Marshall Creative Cybersecurity Action Plan

Objective: Ensure the ongoing resilience of Marshall Creative's digital infrastructure by implementing a comprehensive cybersecurity action plan. This plan is designed to address potential threats, vulnerabilities, and enhance the overall cybersecurity posture of the organization.

1. Cybersecurity Risk Assessment (Timeline: Month 1-2)

- Conduct a thorough cybersecurity risk assessment to identify and evaluate potential threats and vulnerabilities.
- Prioritize risks based on impact and likelihood.
- Develop a risk mitigation strategy outlining specific actions and timelines.

2. Network Security Enhancement (Timeline: Month 3-4)

- Implement and configure robust firewall solutions to monitor and control incoming and outgoing network traffic.
- Deploy intrusion detection and prevention systems to detect and respond to malicious activities.
- Conduct regular network security audits to ensure the effectiveness of implemented measures.

3. Endpoint Security Measures (Timeline: Month 5-6)

- Implement advanced endpoint protection solutions to safeguard computers, mobile devices, and other endpoints.
- Enforce encryption on all endpoints to protect sensitive data.
- Regularly update and patch all endpoints to address vulnerabilities.

4. User Authentication and Access Controls (Timeline: Month 7-8)

- Enhance user authentication mechanisms with multi-factor authentication.
- Conduct a review and update access controls to ensure that employees have the minimum necessary access privileges.
- Educate employees on the importance of strong password management.

5. Incident Response Plan Development (Timeline: Month 9-10)

- Develop a comprehensive incident response plan outlining procedures for reporting, containment, eradication, recovery, and communication.
- Conduct training sessions for key personnel involved in incident response.
- Regularly review and update the incident response plan based on lessons learned and emerging threats.

6. Employee Training and Awareness (Timeline: Ongoing)

- Implement regular cybersecurity training programs for all employees.
- Raise awareness about social engineering tactics, phishing attacks, and other common cybersecurity threats.
- Encourage a culture of cybersecurity responsibility among employees.

7. Encryption Implementation (Timeline: Month 11-12)

- Implement encryption protocols for sensitive data in transit and at rest.
- Ensure that encryption is applied to data stored on servers, databases, and transmitted over internal and external networks.
- Regularly review and update encryption protocols based on industry standards.

8. Regular Security Audits and Assessments (Timeline: Ongoing)

- Conduct regular security audits and assessments to identify vulnerabilities.
- Assess the effectiveness of existing security controls and make improvements based on findings.
- Engage third-party cybersecurity experts for independent assessments.

9. Secure Software Development Practices (Timeline: Ongoing)

- Integrate secure coding practices into the software development lifecycle.
- Conduct regular code reviews to identify and address security vulnerabilities.
- Provide training to developers on secure coding practices and emerging threats.

10. Vendor Security Management (Timeline: Ongoing)

- Establish and enforce cybersecurity requirements for third-party vendors.
- Regularly assess and monitor vendors' security practices.
- Update vendor contracts to include cybersecurity provisions.

11. Continuous Monitoring and Improvement (Timeline: Ongoing)

- Implement continuous monitoring tools for real-time threat detection.
- Regularly update and improve security measures based on emerging threats and technologies.
- Stay informed about industry best practices and incorporate them into the cybersecurity strategy.

12. Review and Revision (Timeline: Annually)

- Conduct an annual review of the cybersecurity action plan.
- Revise and update the plan based on changes in cybersecurity threats, regulations, and organizational needs.
- Ensure that all stakeholders are informed and trained on any updates to the cybersecurity strategy.

This Cybersecurity Action Plan outlines specific steps and timelines for enhancing Marshall Creative's cybersecurity posture. Regular monitoring, training, and updates will be crucial in adapting to the dynamic nature of cybersecurity threats and ensuring the organization's overall resilience.

Signed
Darren Marshall [DIRETCTOR]

21st Jan 2024