

The Perfect Heist: Recipes from Around the World

Jarret M. Lafleur, Ph.D., Liston K. Purvis, Ph.D., and Alex W. Roesler, Ph.D.

Sandia National Laboratories, Livermore, California*

MIDN Paul Westland

U.S. Naval Academy, Annapolis, Maryland

Of the many facets of the criminal world, few have captured society's fascination and awe as has that of high stakes robbery. The combination of meticulousness, cunning, and audacity required to execute a real-life *Ocean's Eleven* may be uncommon among criminals, but it is fortunately common enough to extract a wealth of lessons for the protection of high-value assets. To assist in informing the analyses and decisions of security professionals, this paper surveys 23 sophisticated and high-value heists of cash, gold, gems, artwork, and other valuables that have occurred or been attempted across the world, particularly over the past three decades. The results are compiled in a Heist Methods and Characteristics Database and analyzed qualitatively and quantitatively, with the goals of both identifying common characteristics and characterizing the range and diversity of criminal methods used. The analysis is focused in six areas: (1) Defeated Security Measures and Devices, (2) Deception Methods, (3) Timing, (4) Weapons, (5) Resources, and (6) Insiders. Key lessons are identified in each focus area.

1. Introduction

On the morning of Monday, February 17, 2003, concierge Jorge Dias De Souza descended two levels beneath Antwerp's Diamond Center. Expecting to open the center's vault for a normal day of business, he was astonished to discover the lights on, the vault door open, and 109 of the center's 189 safe deposit boxes wide open, with millions of dollars' worth of discarded contents littering the floor. What was not on the floor was what the thieves *could* carry with them: between \$108 million and \$432 million worth of diamonds, gold, cash, and other valuables, stolen in what was later called the heist of the century.¹

Located in the Secure Antwerp Diamond Area, the Diamond Center had been thought to be among the world's most fortified businesses. Entry into the center's vault required a building access card, a two-story descent underground to a guard-controlled gate, and both a key and one of 100 million possible combinations. If a person somehow entered the vault unauthorized, he would be detected by a broken magnetic seal on the vault door, a motion detector, infrared detector, and light detector. If he tried to tunnel in, he would be detected by seismic sensors. With a police station not more than 200 feet from the Diamond Center's front entrance – and a police kiosk even closer – any detected thief would be captured in minutes. Since all the detectors activated silent alarms, the thief wouldn't know he had been detected until he was already surrounded. Nevertheless, somehow the Antwerp thieves defeated *all* of these measures.¹

The Antwerp heist is one of several that have gained global notoriety, and it is unusual for any modern list of top heists (e.g., see Refs. 1-7) to ignore it. Such heists are often distinguished by the staggering value of items stolen, typically tens or hundreds of millions of dollars. However, from the point of view of a security analyst, the interesting questions include: How did the thieves execute the crime? What security systems did they defeat? What roles did deceptions and insiders play? What attracted the thieves to their targets, what resources did they invest, and what risks did they take? What could security forces have done differently?

* Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

This paper examines 23 sophisticated and high-value heists and heist attempts that have occurred across the world, particularly over the last three decades. The stories of these heists are dissected and analyzed with two goals in mind: First, these stories are used to both quantitatively and qualitatively characterize the range and diversity of criminal methods utilized in large heists. Second, the characteristics of these heists are analyzed to identify commonalities in how they were accomplished. The results, in the form of data, observations, and lessons learned, are intended to help inform the analyses of security professionals.

2. Heists Considered

Table 1 provides a list of all 23 heists considered in this analysis, incorporating major heists and heist attempts that appear frequently in modern lists of notorious heists¹⁻⁷. In some cases, these heists are notorious for the high value of items stolen. In other cases, they are known for the inventive methods the thieves used to gain access to the valuables. In many cases, they are distinguished by both of these features.

Table 1. Identifying information for heists examined.

ID	Name	Date	Location	Category	Approx. Value of Items Stolen* (\$FY12M)
1	Brazil Central Bank Cash Heist	Aug. 6, 2005	Fortaleza, Brazil	Stealth Raid	81.9
2	Sumitomo Mitsui Bank Heist	Oct. 2, 2004	London, UK	Stealth Raid	478.5
3	Antwerp Diamond Heist	Feb. 15, 2003	Antwerp, Belgium	Stealth Raid	332.1
4	Museon Jewel Heist	Dec. 2, 2002	The Hague, Netherlands	Stealth Raid	15.4
5	Société Générale Bank Heist	July 17, 1976	Nice, France	Stealth Raid	40.4
6	Stardust Casino Job	Sept. 22, 1992	Las Vegas, USA	Walk Away	0.8
7	Vastberga Helicopter Heist	Sept. 23, 2009	Stockholm, Sweden	Smash and Grab	6.1
8	Millennium Dome Raid	Nov. 7, 2000	London, UK	Smash and Grab	666.1
9	Tanzanian Airplane Gold Robbery	Jan. 5, 2012	Geita, Tanzania	Subdue and Seize	30.5
10	Munch Museum Art Heist	Aug. 22, 2004	Oslo, Norway	Subdue and Seize	137.9
11	Carlton Hotel Diamond Heist	Aug. 11, 1994	Cannes, France	Subdue and Seize	69.3
12	Brink's-Mat Gold Heist	Nov. 26, 1983	London, UK	Subdue and Seize	85.9
13	Lufthansa Heist	Dec. 11, 1978	New York, USA	Subdue and Seize	28.2
14	British Bank of the Middle East Gold Heist	Jan. 20, 1976	Beirut, Lebanon	Subdue and Seize	204.6
15	Chase Manhattan Bank Robbery	Aug. 22, 1972	New York, USA	Subdue and Seize	1.2
16	Mayfair Graff Diamond Heist	Aug. 6, 2009	London, UK	Deceive, Subdue, and Seize	68.9
17	Harry Winston Diamond Heist	Dec. 4, 2008	Paris, France	Deceive, Subdue, and Seize	111.3
18	Schiphol Airport Diamond Heist	Feb. 25, 2005	Amsterdam, Netherlands	Deceive, Subdue, and Seize	115.8
19	Swissport Heathrow Heist	May 17, 2004	London, UK	Deceive, Subdue, and Seize	71.1
20	Gardner Museum Art Heist	March 18, 1990	Boston, USA	Deceive, Subdue, and Seize	440.0
21	Knightsbridge Safe Deposit Center Heist	July 12, 1987	London, UK	Deceive, Subdue, and Seize	130.0
22	Securitas Cash Depot Heist	Feb. 21, 2006	Tonbridge, UK	Tiger Kidnapping	104.0
23	Northern Bank Cash Heist	Dec. 19, 2004	Belfast, UK	Tiger Kidnapping	60.5

*In the case of failed heists (heists 2, 8, 9, 15, and 19), this refers to the approximate value of items *attempted* to be stolen. Also, except where otherwise noted, all monetary amounts in this paper are given in units of fiscal year 2012 (FY12) equivalent dollars.

2.1. Related Literature

Although individual heists are remarkably popular topics for books, documentaries, and films, systematic studies across multiple high-value heists are difficult to locate. Perhaps the greatest published interest and analysis of high-value heists exists not in the pure criminology or physical security fields, but rather in nuclear security. Early work in this area was summarized in a 1980 report by RAND.⁸ In this report, analysts posed conventional high-value thefts as analogs to potential incidents against nuclear targets, useful since criminal activity against such targets was too low to provide sufficient data. In 1997, Schuller and Ford presented a paper at an IAEA conference⁹ that applied law enforcement property crime investigation techniques to create a model of eight basic tasks criminals must carry out to orchestrate a successful theft. Most recently, in 2007 Bunn examined the plausible spectrum of nuclear weapons or materials thieves.¹⁰ He noted that one-dimensional high, medium or low characterization of thief capability “is itself a substantial simplification, as thieves’ characteristics may vary across several dimensions ...” Bunn proposed two dimensions of characteristics, namely whether thefts were (1) perpetrated by insiders or outsiders and (2) covert or overt.

As a whole, however, the literature contains few systematic characterizations of heists according to their “several dimensions”. This work seeks to augment and update existing literature, and also create a tool and methodology to allow a transparent and thorough exploration of the many dimensions of these historic heists.

2.2. A Heist Taxonomy

Each heist in Table 1 has been methodically researched via open literature, and for each a database entry of 155 fields has been populated to the maximum extent that available information allows. The total collection of information is referred to as the Heist Methods and Characteristics Database (HMCD). The details that comprise most of the database are the subject of Section 3. First, however, it is worth observing that the approaches that thieves took in perpetrating these 23 crimes can be sorted into six distinct categories. These categories, noted in Table 1, are (1) Stealth Raid, (2) Walk Away, (3) Smash and Grab, (4) Subdue and Seize, (5) Deceive, Subdue, and Seize, and (6) Tiger Kidnapping. The categories themselves may be sorted into two classes based on the level of violence employed (see Fig. 1).

The major category within the nonviolent heist class is the *Stealth Raid*. In this type of heist, exemplified by the Antwerp Diamond Heist described in Section 1, thieves actively subvert security measures in order to remain unseen, unheard, and otherwise undetected.

