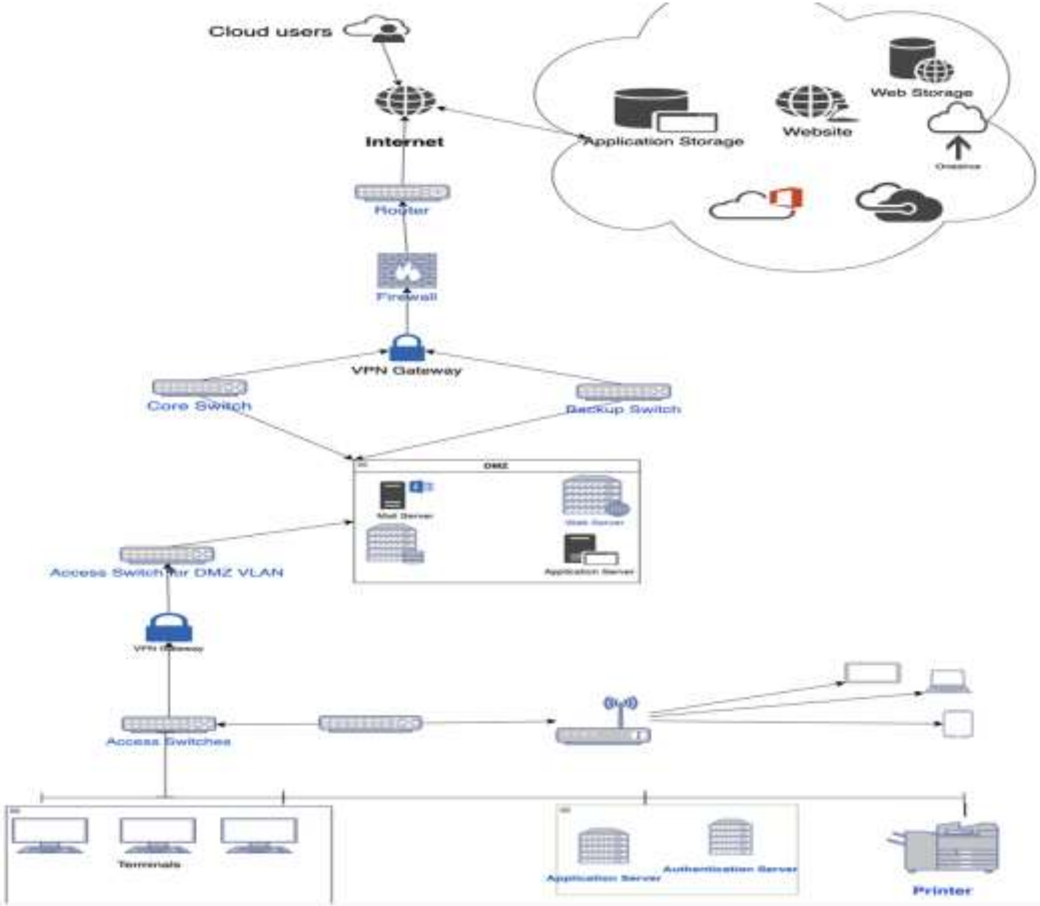
Cybersecurity Risk Assessment and Mitigation Strategies for Jones & Davis

By Oyindamola Olayiwola

Executive Summary

This cybersecurity risk assessment for Jones & Davis, following the acquisition of Garden City Wealth Management, identifies critical threats including data breaches, denial-of-service (DoS) attacks, service downtime, supply chain attacks, ransomware attacks, credential theft, SQL injection, and cross-site scripting. Mitigation strategies include implementing robust access controls and encryption for data breaches, deploying DDoS protection and redundancy for DoS attacks, establishing incident response and recovery plans for service downtime, conducting thorough vetting of third-party vendors for supply chain attacks, regularly backing up data and maintaining updated security software for ransomware attacks, using multi-factor authentication and strong password policies for credential theft, employing parameterized queries for SQL injection, and sanitizing user inputs for cross-site scripting. A well-developed incident response plan and comprehensive business continuity plan are essential for maintaining operations during disruptions. Continuous monitoring and regular updates will ensure resilience against evolving cybersecurity threats.

