Threat Modeling Report

Drafted by

Oyindamola Olayiwola

15th October, 2024.

Executive Summary

This Threat Modeling Report analyzes potential security threats related to the acquisition of Garden City Wealth Management by Jones & Davis, employing the STRIDE framework to identify and categorize threats such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. A Data Flow Diagram (DFD) illustrates data movement across critical systems, facilitating the identification of vulnerabilities.

Identified Systems:

- Jones & Davis: Web portal, mobile banking app, ATM network, OneDrive, Office 365, Salesforce, Azure infrastructure.
- Garden City Wealth Management: Web portal for investment services, potential mobile app, Azure infrastructure, Office 365, Salesforce.

Key Processes:

Customer account management, transaction processing, data storage, communication, and security monitoring were identified as critical operational processes.

Threat Analysis:

Each system was evaluated for threats, focusing on tampering and information disclosure risks. Mitigation strategies include implementing Multi-Factor Authentication (MFA), robust data integrity checks, and strict Role-Based Access Control (RBAC).

Recommendations:

1. Mitigate Data Tampering and Information Disclosure: Enhance data integrity checks and encrypt sensitive information.
2. Strengthen Authentication: Enforce MFA and RBAC to limit access.
3. Enhance Network Security: Implement DDoS protection and network segmentation.
4. Secure Software Development: Conduct regular code reviews and security testing.
5. Improve Security Awareness: Provide ongoing training for employees.
6. Conduct Regular Audits: Establish routine internal audits and consider third-party assessments.
7. Utilize Cloud Security Solutions: Implement Cloud Security Posture Management (CSPM) tools and Cloud Access Security Brokers (CASBs).

Threat Modeling Overview

In this report, we will conduct an in-depth examination of the threat model used in the acquisition of Garden City Wealth Management by Jones & Davis. The methodology employed for this analysis is STRIDE, a framework designed to identify and categorize potential threats to systems and applications based on six distinct threat types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. To effectively apply the STRIDE methodology, we first identified the critical systems and applications involved in the integration process. A Data Flow Diagram (DFD) was created to visualize how data moves through these systems, facilitating a better understanding of potential vulnerabilities and threat vectors.

Identified Systems and Applications

Jones & Davis:

Customer-facing Systems:

- Web portal for online banking
- Mobile banking app
- ATM network (partnered)

Internal Systems:

- OneDrive (Azure) for data storage
- Office 365 for productivity and email
- Salesforce CRM
- Slack and Outlook for communication
- Webex for video conferencing
- Azure cloud infrastructure (public and private)
- In-house cybersecurity monitoring tools and infrastructure

