Cybersecurity Diagnostic Report

Overall Score:

50.0% (250/500)

Recommendations:

Fair. Focus on strengthening key areas like access control and incident response.

Category Scores:

Access Control: 45/80 (56.25%)

Data Protection: 45/70 (64.29%)

Employee Awareness and Training: 30/70 (42.86%)

Governance and Policies: 60/70 (85.71%)

Incident Response and Recovery: 30/70 (42.86%)

Network Security: 30/90 (33.33%)

Third-Party Risk Management: 10/50 (20.0%)

Suggested Tools for Improvement:

Access Control: Okta

Data Protection: VeraCrypt

Employee Awareness and Training: KnowBe4, Infosec IQ

Incident Response and Recovery: Splunk SOAR, IBM Resilient

Network Security: Snort, Wireshark

Third-Party Risk Management: OneTrust, Prevalent

Detailed Answers:

Q1: Do you have a written and approved cybersecurity policy?

Answer: Yes

Q2: Are cybersecurity roles and responsibilities clearly defined within your organization?

Answer: Yes, documented and assigned

Q3: Do you perform annual cybersecurity risk assessments?

Answer: Yes

Q4: Do you have a cybersecurity awareness program in place for employees?

Answer: Yes, ongoing and mandatory

Q5: Do you allocate a specific budget for cybersecurity initiatives?

Answer: Yes, but limited budget

Q6: Do you have a firewall installed and configured on your network?

Answer: Yes

Q7: Do you use intrusion detection and prevention systems (IDS/IPS)?

Answer: No

Q8: Do you monitor network traffic for suspicious activities?

Answer: Yes, but not continuous

Q9: Do you perform regular vulnerability scans on your systems?

Answer: No

Q10: Do you segment your network to isolate sensitive data?

Answer: Partially

Q11: Do all employees have unique login credentials?

Answer: Not Sure

Q12: Is multi-factor authentication (MFA) enabled for all critical systems?

Answer: Yes, for all systems

Q13: Are accounts of terminated employees promptly deactivated?

Answer: Yes, within 24 hours

Q14: Are administrative privileges restricted to essential personnel?

Answer: Yes, strictly enforced

Q15: Are login attempts monitored for suspicious activity?

Answer: No

Q16: Is sensitive data encrypted at rest?

Answer: Yes, with strong encryption

Q17: Is sensitive data encrypted in transit?

Answer: Yes, always

Q18: Do you have a documented incident response plan?

Answer: No

Q19: Are regular backups of critical data performed?

Answer: Yes, but no offsite storage

Q20: Do you conduct phishing simulation exercises?

Answer: Yes, but less frequently

Q21: Do you assess third-party vendors for cybersecurity compliance?

Answer: No

Q22: Do you require third-party vendors to adhere to your cybersecurity policies?

Answer: Partially

Q23: Do you review third-party cybersecurity policies annually?

Answer: No

Q24: Do you conduct regular incident response training exercises?

Answer: No

Q25: Do you enforce strong password policies across the organization?

Answer: No

Q26: Do you implement role-based access controls (RBAC)?

Answer: Partially implemented

Q27: Do you restrict access to sensitive data based on employee roles?

Answer: Yes, enforced rigorously

Q28: Do you use Virtual Private Networks (VPNs) for remote access?

Answer: Yes, but without MFA

Q29: Do you block unauthorized devices from accessing your network?

Answer: No

Q30: Do you maintain a log of all user access to critical systems?

Answer: Yes, with regular audits

Q31: Do you have a documented onboarding and offboarding process for employees?

Answer: No

Q32: Do you conduct mandatory cybersecurity awareness training for new hires?

Answer: Yes, but delayed

Q33: Do you regularly communicate cybersecurity updates to employees?

Answer: No

Q34: Do employees report phishing attempts and suspicious emails?

Answer: Yes, with mandatory reporting

Q35: Do you provide training on safe browsing practices?

Answer: No

Q36: Do you have automated tools to detect and respond to security incidents?

Answer: No

Q37: Do you maintain a log of all security incidents and breaches?

Answer: Yes, but without detailed analysis

Q38: Do you ensure that vendors have cybersecurity insurance?

Answer: No

Q39: Do you enforce a data retention and deletion policy?

Answer: Yes, strictly enforced

Q40: Do you regularly review and update your cybersecurity policies?

Answer: Yes, but less frequently

Q41: Do you enforce password complexity requirements (e.g., length, special characters)?

Answer: No

Q42: Do you have a secure method for sharing sensitive information internally?

Answer: No

Q43: Do you block access to malicious websites using a web filtering solution?

Answer: No

Q44: Do you provide ongoing training on identifying and preventing phishing attacks?

Answer: Yes, quarterly or more frequently

Q45: Do you test your backup restoration process regularly?

Answer: Yes, at least annually

Q46: Do you conduct third-party audits of your cybersecurity program?

Answer: Yes, annually or more frequently

Q47: Do you require vendors to follow data protection regulations (e.g., GDPR, HIPAA)?

Answer: Yes, but without compliance checks

Q48: Do you train employees on securely using mobile and personal devices for work?

Answer: No

Q49: Do you conduct security assessments on cloud services used by your organization?

Answer: Yes, but only once during adoption

Q50: Do you use automated threat intelligence tools to improve your incident response?

Answer: Yes, integrated with response tools