Network and Data Security



Identifying and Vulnerabilities Critical Assets

- Customer Data : Weak Access Controls, Unencrypted Data Misconfigures Cloud Storage
- Databases :Improper input Sanitation, Database SecurityWeak Database Security Configuration
- Application Code : Improper Input Handling, Broken Access Control
- Third Party Systems: unpatched systems, lack of Vendor Management, Lack of Security controls in Third-party APIs
- Monitoring Tool: Weak Detection Algorithms, Insufficient loggings , lack of log integrity, lack of tamperproof monitoring
- Backup System: Unsecured backup, inadequate backup encryption and lack of redundancy

Threat Landscape

Data Breach

Identity Theft

Credential Theft

Brute force Attacks

SQL Injection

Database Compromise

Cross-site Scripting

Vendor Lock-in

Application Logic Flaws

Man-in-the-Middle Attacks

Supply Chain Attacks

Ransomware Attacks

Backup data Corruption

Regulation Non Compliance

Information Leakage of Compliance Information

Lack of in house Expertise

Infringement

Quantifying and Prioritizing Risks

Risk	Likelihood	Impact	Risk rating
Data breaches	4	5	20
Denial-of-service (DoS) attacks	5	5	25
Service Downtime	4	5	20
Supply Chain Attacks	4	5	20
Ransomware Attacks	5	5	25
Credential Theft	4	5	20
SQL Injection	4	5	20
Cross-site Scripting	4	5	20

13 – 25 (High): High-rating risks are serious and very likely to happen threats.

Strategies to Counter Top Cybersecurity Risks

Data Breach

Strong Access control limit unauthorized access to sensitive data.

Encrypt data both in transit and at rest protect it from unauthorized access.

Data loss Prevention solutions to prevent unauthorized data exfiltration.

Multi Factor Authentication(MFA)for access to sensitive systems and data

Implement endpoint data security solutions

Patch systems and ensure basic security hygiene

DOS Attack

Implement blackhole routing preventing malicious trafic from reaching target systems

Implement rate limiting to Limit the number of requests that can be processed from a single IP address or network within a specific time frame.

Ensure continuous monitoring of network trafficto detect unusual traffic patterns or spikes that may indicate a DoS attack.

Implement anycast network diffusion to distribute traffic across multiple point without overwhelming a single point

Create backup of critical information and data.

Have a recovery plan for critical system based on tolerable downtime.

Strategies to Counter Top Cybersecurity Risks

Supply chain Attacks

Implement Strong Access control limit unauthorized access to sensitive data.

Implement strong Network segmentation to isolate sensitive data

Implement robust vendor risk Management process.

Priortorize testing new update in isolated environment before deploying them to production networks

incorporate security practices into your DevSecOps processes to address security issues early in the process.

Ransomware Attacks

Set Up Multi-Factor Authentication (MFA) for Your Accounts

Establish Password Management Guidelines.

Backup All of Your Company Data Regularly.

Update and Patch Your Software Frequently.

Add Tamper Protection for All of Your Corporate Devices.

Deploy endpoint protection solutions.

Develop an Incident response plan, test the plan and establish communication plan about the steps to be taken in case of a ransomware attack.

Employee Education and Awareness .

Current Network Infrastructure

1. Network Devices: Firewalls, Routers Load Balancers, Intrusion Detection/Prevention Systems, VPN Gateways

2. Systems: Web Servers, Database Servers, Application Servers, Backup Servers, Authentication Systems

3. Software: Operating Systems, Mobile Application, Web Application Software, Anti-Virus / Anti-Malware, Vulnerability Scanners, Penetration Testing Tools (e.g., Metasploit, Burp Suite),Database Management Software

4. Cloud Services: Cloud Storage (e.g., OneDrive), SaaS Solutions (e.g., Salesforce), Cloud Identity Management (e.g., Azure Active Directory)

5. Endpoints: laptops, desktops, mobile devices and POS

Vulnerability Assessment of Critical Systems

1. Network Device Vulnerabilities:Misconfigured firewalls or routers, weak access control (e.g., default credentials on devices), unpatched firmware.

2. System Vulnerabilities: SQL injection, weak password policies, unencrypted databases, poor access control, and insecure APIs.