A second nonviolent heist category is the *Walk Away* crime. Unlike the Stealth Raid heist, the Walk Away heist is characterized by little or no subversion of physical security measures, but rather by use of appropriate timing and route planning. Such a heist may be committed in plain sight of security forces. The example of the Stardust Casino Job exists in the HMCD: On September 22, 1992, casino cashier William Brennan took his lunch break at the Stardust Resort and Casino in Las Vegas. As he exited, passing security guards, he was carrying a backpack of cash and chips worth \$800,000 (FY12). Brennan has not been seen since.^{4,11}

The *Smash and Grab* heist is distinguished by overt and often public violence toward property. Unlike in a Stealth Raid, the thieves spend little effort avoiding detection; instead, their success relies on the delay between intrusion detection and response. One such heist is the Vastberga Helicopter Heist: At 5:15 AM on September 23, 2009, four thieves landed a helicopter on the roof of the G4S Cash Depot in Vastberga, Sweden (see Fig. 2). Breaking through a pyramid skylight, the thieves descended to the depot’s counting room and breached the door using custom-fit explosives. Twenty minutes later, the thieves took off from the roof with \$6.1 million (FY12) in cash. The thieves actively hindered police by placing caltrops across roads and packages appearing to be bombs outside the police heliport.¹²⁻¹³

The second violent heist is the *Subdue and Seize* heist, marked by violence to incapacitate or coerce guards or custodians and followed by seizure of high-value items. One example is the Brink’s-Mat Gold Heist: In November 1983, six armed men entered the Brink’s-Mat depot near Heathrow Airport shortly after its 6:30 AM opening. The six employees were subdued, and the two employees with vault keys and combinations were coerced at gunpoint to open the vault. Though the thieves successfully entered the outer vault door, a



Figure 1. Summary of the six heist categories and two heist classes.



Figure 2. Security footage from the G4S Cash Depot. Note the thief in front of the helicopter, preparing to break through the skylight.

combination-holding employee was too distressed to remember combinations to the inner vault doors. Luckily for the thieves, gold bullion worth \$86 million (FY12) sat ready for shipment (or theft) in the vault's outer chamber. It was later revealed that a depot insider had provided the thieves with critical information and assistance.^{6,14}

The third category of violent heists is termed *Deceive, Subdue, and Seize*, and is defined by a Subdue and Seize event preceded by a deception that typically permits the thieves access they would not normally possess. For example, in the Gardner Museum Art Heist, two men posing as Boston Police officers approached the Isabella Stewart Gardner Museum at 1:24 AM on Sunday, March 18, 1990. Claiming to be responding to a disturbance, the men convinced an on-duty security guard to grant them entrance. After the second guard arrived to assist, the phony officers handcuffed both guards, wrapped duct tape around their eyes and mouths, and left them in the basement. Over the course of 81 minutes, the thieves stole thirteen works of art worth some \$440 million (FY12). The outside world did not know of the heist until the guards were scheduled to be relieved at 7:00 AM.¹⁵⁻¹⁶

The final category of violent heists is the *Tiger Kidnapping*. Such a heist involves the kidnapping of an individual with critical access privileges and typically his family, used to coerce the individual to act as an insider. An excellent example is the Securitas Cash Depot Heist: On his way home from work on February 21, 2006, the manager of the Securitas Cash Depot outside of London was pulled over by two men posing as police officers. Simultaneously, two other men posing as police arrived at the manager's residence to inform his family that he had been in an accident. The manager and his family were driven to a farm, and the manager was told his family would be killed if he did not cooperate. The manager was then brought to the Securitas depot, accompanied by a thief dressed as a police officer (see Fig. 3). The manager convinced the control room guard to admit the two and open the main gate, through which three thief vehicles drove. The guard was subdued, and more accomplices entered to subdue the remaining 13 employees in the depot. The thieves drove away with some 6,000 lbs. of cash worth an estimated \$104 million. Inside information from a recently-hired depot employee played an important role in planning the theft.¹⁷⁻²⁰



Figure 3. CCTV image of thieves, including one dressed as a police officer, executing the Securitas robbery.

3. Analysis

The data recorded for each heist in the HMCD are focused in six areas, namely (1) Defeated Security Measures and Devices, (2) Deception Methods, (3) Timing, (4) Weapons, (5) Resources, and (6) Insiders. Next, highlights of analysis in these areas are presented to help identify commonalities, trends, and thief capability envelopes.

3.1. Defeated Security Measures and Devices

For almost every heist in the HMCD, one or more identifiable security measures were defeated. This is summarized in Table 2; a bomb (💣) indicates that a given security measure (in the row) was encountered and defeated during a given heist (in the column). In this context, “defeat” connotes (1) damage or destruction of a security measure or (2) suppression of a security measure via a ruse or a false or forged authentication.

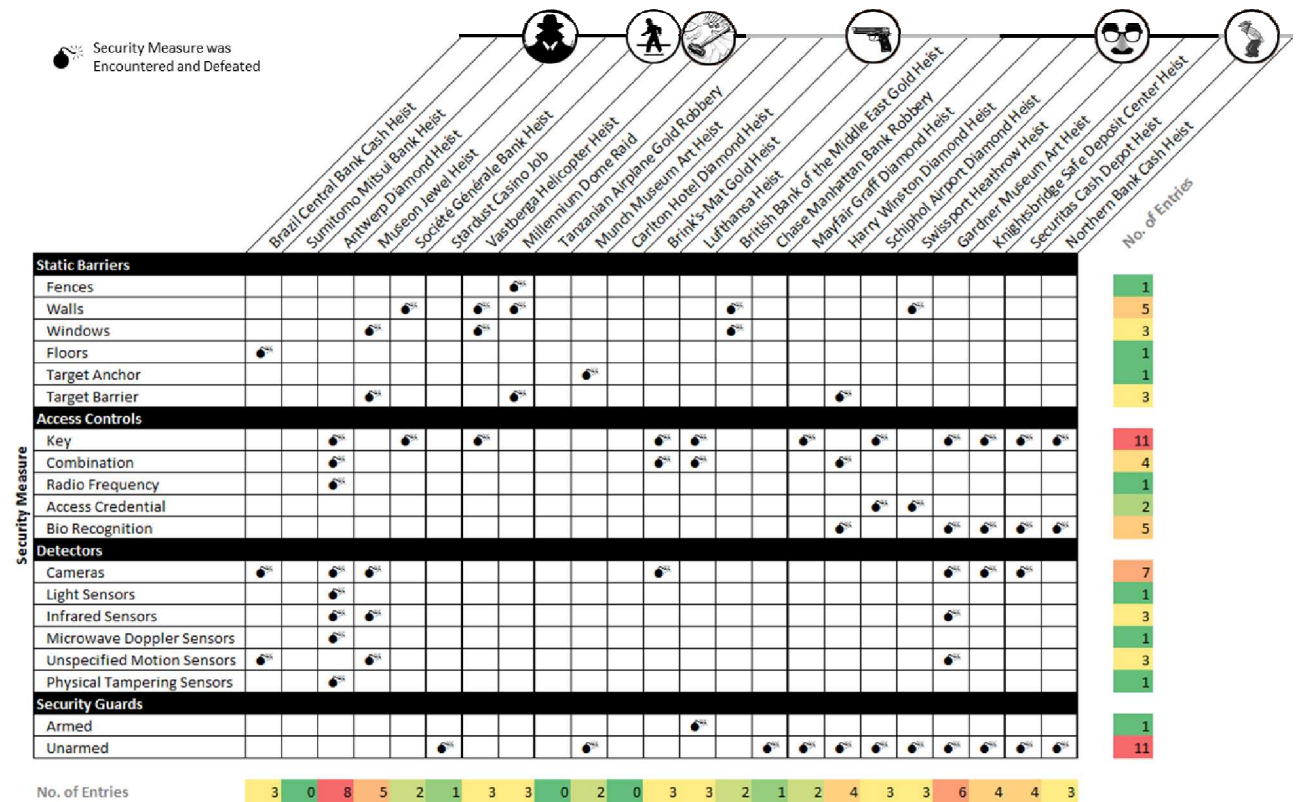
The rightmost column of Table 2 presents a simple count of the number of heists in which each security measure was defeated. Not every security system uses all of the security measures in the table, and so a blank cell neither implies that the security system existed nor that it successfully deterred attack. Thus, while low totals in the right column cannot be used to make statements about the general effectiveness of a security measure, high totals do suggest that certain security measures, such as keyed locks, cameras, and guards, are commonly defeated.

The bottom row of Table 2 displays a count of the number of security measure types defeated in each heist. Topping the list is the Antwerp Diamond Heist with eight defeated security measure types, solely in categories of access controls and detectors. Also significant were the unsolved Gardner Museum Art Heist, in which access controls, detectors, and security guards were attacked, as well as the unsolved Museon Jewel Heist in the Netherlands, where static barriers and detectors were defeated by methods that remain unclear. The most interesting observation from this bottom row is that in 18 heists (78% of the database), more than one security measure was defeated. In fact, the mean number of defeated security measure types is 2.8, and the median is 3.0.

That is, high-value heists typically involve the defeat of multiple security measures, and the criminal team committing such a heist typically possesses a diversity of security defeat capabilities.

