ILESANMI TEMITOPE SAMSON

FE/23/12145024

USING THE NIST CSF 2.0 CYBERSECURITY FRAMEWORK, EXPLAIN HOW TO IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER AND GOVERN THE POTENTIAL RISK FACED IN TECHNOLOGY AND SOFTWARE DEVELOPMENT.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| S/N | RISK CATEGORY | IDENTIFY  (ID) | PROTECT  (PR) | DETECT  (DE) | RESPOND  (RE) | RECOVER  (REC) | GOVERN  (GO) |
| 1 | Social Engineering | Intellectual property | It involves combining of technical, administrative and cultural measures in order to safeguards your IP: Educate and train Employees, implement strong access control, such as Multi−factor Authentication (MFA) | Encourage reporting, monitoring and Analyze, access logs and Audit, deploy Intrusion Detection System (IDS) | Secure physical access, Isolate the affected system, Change compromised credentials, Access the damages. | Restore from the backup, patch vulnerabilities, apply patches or updates to fix any vulnerabilities, reinstall software | By prioritizing the risk based on their potential impact on the organization.  Develop and implement strategies to mitigate identified risks. Establish a committee to oversee all aspect of security, including social engineering. |
| 2 | Malware and Ransomware | Network infrastructure | Provide constant training for staffs | Behavioral analysis, use tools that analyze behavior patterns to detect anomalies that may indicates malware activities, regularly conduct system scans using anti-malware software to detect and remove any infections | Isolation: Immediately isolate infected systems from network to prevent the spread of malware. Investigate the source so as to improve the defense. Report to the appropriate quarters. | Check for backups; verify the availability and integrity of the backups for affected data, ensure that the backups are not infected. Eradication: use reputable antivirus and anti-malware tools to fully remove any malicious software from the systems | Compliance and standards: ensure that your cybersecurity policies align with industries standards e.g (ISO/IEC27001, NIST cybersecurity framework). Regularly conduct risk assessments to identify vulnerabilities that could exploited by malware. |