Risk Management in ATMs

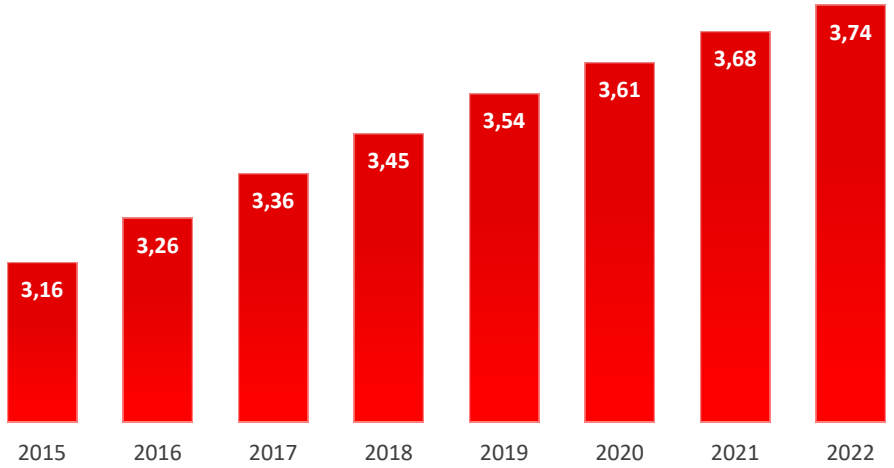
Ziraat Bank
More than a bank

ATMs - the past, present and future

- Automated teller machines (ATM) have been part of our lives since 1967 (51 years old)
- ATMs of 1967 relied not on plastic cards but instead on paper cheques, per transaction was £10
- In 1969, special cards with magnetic strips arrived to be used in ATMs
- ATMs of today do more than just dispense cash (accept cash, money transfer, etc.)
- The number of ATMs installed worldwide grew up to 3.3 million in 2016
- Forecasts that 3.7 million ATMs will be installed worldwide by 2022

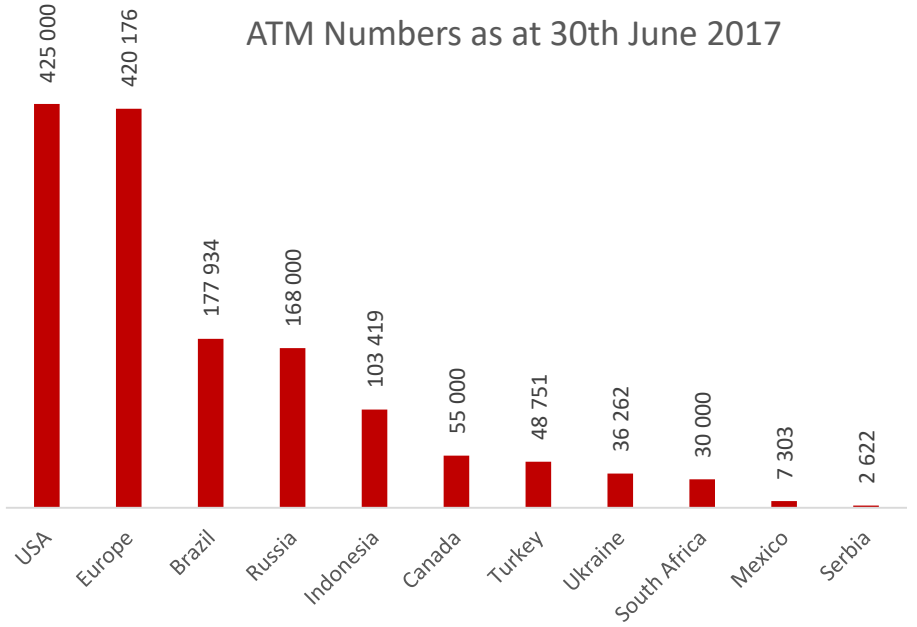
Ziraat Bank

Global ATM installed base (millions), 2005-2022



source: Global ATM Market and Forecasts to 2022 (RBR)

ATM Numbers as at 30th June 2017



source: European Association for Secure Transactions (EAST)

Ziraat Bank

ATM Fraud Attacks

What is it ?

- Customer Targeted Attacks
- Low Tech Attacks
- External Physical Attacks
- Logical Attacks

Ziraat Bank

Attack Types: Customer Targeted Attacks

Robbery

Vandalism. The persons replenishing the ATM are attacked either when moving the cash to / from the ATM, or while conducting cash replenishment activities.

Distraction Theft

The distraction scam involves diverting an ATM user's attention away from the ATM in order to find out their PIN and then steal their card

Card Swapping

Victims are distracted for just a matter of seconds while taking money out of an ATM, enough time for the fraudsters to steal cash from their account or swap their debit card for a fake

Shoulders Surfing

Someone looks over your shoulders to observe you as you enter your PIN at an ATM

Attack Types: Low Tech Attacks

Cash trapping

Attaches a device to the ATM so that when the ATM tries to dispence cash, the cash is trapped and the customer cannot retrieve it. The criminal then returns and retrieves the trapped cash

Reversal Fraud

An error codition is created at the ATM which makes it appear that cash will not be dispensed. This forces a re-credit of the amount withdrawn back to the account when in fact the criminal gets the cash

Card Trapping

A criminal inserts a device into the card reader and the PIN is compromised. Then the ATM keeps hold of the card, the criminal comes back and take the device with the trapped card inside

Skimming

A device attaches to card reader of an ATM to the reads card's magnetic stripe data. The criminal also hides pinhole camera so they can capture the PIN as it is entered. Then use this card data to create counterfeit cards

