's also a good idea to encrypt sensitive data using enterprise-level data encryption software.

8.References

[1] I. Process, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", *Resources.sei.cmu.edu*, 2021. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. [Accessed: 30- Apr- 2021].

[2] *Resources.sei.cmu.edu*, 2021. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf. [Accessed: 30- Apr- 2021].

[3]"Broadband networks - Wikipedia", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Broadband_networks. [Accessed: 30- Apr- 2021].

[4]"Static Application Security Testing | SonarQube", *Sonarqube.org*, 2021. [Online]. Available: https://www.sonarqube.org/features/security/sast/?gads_campaign=ROW-1-SAST&gads_ad_group=SAST&gads_keyword=penetration%20testing%20tools&gclid=EAIaIQobChMI9f-G8Kam8AIVxH0rCh0ZEgO4EAAYASAAEgL4tvD_BwE. [Accessed: 30- Apr- 2021].

[5]2021. [Online]. Available: https://www.hpe.com/emea_europe/en/servers.html. [Accessed: 30- Apr- 2021].

[6]"ThinkSystem, System x & ThinkServer Rack Servers | Lenovo Srilanka", *Lenovo.com*, 2021. [Online]. Available: https://www.lenovo.com/lk/en/data-center/servers/racks/c/racks. [Accessed: 30- Apr- 2021].

[7]"Servers: Dell PowerEdge Servers | Dell USA", *Dell*, 2021. [Online]. Available: https://www.dell.com/en-us/work/shop/dell-poweredge-servers/sc/servers. [Accessed: 30- Apr- 2021].

[8] P. Matrix and M. Arumugam, "Probability and Impact Matrix", *Justgetpmp.com*, 2021. [Online]. Available: https://www.justgetpmp.com/2012/02/probability-and-impact-matrix.html. [Accessed: 30- Apr- 2021].

[9]"Single Loss Expectancy - an overview | ScienceDirect Topics", *Sciencedirect.com*, 2021. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/single-loss-expectancy. [Accessed: 30- Apr- 2021].

[10] C. DNA), "Cisco Catalyst 9000 Wireless and Switching Family Portfolio", *Cisco*, 2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/enterprise-networks/catalyst-9000.html. [Accessed: 30- Apr- 2021].

[11]"Routers - Huawei Enterprise", *Huawei Enterprise*, 2021. [Online]. Available: https://e.huawei.com/en/products/enterprise-networking/routers. [Accessed: 30- Apr- 2021].

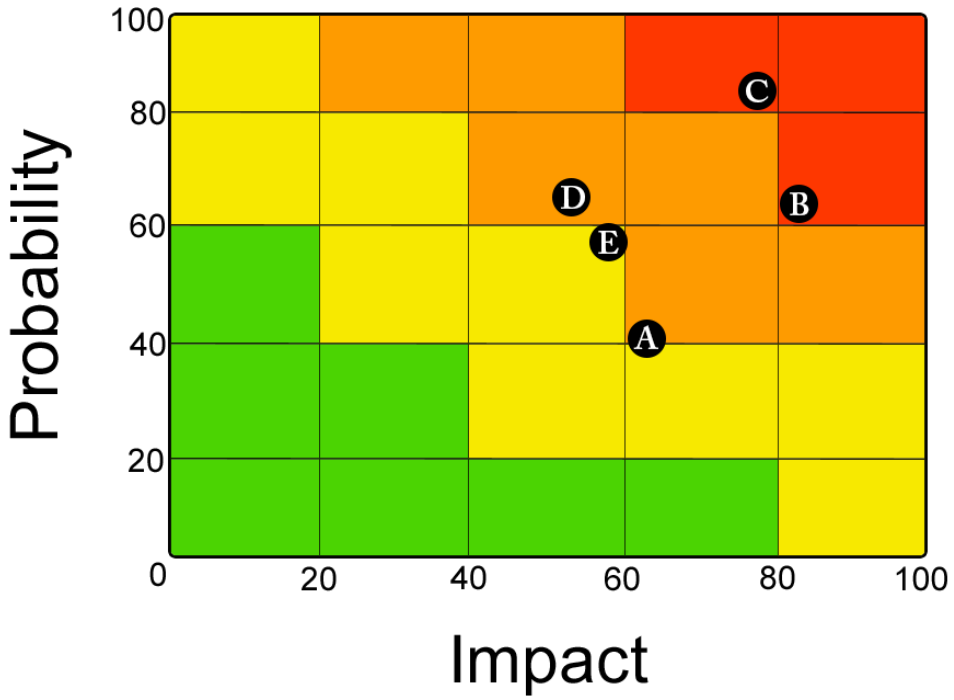
[12]"Windows Server 2019 | Microsoft", *Microsoft.com*, 2021. [Online]. Available: https://www.microsoft.com/en-us/windows-server. [Accessed: 30- Apr- 2021].

