A Treasure Trove Of Failures

What History’s Greatest Heist Can Teach Us About Defense-In-Depth

Who Am I?

Pete Stegemeyer

7 Years of Security Engineer Experience

Author of “HEIST: An Inside Look at the World's 100 Greatest Heists, Cons, and Capers”

Heist Expert for History Channel



The Antwerp diamond heist

WHEN:	February 15-16, 2003
WHERE:	Antwerp, Belgium
WHO:	The School of Turin
WHAT:	Between $100M and $1B in stolen diamonds, gold, cash and more
WHY:	A perfect storm of security failures and dedicated thieves



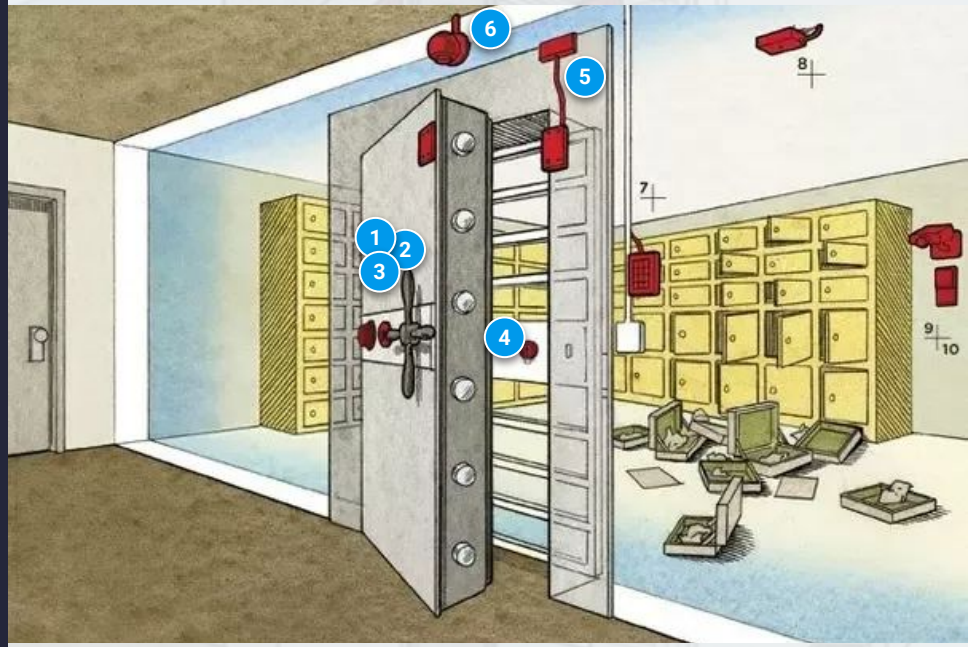
The Antwerp Diamond Centre

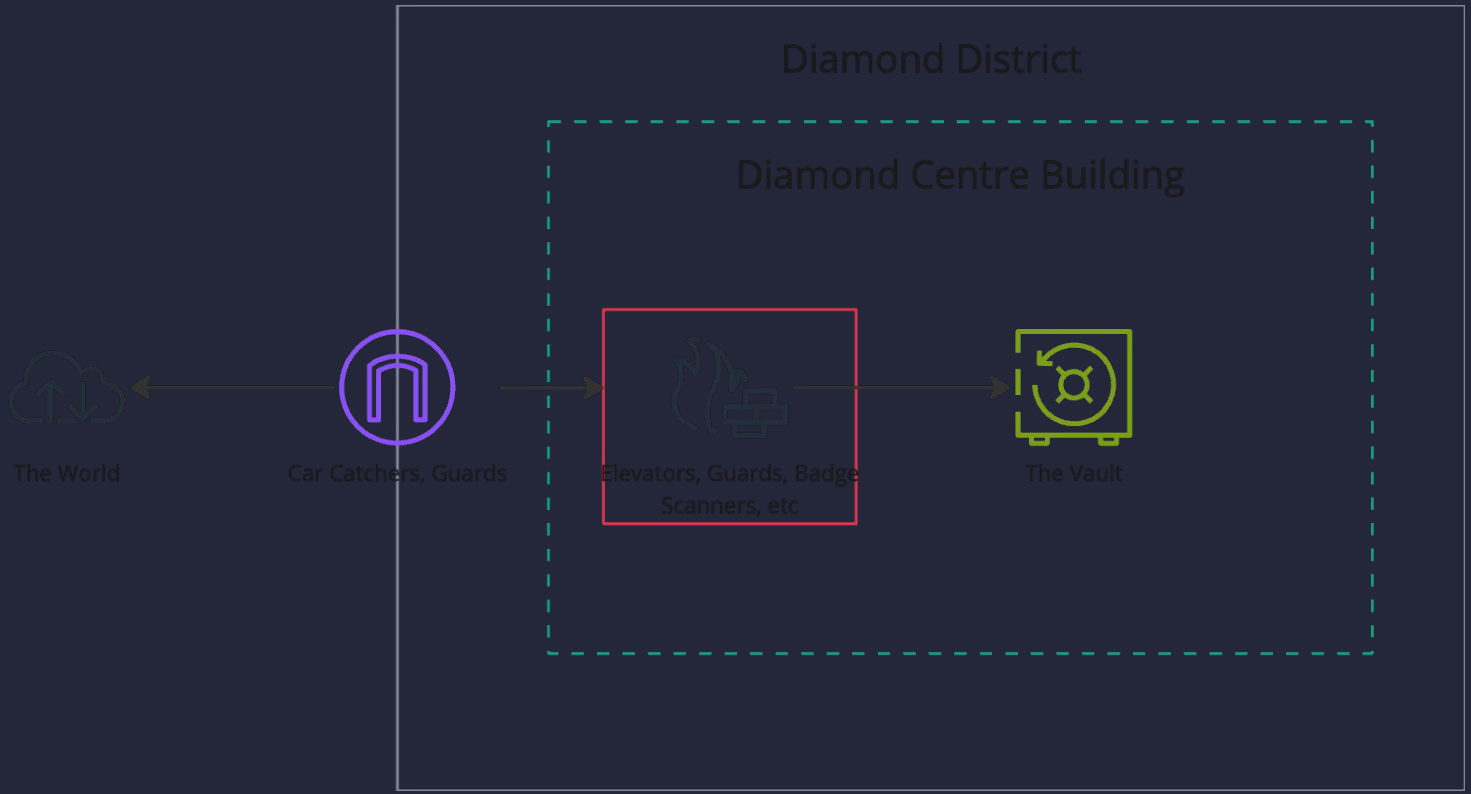
- Handles 80% of all global diamond transactions
- Most secure part of Antwerp
- Dedicated private police force
- Local Police just outside of the district
