Stakeholder

Customer Data

Brand Reputation

Backup Service

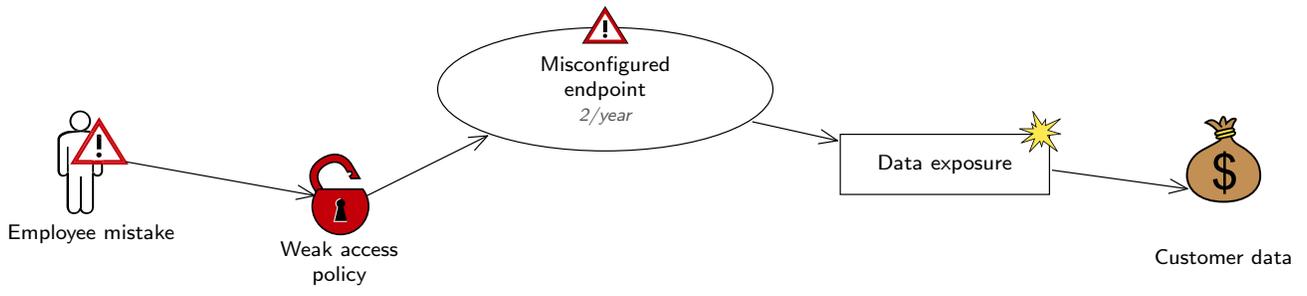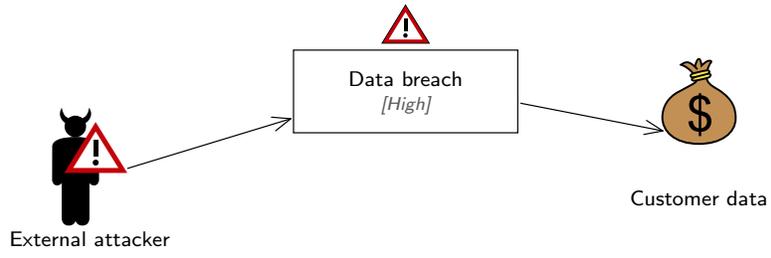Employee mistake → Weak access policy → Misconfigured endpoint *2/year* → Data exposure → Customer data

External attacker

Data breach
[High]

Customer data

Attacker

Weak MFA
policy

Enforce
phishing-resistant
MFA

Compromised account
1/year

Unauthorized
access

Payment service

Credential theft
[High]

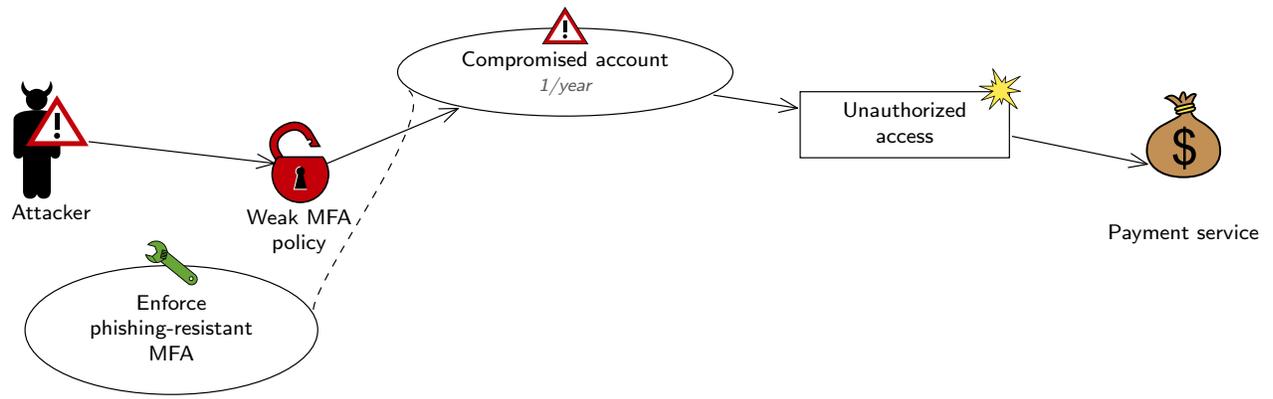Session hijack
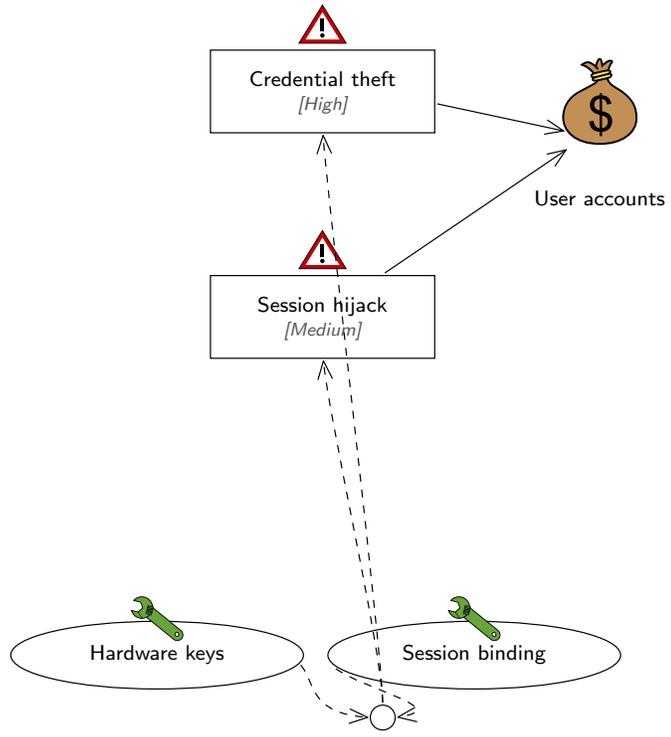*[Medium]*

User accounts

Hardware keys

Session binding
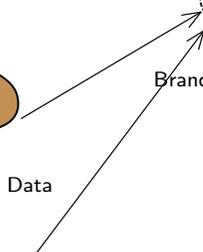
Table 1: High-level analysis excerpt

Who/what causes it?	How? What is the scenario or incident? What is harmed?	What makes it possible?
Hacker	Compromises confidentiality of customer records	Weak access controls on remote interfaces
System failure	Store unavailable due to backend outage	Single points of failure and poor failover routines