The HMCD also records details on the security forces in place at attacked facilities, including the number and activity of personnel defeated, the phases in which knowledge of the heist was attained and response occurred, and the proximity of the facility to external police forces. For example, data show that despite the fact that guards were active on the target premises during 65% of heists and that external security forces were an average of just 0.7 miles away, in 65% of cases no effective security response was mounted until after the thieves had departed. In 35% of heists, security forces did not even detect the heist until after it was complete. These data underscore the importance of thorough detection techniques and rapid response, with the understanding that lack of response force proximity is rarely the reason for lack of a capable response.

Table 2. Summary of Defeated Security Measures.



3.2. Deception Methods

As described in Section 2.2, the Deceive, Subdue, and Seize heist is marked by a deception preceding a subdue-and-seize event, permitting thieves access they would not normally possess. However, Table 3 helps illustrate the point that deceptions are not limited to heists in this category. Within the database, 91% of heists (all but two) are known to have involved some deception, more than three times as many as the 26% of heists in the Deceive, Subdue, and Seize category. That is, deception is the norm for large criminal heists.

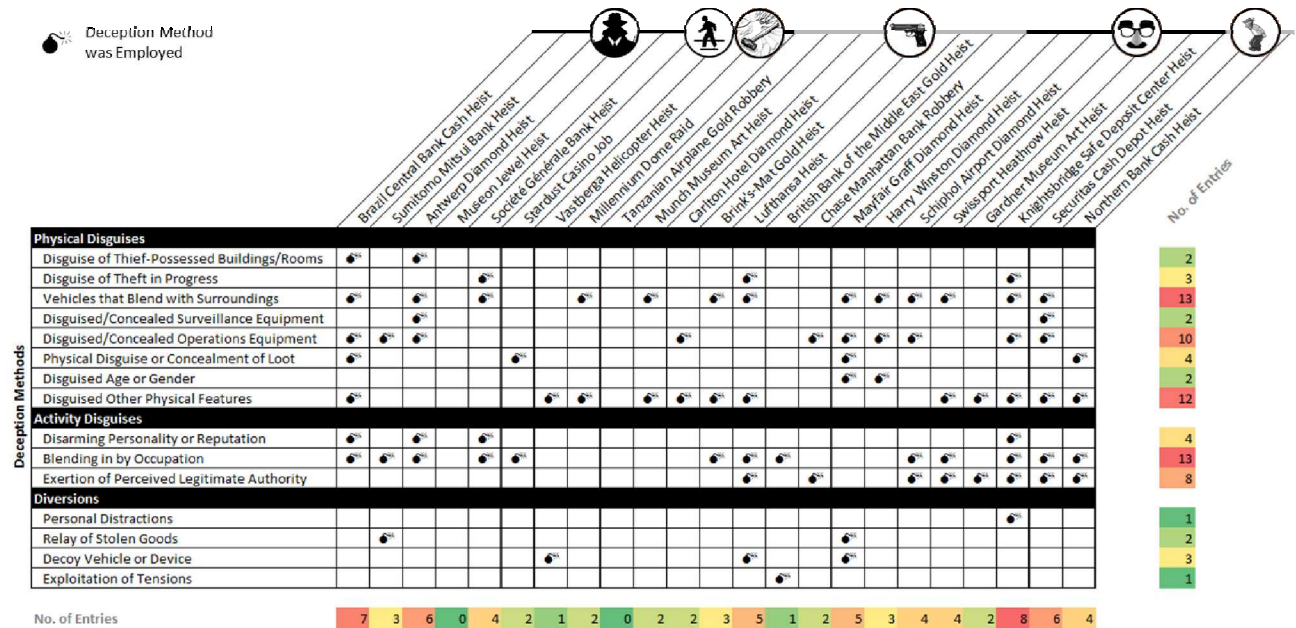
The deceptions noted in Table 3 can be categorized as (1) Physical Disguises, (2) Activity Disguises, or (3) Diversions. Most deceptions fall into the first two categories, involving concealment of a person, place, or object's true identity or purpose via material means (physical disguises) or actions (activity disguises).

As the rightmost column of Table 3 shows, four deception methods are particularly common: vehicles that blend with surroundings, disguised or concealed operations equipment, disguised physical features, and blending in by

occupation. The latter is perhaps the most interesting: The database is replete with examples of criminals who have deceptively played the role of a member of a specific organization or occupation. These roles span from customer to owner, either inside or outside the targeted organization.

Interestingly, the deceptions in large heists tend not to be particularly high-tech or complex. For example, only two heists involved specialized spy gear (cameras hidden in bags or clothing). The thief’s challenge in utilizing deceptions appears not to be in their execution per se, so much as it is in planning and selecting the proper deceptions, since a poor choice could result in suspicion and detection.

Table 3. Summary of Deception Methods



3.3. Timing

Some of the most quantifiable characteristics of this study’s 23 heists relate to thieves’ timing. Timing can be considered both in terms of *absolute timing*, referring to timing with respect to calendar months, days, or times, and *relative timing*, referring to timing with respect to relevant events.

With regard to absolute timing, the heists in the HMCD show no clear preference for particular times or for days of the week. However, Fig. 4 helps to illustrate that the character of heists differs substantially depending on time of execution. In Fig. 4, the durations of 16 heists are plotted on a logarithmic scale against the times at which the heists began. This plot illustrates that many of the heists can be cleanly categorized into four timing archetypes: Early Bird Heists (Archetype I), Broad Daylight Heists (Archetype II), Closing Time Heists (Archetype III), and Night Raids (Archetype IV). Importantly, Fig. 4 illustrates that during the daytime, thieves tend to execute rapid heists, likely to avoid detection and response during hours of high activity. Conversely, rapid heists (e.g., under an hour) are almost nonexistent outside normal work hours. This suggests that thieves have little need to engage in rapid operations when not pressured by the high likelihood of daytime activity and detection.

A less quantifiable but equally important investigation of thief timing is a characterization of the events relative to which thieves planned their heists. Among the heists in the HMCD, three qualitative timing factors are particularly common: First, thieves frequently choose to commit large heists at times of low bystander activity, examples include the late-night Valentine’s Day weekend theft at the Antwerp Diamond Center and the yet-unsolved 4:00 AM theft from the Museon science museum. Second, thieves frequently choose to commit large heists at times of low employee or security activity, examples include the 3:00 AM assault on the small graveyard shift at the Kennedy Airport Lufthansa Cargo Terminal and the 1:30 AM attack on the Gardner Museum, which

was protected only by an overnight force of two unarmed guards. Third, thieves frequently choose to commit large heists at times of high target value. For example, the Lufthansa Heist was expedited as soon as a Lufthansa cargo supervisor and insider informed a preassembled Mafia gang that an unusually large shipment of cash was being stored in the Lufthansa Cargo Terminal over the weekend.

3.4. Weapons

Among the tools that criminals frequently have at their disposal in the commission of a high-value heist are weapons, typically from categories of conventional firearms, explosives and incendiaries, bladed weapons, and blunt weapons. These tools are almost always intended for defeating human components of security systems. The most frequently employed fall into the conventional firearms category, such as the assault rifles, shotguns, and handguns used to threaten the depot manager, his family, and his employees in the Securitas Cash Depot Heist.

Nevertheless, while 70% of heists in the HMCD involved weapon use, seven (30%) involved no known use of weapons. These heists comprise both nonviolent categories (i.e., Stealth Raid and Walk Away heists) plus the Gardner Museum Art Heist. Strikingly, these weaponless heists account for three of the top four valued heists in the database. In short, an unarmed adversary is not an unimportant adversary. Albert Spaggiari, mastermind of the Société Générale Bank Heist, summarized this weapons-free philosophy when he famously wrote on the wall of the vault that he robbed, “Sans arme, ni haine, ni violence,” or “Without weapons, nor hatred, nor violence.”

3.5. Resources

Perhaps the most frequently impressive aspects of high-value heists are the depth of planning and the resources, in both time and money, that thieves will invest in designing the perfect heist. Table 4 provides an overview of some quantitative parameters that illustrate this depth of planning and resource investment.

The first three parameters in Table 4 highlight facets of planning. First, the estimated planning periods of heists in the HMCD span from two weeks to two years. While 70% of heists involved known planning times of less than 30 weeks (7 months), four spanned more than 100 weeks. Among these is the Antwerp Diamond Heist, with a planning time of about 2.4 years; during this time, the crime’s mastermind became an Antwerp Diamond Center tenant to conduct reconnaissance of the center’s security measures. Relatedly, Table 4 shows that thieves rarely attempt a heist without a practice or reconnaissance run. While about two-thirds of the heists for which this data is available likely involved less than six such runs, the remainder involved thirty or more. The latter describes teams with inside access, for example with an inside employee able to make observations at work on a daily basis. The third parameter in Table 4 illustrates the envelope of capabilities thieves can bring to bear on transporting loot. In short, thieves have demonstrated the ability to steal anything from briefcases to trucks full of loot.