- All traffic in and out stopped by hydraulic car catchers
- Multiple “blocks” for the Diamond Centre: A, B, C



The Vault

1. 100m combination lock
2. 1-foot thick steel
3. 12-inch long key (stored in 2 parts)
4. Day gate
5. Magnetic sensor
6. Camera up to guard shack
7. Access card reader
8. Seismic detector
9. Motion and thermal sensor
10. Safe Deposit Boxes




Diamond District
Diamond Centre Building
The World
Car Catchers, Guards
Elevators, Guards, Badge Scanners, etc
The Vault

The School of Turin

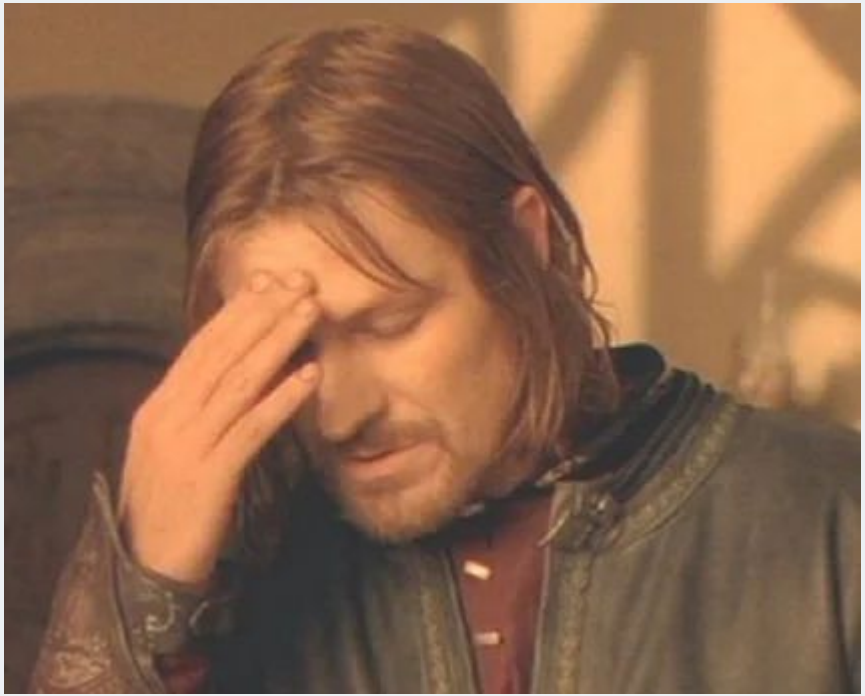
- Group of highly specialized thieves
- Not an official team – a distributed collective
- Referred each other for heists based on specialties needed for each job
- Mastermind: Leonardo Notarbartolo
- INCREDIBLE Code Names
  - The Monster, The Genius, The King of Keys, and “Speedy”



