INSIDER THREAT: MASTER KEY COMPROMISE

Can a bank balance business continuity and security following a compromise at the highest level?

Players enter this exercise as part of the Crisis Management Team (CMT) at Mailbank – a bank run by Brits, for Brits. It strives to provide cost-effective financial services through optimized processes and infrastructure, including profitable partnerships and an aligned leadership team. Security is its core value.

However, Mailbank has a big problem: its master key, which controls all of its cryptographic keys that guard sensitive data, has been stolen. The malicious insiders who committed this crime have embarked on a 10-month long fraud campaign, stealing millions from customers. Now, Mailbank has to uncover the bad actors while creating a new master key – a task rife with operational and regulatory hazards.

In this scenario, players will improve their awareness of **NIST SP 800-57** and **PPI DSS 3.5/3.6** guidelines for cryptographic key management while managing moving parts to find the "least-worst" path through a cyber crisis.

WHAT IS THIS SCENARIO ABOUT?

SECTORS	VECTORS	ACTORS	MOTIVATIONS	IMPACTS	NON-TECHNICAL SKILLS
Financial Services	Insider Threat	Organized Criminals/ Cyber	Financial	Employees	Situational Awareness
Healthcare	Ransomware	Criminal Groups	Political	Customers	Effective Leadership
Transport, Logistics & Supply Chain	DOS	Political/Social Activists	Publicity for a Cause	Operations	Rational & Intuitive Decision Making
Energy & Infrastructure	Cloud	Disgruntled Employees/Former	Personal Malice	Shareholders	Communications
Government	Vulnerability Disclosure/ Reporting	Employees/ Customers	Commercial Advantage	Financial/ Commercial	Stress Management
	Social Engineering, Fear Exploitation, Covid	Terrorist Groups	Cause Operational Delays or Disruption	Reputational	Teamwork
	Data Breach	State Actors		Legal	
	Remote Working			Regulatory	
	Electoral Fraud				
	Impersonation				
	Physical Security Breach				

WHO IS IT AIMED AT?

This scenario is aimed at financial services organizations who rely on a master key to protect their cryptographic keys. In a retail financial services environment, the compromise of a master key is a critical security breach, so it is crucial that financial services organizations understand the latest PCI and NIST guidance on master key management.

However, as this sim deals with **insider threats**, which account for **22% of security incidents** (Verizon 2021 Data Breach Investigations Report), it will benefit any organization.

WHY SHOULD I CARE?

South Africa Postbank's master key was stolen by a group of malicious insiders in December 2018. The insiders managed to remain undiscovered for 10 months and make 25,000 fraudulent transactions, stealing $3.2 million.

After discovering the breach, the bank had to regenerate the master key and replace 12 million customer cards. It ultimately cost the bank $60 million.

This is a threat relevant to any financial services organization relying on a master key.

LEARNING OBJECTIVES

1. Refresh the organization's understanding of PCI DSS/NIST requirements for cryptographic key management.
2. Assess the organization's capability to manage complex internal crises involving multiple actors.
3. Enhance the organization's capability to build situational awareness in a cyber crisis, particularly around regulatory compliance, and to begin recovery.