As with any major undertaking, lawful or criminal, perpetrators of high-value heists accept some financial risk. Equipment must be purchased, getaway vehicles must be procured, and insiders may need to be incentivized. Toward the low end of Table 4’s Total Expenditures spectrum are heists like the Stardust Casino Job, which required expenditures perhaps for the purchase of a backpack to carry stolen money out of the casino. At the other extreme is the Brazil Central Bank Cash Heist, which involved renting a storefront, advance payment of about \$3,000 to members of the tunnel-digging crew, a \$100,000 bribe to a security guard, and the purchase of about 10

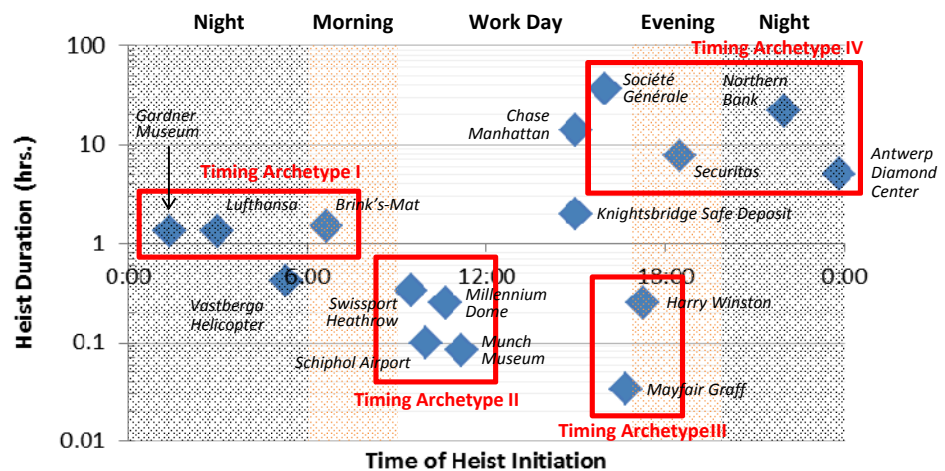


Figure 4. Heist Duration vs. Time of Heist Initiation.

Data shown for 16 heists for which both pieces of data could be obtained.

cars in which to hide portions of the loot. The Return on Investment Ratio metric, however, shows why such expenditures are justified: The potential returns on investment are enormous. The *minimum* estimated return on investment ratio in the data was 110, corresponding to the high-cost Brazil Central Bank Cash Heist. Return on investment ratios in the database span several orders of magnitude above this (consider, for example, the Sumitomo Mitsui Bank Heist, which would have had a cost in the tens of dollars but netted over \$400 million); the arithmetic mean is about 1.5 million, and the median is 39,000. Even in the worst case, these high-value heists have the potential for orders of magnitude returns on investment.

Table 4. Heist Resources and Planning Characteristics.

Parameter	Units	Sample Size	Mean	Minimum	25 th Percentile	Median	75 th Percentile	Maximum
<i>Planning and Transportation</i>								
Planning Time	Weeks	15 heists	39	2	9	17	67	124
No. of Practice and Reconnaissance Runs	Runs	17 heists	79	0	1	2	34	1000
Weight of Stolen Items	Pounds	23 heists	2,500	0	15	100	2,250	20,200
<i>Financial Stakes and Returns</i>								
Total Expenditures	\$FY12	20 heists	48,800	0	200	750	8,320	745,000
Return on Investment Ratio	N/A	19 heists	1,500,000	110	5,960	39,000	308,000	23,900,000
<i>Human Resources</i>								
No. of Willing Accomplices at Crime Scene	People	22 heists	5	1	3	4	7	14
No. of Teams in Crime Scene Vicinity	Teams	22 heists	2	1	1	1	2	4
Accomplice Age	Years	83 people	36	18	31	34	42	74

In addition to time and financial resources, a key component in the planning of a major heist is the selection and management of human resources. This includes decisions on the number and size of teams as well as the characteristics of individual team members. The data show that solo heists are exceedingly rare; the only such heist in the database is the Stardust Casino Job. However, heists consisting of crime-scene teams of more than eight are also exceedingly rare. On average, heists in the HMCD involved 4-5 willing on-scene accomplices. Such a team is large enough to possess a diversity of skills and appreciable manpower, but also small enough to avoid undue risk of detection. Table 4 also highlights a preference for the low complexity of single-team operations; just over half of the heists in the database involved a single team in the crime scene vicinity. The number of heists with two, three, and four teams decreases almost geometrically. Among the data in the HMCD are also basic age, gender, occupation, and nationality profiles for criminals responsible for the 23 heists. These data provide the basis for three interesting observations: First, all 133 criminals in the database for whom gender was known were male. Second, the average age for the 83 criminals in the database for whom age (at the time of the crime) was known is 36 years (see Table 4), about a decade older than typical robbers, burglars, or other property criminals.²¹ This may be linked to the fact that high-value heist criminals in the database have typically made a career out of theft and are highly experienced. Third, 74% of heists in the database involved criminal teams that were native to the country in which the heist took place. In 16% of heists, the criminal team included both foreign and native citizens, and in only 10% of heists (specifically, the Antwerp Diamond Heist and British Bank of the Middle East Gold Heist) were the teams thought to consist entirely of citizens from foreign nations.

3.6. Insiders

Insider involvement is exceedingly common in the planning and execution of high-value heists. For the purposes of this paper, an insider is defined as a person recognized or accepted as a member of a group or organization who has authorized access to restricted areas, equipment, or information. These individuals take a wide variety of forms and can be characterized by at least two dimensions: Origin and Role.

Origin refers to the means by which an insider became an insider. For the heists of the HMCD, the Origin dimension is well summarized by five categories: Planted, Recruited, Opportunistic, Unwitting, and Coerced. Role refers to the type of actions that an insider takes in the commission of a heist. For the heists of the HMCD, role is well summarized by three categories: Active Violent, Active Nonviolent, and Passive.

Figure 5 summarizes the distribution of insiders in the HMCD among different origins and roles. The most striking characteristic about this joint distribution is that there exist nearly three times as many examples of coerced, active nonviolent insiders as any other type of insider. That is, the most common inside help that thieves receive during a high-value heist comes from unwilling participants. This is simultaneously troubling and promising. It is troubling in that it suggests executing a heist is not simply about bypassing networks of alarms and sensors, but very frequently about subverting human will and manipulating individuals to take actions that they do not wish to take. It is promising in the sense that, for these coerced insiders, the will to subvert the security system never existed. If security system designers can provide these potentially coerced insiders with tactics to free themselves from such coercion when it occurs, the insider problem may largely be mitigated. For example, in the Securitas Cash Depot Heist, the security booth contained a sign that advised staff: “Don’t Be a Hero” While sound advice aimed at saving the lives of employees, the same advice invites attacks by criminals who know the staff will surrender at the sight of a weapon. An important consideration in security system design is whether tactics can be devised that simultaneously preserve human life and undermine the thief plans.

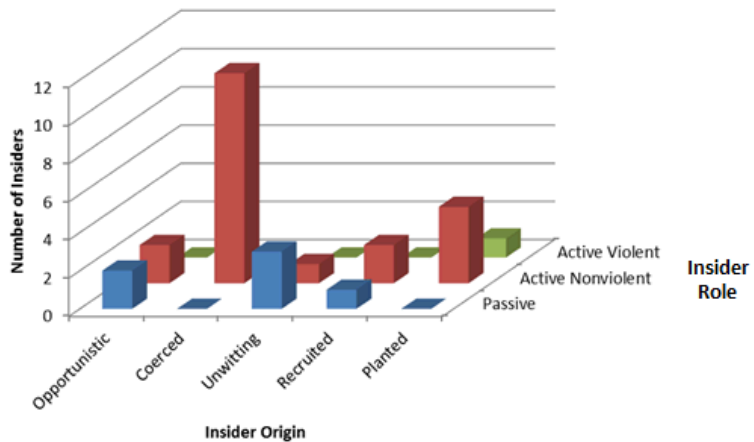


Figure 5. Distribution of Insiders over Origins and Roles.

One important aspect of insiders not visible from Fig. 5 is the number of insiders typically involved in a heist. First, it is interesting to note that the number of *willing* insiders was limited to one in all but one of the heists in the database; the exception was the Knightsbridge Safe Deposit Center Heist, in which both the owner and a safe deposit box renter colluded to perpetrate the heist. Second, heists in the database with *coerced* insiders are rarer than heists with willing insiders but involve more insiders per incident. An example of collusion among unwilling insiders occurred in the Northern Bank Cash Heist, in which the families of two bank employees, Chris Ward and Kevin McMullan, were held hostage while Ward and McMullan assisted thieves in robbing the bank. However, looking at the aggregate of willing and unwilling insiders shows that multiple-insider heists are actually more common in the database than single-insider heists. In summary, not only are insiders common among high-value heists, but clear threats also originate from multiple insiders, both unwillingly and willingly colluding.

4. Conclusion

This paper has presented key findings from a recent survey of 23 sophisticated and high-value heists, with particular emphasis on events from the past three decades. The results of this survey have been compiled in a Heist Methods and Characteristics Database (HMCD) and analyzed qualitatively and quantitatively, with the goals of (1) characterizing the range and diversity of criminal methods and (2) identifying characteristics that are common (or uncommon) in high-value heists. The analysis has been structured into six focus areas: (1) Defeated Security Measures and Devices, (2) Deception Methods, (3) Timing, (4) Weapons, (5) Resources, and (6) Insiders.