[13] *Fortinet.com*, 2021. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-4400f-series.pdf. [Accessed: 30- Apr- 2021].

9.Appendices

9.1 Appendix A

9.1.1 Heat Map



A: LEGION Broadband System (LBS),
B: Internet Service Providing System (ISPS)
C: Subscriber Information Management System
D: Base Station Management System (BSMS)
E: Employee Management System (EMS).

9.2 Appendix B

LBS – LEGION Broadcasting System

LBN – LEGION Broadcasting Networks

ISPS – Internet Service Providing System

SIMS – Subscriber Information Management System

BSMS – Base Station Management System

EMS – Employee Management System

SLE – Single Loss Expectancy

- Asset Value x Exposure Factor

ARO – Annualized Rate of Occurrences

- Frequency a threat will occur within a year.

ALE – Annualized Loss Expectancy

- SLE x ARO

Safeguard Cost/Benefit

- ALE Before Safeguard – ALE After Safeguard – Annual Cost of Safeguard

EF – Exposure Factor

1. Does the system under attack have any redundancies/ backups/ copies?
   Subtract 30% if the answer is YES.

2. Is the attack from outside?
   Subtract 20% if the answer is YES.

3. Is the system under attack behind a firewall?
   Subtract 10% if the answer is YES.

4. What is the likelihood that the attack will go undetected in time for a full recovery?
   Subtract 10% if the probability of being undetected is less than 20%
   Subtract 30% if the probability of being undetected is less than 10%

5. How soon can a countermeasure be implemented in time if at all?
   Subtract 20% if the countermeasure can be implemented within ½ hour.
   Subtract 10% if the countermeasure can be implemented within 1 hour.
   Subtract 5% if the countermeasure can be implemented within 2 hours.

9.3 Appendix C – Allegro Worksheets

9.3.1 LEGION Broadband System (LBS)

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Important Asset **What is the most important piece of data?**	**(2) Selection Justification** **What is the significance of this information asset to the organization?**	**(3) Explanation** **What is the description of this information asset that everyone agrees on?**
Legion Broadband System (LBS)	LBS is the LEGION's most valued asset. LBS is in charge of all telecommunications systems, including voice, MMS, SMS, 3G, 4G, and 5G networks	Everything you need to know about broadband communications, device specifications, and 4G and 5G coverage networks. Information and statistics on voice calls, as well as other important details
(4) Owner(s) *Who owns this information asset?*		
Director Broadband Systems		
(5) Security Requirements *What are the security requirements for this information asset?*		
☑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Staff – Broadband System
☑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Manager – Broadband System
☑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Staff – Broadband System Internet Services Team
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	99.99%
☐ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Continuous Surveillance (24/7)
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
☐ Confidentiality	☐ Integrity	☑ Availability ☐ Other

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Information Asset	LEGION Broadband System (LBS)		
	Area of Concern	Firewalls installed are not adequate because of increment of subscribers		
Threat	(1) Actor *Who would exploit the area of concern or threat?*	Hacker		
	(2) Means *How would the actor do it? What would they do?*	Use of Web Interface and MITM or Using DDoS		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ✓ ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Total loss of the business process can expect if the system was compromised, accessing to the systems can disrupted.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	✓ ❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Reputational damage could expect, if the attacker compromised all the services. Customer confidence can loss	Reputation & Customer Confidence	7	2
	Financial	9	3
	Productivity	8	2.5
	Safety & Health	-	-
	Fines & Legal Penalties	6	2
	User Defined Impact Area	-	-
	Relative Risk Score		**9.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	☑ **Defer**	❑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Windows Server 2019	To accommodate the significant increase in subscribers, FORTINET FortiGate4400f Firewalls are being installed.		

