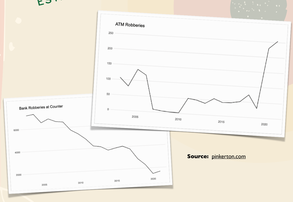
2024
THE RAPID RISE OF ATM THREATS

Cash TRANSACTIONS EST. 1996

CTX



Source: pinkerton.com

"Studies show that criminals steal 10 times more money in the average ATM robbery the average bank robbery."

~ *Doug Johnson, Senior Vice President for the ABA.*

Source: amazon.com

THE EVOLUTION OF ATM THREATS

ATM

'67–'73
Introduction

Brief introduction to the ATM invention and early networking by Lloyd Bank.

'16–'20
Geographical Hotspots

Focus on the spread to regional institutions and new records in ATM theft losses.

1990s
Rising Threats

Depiction of the shift from mechanical to more aggressive theft methods.

2023
Current Landscapes

ATM Robberies are now setting records in cases/losses. Over 24k annual incidents reported.

TODAY

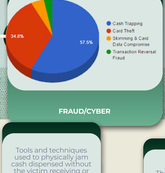
Develop continuous innovation in ATM security (Physical & Fraud/Cyber), measures.

'08–'15
Technology Exploits

Highlight the emergence of skimming, malware, and a significant increase in ATM fraud cases.

PHYSICAL

FRAUD/CYBER



smash & grab
Valuable media and/or components are stolen from the ATM.

ATM theft
The ATM is physically stolen, removed from its location.

CIT attacks
ATM service-related attacks on CIT or Service Staff.

cash trapping
Tools and techniques used to physically jam cash dispensed without the victim receiving or observing the cash.

card theft
The physical theft of a genuine card at an ATM, aka "card trapping"

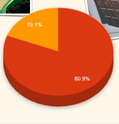
skimming & card data compromise
The compromise and theft of card data

transaction reversal fraud
The fraudulent theft of cash from an ATM during a transaction. The account is not debited but reversed in such a way that the account is not depleted.

jackpotting
Cash is forced to be fraudulently dispensed by the ATM without any account being debited.

cash out
Withdrawal limits are eliminated or inflated to remove limits on how much cash can be withdrawn.

Source: ATMIA | ATM security association "Crime Trends"



RAPID Response MANAGED SERVICES

RECOGNIZE THREATS

ASSESS YOUR FLEET

PLAN YOUR SECURITY REQUIREMENTS

MONITOR & TEST

DEVELOP YOUR RESPONSE PLAN

BATTLE PLAN

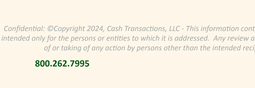
MY CHECKLIST

- [ ] ADD ADDITIONAL SECURITY BY CHANGING THE STANDARD MFG LOCKS TO A UNIQUE INSTITUTIONAL LOCK.

- [ ] SECURE SENSITIVE AREAS WITH ADD'L ALARM CONTACTS AND KEYPADS FOR AUTHORIZED PERSONNEL.

- [ ] IMPLEMENT SUSPICIOUS ACTIVITY PROTOCOLS ON YOUR IP CAMERA NETWORK & TEST!
- [ ] TIE ALARM & CAMERA ALERTS TO A PHYSICAL "ON PREMISE" SIREN / STROBE
- [ ] CONSIDER ENHANCED MFG & DTC ELECTRONIC LOCKS THAT YOU CAN USE TO TRACK DETAILED USER ACTIVITY.

- [ ] BASED ON YOUR PHYSICAL ENVIRONMENT CONSIDER ADD'L BARRIER SOLUTIONS, (BOLLARDS, SECURITY GATES, PLANTERS)



- [ ] DEVELOP DAILY/WEEKLY/MONTHLY AUDIT PROCEDURES.
  - CARD READER INSPECTIONS FOR SUSPICIOUS SKIMMER DEVICES.
  - PENETRATION TESTING
  - PATCH REPORTS
  - SOCIAL ENGINEERING
  - SECURITY LOGS
  - SUSPICIOUS ACTIVITY JOURNAL (CAMERA TEST)

- [ ] SECURE YOUR BIOS
  - ONLY ALLOW BOOT FROM THE PRIMARY HARD DISK
  - EDITING OF BIOS SETTINGS MUST BE PASSWORD PROTECTED
- [ ] IMPLEMENT USER ACCESS CONTROLS
  - ESTABLISH CENTRAL POLICY MGT W/ ACCESS CONTROLS & MONITOR
  - HAVE AN OPERATIONAL PASSWORD POLICY FOR ALL DEVICES
- [ ] ENSURE TLS ENCRYPTED COMMUNICATIONS IS ENABLED
  - FROM THE NETWORK
  - TO THE ATM
- [ ] ESTABLISH & TEST SECURE FIREWALL CONNECTIONS
  - ATM FIREWALL MUST BE CONFIGURED TO ONLY ALLOW KNOWN AUTHORIZED INCOMING AND OUTGOING CONNECTIONS NECESSARY FOR YOUR ATM ENVIRONMENT
- [ ] REMOVE UNUSED SERVICES & APPLICATIONS FROM YOUR OPERATING ENVIRONMENT.
  - IMPLEMENT ZERO-DAY PROTECTION FOR MALICIOUS ATTACKS.
  - ENSURE APPLICATIONS RUN IN A LOCKED DOWN ACCOUNT W/ MINIMUM PRIVILEGES.
  - DISABLE AUTO PLAY
  - REQUEST/GENERATE SECURITY LOGS
- [ ] DEPLOY NETWORK AUTHENTICATION BASED HDD ENCRYPTION
  ENSURE ATM CORE HAS TPM MODULE - WOULD NEED TO BE PHYSICALLY VERIFIED. THE TPM STORES ENCRYPTION CODES BETWEEN ATM OS & NTS LAYERS
  LOCK DOWN USB PORT ACCESS
- [ ] **DISABLE EMV FALLBACK TO MAGSTRIPE FROM NETWORK.**
  CONSIDER EFT FRAUD LIMITS (EX. 3 CARD ATTEMPTS THEN DE-ACTIVATE CARD)
- [ ] **ESTABLISH A CONSISTENT OS PATCHING PROCESS**
  KEEP ATM SOFTWARE & FIRMWARE UP TO DATE WITH THE LATEST "TESTED" PATCHES AND UPDATES. REGULARLY MONITOR FOR SECURITY ADVISORIES AND APPLY PATCHES TO MITIGATE RISKS.

"99% of all cyber threats can simply be mitigated through effective patch management."
~ ***Safe Systems***

800.262.7995 **www.cashtrans.com**