Several key lessons have been identified in each focus area. In brief, the typical perpetrator of a high-value heist is a 30-39 year old man and experienced career criminal who is native to the country whose valuables he is targeting. The typical on-scene criminal team consists of 2-8 accomplices, typically perpetrating the robbery as a single team, although breaking into multiple sub-teams is not uncommon. Use of weapons is typical but in many cases not required for success. Thieves are willing to devote substantial resources to planning, spending in some cases more than two years, hundreds of thousands of dollars, and procuring transportation for thousands of pounds of loot. Thieves are frequently thorough and innovative in their planning, developing security defeat methods that

are physically simple but highly targeted toward vulnerabilities the thieves have identified in advance of the heist. In the identification and exploitation of these vulnerabilities, deceptions and insiders almost always play a role. Multiple insiders, unwillingly or willingly colluding, are not uncommon; and while insiders span a variety of origins and roles, by far the most common type is the coerced insider who unwillingly assists in the crime, often upon threat of losing his own life or the lives of his family members.

The survey and analysis presented in this paper has certainly only scratched the surface of security insights that may be gained through the study of high-value heists and related crimes. Future work is recommended in a variety of areas, including database expansion, and comparative analysis between high-value heist methods and methods used to perpetrate lower-value heists, illicit tunneling, high-firepower criminal raids, prison breaks, and even fictional novel and motion picture heists.

Ultimately, the insights from studies such as this are aimed at assisting the security systems design and operations communities in more completely protecting against the threats they face and, at a minimum, ensuring that methods thieves have used so successfully in the past are rendered obsolete.

5. References

- ¹ Selby, S. and Campbell, G., *Flawless: Inside the Largest Diamond Heist in History*, Sterling, New York, 2010.
- ² Time Staff, "Top 10 Brazen Heists," *Time*, 4 Aug. 2011, Available: http://www.time.com/time/specials/packages/article/0,28804,1865132_1865133_2086915,00.html [8 Aug. 2012].
- ³ British Broadcasting Corporation, "High-profile heists," *BBC News*, 11 Aug. 2009, Available: http://news.bbc.co.uk/2/hi/uk_news/7019889.stm [14 Aug. 2012].
- ⁴ Discovery Communications, "Top 10 Heists," *Investigation Discovery*, 2012, Available: <http://investigation.discovery.com/investigation/crime-countdowns/heists/heists.html> [8 Aug. 2012].
- ⁵ Shaw Media, "Top Ten Heists of All Time," *History Television*, 2012, Available: <http://www.history.ca/content/contentdetail.aspx?contentid=226> [8 Aug. 2012].
- ⁶ Wilson, C., Schott, I., Shedd, E., Wilson, D., and Wilson, R. (Eds.), *The World's Greatest True Crime Stories*, Barnes & Noble, New York, 2004.
- ⁷ Cummins, J., *Heists: Gripping Exposés of the World's Most Notorious Robberies*, Pier 9, Millers Point, 2011.
- ⁸ Reinstedt, R.N. and Westbury, J., "Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs," *RAND Note N-1498-SL*, April 1980.
- ⁹ Schuller, C.R. and Ford, J.L., "Demand Side Analysis of Theft of Nuclear Materials – Some Insights from the Study of Complex Crime," *Conference on Physical Protection of Nuclear Materials, Proceeding Series of the International Atomic Energy Agency*, Vienna, 10-14 Nov. 1997, pp. 385-393.
- ¹⁰ Bunn, M., *Guardians at the Gates of Hell*, Ph.D. Thesis, MIT, Cambridge, Jan. 2007, Ch. 4.
- ¹¹ Mead Publishing, "Theft nets \$500,000 from Stardust Hotel," *Loose Change*, Vol. 15, No. 1, Nov. 1992, p. 13.
- ¹² Ratliff, E., *Lifted*, Atavist, New York, Available: <https://www.atavist.com/stories/lifted/> [28 Oct. 2012].
- ¹³ "Seven convicted of spectacular helicopter heist," *The Telegraph*, 7 Oct. 2010, Available: <http://www.telegraph.co.uk/news/newsvideo/8049390/Seven-convicted-of-spectacular-helicopter-heist.html> [28 Oct. 2012].
- ¹⁴ Ali, M., *Britain's Biggest Heists: The Brink's Mat Robbery*, Crime and Investigation Network, 2009.
- ¹⁵ Boser, U., *The Gardner Heist*, HarperCollins, New York, 2009.
- ¹⁶ Naughton, T., "Art Attack," *Daring Capers*, New Dominion Pictures, 2009, DVD Disc 1.
- ¹⁷ Sounes, H., *Heist: The True Story of the World's Biggest Cash Robbery*, Simon & Schuster, London, 2009.
- ¹⁸ Austin, M., "Britain's Biggest Heist," *Real Crime*, ITV Studios, 2010.
- ¹⁹ "Securitas robbery: how it happened," *BBC News*, 27 Feb. 2006, Available: http://news.bbc.co.uk/2/hi/uk_news/england/kent/4754786.stm [14 Jan. 2013].
- ²⁰ Campbell, D., "Caught on video: UK's biggest cash robbery," *The Guardian*, 1 Aug. 2007, Available: <http://www.guardian.co.uk/uk/2007/aug/02/ukcrime.topstories3> [14 Jan. 2013].
- ²¹ "Age-Specific Arrest Rates and Race-Specific Arrest Rates for Selected Offenses 1993-2001," *Uniform Crime Reports*, U.S. Department of Justice Federal Bureau of Investigation, Nov. 2003.

SANDIA REPORT

SAND 2014-1790

Unclassified Unlimited Release

Printed April 2014

The Perfect Heist

Recipes from Around the World

Jarret M. Lafleur, Ph.D.

Liston K. Purvis, Ph.D.

Alex W. Roesler, Ph.D.

Sandia National Laboratories, Livermore, California

MIDN Paul Westland

U.S. Naval Academy, Annapolis, Maryland

Prepared by

Sandia National Laboratories

Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: <http://www.osti.gov/bridge>

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>



SAND2014-1790
Unlimited Release
Printed April 2014

The Perfect Heist: Recipes from Around the World

Jarret M. Lafleur, Ph.D., Systems Research and Analysis IV
Liston K. Purvis, Ph.D., Systems Research and Analysis I
Alex W. Roesler, Ph.D., National Security and Policy Analysis

Sandia National Laboratories
P.O. Box 969
Livermore, California 94550

MIDN Paul Westland
U.S. Naval Academy
121 Blake Road
Annapolis, Maryland 21402

Abstract

Of the many facets of the criminal world, few have captured society's fascination as has that of high stakes robbery. The combination of meticulousness, cunning, and audacity required to execute a real-life *Ocean's Eleven* may be uncommon among criminals, but fortunately it is common enough to extract a wealth of lessons for the protection of high-value assets. To assist in informing the analyses and decisions of security professionals, this paper surveys 23 sophisticated and high-value heists that have occurred or been attempted around the world, particularly over the past three decades. The results, compiled in a Heist Methods and Characteristics Database, have been analyzed qualitatively and quantitatively, with the goals of both identifying common characteristics and characterizing the range and diversity of criminal methods used. The analysis is focused in six areas: (1) Defeated Security Measures and Devices, (2) Deception Methods, (3) Timing, (4) Weapons, (5) Resources, and (6) Insiders.

ACKNOWLEDGEMENTS

The authors owe thanks to numerous individuals at the New Mexico and California sites of Sandia National Laboratories, especially technical staff members in the Homeland Security and Defense Systems Center in California and the Security Systems and Analysis Center in New Mexico. Particular thanks are owed to Greg Wyss, John Clem, Carla Ulibarri, Felicia Duran, Bill Rorke, John Hinton, Gary Richter, Matthew Sumner, and Amy Askin for their helpful comments, suggestions, and insights. The helpful suggestions of Rizwan Ladha of Tufts University were also much appreciated. Additionally, much of the research in this paper was facilitated by the tireless work of Tiffany Vargas and Susan Fourt in the Sandia California Technical Library. We also very gratefully acknowledge the work of MIDN Meredith Lipp and the coordinators of Sandia's Military Academic Collaboration program in both New Mexico and California, Staci Dorsey and Lisa Corcoran.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

TABLE OF CONTENTS

Executive Summary	9
1. Introduction: How to Steal \$100,000,000	11
2. Heists Considered	13
2.1. Related Literature.....	13
2.2. A Heist Taxonomy	17
2.2.1. Nonviolent Class of Heists.....	17
2.2.2. Violent Class of Heists.....	20
3. Analysis	27
3.1. Defeated Security Measures and Devices	27
3.1.1. Security Measure Defeats	27
3.1.2. Security Forces.....	33
3.2. Deception Methods	38
3.2.1. Common Deception Methods	39
3.2.2. Deception Methods per Heist.....	40
3.3. Timing and Target Selection.....	44
3.3.1. Absolute Timing	44
3.3.2. Relative Timing.....	49
3.3.3. Target Selection	50
3.4. Weapons Employed	53
3.5. Resources and Risk Acceptance	55
3.5.1. Planning Time and Schedule.....	55
3.5.2. Practice Runs and Testing.....	57
3.5.3. Transportation Capabilities	57
3.5.4. Human Resources	58
3.5.5. Financial Risks and Returns.....	61
3.5.6. Risk Acceptance.....	62
3.6. Insiders.....	64
3.7. Failures and Mistakes	68
3.7.1. Security Failures	69
3.7.2. Thief Failures	69
4. Conclusions.....	71
4.1. Who is the adversary?.....	71
4.2. Lessons Learned.....	72
4.3. Future Work.....	75
5. References.....	77
6. Appendix: Compiled Heist Details	81
6.1. Nonviolent Heists.....	81
6.2. Violent Heists.....	88
Distribution	105