Phase 1: Recon

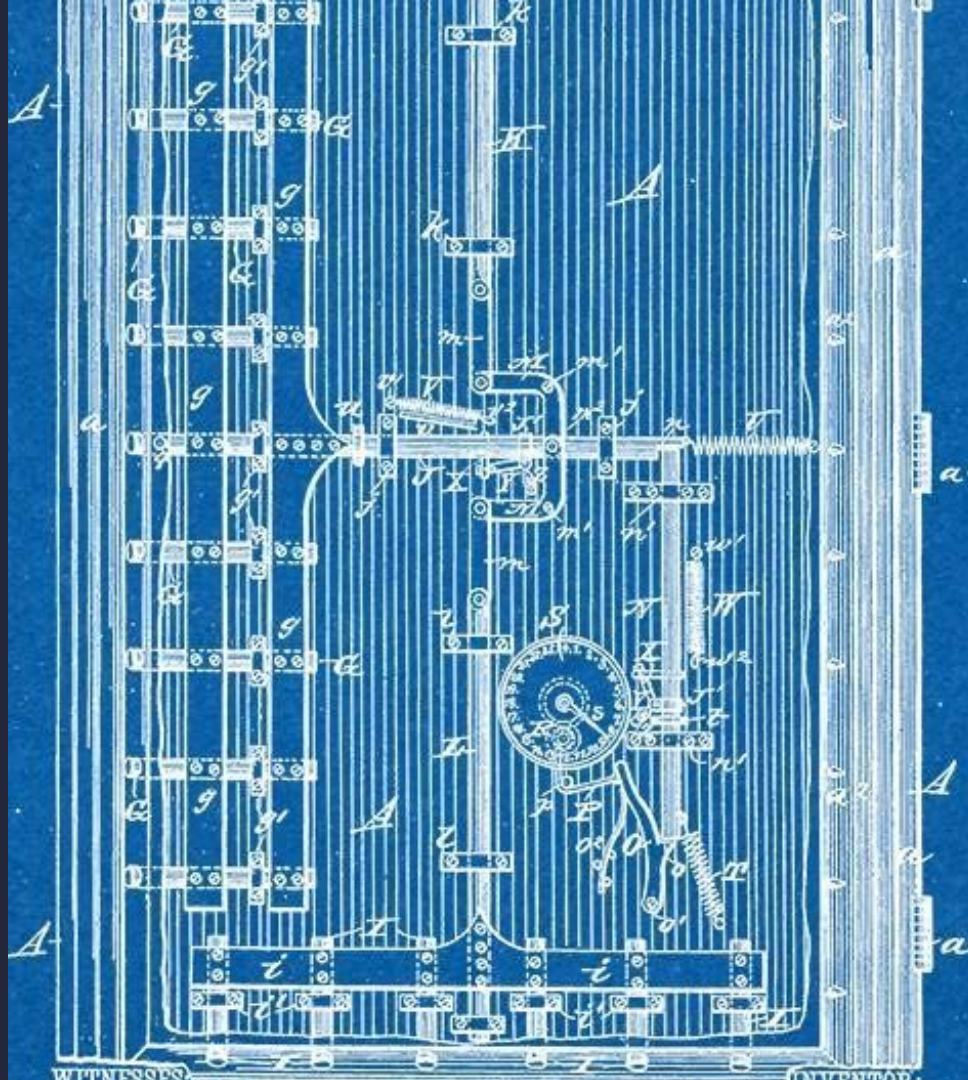
- 18 months prior to the heist, Notarbartolo rents office space in the diamond center
- This gives him access to the vault and his own safe deposit box
- No background check is completed.
- Persistence is established and patterns are identified

They just... walked in.



Phase 2: Expanding the footprint

- Notarbartolo starts making regular trips into the vault wearing hidden cameras
- Notarbartolo asks for blueprints to rent a larger office, and is given the complete set ***including*** the vault room and garage
  - Two key vulnerabilities found:
  - An exterior access door to the antechamber
- The team builds a replica vault to practice their movements in the dark



Planning

- Heist is planned for Valentine's Day weekend
- Chosen for multiple factors
  - Higher inventory and cash
  - Big tennis match across town
  - Long weekend due to bank holiday
- Not unsimilar to the Bank of Bangladesh cyber heist