3. Data Vulnerabilities: Unencrypted data in transit or at rest, poorly defined access controls, lack of log analysis.

4. Software Vulnerabilities: Unpatched operating systems, vulnerable web applications (SQLi, XSS), poor session management.

5. Cloud Service Vulnerabilities: Misconfigured permissions in cloud storage (OneDrive), insecure APIs in SaaS solutions, lack of encryption.

6. Endpoint Vulnerabilities: Lack of endpoint protection, unpatched devices, and insecure POS systems.

Security Controls for Critical Infrastructure

Network Device

Configuration Management: Regularly review and update configurations to ensure they follow security best practices.

Access Controls: Implement strong access control policies, including the use of complex passwords and disabling default credentials.

Regular Patching: Establish a routine for updating firmware and software on all network devices to mitigate known vulnerabilities.

Network Segmentation: Use VLANs to separate sensitive data and systems from general network traffic to reduce lateral movement.

Application

Web Application Firewalls (WAF): Deploy WAFs to protect web applications from common attacks like SQL injection and XSS.

Input Validation: Ensure robust input validation and sanitization processes are in place to prevent injection attacks.

Encryption: Use strong encryption methods for sensitive data stored in databases and transmitted over the network.

User Training: Provide training for users on strong password practices and the importance of account security.

Security Controls for Critical Infrastructure

Software Security Controls

Patch Management: Regularly update software and applications to address vulnerabilities.

Security Testing: Perform regular security testing (e.g., penetration testing and vulnerability assessments) on applications.

Secure Coding Practices: Adopt secure coding guidelines to minimize vulnerabilities during application development.

Session Management: Implement secure session management practices, including timeout features and secure cookie handling.

Systems

Identity and Access Management (IAM): Use IAM tools to enforce least privilege access policies for cloud services.

Encryption: Ensure data stored in cloud services is encrypted and access is controlled.

Monitoring and Logging: Implement monitoring and logging of access to cloud resources to detect and respond to suspicious activity.

Shared Responsibility Model: Understand and implement security controls based on the shared responsibility model for cloud services.

Third Party Risk Management :

Microsoft Azure: Data Breach, Misconfiguration, Vendor Lock In

OneDrive: Insecure File Sharing, Data loss, failure to comply with regulatory standard

Salesforce: API Vulnerability leading to unauthorised access, Inadequate Access Control Leading to data exposure, Vulnerabilities in system leading to data exposure during integration

Office 365:Phishing Attacks on targeted users to gain access to their information, Account compromise, insufficient endpoint security

Continuity Strategy and Backup Plan

Risk Assessment Results

Key Risk:

- Regulatory Non-Compliance
- Employee Resistance
- Data breaches
- Denial-of-service (DoS) attacks
- Service Downtime
- Supply Chain Attacks
- Credential Theft
- SQL Injection
- Cross-site Scripting

Critical Operations:

- Account Management ,Transaction Processing

Financial Impact:

- Potential losses from downtime/data breaches

Customer Impact:

- Risk of dissatisfaction and attrition

Business Continuity Strategy

Proactive Planning:

- Risk Mitigation: Making changes step by step helps manage risks and fix issues as they come up.
- Resource Allocation: This approach ensures that resources are used effectively and support is available when needed.
- Testing and Feedback: Each phase acts as a test for the next one, allowing the team to gather feedback and improve processes.
- Change Management: Gradual changes help employees and customers adapt easily, reducing resistance.
- Continuous Improvement: Lessons learned in earlier phases help improve future phases, creating a culture of adaptability.

Redundancy:

- Establish Backup systems/processes to ensure operational continuity

Cross-Training:

- Train staff on legacy and new systems to enhance flexibility and resource availablilty

Backup and Recovery Plan

Data Backup Procedures:

- Daily Backups: Conduct daily backups to secure offsite locations.
- Types: Full and incremental backups with encryption and access controls.

Data Restoration:

- Regularly test backup restorations to ensure reliable recovery.
- Maintain documentation of restoration processes.

Retention Policy:

- Define how long backups are kept to comply with regulations.
- Schedule reviews to purge outdated backups.

Roles and Responsibilities:

- Assign staff roles for managing backups and recovery efforts.

Monitoring and Maintenance:

- Monitor backup success and update configurations as needed.

Communication Plan:

- Inform stakeholders about backup status and recovery efforts.

Thank you