LIST OF TABLES

Table 1. Identifying information for heists examined.....	14
Table 2. Traceability for heists in this study among sources recognizing top heists	15
Table 3. Summary of Defeated Security Measures.....	31
Table 4. Known Security Measure Defeat Methods.	32
Table 5. Summary of Deception Methods.	41
Table 6. Known Deception Methods.	42
Table 7. Summary of roles that heist accomplices (willing or coerced) have taken when blending in by occupation.	44
Table 8. Distribution of Heists in the HMCD among Targeted Valuables and Settings.	51
Table 9. Estimated Latitude/Longitude Coordinates of Heists in the HMCD.	53
Table 10. Summary of Weapons Used by Thieves.....	56
Table 11. List of Occupations for High-Value Heist Accomplices.	61

LIST OF FIGURES

Figure 1	Distribution among class and categories	17
Figure 2	Hierarchical summary of the six heist categories and two heist classes	18
Figure 3	Promotional Grama Sintética (Synthetic Grass) company baseball caps	18
Figure 4	Vault of the Antwerp Diamond Center after the 2003 heist	19
Figure 5	Entrance to Spaggiari's tunnel	19
Figure 6	Security camera footage of the helicopter on the roof of the G4S Cash Depot	20
Figure 7	Security camera footage of the backhoe driving through a fence	20
Figure 8	Thieves making their getaway	21
Figure 9	Computer rendering of the interior of the Brink's-Mat inner and outer vaults	21
Figure 10	CCTV image of thieves being let in to Graff Diamonds.49	22
Figure 11	Empty frames where artwork once stood in the Gardner Museum	23
Figure 12	Knightsbridge safe deposit boxes in the aftermath of the 1987 heist	24
Figure 13	CCTV image of thieves, including one dressed as a police officer	24
Figure 14	Statuses of Guard Stations at Target Premises during Heists	33
Figure 15	Existence of Active Guards at Target Premises during Heists	33
Figure 16	Correlations between the existence of active security personnel and thieves' use of weapons. 34	
Figure 17	Distribution of Heist Knowledge-Response Profiles	35
Figure 18	Number of Security Personnel Defeated	36
Figure 19	Weak correlations between thief force size and both security force size and number of non-thief witnesses	36
Figure 20	Distances to Nearest External Guard Post or Police Station	37
Figure 21	Time of Day Distribution of Heists in the HMCD	45
Figure 22	Heist Duration vs. Time of Heist Initiation	47
Figure 23	Daily Distribution of Heists in the HMCD	47
Figure 24	Monthly Distribution of Heists in the HMCD	48
Figure 25	Seasonal Distribution of Heists in the HMCD	48
Figure 26	Fraction of Local Accessible Valuables Stolen among Heists in the HMCD	51
Figure 27	Target Environments among Heists in the HMCD	52
Figure 28	Continental Distribution among Heists in the HMCD	52
Figure 29	Distribution of Heist Planning Times	55
Figure 30	Distribution of Number of Practice and Reconnaissance Runs	57
Figure 31	Weight of Stolen Items for HMCD Heists	58
Figure 32	Renault truck recovered in connection with the Securitas Cash Depot Heist	58
Figure 33	Number of Willing Accomplices at Crime Scene	59
Figure 34	Number of Teams in Crime Scene Vicinity	59
Figure 35	Crime Scene Participation Rate	59
Figure 36	Distribution of Accomplice Ages (n = 83)	60
Figure 37	Criminal Team Nationality	60
Figure 38	Estimated Thief Expenditures	61
Figure 39	Estimated Thief Return on Investment Ratio	62
Figure 40	Was an insider used?	64
Figure 41	Examples of insiders, ordered by their degree of inside access	65
Figure 42	Summary of Activity among Insiders within the HMCD	67
Figure 43	Distributions of Insider Numbers across Heists	68

EXECUTIVE SUMMARY

Of the many facets of the criminal world, few have captured public fascination and awe as has that of high stakes robbery. From the 1960 *Ocean's 11* to the 2001 *Ocean's Eleven*, from the 1969 *Italian Job* to the 2003 *Italian Job*, and from the 1968 *Thomas Crown Affair* to the 1999 *Thomas Crown Affair*, the public to this day remains enamored with the daring, the complexity, and the romance of robbery. While much of what they know comes from recreations on the big screen, reality is often not dissimilar from these retellings. Criminals with enough motivation frequently find ways to overcome all obstacles between them and their targets. These criminals plague and frustrate the security forces of banks, museums, and other protective services around the world.

This paper extensively surveys 23 sophisticated and high-value heists of cash, gold, gems, artwork, and other valuables that have occurred or been attempted across the world, particularly over the past three decades. The results of this survey are compiled in a Heist Methods and Characteristics Database (HMCD) and analyzed qualitatively and quantitatively, with the goals of characterizing both the range and diversity of criminal methods and identifying characteristics that are common (or uncommon) in such high-value heists. The analysis is structured into seven focus areas: (1) Defeated Security Measures and Devices, (2) Deception Methods, (3) Timing and Target Selection, (4) Weapons Employed, (5) Resources and Risk Acceptance, (6) Insiders, and (7) Failures and Mistakes.

Several key lessons are identified in each focus area, and an overview of the commonalities and bounds of criminal team characteristics and capabilities is provided. In brief, the typical criminal is a 30-39 year old man and experienced career criminal who is native to the country whose valuables he is targeting. The typical on-scene criminal team consists of 2-8 accomplices, typically perpetrating the robbery as a single team, although breaking into multiple sub-teams is not uncommon. Use of weapons is typical but in many cases not required for success. Thieves are willing to devote substantial resources to planning, spending in some cases more than two years, hundreds of thousands of dollars, and procuring transportation for thousands of pounds of loot. Thieves are frequently thorough and innovative in their planning, developing security defeat methods that are physically simple but highly targeted toward vulnerabilities the thieves have identified in advance of the heist. In the identification and exploitation of these vulnerabilities, deceptions and insiders almost always play a role. Multiple insiders, unwillingly or willingly colluding, are not uncommon; and while insiders span a variety of origins and roles, by far the most common type is the coerced insider who unwillingly assists in the crime, often upon threat of losing his own life or the lives of his family members.

Lessons such as these, developed through rigorous analysis of available data, are intended to assist in informing the analyses and future decisions of security professionals, particularly those charged with the task of guarding assets of particularly high value.

1. INTRODUCTION: HOW TO STEAL \$100,000,000

On the morning of Monday, February 17, 2003, concierge Jorge Dias De Souza descended two levels beneath Antwerp's Diamond Center. Expecting to open the center's vault for a normal day of business, he was astonished to discover the lights on, the vault door open, and 109 of the center's 189 safe deposit boxes wide open, with millions of dollars' worth of discarded contents littering the floor. What was not on the floor was what the thieves *could* carry with them: between \$108 million and \$432 million worth of diamonds, gold, cash, and other valuables. The theft was later dubbed the heist of the century.¹

Located within the Secure Antwerp Diamond Area, the Diamond Center had been thought to be among the most fortified businesses in the world. Entry into the center's vault required a controlled access card to enter the building, a two-story descent underground to a guard-controlled gate, and both a key and one of 100 million possible combinations to open the foot-thick steel vault door. If a person somehow entered the vault unauthorized, he would be detected by a broken magnetic door seal as well as a microwave Doppler motion detector, infrared energy detector, and light detector within the vault itself. If he tried to tunnel in, he would be detected by seismic sensors. With a police station not more than 200 feet from the Diamond Center's front entrance – and a police kiosk even closer – any detected thief would be captured in minutes. Since all the detectors were silent alarms, the thief wouldn't know he had been detected until he was surrounded. Remarkably, the Antwerp thieves discovered how to defeat *all* of these measures.¹

The Antwerp diamond heist is one of several that have gained global notoriety, and it is unusual for any modern list of top heists (e.g., see Refs. 1-7) to ignore it. Such heists are often distinguished by the staggering value of items stolen, typically tens or hundreds of millions of dollars. However, from the point of view of a security systems analyst, the questions of greater interest than the value of items stolen include: How did the thieves execute the crime? What security systems did they defeat? What roles did deceptions and insiders play? What attracted the thieves to their targets, what resources did they invest, and what risks did they take? What could security forces have done differently?

This paper examines 23 sophisticated and high-value heists and heist attempts that have occurred across the globe, particularly over the last three decades. The stories of these heists are dissected and analyzed in substantial depth with two goals in mind: First, they are used to both quantitatively and qualitatively characterize the range and diversity of criminal methods utilized in large heists. Second, the characteristics of these heists are analyzed to identify commonalities in how they were accomplished. The results, in the form of data, observations, and lessons learned, are intended to help inform the analyses of security professionals.