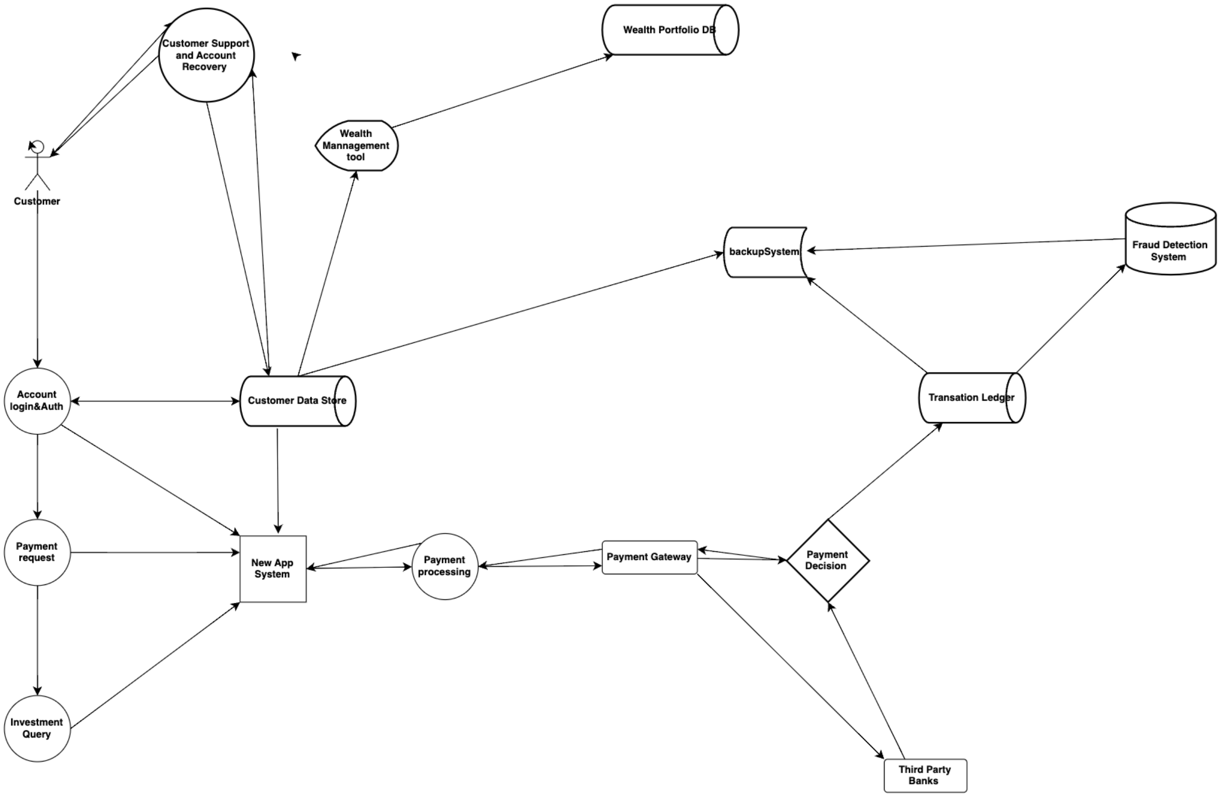
Garden City Wealth Management:

- Customer-facing Systems:
- Web portal for investment services
- Mobile investment app (potential)

Internal Systems:

- Azure cloud infrastructure
- Office 365 for productivity and email
- Salesforce CRM
- Outlook and Microsoft Teams for communication
- Third-party cybersecurity monitoring tools and infrastructure

Data Flow Diagram



Data Flow Diagram

Key Processes:

- Customer Account Management: Systems for managing customer accounts, KYC (Know Your Customer) information, transaction history, and balances.
- Transaction Processing: Systems for processing various financial transactions, including payments, transfers, and investments.
- Data Storage and Management: Databases and systems for storing and managing sensitive customer data, financial records, and transaction logs.
- Communication and Collaboration: Tools for internal and external communication, including email, messaging, and video conferencing.
- Security Monitoring and Incident Response: Systems for detecting, analyzing, and responding to security threats and incidents.

Office 365 for productivity and email(Garden City Wealth Management)

No	Type	Priority	Status	Score	Description	Mitigation
1	Spoofing	Medium	Mitigated	6	Attackers may spoof user identities to gain unauthorized access to customer data.	MFA, Strong Password Policies
2	Tampering	High	Ongoing	8	Unauthorized changes to customer data, potentially leading to data corruption or manipulation.	RBAC, Data Integrity Check
3	Repudiation	low	Mitigated	2	Attacker could deny performing suspicious transactions if logs or detection records are tampered with.	
4	Information Disclosure	low	Mitigated	0	Sensitive customer data could be exposed due to weak access controls or phishing attacks.	Encrypt data both at rest and in transit using AES-256. Conduct regular security awareness training.
5	Denial of Service	low	Ongoing	5	Encrypt data both at rest and in transit using AES-256. Conduct regular security awareness training.	Use DDOS protection, Implement Failover Mechanism
6	Elevation of Privilege	low	Mitigated	0	Insufficient role-based access controls (RBAC) could allow users to access sensitive data.	Enforce RBAC with least privilege principles. Regularly audit privileges.