Ziraat Bank

Skimming still one of the biggest threats

Deep insert skimming devices, also known as 'card reader internal skimming devices' are placed deep inside the card reader. Deep insert skimming is the biggest skimming threat facing the global ATM industry because deployers are not prepared. Current anti-skimming solutions are not designed to protect against deep insert skimming

Ziraat Bank

ATM fraud monitoring and detect criminal

Ziraat Bank

Skimming - Recommendations

- Device that prevent skimming (invisible)
- Foreign object detection
- Skimmer jamming signals
- Pin pad cover / shield
- Customer Education

Our most important security tip is: Protect your PIN by standing close to the ATM and shielding the key pad with your other hand

Ziraat Bank

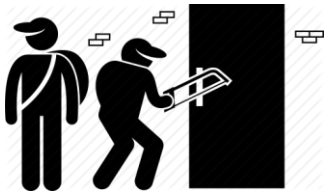
Until

EMV is fully implemented worldwide, skimming will continue to be a major industry concern, and deep insert skimming will be a real and present danger

Ziraat Bank

Ziraat Bank

Attack Types: External Physical Attacks



Burglary

- Pull Out
- Various Method

Brute Force

Attempts yo physically remove an ATM and its contents from its location

- Ram Raid
- Lobby: Pull Out

Explosive

- Plastic
- Gas

Ziraat Bank

Attack Types: Logical Attacks

Maintenance Manipulation

- Utilising normal maintanence functionally
- Changing cassette places

Malware

In these attacks the goal is to deploy software in the ATM PC so that the software will be running in the background when the ATM is operating normally

Black Box Attacks

Black (Unknown) Box is the connection of an unauthorised device which sends dispense commands directly to the ATM cash dispenser unit in order to "Cash-Out" the ATM

Ziraat Bank

ATM malware attacks hit Europe

EUROPEAN PAYMENT TERMINAL CRIME STATISTICS - SUMMARY						
Terminal Related Fraud Attacks	2013	2014	2015	2016	2017	% +/- 16/17
Total reported Incidents	21,346	15,702	18,738	23,588	20,971	-11%
Total reported losses	€248m	€280m	€327m	€332m	€353m	+6%
ATM Related Physical Attacks	2013	2014	2015	2016	2017	% +/- 16/17
Total reported Incidents	2,102	1,980	2,657	2,974	3,584	+21%
Total reported losses	€23m	€27m	€49m	€49m	€31m	-37%
ATM Malware & Logical Attacks	2013	2014	2015	2016	2017	% +/- 16/17
Total reported Incidents	0	51	15	58	192	+231%
Total reported losses	€0	€1.2m	€0.74m	€0.46m	€1.52	+230%

source: European Association for Secure Transactions (EAST)

A total of 192 ATM malware and logical attacks were reported, up from 58 in 2016, a 231% increase. 189 of the attacks were logical attacks where equipment typically referred to as a **'black box'** is used to send dispense commands directly to the ATM cash dispenser in order to cash-out the ATM.

Ziraat Bank

Recommendations Regarding Logical Attacks on ATMs

Physical access to the ATM

- Only authorised personnel should be allowed to carry out work on an ATM

Ofline protection

- Protect BIOS
- Hard disk encryption
- Cash dispenser communications

Online protection

- Network
- Firewall
- USB protection
- Anti-malware and logical protection

Additional Measures

- Fraud monitoring
- ATM Monitoring
- Test vulnerability
- Secure software delivery

Ziraat Bank

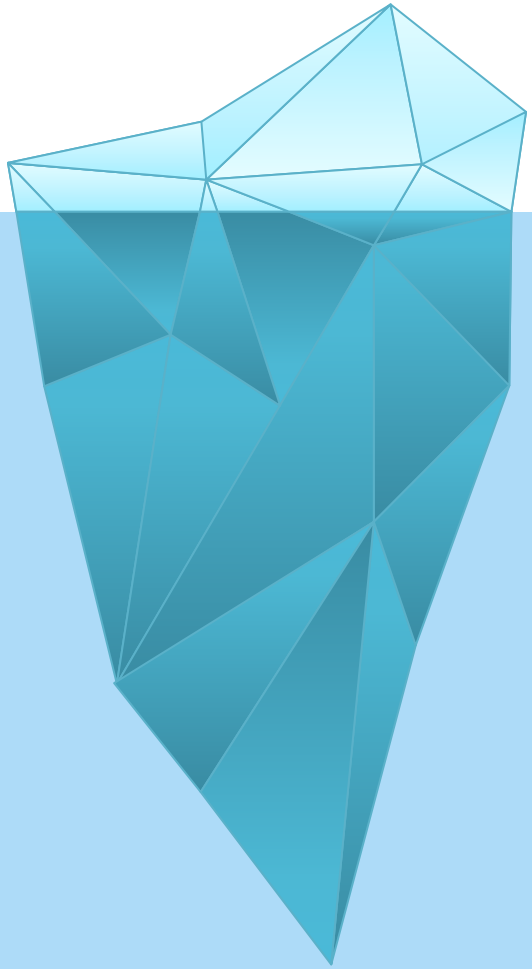
Balance The Risks

Transference

Share some of the burden of the risk, such as an insurance company

Annualized Loss Expectancy

How much an organization could estimate to lose from an asset based on the risks, threats and vulnerabilities



Mitigation

Accomplished anytime you take steps to reduce the risks

Avoidance

Involves identifying a risk and making the decision to no longer engage in the actions associated with that risk

Ziraat Bank

Thanks!

mcitpis@ziraatbank.com.tr

Ziraat Bank

More than a bank