9.3.2 Internet Service Providing System (ISPS)

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Internet Service Providing System (ISPS)	The company application's second richest asset. This system also includes internet distribution, load balancing, and gateway management.	This system is linked to the delivery of Internet services and continuous vigilance. Data transmitted over the system must be kept in strict confidence.
(4) Owner(s) *Who owns this information asset?*		
Director Internet Service Provider		
(5) Security Requirements *What are the security requirements for this information asset?*		
☑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Staff – Internet Services
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Manager – Internet Service and operation division.
☑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Staff – Internet Services Operations Team

	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	99.9%
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Continuous Monitoring and Auditing (24/7)

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

☑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk — Threat	Information Asset	Internet Service Providing System (ISPS)		
	Area of Concern	System connected to internet – Continuous monitoring required		
	(1) Actor *Who would exploit the area of concern or threat?*	Hacker		
	(2) Means How would the actor do it? What would they do?	Web Interface, MITM, Server Software Vulnerabilities		
	(3) Motive *What is the actor's reason for doing it?*	Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ☑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*			
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	☑ **Medium**	❑ **Low**

(7) Consequences	(8) Severity		
What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?	*How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Disclosure of client sensitive information and browsing data can lead to financial damage	Reputation & Customer Confidence	9	4.5
	Financial	7	3.5

		Productivity	4	2
		Safety & Health	-	-
	Disclosure of client sensitive information and browsing data can lead to legal penalties	Fines & Legal Penalties	6	3
		User Defined Impact Area	-	-
			Relative Risk Score	**13**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Windows 2019 Server	Even as server is constantly linked to the web, several 0-day weaknesses should be expected when hiring an employee for internet operations and threat detection.		

9.3.3 Subscriber Information Management System (SIMS)

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Subscriber Information Management System (SIMS)	SIMS manages all subscriber and committed relevant details, loyalty card members, corporate profiles, and enterprise subscription bundles.	It is able to control pertinent data pertaining to around 15.5 million customers. Confidentiality, integrity, and accessibility are highly valued.
(4) Owner(s) *Who owns this information asset?*		
Head of the Department (Subscribers and Service)		
(5) Security Requirements *What are the security requirements for this information asset?*		

☑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Subscribers and Services Staff, Call center
☑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Tech lead and head of the (SnS) department
☑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Call Center and Loyalty Call center management
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	99.99%
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Continuous Monitoring and Auditing (24/7)

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

☑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro - Worksheet 10		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Information Asset	Subscriber Information Management System (SIMS)		
		Area of Concern	Currently using Oracle Database version is outdated		
		(1) Actor *Who would exploit the area of concern or threat?*	Hacker or Employee		
		(2) Means *How would the actor do it? What would they do?*	Physical Access Software Vulnerabilities		
		(3) Motive *What is the actor's reason for doing it?*	Accidental or Deliberate		
		(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	This will encourage the attackers for information disclosure attacks		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High**	❑ **Medium**	❑ **Low**

	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
		Impact Area	**Value**	**Score**
		Reputation & Customer Confidence	9	5.5
		Financial	8	5
		Productivity	6	3.2
		Safety & Health	-	-
	Legal penalties and can apply due to sensitive information disclosure	Fines & Legal Penalties	5	2
		User Defined Impact Area	-	-
			Relative Risk Score	**15.7**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Oracle Database System	By updating the Oracle Database Version to the most recent version available, you can reduce the risk of assaults on this system.

9.3.4 Base Station Management System (BSMS)

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Base Station Management System (BSMS)	This system is responsible of all radio signaling and devices related with towers. Individual parts and ground-level processes are essentially controlled.	Base Stations, Base Station Subsystems, MSC, and handover workflow details, as well as VLR relevant data, are all did manage with high availability.
(4) Owner(s) *Who owns this information asset?*		
Director Technical Services		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Technical Team
☑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Technical Staff, Physical Device maintain staff
☑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Broadband Team Internet Services Team
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	99%
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Monitored by ground level staff, Non-repudiation
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
❑ Confidentiality	❑ Integrity	☑ Availability ❑ Other

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk — Threat	Information Asset	Base Station Management System (BSMS)		
	Area of Concern	Physical level vulnerabilities are applied to this system		
	(1) Actor *Who would exploit the area of concern or threat?*	Hacker or Employee		
	(2) Means *How would the actor do it? What would they do?*	Physical Access Firmware issues		
	(3) Motive *What is the actor's reason for doing it?*	Accidental or Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ☑ **Destruction** ❑ **Modification** ❑ **Interruption**		
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Physical devices used in the BSMS are vulnerable to security threats		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High**	❑ **Medium**	❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
If the radio signaling devices lost, all the connections will be lost this will cause reputation and customer confidence	Reputation & Customer Confidence	9	7
	Financial	7	5
	Productivity	4	2
	Safety & Health	-	-
	Fines & Legal Penalties	6	2.5
	User Defined Impact Area	-	-
	Relative Risk Score		16.5

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Base Stations and associated components	By putting in place a bogus base station identification system and educating people who operate on ground station grounds.		

