|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset** | **Threats** | **Likelihood** | **Impact** | **Priority** | **Justification** | **Recommendation** |
| Central database | Data breaches  Unauthorized access  Data corruption  Denial of Service (DoS) attack  Insider threat  Lack of data encryption  Physical security risk | 3 | 3 | 9 | The likelihood of this threat is high due lack of data encryption and this could lead to loss of data, and data breach and could lead to lawsuit from clients.  The impact is high as it could lead to discontinuity of business from heavy lawsuit settlement. | To mitigate these threats, ACG should implement robust security measures such as access controls, encryption, regular security audits, patch management, employee training, and disaster recovery plans. Additionally, adopting security best practices and staying updated on emerging threats is crucial for maintaining the security of central databases. |
| Web application | Injection attacks  Security misconfiguration  Sensitive data exposure  Broken authentication  File upload vulnerabilities | 3 | 3 | 9 | The likelihood of this threat is high due to security misconfiguration and sensitive data loss to threat actors.  The impact is high as any data loss could lead to ransomware and spyware and the integrity of the financial institution could be on the line. | To mitigate these threats, web developers should follow secure coding practices, implement proper security controls, regularly update and patch software components, conduct security assessments and audits, and provide ongoing security training to personnel. Additionally, employing web application firewalls (WAFs) and regularly testing the application for vulnerabilities can help improve overall security posture.  Pen test web application. |
| Main server | Lack of monitoring and logging  Social engineering attack  Data breaches  Malware infections  Distributed Denial of Service (DDoS)  Unauthorized access  Least of privilege | 3 | 3 | 9 | The likelihood of this threat is high due to data breach due to unauthorize access and social engineering attacks by threat actors.  The impact is high as any data loss from failure to backup server could lead to data in the hands of wrong persons. | To mitigate these threats, organizations should implement robust security measures, such as firewalls, intrusion detection or prevention systems, antivirus software, access controls, encryption, regular security audits, employee training, and incident response plans. Regular security assessments and proactive monitoring can help identify and address security vulnerabilities before they are exploited by attackers.  Restrict access to unauthorised person by using Access card to prevent backdoor.  Installation of firewall on servers and regular maintenance |
| Employees Laptop | Malware infections through infected USB  Phishing attack  Social engineering  Weak passwords  Outdated software  Lost or stolen laptop  Unsecured Wi-Fi networks | 3 | 3 | 9 | The likelihood of this threat is high due to malware infections through infected USB.  The impact is high as any data loss could lead to ransomware and spyware and the integrity of the financial institution could be on the line. | To mitigate these threats, IT firms should implement comprehensive security measures, including security awareness training for employees, strong password policies, regular software updates and patch management, encryption of sensitive data, endpoint protection solutions, remote wipe capabilities for lost or stolen devices, and strict access controls to prevent unauthorized access to corporate systems and data. Additionally, organizations should enforce policies for secure remote work practices and provide employees with guidelines for securely using their laptops in various environments. Regular security audits and monitoring can help detect and respond to security incidents promptly. |
| IT Infrastructure | Cyberattack  Physical security breach  Inadequate authentication and access control  Network attacks  Compliance violation  Emerging threats |  |  |  | The likelihood of this threat is high due to cyberattack that could come from unauthorized access that could lead to loss of sensitive information to the hand of hackers.  The impact is high as any data loss could lead to ransomware and spyware and the integrity of the financial institution could be on the line. | Implement comprehensive security measures, such as network segmentation, encryption, intrusion detection or prevention systems, security awareness training, regular security assessments and audits, incident response planning, and collaboration with industry partners and cybersecurity professionals. Additionally, organizations should stay vigilant and proactive in monitoring, detecting, and responding to security incidents to protect their IT infrastructure from evolving threats.  Performing firewall maintenance regularly. |
| Main site office and branches | Cyberattacks  Data breaches  Insider threats  Payment fraud  Regulatory compliance risks  Operational risks | 3 | 3 | 9 | The likelihood of this threat is high due to data breach from insider threats.  The impact is high as any data loss could lead to ransomware and spyware and the integrity of the financial institution could be on the line. | Employ various security measures, including robust cybersecurity controls, encryption, multi-factor authentication, fraud detection systems, transaction monitoring, anti-money laundering (AML) programs, regulatory compliance frameworks, physical security measures, employee training, and incident response plans. Collaboration with industry peers, government agencies, and law enforcement authorities is also essential for sharing threat intelligence and best practices to enhance the resilience of financial institutions against evolving threats |
| Website | Insecure password storage  Insecure APIs  DDoS attack  Brute force attack  Phishing  Malware infections | 3 | 3 | 9 | The likelihood of this threat is high due to insecure API which can expose sensitive data or allow unauthorized access to website resources.  The impact is high as any data loss could lead to ransomware and spyware and the integrity of the financial institution could be on the line. | Implement security best practices such as regular security audits, software updates and patches, input validation, secure coding practices, firewalls, intrusion detection systems, SSL/TLS encryption, strong authentication mechanisms, and user education and awareness programs. Additionally, website owners should have a robust incident response plan in place to respond to security incidents promptly and minimize the impact on their website and users. |