RISK ASSESSMENT FOR MEDIUM-SIZED E-COMMERCE COMPANY

Executive Overview: An e-commerce company faced rising concerns over the security of customer transactions and financial data. Brought in as a Cybersecurity Expert, I conducted a thorough risk assessment, identifying vulnerabilities that threatened data confidentiality, integrity, and availability. By enhancing security controls and aligning measures with ISO 27001 standards, I strengthened the company's defences, ensuring compliance while safeguarding critical assets against cyber threats.

Step 1: Risk Assessment Using ISO 27001 Guidelines

ISO 27001 Framework Overview: ISO 27001 is an international standard for information security management systems (ISMS). The risk assessment process involves:

1. **Defining the Context and Scope**: Understand the organisation's environment, assets, and processes that are in scope for the assessment.
2. **Risk Identification**: Identify potential threats, vulnerabilities, and risks to the assets.
3. **Risk Analysis**: Assess the impact and likelihood of each identified risk.
4. **Risk Evaluation**: Determine the level of risk and prioritise it.
5. **Risk Treatment Plan**: Develop strategies to treat risks based on their evaluation.

Step 2: Identifying Potential Threats, Vulnerabilities, and Impacts

1. **Potential Threats:**
   - **Malware Attacks**: Virus, ransomware, trojans that could compromise data integrity and availability.
   - **Phishing Attacks**: Social engineering tactics to gain unauthorised access to sensitive information.
   - **Insider Threats**: Employees or contractors with malicious intent or accidental actions leading to data breaches.
   - **DDoS (Distributed Denial of Service) Attacks**: Flooding services to make them unavailable to users.
   - **Data Breaches**: Unauthorised access or exposure of customer data.
   - **SQL Injection Attacks**: Exploiting web application vulnerabilities to gain unauthorised database access.
   - **Weak Passwords**: Poor authentication mechanisms that could be easily compromised.
   - **Third-Party Vendor Risks**: Security vulnerabilities within third-party providers.
2. **Vulnerabilities:**
   - Lack of encryption for sensitive data.

- Outdated software and unpatched vulnerabilities.
- Weak access controls and authentication mechanisms.
- Inadequate network segmentation.
- Insufficient monitoring and logging of activities.
- Lack of employee security awareness training.
- Inadequate backup and disaster recovery plans.
- Misconfigured cloud services and storage.

3. Potential Impacts:

- **Confidentiality Impact**: Unauthorised access to sensitive customer and financial information.
- **Integrity Impact**: Modification or deletion of critical data, leading to data corruption or loss.
- **Availability Impact**: Downtime of the website, causing loss of sales and damage to reputation.

Step 3: Assessing the Likelihood and Impact of Each Risk

Risk	Threat	Likelihood (High, Medium, Low)	Impact (High, Medium, Low)	Risk Level (Combined Assessment)
Malware Attacks	Virus, ransomware, etc.	Medium	High	High
Phishing Attacks	Social engineering	High	High	High
Insider Threats	Malicious/Accidental actions	Medium	High	High
DDoS Attacks	Flooding of services	Medium	High	High
Data Breaches	Unauthorised access/exposure	High	High	High
SQL Injection Attacks	Exploiting web vulnerabilities	Medium	High	High
Weak Passwords	Poor authentication	High	Medium	High

Risk	Threat	Likelihood (High, Medium, Low)	Impact (High, Medium, Low)	Risk Level (Combined Assessment)
Third-Party Vendor Risks	Security vulnerabilities	Medium	High	High

---

Step 4: Risk Treatment Plan Based on Findings

Risk Treatment Plan:

Risk	Treatment Strategy	Recommended Controls
Malware Attacks	Mitigation	Implement endpoint protection, regular patching, and use antivirus/anti-malware software.
Phishing Attacks	Mitigation	Conduct regular employee security awareness training, implement email filtering, and use multi-factor authentication (MFA).
Insider Threats	Mitigation/Avoidance	Implement role-based access control (RBAC), conduct background checks, and establish user activity monitoring.
DDoS Attacks	Mitigation/Transfer	Use a Content Delivery Network (CDN) and Web Application Firewall (WAF) and consider DDoS protection services.
Data Breaches	Mitigation	Encrypt sensitive data at rest and in transit, implement strong access controls, and regularly audit systems.
SQL Injection Attacks	Mitigation	Use prepared statements and parameterised queries, regularly test web applications, and implement a WAF.
Man-in-the-Middle Attacks	Mitigation	Enforce HTTPS for all data transmissions, use VPNs for internal communications, and regularly review SSL/TLS certificates.
Weak Passwords	Mitigation	Implement MFA, enforce strong password policies, and use a password manager.
Third-Party Vendor Risks	Mitigation/Transfer	Conduct regular security assessments of third-party vendors and include security clauses in contracts.

Step 5: Prioritising and Recommending Security Controls

❖ **High Priority Controls:**

- **Data Encryption**: Encrypt all sensitive data both at rest and in transit.
- **Multi-Factor Authentication (MFA)**: Implement MFA for all critical systems.
- **Endpoint Protection**: Deploy robust antivirus and anti-malware software.
- **Access Control**: Implement RBAC and least privilege access controls.
- **Regular Security Training**: Conduct regular security awareness training for all employees.
- **Vulnerability Management**: Regularly patch and update software to address vulnerabilities.
- **Web Application Security**: Implement a WAF and secure coding practices to prevent SQL injection and other web-based attacks.

❖ **Medium Priority Controls:**

- **Network Segmentation**: Isolate sensitive data and critical systems from the rest of the network.
- **Monitoring and Logging**: Implement continuous monitoring and logging of network activities.
- **Incident Response Plan**: Develop and test an incident response and disaster recovery plan.
- **DDoS Mitigation Services**: Use a CDN and DDoS protection services to handle potential attacks.

❖ **Low Priority Controls:**

- **Third-Party Risk Management**: Establish a process for regularly assessing and managing third-party risks.
- **Password Management**: Use password managers and enforce strong password policies.

Conclusion

This risk assessment identified several key risks to the confidentiality, integrity, and availability of the company's data. By implementing the recommended controls, the company was able to significantly reduce the likelihood and impact of potential threats. Also, regular review and update of the risk assessment ensured that emerging threats and vulnerabilities were promptly addressed.