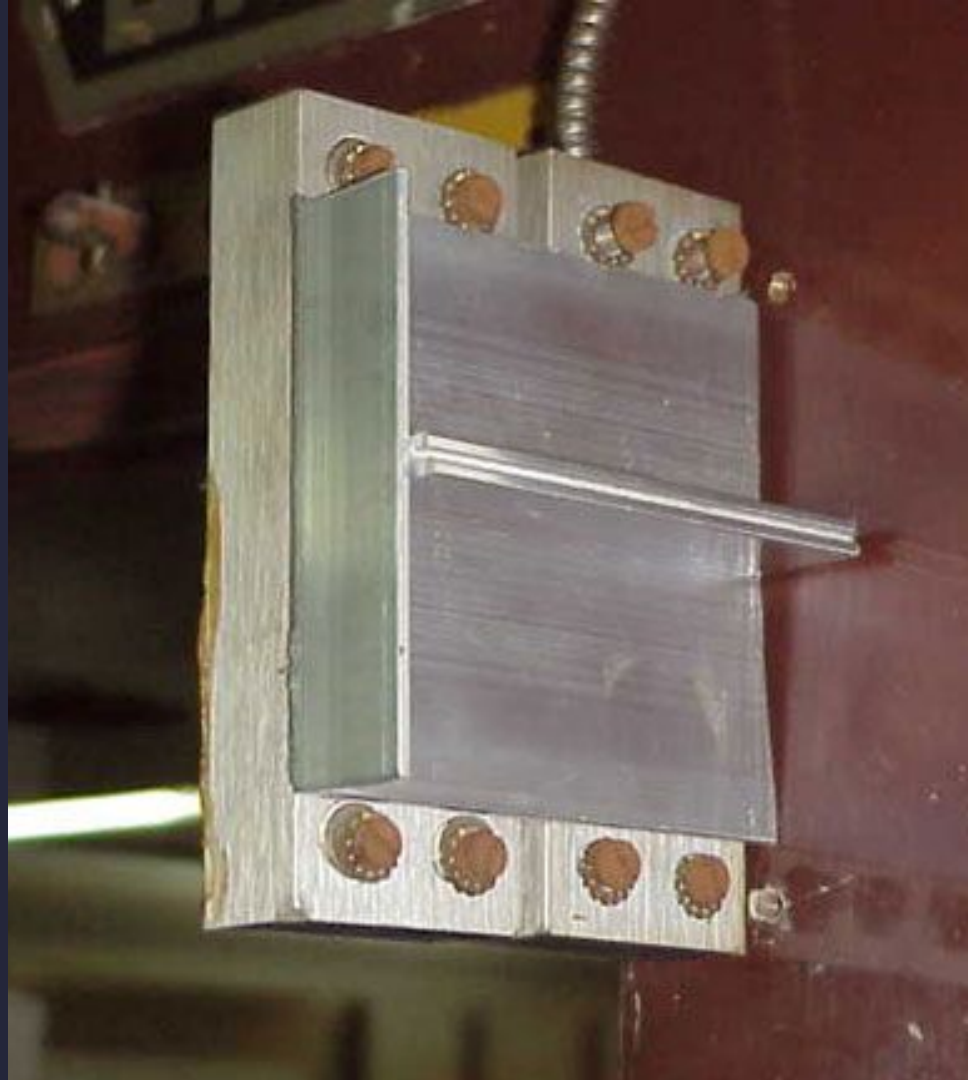
Final Prep Work

- T-5 Days
  - Genius accesses the vault to bypass magnetic sensor with Notarbartolo's key card
- T-3 Days
  - Hidden Camera placed over vault door
- T-1 Day
  - Notarbartolo covers the heat and motion sensor with hairspray and stays until close to observe guards
  - A nice lunch tray the day before



The Heist

- Entered through garage
- Cameras covered and elevators bypassed
- **Genius** reapplies the aluminum device
- Lights are turned off until sensor is covered
- Key is kept in closet next to vault - in 1 piece
- Combination lock is opened
- Day gate pried open
- Motion/Heat sensor deactivated via foam shield



The Haul

- **123** of **160** safe deposit boxes were looted with special tool
  - Reinforced boxes are left unopened
- So much stolen that they had to leave behind millions of less valuable loot
- Tapes are removed from security room and replaced with blanks
  - VCRs were not updated to DVRs due to cost



The Getaway

- **Speedy** panicked and started dumping evidence before it could be burned hours after the heist
- A local discovered it and called police
- Half eaten sandwich and diamonds, gold, etc found with security tapes that were unusable
- Pointer Emeralds found in Notarbartolo's carpet



Takeaways

- Defense in depth only works if done properly
- The spectre of security ***is not*** security in practice
- Complacency is the enemy of complexity
- Stupid and/or lazy can be exploited both ways



Questions?