9.3.5 Employee Management System (EMS)

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
Employee Management System (EMS).	Most HR Department procedures are managed by this platform. Recruiting employees and managing payments are two things that come to mind when it comes to running a business.	The system is responsible of all confidential material relating to the EM and HR departments.
(4) Owner(s) *Who owns this information asset?*		
Director Human Resources		
(5) Security Requirements *What are the security requirements for this information asset?*		
☑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	Manager – Human Resources
☑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	Manager – HR Manager - DBMS
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Manager – HR, Other Department Managers

	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	99.99%
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Auditing, Integrity Checking.

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

☑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro - Worksheet 10	**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk — **Threat**	Information Asset	Employee Management System (EMS).		
	Area of Concern	Some information stored in the database are not encrypted		
	(1) Actor *Who would exploit the area of concern or threat?*	Unauthorized personnel		
	(2) Means *How would the actor do it? What would they do?*	Web Interfaces, Mobile Application		
	(3) Motive *What is the actor's reason for doing it?*	Accidental or Deliberate		
	(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☑ **Modification**	❑ **Destruction** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	If the vulnerabilities are exploited, services can be disrupted.		
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	☑ **Medium**	❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
	Reputation & Customer Confidence	8	4
	Financial	6	3
	Productivity	4	2

		Safety & Health	-	-
	Information disclosure may lead to fines and legal penalties related issues.	Fines & Legal Penalties	5	2.5
		User Defined Impact Area	-	-
			Relative Risk Score	**11.5**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*		
Database Software	By utilizing venture data encryption software, weaknesses can be mitigated.		

9.4 Appendix D

9.4.1 Techniques Used.

Techniques	Description
Assessment Tools	Inside the risk evaluation procedure, enterprise-level and high susceptibility measurement tools were used. Wireshark, Nessus, Genymotion, Libertylite, and BurpSuite are some of the tools available..
Questionnaire used for Risk Assessment Purpose	With both the support of a risk review panel, the Information Security Risk Assessment team created a questionnaire that covered all areas of data protection in each and every field. The Security Risk Assessment Questionnaire (SRAQ) – v1.8 and the Software Engineering Institute's (SEA) Information Security Risk Assessment Process guide were used to create the survey..

Interviews	Selected participants were interviewed by qualified interviewers, and each recognized participant was notified the about discussion prior to the event.
Standard Awareness Documents Used	The Assessment Team used standard awareness publications from many organizations, some of which are listed below. • National Vulnerability Database • OWASP Top 10 • Vulnerability Intelligence Database
Onsite inspections	The actual locations of the LEGION Broadband Network are dispersed around the island. As a result, the risk assessment team has covered nearly all of the actual areas in order to continue with the risk assessment procedure. • LEGION Broadband Network Headquarters • Experience Center • Server Locations

9.4.2 Technology Components

Component	Description
Applications	• SecureCRT • OmnetPP • Wireshark • Ericsson Software • Exterity Mobile telecommunications, IPTV, and broadband services are all examples of applications. • Adobe software is used to promote products. • Documentation and reporting services are provided by the Microsoft Office 365 suite.
Operating Systems	• Microsoft Windows 10 • Microsoft Server NT • Kali Linux 2021.4 • CentOS
Database Management System Software	• Oracle 20c and 21c • Microsoft SQL Server 2020 • Microsoft SQL Server Management Studio

Networking Devices	• CISCO Catalyst 9200 Switch (Used in layer 2) • CISCO Catalyst 9300 Switch (Used in layer 3) • CISCO 1921/K9 Routers • Huawei NetEngine 8000 Series • Vitec Devices for IPTV • HP and Apple MacBook Pro as personal computers.
Protocols	• TCP/IP • UDP • ICMP • HTTP • POP • IMAP

9.4.3 Physical Locations

Department/Facility Description	Location / Address
LEGION Broadband Networks (Private) Limited, Headquarters.	LEGION Broadband Networks (Private) Limited No 257/17A, Duke Street, Colombo 07
Innovations Experience Arcade	LEGION Experience Arcade No 12/B1, Lotus Road, Colombo 04
Main Operations Center (No 1)	LEGION Engineering & Operations No 11, Jasmine Park, Colombo 06
Operations Center (No 2) / Training Center	LEGION Engineering & Operations (No 2) 24/2, Jesmine Park, Narahenpita Road, Nawala.
Internet Services Center	LEGION Internet Services Center No 24/3, Galle Road, Matara
Call Center	LEGION Call Center No 43/1B, Sir Marcus Fernando Mawatha, Malabe