Adversarial Risk Analysis of Biometric Customer Identification Controls in a Bank

Project Overview

Your assignment is to analyze a security scenario at **BlueRiver Bank**, which recently deployed a **biometric customer identification system** (facial recognition + fingerprint verification) for high-value transactions. You will perform a structured **Adversarial Risk Analysis (ARA)** to evaluate both **preventive** and **detective** controls, focusing on how an intelligent, adaptive adversary may try to defeat the system.

This assignment is designed to integrate:

- Application of **risk analysis concepts**
- Testing and evaluation of **preventive and detective controls**
- Use of an **adversarial risk-thinking mindset**
- Communication of findings as if presenting to bank executives

Scenario Background

BlueRiver Bank processes high-value customer transactions using a new **Biometric Identity Verification Platform (BIVP)** installed at all branches. The system uses:

- **Facial recognition**
- **Fingerprint scanning**
- **Liveness detection**
- **Behavioral analytics (typing and movement patterns)**

Business Goal

Reduce fraud and unauthorized withdrawals.

Primary Risk

A financially motivated adversary attempts to impersonate legitimate customers by bypassing or manipulating the biometric system.

Threat Actor Profile

- Skilled fraudster with moderate technical capability
- Access to black-market biometric replicas (deepfake video, silicone fingerprints)

- Motivated by high-value payouts
- Adaptive: changes tactics when controls are detected

The bank wants your analysis of whether its current controls are sufficient, and what additional measures are needed.

Assignment Tasks

1. Build an Adversarial Risk Model (ARA Layering)

Using ARA concepts:

1. Identify the **adversary's objectives**
   - What does the adversary want to achieve?
   - What payoff does the attacker expect?
2. Identify the **bank's defensive objectives**
   - What is the value the bank seeks to protect?
   - What are the success metrics?
3. Create an **adversary decision model**, including:
   - Possible actions (e.g., using deepfake video, stolen phone, silicone fingerprints, social engineering the teller, etc.)
   - Estimated probability of success for each
   - Estimated cost and required expertise
   - Likely adversary belief about your detection capabilities
4. Identify **defender actions** (bank controls) to mitigate these.

Deliverable: **A brief ARA adversary/defender model.**

2. Identify and Test Preventive Controls

Analyze the BIVP's **preventive controls**, such as:

- Multi-modal biometrics (face + fingerprint)
- Liveness detection (blink detection, skin texture)
- Branch-level secure kiosk design
- Anti-deepfake detection algorithms
- Rate-limiting and lockouts

For each preventive control:

1. Describe what the control prevents.
2. Identify how an adversary might attempt to bypass it (ARA perspective).
3. Propose **tests you would run** to validate the control's strength.
4. Score the control's effectiveness (high/medium/low or a numeric scoring system).

Deliverable: **Preventive Control Testing Matrix.**

3. Identify and Test Detective Controls

Detective controls include:

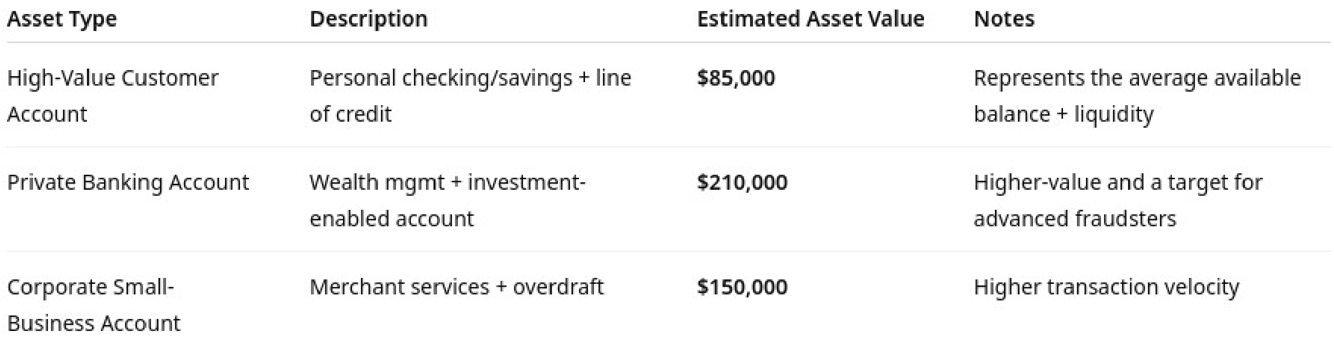
- Biometric mismatch alerts
- Transaction anomaly detection
- Behavioral analytics deviation flags
- Manual teller override and secondary verification
- Audit logging and monitoring

For each detective control:

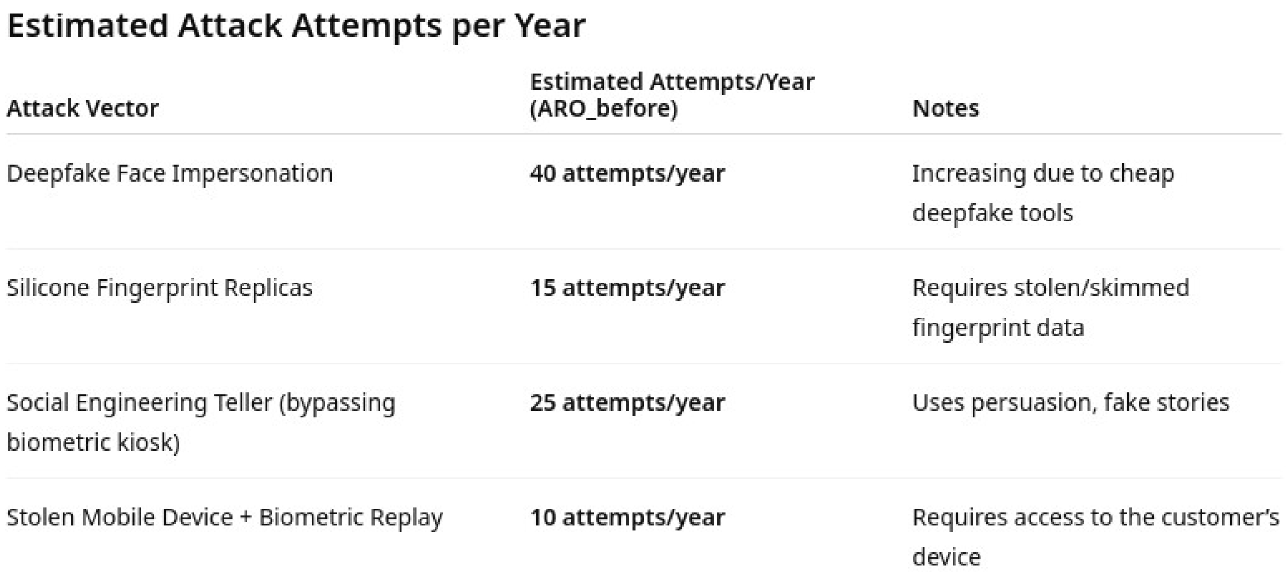
1. Describe what the control is designed to detect.
2. Explain how an adversary might try to avoid triggering it.
3. Propose testing methods (simulation, red-team exercises, log review).
4. Provide detection effectiveness scores.

Deliverable: **Detective Control Test Plan.**

4. Build a Quantitative Risk Analysis Estimate

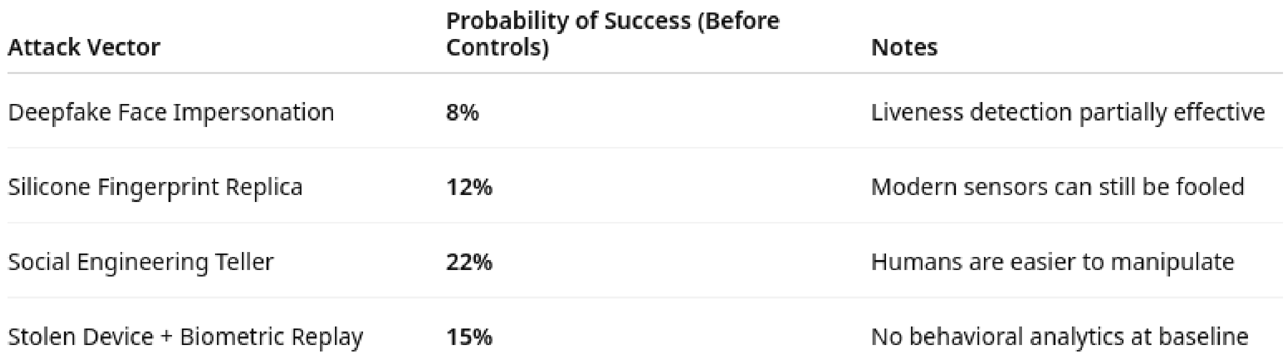


Asset Type	Description	Estimated Asset Value	Notes
High-Value Customer Account	Personal checking/savings + line of credit	**$85,000**	Represents the average available balance + liquidity
Private Banking Account	Wealth mgmt + investment-enabled account	**$210,000**	Higher-value and a target for advanced fraudsters
Corporate Small-Business Account	Merchant services + overdraft	**$150,000**	Higher transaction velocity



Estimated Attack Attempts per Year

Attack Vector	Estimated Attempts/Year (ARO_before)	Notes
Deepfake Face Impersonation	**40 attempts/year**	Increasing due to cheap deepfake tools
Silicone Fingerprint Replicas	**15 attempts/year**	Requires stolen/skimmed fingerprint data
Social Engineering Teller (bypassing biometric kiosk)	**25 attempts/year**	Uses persuasion, fake stories
Stolen Mobile Device + Biometric Replay	**10 attempts/year**	Requires access to the customer's device



Attack Vector	Probability of Success (Before Controls)	Notes
Deepfake Face Impersonation	**8%**	Liveness detection partially effective
Silicone Fingerprint Replica	**12%**	Modern sensors can still be fooled
Social Engineering Teller	**22%**	Humans are easier to manipulate
Stolen Device + Biometric Replay	**15%**	No behavioral analytics at baseline

If you want a single clean set of inputs, use this:

- Asset Value (AV): $85,000
- Attack Frequency (ARO): 30 attempts per year
- Attacker Success Probability: 10%

Use quantitative measures to model ARA outputs:

1. Estimate attacker success probabilities for each attack path.
2. Assign Single Loss Expectancy (SLE) values to a successful fraudulent transaction.
3. Estimate Annualized Rate of Occurrence (ARO) based on industry data or reasonable assumptions.

4. Compute Annualized Loss Expectancy (ALE).
    - One baseline ALE (current controls)
    - One ALE after adding at least **two new controls** of your choice

Identify any data you need and a plan for getting it.

5. Provide Recommended Mitigations (ARA-Informed)

Based on your adversarial model and control tests:

1. Propose new or strengthened controls.
2. Explain how each affects the adversary’s strategy or payoff.
3. Recalculate the attacker’s optimal strategy if your controls were implemented.

Deliverable: **One-page mitigation recommendations brief.**

6. Executive Summary for Bank Leadership

Write a bried summary that includes:

- Main findings
- Key weaknesses in the biometric system
- How adversarial thinking changed your risk evaluation
- Projected reduction in expected loss
- Recommendations for next quarter

This summary must be at a business level, not technical.

Deliverable: **Executive-level report.**