Cybersecurity Diagnostic Report

Overall Score:

280/500 (56.0%)

Category Scores:

Access Control: 60/80 (75.0%)

Data Protection: 50/70 (71.43%)

Employee Awareness and Training: 45/70 (64.29%)

Governance and Policies: 25/70 (35.71%)

Incident Response and Recovery: 35/70 (50.0%)

Network Security: 55/90 (61.11%)

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

Recommendations:

Focus on strengthening key areas: Governance and Policies, Third-Party Risk Management.

Suggested Tools for Improvement:

Governance and Policies: NIST Cybersecurity Framework, CIS Controls

Third-Party Risk Management: OneTrust, Prevalent

Detailed Answers:

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

Answer: No

Recommendation: Develop formal security policies and ensure organization-wide enforcement.

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

Answer: Yes, documented and assigned

Recommendation: Maintain a strong governance framework and review policies periodically.

Q3: Do you perform annual cybersecurity risk assessments?

Answer: Occasionally

Recommendation: Enhance governance measures by aligning with industry best practices.

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

Answer: Yes, but infrequent

Recommendation: Enhance governance measures by aligning with industry best practices.

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

Answer: No

Recommendation: Develop formal security policies and ensure organization-wide enforcement.

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

Answer: No

Recommendation: Implement firewall, IDS/IPS, and network segmentation to improve security.

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

Answer: No

Recommendation: Implement firewall, IDS/IPS, and network segmentation to improve security.

Q8: Do you monitor network traffic for suspicious activities?

Answer: Yes, continuously

Recommendation: Regularly review and update network security configurations and segment networks appropriately.

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

Answer: Yes, monthly or more frequently

Recommendation: Regularly review and update network security configurations and segment networks appropriately.

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

Answer: No

Recommendation: Implement firewall, IDS/IPS, and network segmentation to improve security.

Q11: Do all employees have unique login credentials?

Answer: Yes

Recommendation: Continue enforcing strict access controls and review policies regularly.

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

Answer: Yes, for all systems

Recommendation: Continue enforcing strict access controls and review policies regularly.

Q13: Are accounts of terminated employees promptly deactivated?

Answer: Yes, within 24 hours

Recommendation: Continue enforcing strict access controls and review policies regularly.

Q14: Are administrative privileges restricted to essential personnel?

Answer: Partially

Recommendation: Enhance access control measures by implementing multi-factor authentication.

Q15: Are login attempts monitored for suspicious activity?

Answer: Yes, real-time monitoring

Recommendation: Continue enforcing strict access controls and review policies regularly.

Q16: Is sensitive data encrypted at rest?

Answer: Yes, but weak encryption

Recommendation: Expand encryption and data protection measures to cover all critical information.

Q17: Is sensitive data encrypted in transit?

Answer: Yes, always

Recommendation: Ensure encryption standards remain updated and review data protection policies regularly.

Q18: Do you have a documented incident response plan?

Answer: No

Recommendation: Develop and implement an incident response plan to minimize downtime.

Q19: Are regular backups of critical data performed?

Answer: Yes, with offsite storage

Recommendation: Test and refine the incident response plan regularly to improve effectiveness.

Q20: Do you conduct phishing simulation exercises?

Answer: No

Recommendation: Develop a mandatory security training program to educate employees on risks.

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

Answer: Yes, but less frequently

Recommendation: Strengthen vendor security assessments and require compliance documentation.

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

Answer: No

Recommendation: Implement a vendor risk management program to evaluate third-party security.

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

Answer: No

Recommendation: Implement a vendor risk management program to evaluate third-party security.

Q24: Do you conduct regular incident response training exercises?

Answer: No

Recommendation: Develop and implement an incident response plan to minimize downtime.

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

Answer: Yes, but updates are optional

Recommendation: Expand encryption and data protection measures to cover all critical information.

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

Answer: Yes, strictly enforced

Recommendation: Ensure encryption standards remain updated and review data protection policies regularly.

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

Answer: Yes, enforced rigorously

Recommendation: Ensure encryption standards remain updated and review data protection policies regularly.

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

Answer: Yes, with MFA enabled

Recommendation: Regularly review and update network security configurations and segment networks appropriately.

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

Answer: Yes, strictly enforced

Recommendation: Regularly review and update network security configurations and segment networks appropriately.

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

Answer: No

Recommendation: Implement strict access control mechanisms to prevent unauthorized access.

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

Answer: Yes, with cybersecurity measures included

Recommendation: Continue enforcing strict access controls and review policies regularly.

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

Answer: Yes, within the first month

Recommendation: Continue regular security awareness training and phishing simulations.

Q33: Do you regularly communicate cybersecurity updates to employees?

Answer: No

Recommendation: Develop a mandatory security training program to educate employees on risks.

Q34: Do employees report phishing attempts and suspicious emails?

Answer: Yes, but voluntary

Recommendation: Increase training frequency and introduce interactive security awareness programs.

Q35: Do you provide training on safe browsing practices?

Answer: Yes, regularly

Recommendation: Continue regular security awareness training and phishing simulations.

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

Answer: No

Recommendation: Develop and implement an incident response plan to minimize downtime.

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

Answer: Yes, but without detailed analysis

Recommendation: Expand and formalize the incident response plan with clear response actions.

Q38: Do you ensure that vendors have cybersecurity insurance?

Answer: No

Recommendation: Implement a vendor risk management program to evaluate third-party security.

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

Answer: Yes, but loosely followed

Recommendation: Expand encryption and data protection measures to cover all critical information.

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

Answer: No

Recommendation: Develop formal security policies and ensure organization-wide enforcement.

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

Answer: Partially enforced

Recommendation: Enhance access control measures by implementing multi-factor authentication.

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

Answer: Partially implemented

Recommendation: Expand encryption and data protection measures to cover all critical information.

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

Answer: Yes, with real-time updates

Recommendation: Regularly review and update network security configurations and segment

networks appropriately.

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

Answer: Yes, quarterly or more frequently

Recommendation: Continue regular security awareness training and phishing simulations.

Q45: Do you test your backup restoration process regularly?

Answer: Yes, at least annually

Recommendation: Test and refine the incident response plan regularly to improve effectiveness.

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

Answer: Yes, but infrequently

Recommendation: Enhance governance measures by aligning with industry best practices.

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

Answer: Yes, but without compliance checks

Recommendation: Strengthen vendor security assessments and require compliance documentation.

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

Answer: Yes, regularly

Recommendation: Continue regular security awareness training and phishing simulations.

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

Answer: Yes, but only once during adoption

Recommendation: Strengthen network security by adding additional monitoring and segmentation controls.

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

Answer: Yes, integrated with response tools

Recommendation: Test and refine the incident response plan regularly to improve effectiveness.