# Threat Modelling Exercise

Albion Trust Bank is a leading UK based financial institution specialising in secure digital banking services for individuals and businesses worldwide. The bank’s cybersecurity programme is overseen by Arthur Blake, Head of Information Security, who is responsible for ensuring the integrity, confidentiality and availability of Albion's critical financial systems.

## Objectives

The primary objective of this threat model is to identify, analyse and prioritise potential security threats to the bank’s digital services and infrastructure. By evaluating risks across the online and mobile banking platforms, this model aims to:

- Identify vulnerabilities that could be exploited by threat actors.
- Understand likely attack vectors.
- Assess the impact and likelihood of various threats.
- Propose effective mitigation strategies.
- Improve the overall security posture of the bank’s digital ecosystem.

## Scope

This threat model focuses on the bank’s customer facing digital banking systems and the core systems that support them, including:

- Online banking platform – Customer access via web browsers for account management, payments and financial activity.
- Mobile banking app – Native applications on iOS/Android used for the same services as the web platform.
- Payment processing system – Infrastructure that processes domestic and international transactions.
- Customer accounts and transactions – All associated data including balances, transfers and financial history.
- Core banking infrastructure – Authentication services, back-end databases and internal services supporting customer transactions.

## Assumptions

| Assumption | Justification |
|---|---|
| MFA is enforced for all user logins | Required under PSD2 |
| TLS is used for all communications | Industry standard |
| Backend systems are hosted in a secure private cloud | Common enterprise practice |
| Customer data is encrypted | Regulatory expectation |
| Admin access is role-based and monitored | Standard for financial institutions |

## Threat identification (STRIDE)

| Component | STRIDE Category | Threat |
|---|---|---|
| Login System | Spoofing | Attacker obtains a user’s credentials through a phishing email and logs in as them |
| API Gateway | Tampering | Attacker modifies transaction amount in API request using intercepted tokens |
| Transaction Logs | Repudiation | Customer denies making a transaction and logs are missing or incomplete |
| Database | Information Disclosure | SQL injection attack reveals other users' data |
| Web/Mobile App | Denial of Service | Automated bots flood the login form, making the system unresponsive |
| Admin Portal | Elevation of Privilege | Internal staff abuses misconfigured role to access restricted customer records |

## Risk Assessment (DREAD)

| Threat | D | R | E | A | D | Total | Risk Level |
|---|---|---|---|---|---|---|---|
| Phishing login credentials | 8 | 9 | 9 | 10 | 7 | 43 | High |
| API tampering with transaction amounts | 9 | 8 | 8 | 10 | 6 | 41 | High |
| Missing/incomplete transaction logs | 7 | 5 | 6 | 9 | 4 | 31 | Medium |
| SQL injection exposing user data | 10 | 8 | 8 | 9 | 7 | 42 | High |
| Login flood | 6 | 8 | 7 | 10 | 8 | 39 | High |
| Privilege escalation by staff | 9 | 7 | 6 | 7 | 5 | 34 | Medium |

## Mitigations

| Threat | Mitigation Strategy | Purpose |
|---|---|---|
| Phishing login credentials | - Enforce app-based MFA<br>- Monitor login patterns<br>- User education and anti-phishing campaigns | Makes it harder to reuse stolen credentials and improves early detection |
| API tampering with transaction amounts | - Implement input validation and strict API schema enforcement<br>- Use digital signatures<br>- Implement access control | Prevents manipulation of data in transit and enforces request authenticity |
| Missing/incomplete logs | - Enable tamper proof, centralised logging<br>- Use timestamps and digital signatures<br>- Apply audit trails with role-based log access | Ensures accountability and traceability for actions taken |
| SQL injection | - Use parameterised queries/prepared statements<br>- Apply input validation and sanitisation<br>- Employ Web Application Firewall (WAF) | Prevents attackers from injecting harmful SQL queries |
| Login flood | - Apply rate limiting and CAPTCHA<br>- Use DDoS protection from cloud/CDN providers<br>- Monitor traffic anomalies and set up alerts | Helps maintain system availability during malicious traffic spikes |
| Privilege escalation by staff | - Enforce least privilege access<br>- Review access rights regularly<br>- Enable admin activity logging and alerts | Limits exposure and enables rapid detection of abuse |

## Review and Recommendations

Threat modelling is an ongoing process. This initial assessment has identified high priority threats and proposed appropriate mitigations. Regular reviews should be carried out as the system evolves, especially when introducing new features, third-party integrations or major infrastructure changes.