Cybersecurity Diagnostic Report

Overall Score:

195/500 (39.0%)

Category Breakdown:

Access Control: 40/70 (57.14%)

Asset Management: 5/10 (50.0%)

Business Continuity: 0/10 (0.0%)

Compliance: 5/10 (50.0%)

Data Protection: 40/70 (57.14%)

Employee Awareness and Training: 20/70 (28.57%)

Governance and Policies: 20/70 (28.57%)

Incident Response: 0/10 (0.0%)

Incident Response and Recovery: 30/40 (75.0%)

Network Security: 25/90 (27.78%)

Risk Management: 5/10 (50.0%)

Security Awareness: 5/10 (50.0%)

Third-Party Risk Management: 0/30 (0.0%)

Recommendations:

Focus on strengthening key areas: Governance and Policies, Network Security, Incident Response, Business Continuity, Third-Party Risk Management, Employee Awareness and Training.

Suggested Tools for Improvement:

Employee Awareness and Training: KnowBe4, Infosec IQ

Governance and Policies: NIST Cybersecurity Framework, CIS Controls

Network Security: Snort, Wireshark

Third-Party Risk Management: OneTrust, Prevalent

Answers Summary:

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

Answer: In Progress

Recommendation: Complete the development of your cybersecurity policy and seek expert validation.

Q2: Has your organization conducted a formal risk assessment in the past year?

Answer: In Progress

Recommendation: Ensure the ongoing risk assessment covers all critical business areas.

Q3: Are all company assets inventoried and categorized?

Answer: In Progress

Recommendation: Finalize the implementation of security measures and conduct validation tests.

Q4: Is multi-factor authentication (MFA) required for accessing critical systems?

Answer: Yes

Recommendation: Maintain adherence to best practices and continuously improve security controls.

Q5: Do you have a documented incident response plan?

Answer: No

Recommendation: Develop a formal incident response plan with clear roles and escalation procedures.

Q6: Has your organization conducted a business impact analysis?

Answer: No

Recommendation: Implement the necessary security measures to mitigate potential vulnerabilities.

Q7: Do employees receive regular cybersecurity awareness training?

Answer: No

Recommendation: Implement a mandatory security awareness program for all employees.

Q8: Are backups performed regularly and tested for integrity?

Answer: In Progress

Recommendation: Finalize the backup process and verify its effectiveness in a simulated scenario.

Q9: Do you comply with GDPR, ISO 27001, or other relevant data protection regulations?

Answer: Yes

Recommendation: Maintain adherence to best practices and continuously improve security controls.

Q10: Do you have an access control policy defining user roles and privileges?

Answer: In Progress

Recommendation: Complete the development of your cybersecurity policy and seek expert validation.

Q11: Do you maintain a log of all user access to critical systems?

Answer: Yes, with regular audits

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

Q12: 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.

Q13: Do you block unauthorized devices from accessing your network?

Answer: No

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

Q14: Do you conduct third-party audits of your cybersecurity program?

Answer: Yes, but infrequently

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

Q15: Do you restrict access to sensitive data based on employee roles?

Answer: Partially enforced

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

Q16: Do you regularly review and update your cybersecurity policies?

Answer: Yes, but less frequently

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

Q17: Are administrative privileges restricted to essential personnel?

Answer: Yes, strictly enforced

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

Q18: 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.

Q19: Do you have a firewall installed and configured on your network?

Answer: Not Sure

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

Q20: Do you use Virtual Private Networks (VPNs) for remote access?

Answer: Yes, but without MFA

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

Q21: Do you segment your network to isolate sensitive data?

Answer: No

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

Q22: Do you allocate a specific budget for cybersecurity initiatives?

Answer: No

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

Q23: Do you monitor network traffic for suspicious activities?

Answer: No

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

Q24: 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.

Q25: Do you have automated tools to detect and respond to security incidents?

Answer: Yes, fully automated

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

Q26: Are login attempts monitored for suspicious activity?

Answer: Yes, real-time monitoring

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

Q27: Do you conduct phishing simulation exercises?

Answer: No

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

Q28: Do you train employees on securely using mobile and personal devices for work?

Answer: Yes, but infrequently

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

Q29: Is sensitive data encrypted in transit?

Answer: No

Recommendation: Implement encryption and data loss prevention tools to safeguard sensitive data.

Q30: Do all employees have unique login credentials?

Answer: No, shared accounts are used

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

Q31: Are regular backups of critical data performed?

Answer: Yes, with offsite storage

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

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

Answer: No

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

Q33: Do you provide training on safe browsing practices?

Answer: No

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

Q34: 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.

Q35: Are cybersecurity roles and responsibilities clearly defined within your organization?

Answer: Yes, but informal

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

Q36: Do employees report phishing attempts and suspicious emails?

Answer: Yes, with mandatory reporting

Recommendation: Continue regular security awareness training and phishing simulations.

Q37: Do you regularly communicate cybersecurity updates to employees?

Answer: No

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

Q38: Do you use intrusion detection and prevention systems (IDS/IPS)?

Answer: No

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

Q39: Are accounts of terminated employees promptly deactivated?

Answer: No

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

Q40: Do you maintain a log of all security incidents and breaches?

Answer: No

Recommendation: Develop and implement an incident response plan to minimize

downtime.

Q41: Do you perform annual cybersecurity risk assessments?

Answer: No

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

Q42: Do you require vendors to follow data protection regulations (e.g., GDPR, HIPAA)?

Answer: No

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

Q43: Do you conduct regular incident response training exercises?

Answer: Yes, annually or more frequently

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

Q44: Do you have a cybersecurity awareness program in place for employees?

Answer: No

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

Q45: Do you enforce a data retention and deletion policy?

Answer: Yes, strictly enforced

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

Q46: Do you ensure that vendors have cybersecurity insurance?

Answer: No

Recommendation: Implement a vendor risk management program to evaluate

third-party security.

Q47: Do you implement role-based access controls (RBAC)?

Answer: Partially implemented

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

Q48: Do you provide ongoing training on identifying and preventing phishing attacks?

Answer: Yes, annually

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

Q49: Is multi-factor authentication (MFA) enabled for all critical systems?

Answer: No

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

Q50: 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.