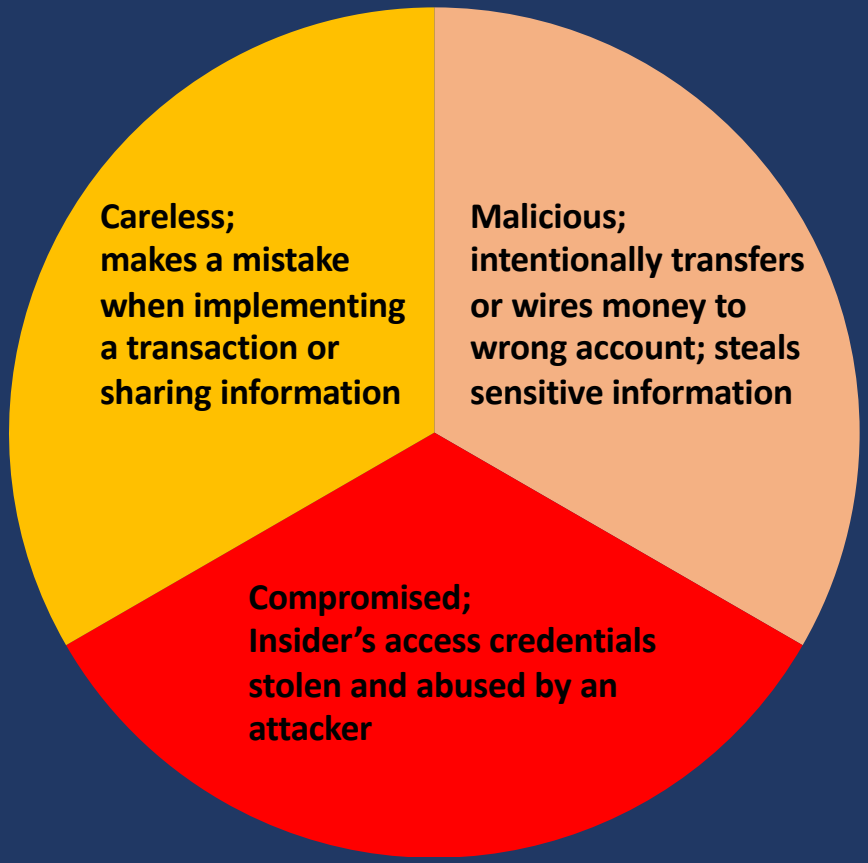
Technical solutions for insider threat management in banking

Kiowa
INFORMATION SECURITY

“Insider threats” are threats to the organisation that come from careless, malicious or compromised insiders.



“An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.” CISA

Kiowa
INFORMATION SECURITY

Postbank (S Africa); employees stole encryption key allowing them to access systems and accounts and reset bank cards

Punjab National Bank; huge scam that involved unauthorised use of SWIFT passwords by insiders.

J.P. Morgan; bankers were able to access and issue ATM cards for elderly and deceased clients, and withdrew $400,000 from their accounts

Kiowa
INFORMATION SECURITY

Identity Access Management (IAM)

- Control user access to systems and data
- Right access, right person, right time
- Multi-Factor Authentication
- Single Sign On
- Remote and on-site access

PREVENT UNAUTHORISED ACCESS TO SYSTEMS AND DATA

Privileged Access Management (PAM)

- Restrict and monitor privileged access
- Identify over-privileged accounts
- Protect privileged account credentials

PREVENT ABUSE OF PRIVILEGED ACCESS RIGHTS

User Behaviour Analytics (UBA)

- Analyse data to determine baseline "normal" activity
- Identify potentially harmful activity
- Generate risk scores for users

DETECT MALICIOUS ACTIVITY

Data Loss Prevention

- Detect sensitive information (account numbers, card credentials, personal information) going out of organisation
- Emails, IM, uploads, printing
- Manage by blocking or alerting

PREVENT UNAUTHORISED DATA TRANSMISSION

Kiowa
INFORMATION SECURITY

Case Study: North African Bank

- Information systems update driven by periodic risk assessment
- Client prioritised Identity and Access Management (IAM) and Privileged Access Management (PAM)

- Solution should offer:
  - Secure and manage privileged passwords
  - Role Based Access Management
  - User Behaviour Analytics (UBA)
  - Assessment of privileged account security risks
  - Solution alerts on high-risk activity

- ✓ **Select optimal vendor solution**
- ✓ **Implement the solution**
- ✓ **Integrate and configure according to client requirements**

Kiowa
INFORMATION SECURITY

Gather feedback from client regarding specific concerns in this area

Further discussion regarding insider threat risks and their mitigation

Provide shortlist of appropriate vendor solutions

Implement, integrate and configure the solution

Provide ongoing technical support and training

Kiowa
INFORMATION SECURITY