2. HEISTS CONSIDERED

Table 1 provides a list of all 23 heists considered in this analysis. While by no means comprehensive, and open for expansion, this list incorporates major heists and heist attempts that appear frequently in modern lists of the most notorious heists (e.g., Refs. 1-7). In some cases, these heists are notorious for the high value of the items stolen; the average value of items stolen from the heists in Table 1 is well over \$100 million in equivalent fiscal year (FY) 2012 American dollars. In other cases, they are known for the inventive methods the thieves used to gain access to the target valuables. In many cases, they are distinguished by both of these characteristics.

Table 2 shows which of the 23 heists are recognized in Refs. 1-7. On average, each heist in this database is recognized in two of these seven sources. Five heists are considered “failed” in that the thieves were unsuccessful in removing high-value items from the targeted locations; although none of these are recognized in any of the seven sources, they are included as important sources of information regarding methods used by thieves of high-value items.

2.1. Related Literature

Although individual heists are remarkably popular topics for books, documentaries, and mainstream motion pictures,* systematic studies across multiple high-value heists are difficult to locate. Quantitative, data-driven studies are rarer still. While the field of criminology has its origins in the 18th century, quantitative criminology is still gaining acceptance, to the extent that a former editor of the *Journal of Quantitative Criminology* noted in 2010, “Some criminologists also continue the anti-intellectual practice of rejecting quantitative methods entirely.”⁹

Even within the field of physical security, Bitzer and Hoffman note, “The current state of research in the field of physical security could be described as fragmented or multidisciplinary, depending on your outlook. Physical security is primarily an applied field so, unlike areas like mathematics or physics, it has no dedicated line of research.”¹⁰ Furthermore, Warner observes that “there are few peer-reviewed journals dedicated to the field of physical security. Papers about physical security are scattered throughout the (not very large) universe of existing periodicals, but perhaps not in the numbers we might expect for a field of this importance.”¹¹

* See Ref. 8 for some history on heist (or caper) films, the popularity of which dates back to the 1950s but has seen a recent resurgence through movies such as *The Thomas Crown Affair*, *Ocean’s Eleven*, and *The Italian Job*.

Table 1. Identifying information for heists examined.

ID	Name	Date	Location	Category	Success?	Approx. Value of Items Stolen* (\$FY12M)
1	Brazil Central Bank Cash Heist	Sat., Aug. 6, 2005	Fortaleza, Brazil	Stealth Raid	✓	81.9
2	Sumitomo Mitsui Bank Heist	Sat., Oct. 2, 2004	London, UK	Stealth Raid		478.5
3	Antwerp Diamond Heist	Sat., Feb. 15, 2003	Antwerp, Belgium	Stealth Raid	✓	332.1
4	Museon Jewel Heist	Mon., Dec. 2, 2002	The Hague, Netherlands	Stealth Raid	✓	15.4
5	Société Générale Bank Heist	Sat., July 17, 1976	Nice, France	Stealth Raid	✓	40.4
6	Stardust Casino Job	Tues., Sept. 22, 1992	Las Vegas, USA	Walk Away	✓	0.8
7	Vastberga Helicopter Heist	Wed., Sept. 23, 2009	Stockholm, Sweden	Smash and Grab	✓	6.1
8	Millennium Dome Raid	Tues., Nov. 7, 2000	London, UK	Smash and Grab		666.1
9	Tanzanian Airplane Gold Robbery	Thurs., Jan. 5, 2012	Geita, Tanzania	Subdue and Seize		30.5
10	Munch Museum Art Heist	Sun., Aug. 22, 2004	Oslo, Norway	Subdue and Seize	✓	137.9
11	Carlton Hotel Diamond Heist	Thurs., Aug. 11, 1994	Cannes, France	Subdue and Seize	✓	69.3
12	Brink's-Mat Gold Heist	Sat., Nov. 26, 1983	London, UK	Subdue and Seize	✓	85.9
13	Lufthansa Heist	Mon., Dec. 11, 1978	New York, USA	Subdue and Seize	✓	28.2
14	British Bank of the Middle East Gold Heist	Tues., Jan. 20, 1976	Beirut, Lebanon	Subdue and Seize	✓	204.6
15	Chase Manhattan Bank Robbery	Tues., Aug. 22, 1972	New York, USA	Subdue and Seize		1.2
16	Mayfair Graff Diamond Heist	Thurs., Aug. 6, 2009	London, UK	Deceive, Subdue, and Seize	✓	68.9
17	Harry Winston Diamond Heist	Thurs., Dec. 4, 2008	Paris, France	Deceive, Subdue, and Seize	✓	111.3
18	Schiphol Airport Diamond Heist	Fri., Feb. 25, 2005	Amsterdam, Netherlands	Deceive, Subdue, and Seize	✓	115.8
19	Swissport Heathrow Heist	Mon., May 17, 2004	London, UK	Deceive, Subdue, and Seize		71.1
20	Gardner Museum Art Heist	Sun., March 18, 1990	Boston, USA	Deceive, Subdue, and Seize	✓	440.0
21	Knightsbridge Safe Deposit Center Heist	Sun., July 12, 1987	London, UK	Deceive, Subdue, and Seize	✓	130.0
22	Securitas Cash Depot Heist	Tues., Feb. 21, 2006	Tonbridge, UK	Tiger Kidnapping	✓	104.0
23	Northern Bank Cash Heist	Sun., Dec. 19, 2004	Belfast, UK	Tiger Kidnapping	✓	60.5

*In the case of failed heists, this refers to the approximate value of items *attempted* to be stolen. Also, except where otherwise noted, all monetary amounts in this paper are given in units of fiscal year 2012 (FY12) equivalent dollars.

Table 2. Traceability for heists in this study among sources recognizing top heists

ID	Heist Name	Internet Sources				Book Sources		
		Time ²	BBC ³	Discovery ⁴	History ⁵	Flawless ¹	True Crime ⁶	Heists ⁷
1	Brazil Central Bank Cash Heist	✓	✓			✓		✓
2	Sumitomo Mitsui Bank Heist							
3	Antwerp Diamond Heist	✓		✓	✓	✓		✓
4	Museon Jewel Heist			✓				
5	Société Générale Bank Heist						✓	✓
6	Stardust Casino Job			✓				
7	Vastberga Helicopter Heist	✓						
8	Millennium Dome Raid							
9	Tanzanian Airplane Gold Robbery							
10	Munch Museum Art Heist			✓				✓
11	Carlton Hotel Diamond Heist				✓	✓		
12	Brink's-Mat Gold Heist		✓			✓	✓	✓
13	Lufthansa Heist	✓			✓			✓
14	British Bank of the Middle East Gold Heist	✓	✓		✓	✓		
15	Chase Manhattan Bank Robbery							
16	Mayfair Graff Diamond Heist		✓			✓		
17	Harry Winston Diamond Heist			✓		✓		
18	Schiphol Airport Diamond Heist					✓		
19	Swissport Heathrow Heist							
20	Gardner Museum Art Heist	✓		✓	✓			
21	Knightsbridge Safe Deposit Center Heist		✓			✓	✓	
22	Securitas Cash Depot Heist		✓			✓		✓
23	Northern Bank Cash Heist		✓			✓		

Perhaps the greatest published interest and analysis of high-value heists exists not in the pure criminology or physical security fields, but rather in the area of nuclear security. Some of the earliest work in this area was summarized in a 1980 report by the RAND Corporation.¹² In this report, the analysts pose the study of conventional but high-value robberies and burglaries as reasonable analogs to potential incidents against nuclear programs or facilities, useful since criminal activity against nuclear targets was too low to provide sufficient data to study. The RAND database consisted of 121 sophisticated and high-value burglaries, robberies, and other analogous crimes, and these were analyzed in areas such as insider involvement, number of perpetrators, value of loot, use of violence, coercion, and use of deception. The report aimed at using these examples to emphasize particular areas of vulnerability and to observe correlations between heist characteristics (e.g., value of loot vs. insider participation, value of loot vs. number of perpetrators). Unlike the present study, however, the heists within the RAND database tend to be:

- of much smaller value (120 of the 121 RAND heists are valued at less than \$30 million in FY12 dollars, very different from the 78% of the heists in Table 2 in excess of \$30 million)
- executed by smaller teams (45% of RAND heists involve teams of 1-3 participants, but these heists account only for 18% of the present study's heists)

- less frequently executed using insiders (the ratio of known or suspected insider heists to outsider-only heists in the RAND study is 1.13, while this ratio is 6.00 for the present study)

The reasons for these differences between the RAND heists and those in Table 2 are not immediately clear, though one conceivable explanation is that the passage of the three decades since 1980 may have introduced the world to more massive and complex heists, executed by criminal teams that are larger and that consider insiders a standard element of their modus operandi.

In 1997, Schuller and Ford presented a paper at an International Atomic Energy Agency conference¹³ that applied law enforcement property crime investigation techniques to create a process model of eight basic tasks that criminals must carry out in order to orchestrate a successful theft. An additional five basic requirements were identified, with an apparent focus on stealthy heists of nuclear materials. One finding from the work was that the degree of complexity required for a successful nuclear material theft is formidable, a conclusion that can find further support in the execution details and resource requirements of many high-value heists in the present study.