Web portal for investment services (Garden City Wealth Management)

No	Type	Priority	Status	Score	Description	Mitigation
1	Spoofing	medium	Ongoing	6	Attackers may impersonate users to manipulate portfolios or execute unauthorized trades.	MFA, Session Management, Input validation Cross-siste Scripting protection, User Education, token-Based Authentication, oken-Based Authentication, Use Secure protocol Such as HTTPs
2	Tampering	High			Unauthorized changes to financial data or portfolio records may result in financial losses.	Data Validation, Access restriction, input sanitization & validation,
3	Repudiation	Medium	Mitigated	0	Attacker could deny performing suspicious transactions if logs or detection records are tampered with.	Encryption, Strict Access Control , Hashing verification
4	Information Disclosure(ID)	low	Mitigated	0	Sensitive portfolio data could be exposed to unauthorized users.	encryption, Enforce strong access controls.
5	Denial of Service	High	Mitigated	8	Disruption of platform availability through DDoS attacks.	Deploy DDoS protection and ensure redundancy for service availability.
6	Elevation of Privilege	High	Mitigated		Attacker gaining elevated privileges to access portfolios.	Enforce Princiciple of lease privilege,Strong Authentication(MFA, complex password), RBAC,

Azure cloud infrastructure (Garden City Wealth Management)

No	Type	Priority	Status	Score	Description	Mitigation
1	Spoofing	High	Open	8	Attackers could impersonate legitimate users to access cloud resources and data.	MFA , Employ analytics to detect unusual login pattern, Implement Identity and Access Management (IAM)
2	Tampering	High	Open	8	Cloud-stored data or configurations could be tampered with, leading to service disruption or data compromise.	Data Integrity Checks, Implement strict configuration management, Monitoring and Alerts
3	Repudiation	Medium	Open	6	Attackers could impersonate legitimate users to access cloud resources and data.	Comprehensive Logging, Audit Trails, Audit Trails, Digital Signature
4	Information Disclosure	High	Open	9	Sensitive cloud data could be exposed due to misconfigurations or access control failures.	Implement strict access controls, Data Encryption, Regular Security Audits, DLP
5	Denial of Service	High	Open	7	A DDoS attack on the cloud infrastructure could render services and applications unavailable.	DDoS Protection, Implement load balancing, Use Azure's scalable infrastructure, Content Delivery Network to distribute traffic
6	Elevation of Privilege	Hifh	Open	8	Attackers gaining elevated privileges could control all cloud resources, potentially leading to a full system compromise.	Enforce the principle of least privilege, Use PAM solutions, Conduct regular audits of user privileges, Implement privileged access management (PAM) solutions

Mobile investment app

No	Type	Priority	Status	Score	Description	Mitigation
1	Spoofing	High	Open	8	An attacker could Impersonate a legitimate user and manipulate account information leading to financial loss	Strong Authentication susch as MFA, Device Fingerprinting, Behavioral analytics
2	Tampering	High	Open	9	An attacker could Tamper with the app code or data to manipulate Investment or steal sensitive Information	Encryption, Code Signing and Integrity Checks
3	Repudiation	Medium	Open	6	An attacker could deny responsibility for unauthorized actions, making it difficult to hold them accountable.	logging and monitoring, Maintain audit trails, digital signatures
4	Information Disclosure	High	Open	8	An attacker could gain unauthorized access to sensitive user data, such as financial information or investment strategies.	Encrypt sensitive data, strong access controls ,
5	Denial of Service	Medium	Open	6	An attacker could overload the app's servers or network to prevent legitimate users from accessing the service.	rate limiting, DDoS protection, Network Monitoring.
6	Elevation of Privilege	High	Open	8	An attacker could exploit vulnerabilities to gain unauthorized access to privileged functions or data.	RBAC, patch and update the app, regular security audits

Salesforce CRM(Jones & Davis)

