SALAMI GANIYU OLADELE

Risk Assessment for Angels Credit Group (ACG), Abeokuta

Asset	Threat	Likelyhood	Impact	Priority	Justification	Recommendation
Customer record	Unauthorized access	3	3	9	Unauthorized access is the entry point to all endpoints/hosts or. This could be achieved when the organization is not enforcing strong password policy, lacking awareness against phishing attack, presence of insider threat, stolen credentials, no adequate access control in place, lack of physical security control, non enforcement of strong encryption. One or all of these put customers records/accounts to free for all.	Encryption of data (at-rest and intransit) should be introduced. The principle of least privilege and need to know should be applied. Strong access authentication method should be put in place and the policy of secure password be enforced. Proper configuration of application software and hosts to prevent XSS, SSRF among other attacks. Enforcing rate limiting to mitigate against password bruteforcing is also a good idea.
Local web server	Unavailability of server	3	1	3	This could result from system update and upgrade or some other maintenance. Other cause may be application failure or bug that may make the application server behave in an unexpected manner. Excess traffic request or DOS may also be a cause.	Creation of alternative server to help in sharing of high traffic using load ballancer. Provision of backup server to fallback to in case of failure of a single server. Installation of IDS/IPS to prevent the instance of DOS/DDOS, by filtering multiple requests from identified(rouge) IP.
Company laptop	Malware	1	3	3	User behaviour, security practices and endpoint security are determinant of possible malware infection. As it contributes to data loss, financial impact, intellectual property and network propagation.	Implementation of security policies such as USB security policy, patch management, incident response plan, mobile device management, backup and recovery plan, network security measures, access controls, employee training, regular software updates and endpoint security software among others will secure the company's laptop from malware threats
Employees laptop	Compromised customers' and company's data	1	3	3	Bring Your Own Devices(BYOD) policies has its associated risks such as data leakage, malware threats and device theft among others. Insufficient update management, regulatory compliance, and compatibility issues as well	Organization must establish clear security guidelines, enforce strong authentication, implement Mobile Device Management(MDM) solutions and educate employees. Regular security updates, audits and monitoring can also help to mitigate potential risks.

SALAMI GANIYU OLADELE

Risk Assessment for Angels Credit Group (ACG), Abeokuta

					as privacy concern are issues to contend with.	
Employees records	Social Engineering	3	3	9	If the identity or information of employees are publicly available, threat actors could take the advantage, performing social engineering within the organization's employees. In case where attacker have access to employee's names, location, official mail and the rest, attacker can perform identity theft, fraud, phishing, corporate espionage and business disruption.	Employees record and details must be placed with high priority as their official identity must be secretive. Personal information should not be mixed with official information, i. e. personal mail should be used for official transactions Regular training must me given to employees to identify social engineering devices. Proper incident response plan be put in place against such occurrences, as well as regular audits and monitoring, compliance and regulations.
Business records & information	Data Breach	1	3	3	Unauthorized access, malware, possibility to compromise customers' or/and company's data, social engineering to mention but a few are all indication to data breaches. This is an unauthorized access to business records, exposing sensitive information and reputation damage which could lead to business collapse that may also include fines.	Strong encryption method to protect sensitive business records, strict access control and users' authentication mechanism, regular data backup, employees training, robust security endpoint solution, regular test of incident response plan, implementation of IDS/IPS to prevent network, data classification based on sensitivity, as well as employee awareness are all needed to mitigate against this form of attack/threat.