Ranking	Threats (1)	Vulnerabilities (2)	Contextual factors
12 - High	Unauthorized access - direct crime related threat	- Weak Passwords that can be cracked by simple password cracking software and overuse of a single password are both vulnerabilities that can give life to unauthorized access threat	- People often reuse passwords because it is more convenient to memorize one password that unlocks all their accounts
20 - Critical	Data leak	Weak end to end encryption and softaware vulnerabilities can cause data to be leaked	In many countries it is enforced by law that personal and financial data are stored in proper methods to prevent data leaks
2 - Very low	Hardware problems	Server is full or Maintenance scheduled	Slow software performance during maintenance

8 - Medium	Interruption in Service Delivery	Software glitches, reliance on interconnected systems	Dependence on uninterrupted service for core operations, intricate software integrations.
12 - High	Corruption of the Data	when data input is not inaccurate, it becomes impossible to validate the data output	Not all humans are contientous about the data they handle
20 - Critical	SQL Injection	Web applications that do not sanitize user input, reliance on outdated or vulnerable database systems.	Use of web applications for processing sensitive transactions and storing personal customer data.
12 - High	DDoS Attack (Distributed Denial of Service Attack)	Network infrastructure that lacks redundancy, absence of a scalable DDoS protection solution.	Increasing reliance on online services for business operations and customer engagement.
9 - Medium	Internal Security Risk	Over-privileged user accounts, inadequate user activity monitoring, and insufficient policy enforcement.	High-turnover environments and large numbers of contractors can increase the risk of insider threats.

10 - Medium	Ransomware Attack	Insufficient disaster recovery planning, inconsistent application of security updates and patches.	Use of diverse operating systems and applications increases the complexity of maintaining uniform security measures.
5 - Low	Lost/Stolen Devices	Unencrypted data storage, lack of robust access controls, and insufficient employee training regarding physical device security.	The growing trend of remote work and the use of personal devices for work purposes increase the risk of devices being lost or stolen.
12 - High			

RISK ANALYSIS TABLE for Condo Care

Last Update: 2024 - 02 - 07

Risks (3)	Likelihood from 1 to 5	Impact from 1 to 5	Reduction of Threats (Acceptance Strategy)
Risk of account theft or data loss	4	4	Using a password management system like "LastPass"'
Risk of account theft, and financial abuse	3	4	Using end to end encryption with public and private keys
	3	3	Upgrading server capacity, scheduling maintenance during non-peak hours, providing user notifications.

Periodic service outages affecting user functionality.	3	3	
Risk of showing wrong results and skewing opinions in the wrong direction	2	1	
Unauthorized access to or manipulation of database content, leading to data breaches and system compromise.	4	4	Regular code reviews, use of web application firewalls (WAF), and implementation of secure coding practices.
Extended downtime of online services, loss of revenue, erosion of customer trust.	3	4	Contract with a DDoS mitigation service provider that offers scalable solutions to protect against large-scale attacks
Intellectual property theft, sabotage of IT systems, compliance violations.	3	4	Conduct thorough background checks, implement a policy of least privilege, and provide regular security awareness training.

Disruption to business continuity, loss of sensitive data, financial impact due to ransom demands.	4	5	Maintain an updated disaster recovery and business continuity plan that includes ransomware scenarios. Simulate ransomware attacks to test the resilience of systems.
Exposure of corporate data, potential access by unauthorized individuals, legal and regulatory repercussions.	3	3	Implement and enforce mobile device management policies, including device tracking and remote wiping capabilities.

Reduction of Vulnerabilities (Protection Strategy)	Level of residual Risk
The importance of having strong password policies, strong authentication, and training stakeholders on security issues cannot be overstated. So the password validaiton doesn't accept weak passwords, and users are asked not to use previous passwords	**16 - High**
Hiring a private company to help with data transfer	**12 - High**
	9 - Medium

	9 - Medium
Stakeholders need to be made aware of handling data properly. As well as constructing mechanisms that validate data during the input process as well as the output process	**2 - Very low**
Utilize prepared statements and parameterized queries, conduct vulnerability scanning and penetration testing.	**16 - High**
Strengthen network infrastructure, implement redundant pathways, and conduct regular stress testing.	**12 - High**
Deploy advanced security monitoring tools to detect and respond to suspicious activities in real-time	**12 - High**

Regularly update and patch systems, enforce strict cybersecurity policies, and ensure that all data is backed up in a secure and segmented manner.	**20 - Critical**
Mandate full-disk encryption for all company-owned devices, require strong authentication methods, and train employees in security best practices for device handling.	**9 - Medium**