No.	Type	Priority	Status	Score	Description	Mitigation
	Spoofing	High	Open	7	Attackers may impersonate legitimate payment gateways to steal payment data.	MFA, User Access Control, field Level security and Data vALIDATION , Data Encryption, User Access Control
	Tampering	High	Open	8	Tampering with payment data may result in unauthorized or fraudulent transactions.	MFA, User Access Control(RBAC), Encryption, Data Validation & Integrity Check, Education & Training
	Repudiation	Medium	Open	5	Attacker could deny performing suspicious transactions if logs or detection records are tampered with.	Enable Audit Trails, MFA, Digital Signatures, Transaction and Login History Logs, Data Encryption and Secure Communication, Strong Access Controls, Data Integrity Checks
	Information Disclosure	High	Open	8	unintended or unauthorized exposure of sensitive, confidential, or proprietary data to individuals or entities who should not have access to it.	Data Encryption, User Access Control(MFA, RBAC, Session Timeout Settings), DLP, User Education and Awareness, Backup and Data Recovery
	Denial of Service	Medium	Open	8	DoS attacks may disrupt payment processing, affecting customer transactions and revenue.	Rate Limiting, User Authentication and Access Control, DDoS Protection(such as WAF),Backup and Recovery Plans
	Elevation of Privilege	High	Open	8	A compromised payment processing account could allow an attacker to initiate fraudulent transactions on a large scale.	Implement principle least-privilege, enforce privilege access management control

OneDrive (Azure) for data storage (Johns&Davis)

No.	Type	Priority	Status	Score	Description	Mitigation
1	Spoofing	High	Open	8	Attackers could spoof backup servers or users to gain access to stored backups.	MFA, RBAC, Strong Password Policies
2	Tampering	hIGH	Open	8	Unauthorized changes to backup data could lead to corrupted or incomplete restorations.	Input Validation, Encryption, Access control(least privilege, MFA, IAM), Data integrity Checks , versioning and immutable storage,DLP, Secure API Access, Regular pATCHING AND update
3	Repudiation	Medium	Open	6	Without proper logging, users could deny modifying or deleting backup data.	Maintain tamper- proof log , Digital Signature, MFA, Timestamping and Hashing, Encryption
4	Information Disclosure	High	Open	9	Sensitive backup data could be exposed if not properly encrypted or secured.	Data Encryption, Access Control, Data masking and Tokenization,DLP,
5	Denial of Service	High	Open	7	A DoS attack could disrupt access to backup data, delaying recovery efforts.	Implement Failover backup solution, Geographically redundant backups, Backup and Redundancy, Secure API Endpoints, Content Delivery Network (CDN), Rate Limiting, Load Balancing, Implement WAF, ddos Protection Services
6	Elevation of Privilege	High	Open	8	Attackers with elevated access could modify or delete backups, preventing data recovery.	Least Privilege Principle, MFA,Implement Strong Password Policies,

ATM network (partnered)(Jones & Davis)

Number	Type	Priority	Status	Score	Description	Mitigation
1	Spoofing	High	Open	9	Attackers can disguise their identity or mimic legitimate devices to gain unauthorized access.	MFA, Strong Authentication, Secure protocol such as HTTPS, End -End Encryption Physical Security Measures susch as Tamper proof Hardware and Surveillance User Education
2	Tampering	High	Open	8	Physical or software modifications can compromise ATM functionality and security.	Tamper-Evident Seals, Encryption, Access Controls, VPNs or secure protocols, Transaction Monitoring, Customer Awareness
3	Repudiation	medium	Open	7	Parties involved in transactions may deny their involvement, leading to disputes.	MFA, Transaction Logging, regular audits of transaction logs, Encryption,User Awareness
4	Information Disclosure	High	Open	10	Sensitive customer data can be exposed due to vulnerabilities or attacks.	Encryption , Data Minimization, RBAC, Authentication, software update Logging and Monitoring
5	Denial of Service	Medium	Open	5	Attacks can disrupt ATM operations and prevent legitimate access.	Segmentation and Redundancy , Intrusion Prevention system, Rate Limitingm Monitoring and Alert
6	Elevation of Privilege	Medium	Open	6	Attackers can gain unauthorized access to privileged accounts or systems.	MFA, RBAC, Secure Software Development, Monitoring and logging, Firewal and IDS

Web portal for online banking (Johnes & Davis)

