Risk Assessment Report for Kulture Reimagined Consulting

Kulture Reimagined Consulting has experienced significant growth, expanding its client base and increasing its digital presence. The company handles sensitive client data, including personal details, payment information, and proprietary intellectual property related to trainings, documents, and client interactions.

The growing workforce, now with a small team of contractors and collaborators, uses a variety of devices to access company systems and work remotely. An emerging concern is that some employees may use personal devices for work, potentially introducing vulnerabilities into the company's network.

Given the rising complexity of cyber threats, Kulture Reimagined is increasingly exposed to risks such as phishing, ransomware, and data breaches. A breach of client information or intellectual property could damage the company's reputation and financial stability, jeopardizing client trust.

Potential Threats:

1. Employees bringing personal devices to the workplace or using company's systems remotely
2. Data breaches involving client or proprietary information
3. Phishing, ransomware, DDoS attacks
4. Disgruntled contractors or collaborators potentially causing internal harm

Evaluate Risks:

1. High concern: Employees using personal devices for work and accessing company systems remotely
2. High concern: Data breaches, including leaks of sensitive client data
3. High concern: Phishing, ransomware, DDoS attacks
4. Medium Concern: Disgruntled contractors or collaborators creating internal threats

Countermeasures for Risks

1. Identity Management & Active Directory
    A. Use an AI tool to track unusual behavior on the network
    B. Implement group policies to define access levels for different roles
2. Zero Trust Model (All users must be authenticated before accessing company systems)
3. Network segmentation
    - Separate networks for personal devices and sensitive business operations
4. Regular Security Awareness training for contractors, collaborators, and employees.

Comprehensive Data Protection

1. Obtain consent from clients to utilize their data
2. Ensure regular security updates and patch management

3. Implement Multi-Factor Authentication (MFA) and biometric security strategies
4. Use email filtering and anti-malware software to block phishing attempts
5. Create robust response protocols for potential data breaches

Personal Device Policy

1. Require that personal devices use a separate network from company systems
2. Employees and contractors must agree to an Acceptable Use Technology Policy

MFA and biometric security strategy

Incident Response Strategy

1. Establish a response team and update protocols regularly
2. Isolate impacted devices on the network during an incident
3. Implement enhanced endpoint security and access control policies
4. Ensure regular reviews of incident response strategies and training for all team members

Continuous Monitoring and Mitigation Plan

1. Perform regular security audits
2. Provide ongoing employee and contractor training on cybersecurity threats
3. Conduct periodic reviews of security standards, guidelines, and policies