**3MTT COHORT 2**

**CYBERSECURITY**

**GROUP 3 BATCH B**

**TEDPRIME HUB, IDI ABA, ABEOKUTA**

**OGUN STATE**

**GROUP MEMBETRS**

**1. SIMAN BITRUS BOAZ FE/23/64112618**

**2. ILESANMI TEMITOPE SAMSON FE/23/12145024**

**3. EYIOWUAWI MAHMUD FE/23/2770926**

**4. RUKAYAT OLOYEDE FE/23/32793059**

These are some potential risks in technology and software development industries

1. Data Breaches: Unauthorized access to sensitive data, such as customer information, intellectual property, or financial records, can lead to significant financial losses and damage to reputation.
2. Malware and Ransomware: Malicious software can be introduced into systems to steal data, disrupt operations, or hold data hostage until a ransom is paid.
3. Supply Chain Vulnerabilities: Third-party vendors and open-source components can introduce vulnerabilities if not properly vetted. A compromised supplier can lead to widespread issues.
4. Insider Threats: Employees or contractors with access to sensitive information may intentionally or unintentionally cause data leaks or system breaches.
5. Insecure Software Development Practices: Poor coding practices, lack of security testing, and failure to follow secure development life cycle (SDLC) principles can lead to vulnerabilities in software products.
6. Phishing Attacks: Cybercriminals often use social engineering tactics to trick employees into providing access credentials or sensitive information.
7. DDoS Attacks: Distributed Denial of Service attacks can overwhelm servers, making services unavailable and leading to downtime and loss of revenue.
8. Weak Authentication Mechanisms: Inadequate password policies, lack of multi-factor authentication (MFA), and poor session management can expose systems to unauthorized access.
9. Legacy Systems: Older software and hardware that are no longer supported may have unpatched vulnerabilities that can be exploited by attackers.
10. Cloud Security Risks: Misconfigurations in cloud environments can lead to data exposure. Additionally, reliance on third-party cloud providers can create additional risks if their security practices are inadequate.
11. IoT Vulnerabilities: The proliferation of Internet of Things (IoT) devices can create new attack vectors due to their often-limited security features.
12. Compliance and Regulatory Risks: Failure to comply with data protection regulations (like GDPR, HIPAA, etc.) can lead to legal penalties and loss of customer trust.
13. Lack of Incident Response Planning: Without a well-defined incident response plan, organizations may struggle to respond effectively to a cybersecurity incident, exacerbating the damage.
14. Social Engineering: Attackers may manipulate individuals into divulging confidential information, often exploiting human psychology rather than technical vulnerabilities.
15. Artificial Intelligence (AI) Exploits: As AI technology becomes more prevalent, there is a risk of adversarial attacks that manipulate AI systems or use AI to enhance cyberattacks.

Analysis of some Cybersecurity risk

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| s/n | Asset | Threat | Likelihood | Impact | Risk | Justification |
| 1 | System | Disruption of operation | 4 | 4 | 16 | The likelihood and impact of malware and Ransomware attack is high due to the profit motive and privacy issues.  The impact is high because many systems and data will be corrupted and possibilities of company incurring many expenses |
| 2 | Customer’s information | Data breach | 4 | 4 | 16 | The likelihood of this threat is high because of poor access control of the system. The impact is very high because it could lead to loss of customer's trust and damage of company’s reputation |
| 3 | Intellectual Property | Unauthorized Access and Theft | 3 | 5 | 15 | The likelihood of this threat is moderate, especially if there are inadequate access controls and monitoring. The impact is very high because the theft of proprietary information can lead to loss of competitive advantage, financial losses, and legal repercussions. The high value of intellectual property to the business makes this a significant risk. |
| 4 | Network Infrastructure | Distributed Denial of Service (DDoS) Attack | 4 | 3 | 12 | The likelihood of the attack is high due to the increasing frequency of such attacks across industries. The impact is moderate because, while it can disrupt services temporarily, proper mitigation strategies (such as using a Content Delivery Network (CDN) or DDoS protection services) can minimize the damage. However, a prolonged attack could lead to downtime, loss of revenue, and customer dissatisfaction, making it a moderate risk that needs attention. |