Number	Type	Priority	Status	Score	Description	Mitigation
1	Spoofing	High	Open	9	Attackers could impersonate users or systems to manipulate transaction records.	MFA , Implement Digital Signature, RBAC
2	Tampering	High	Open	8	Transaction data could be altered, leading to financial discrepancies and fraud.	Data Integrity checks, maintain audit logss, Non-Repudiation Controls such as digital Signature
3	Repudiation	Medium	Open	7	Without secure logs, users or attackers could deny fraudulent transactions or changes made to the ledger. logging and verification mechanisms are not in place.	Non-Repudiation Controls such as digital Signature, comprehensive log
4	Information Disclosure	High	Open	10	Transaction data could be exposed to unauthorized entities, compromising customer privacy.	Data Encrypption, Enforce strict access controls, Data Maskng
5	Denial of Service	Medium	Open	6	Attacks on the ledger could prevent users from accessing transaction records, affecting financial operations.	Use DDoS mitigation services, Implement redundancy and failover systems,Use caching mechanisms
6	Elevation of Privilege	High	Open	8	A privileged user could manipulate or erase transaction data, causing significant financial and operational issues.	Enforce least privilege principles, Implement Privileged Access Management (PAM), regular access audit

Recommendation

The provided information is a comprehensive threat assessment for various systems and applications within Garden City Wealth Management and Jones & Davis. Based on the identified threats, their priority, status, and proposed mitigations, I would recommend the following security improvements:

1. Prioritize Data Tampering and Information Disclosure:

- Data Tampering: Implement robust data integrity checks, regular backups, and version control to ensure the accuracy and integrity of data.
- Information Disclosure: Encrypt sensitive data both at rest and in transit, enforce strong access controls, and conduct regular security awareness training to prevent unauthorized access and data breaches.

2. Strengthen Authentication and Access Controls:

- Multi-Factor Authentication (MFA): Require MFA for all user accounts to enhance authentication and prevent unauthorized access.
- Role-Based Access Control (RBAC): Enforce strict RBAC policies to grant users only the minimum privileges necessary to perform their job functions.
- Regular Access Reviews: Conduct regular reviews of user privileges to ensure they remain appropriate.

3. Enhance Network Security:

- DDoS Protection: Implement DDoS protection measures to mitigate the risk of service disruptions.
- Network Segmentation: Segment networks to isolate critical systems and limit the spread of potential attacks.
- Firewall and Intrusion Detection Systems (IDS): Deploy firewalls and IDS to monitor network traffic and detect suspicious activity.

4. Implement Secure Software Development Practices:

- Code Reviews: Conduct regular code reviews to identify and address vulnerabilities.
- Security Testing: Perform security testing, including penetration testing, to identify weaknesses in applications and systems.
- Patch Management: Keep software and systems up-to-date with the latest security patches.

5. Improve Security Awareness and Training:

- Regular Training: Provide ongoing security awareness training to educate employees about best practices and potential threats.
- Phishing Simulations: Conduct phishing simulations to test employees' ability to identify and report suspicious emails.

6. Conduct Regular Security Audits and Assessments:

- Internal Audits: Conduct regular internal security audits to assess compliance with security policies and procedures.
- Third-Party Assessments: Consider engaging third-party security experts for independent assessments.

7. Consider Cloud-Based Security Solutions:

- Cloud Security Posture Management (CSPM): Utilize CSPM tools to monitor and manage cloud security posture.
- Cloud Access Security Broker (CASB): Deploy a CASB to control and monitor cloud access and data usage.

Conclusion

This Threat Modeling Report highlights key security threats related to the acquisition of Garden City Wealth Management by Jones & Davis, particularly focusing on tampering and information disclosure risks. While current security measures exist, enhancements are crucial to effectively address identified vulnerabilities.

Implementing strategies such as Multi-Factor Authentication (MFA), strict Role-Based Access Control (RBAC), and robust data integrity checks will protect sensitive information during integration. Strengthening these security protocols not only safeguards customer data but also ensures regulatory compliance and builds trust.

Ultimately, the recommendations provide a roadmap for mitigating risks and fostering a culture of security awareness, enabling Jones & Davis to successfully navigate the acquisition while enhancing its cybersecurity posture and positioning itself for future growth in the financial sector.