In 2007, Bunn examined the plausible spectrum of thieves who might seek to steal nuclear weapons or nuclear materials.¹⁴ He noted, “Conceptualizing the problem of the range of different capabilities thieves might have as a spectrum of greater or lesser capability – an essentially one-dimensional concept – is itself a substantial simplification, as thieves’ characteristics may vary across several dimensions ...” The two main dimensions that Bunn proposed were (1) whether thefts were perpetrated by insiders, outsiders, or a mix of the two and (2) whether thefts were covert or overt.[†] Moreover, Bunn described several threats that have been evident in the recent history of crimes involving high-value, guarded non-nuclear targets:

- Large overt attack
- Multiple coordinated teams
- Significant covert attack
- Use of deception and diversion
- Intelligence collection/planning/acquisition of specialized skills
- Use of heavy weapons and sophisticated explosives
- Use of unusual vehicles
- Theft of material in transit
- Use of insiders

Bunn further suggested in 2010 that lessons may be learned from incidents at non-nuclear facilities.¹⁵ Additionally, Bunn and Glynn recently drew analogies to the casino and pharmaceutical industries to better understand how to prevent insider theft in the nuclear industry.¹⁶ Their work largely focused on preventing the diversion of materials by employees.

As a whole, however, with the notable exception of the 1980 RAND study, the current literature only limitedly offers systematic analyses of heists according to their multitude of dimensions or characteristics. The present work seeks to augment and update the existing literature and to create a tool and

[†] While some thefts may be clearly covert (e.g., a crime perpetrated on a weekend that is not discovered until employees return on Monday) or clearly overt (e.g., a smash-and-grab jewelry theft), many crimes fall in a gray area between the two. For example, it is not clear how Bunn would have categorized a crime in which thieves subdue guards before they have a chance to call for help, such that the thieves have plenty of time to commit the theft without needing to worry about a police response. Such a crime is *overt* from the perspective of the guards but *covert* to the outside world.

methodology enabling a transparent and thorough exploration of data associated with the many dimensions of these historic heists.

2.2. A Heist Taxonomy

Each of the individual heists in Table 1 has been methodically researched through open literature such as books, print and online news articles, and documentary films and videos. For each heist, a database entry of 155 fields is populated to the maximum extent that the publicly-available information allows; in total, this collection of information is referred to as the Heist Methods and Characteristics Database (HMCD). The detailed characteristics that comprise most of the database are the subject of Section 3; however, before delving into the details of the data, it serves as an appropriate introduction to observe that the approaches taken by thieves in perpetrating these 23 crimes can be sorted into six conceptually distinct categories. These categories are noted in Fig. 1 and in the fifth column of Table 1 as (1) Stealth Raid, (2) Walk Away, (3) Smash and Grab, (4) Subdue and Seize, (5) Deceive, Subdue, and Seize, and (6) Tiger Kidnapping. The categories themselves might also be sorted into two broad classes based on the level of violence used toward people and property. Characterizations of these classes and categories follow and are also summarized in Fig. 2.

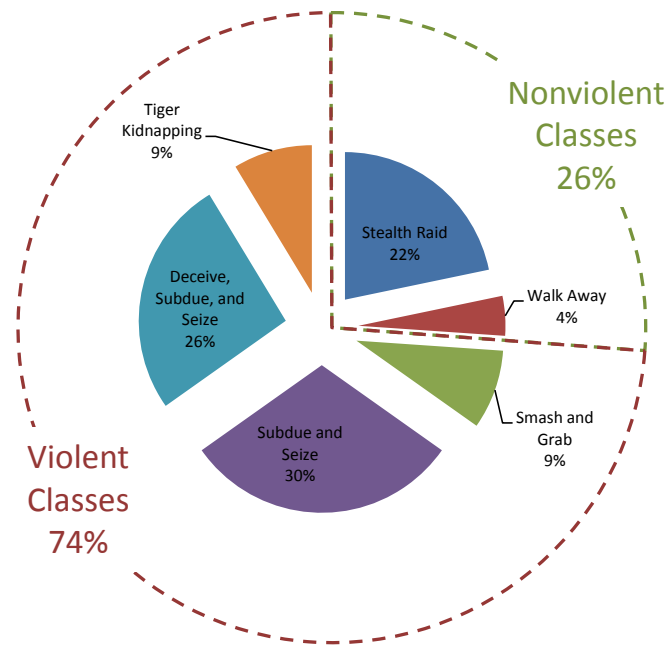


Figure 1. Distribution among class and categories for the 23 heists in this analysis.

2.2.1. Nonviolent Class of Heists

The first two heist categories (Stealth Raid and Walk Away) may be reasonably considered nonviolent heists. These heists tend to involve exceptionally well-planned infiltrations, averaging nearly twice as much planning time as violent heists. The majority of these robberies use insiders, and all but one (which was so stealthy that it remains unsolved) are known to have taken advantage of at least one significant deception, disguise, or diversion. As a result of thieves' extensive planning and use of diversions and deceptions, these heists are executed with minimal use of violence against people and property.

Nonviolent Classes



Stealth Raid

Thieves actively circumvent security measures without the knowledge of security forces.



Walk Away

Thieves passively circumvent security measures without the knowledge of security forces.

Violent Classes



Smash and Grab

Employing violence toward property rather than people, thieves seize valuables by relying on the delay between theft detection and security force response.



Subdue and Seize

Via violent means, individuals and/or security systems are controlled or incapacitated prior to seizure of valuables.



Deceive, Subdue, and Seize

A Subdue and Seize event is preceded by a deception or diversion, typically permitting the thieves access that they would not normally have.



Tiger Kidnapping

A Subdue and Seize event is preceded by a kidnapping, typically of an individual with access and his family, coercing a person with access the thieves need to act as an insider.

Figure 2. Hierarchical summary of the six heist categories and two heist classes.

The major category within the Nonviolent Heist class is the *Stealth Raid*. In this type of heist, exemplified by the Antwerp Diamond Heist described in Section 1, thieves actively subvert security measures in order to remain unseen, unheard, and otherwise undetected by security forces. Heists in this category include:

- **Brazil Central Bank Cash Heist.** Over a period of three months, more than a dozen men posing as employees of a synthetic grass company (see Fig. 3) dug a 656-foot-long tunnel 13 feet under Fortaleza, Brazil, in order to access the vault of the local branch of the Brazil Central Bank. On Saturday, August 6, 2005, the thieves transferred over 7,700 lbs. of cash worth \$81.9 million (FY12 equivalent) out of the bank through their elaborate electrically-lit, air-conditioned, and structurally reinforced tunnel.¹⁵⁻²⁰
- **Sumitomo Mitsui Bank Heist.** On September 16, 2004, two computer hackers in collusion with the security chief of the Sumitomo Mitsui Bank in London installed keylogging software on fund transfer computer terminals. Just over two weeks later, on a weekend, the thieves returned to use this data to attempt \$478.5 million (FY12) in fraudulent transfers to twenty bank accounts in ten countries. To reduce the likelihood that the thieves could be identified, the security chief had dialed down the sensitivity of most of the bank's motion-sensor-triggered cameras. The thieves' plans were foiled only by their improper completion of an interbank communications form. Bank employees called the authorities after returning to work on a Monday and noticing the attempted transactions and severed network cables.²¹⁻²²



Figure 3. Promotional *Gramma Sintética* (Synthetic Grass) company baseball caps handed out by Brazil Central Bank thieves.²⁰

- **Antwerp Diamond Heist.** As detailed in Section 1, Valentine’s Day weekend in 2003 saw the theft of between \$108 million and \$432 million (FY03) worth of diamonds, gold, cash, and other valuables that wealthy diamantaires had stored in safe deposit boxes in the highly secure basement vault of the Antwerp Diamond Center. A career criminal posing as a diamond merchant planted himself as a tenant at the Diamond Center more than two years in advance of the robbery in order to conduct reconnaissance and discover security vulnerabilities. As a result, the Saturday night robbery was executed with such stealth that it was not discovered until the subsequent Monday (see Fig. 4).¹



Figure 4. Vault of the Antwerp Diamond Center after the 2003 heist.²³

- **Museon Jewel Heist.** At 4:00 AM on December 2, 2002, thieves gained entry to a popular Dutch science museum, the Museon, which was hosting a diamond exhibit. The thieves circumvented 24-hour camera surveillance, motion detection, infrared sensors, and security guards to steal approximately \$15.4 million (FY12) worth of diamonds and other jewelry from six of the 28 exhibit reinforced-glass display cabinets. Outside of the missing jewelry, the only evidence of a break-in the thieves left behind was the smashed window through which they entered.²⁴⁻²⁵
- **Société Générale Bank Heist.** In the afternoon of Saturday, July 17, 1976, several men under the leadership of Albert Spaggiari, a French army paratrooper-turned-criminal, finished a two-month job of tunneling 60 feet from the city sewers into the underground vault of the Société Générale Bank in Nice, France (see Fig. 5). In a heist lasting 36 uninterrupted hours, the criminals, including an appraiser to identify the most valuable items, stole \$40.4 million (FY12) in contents from 400 of the 4,000 safe deposit boxes within the bank’s vault, as well as from the bank’s own supply of cash and gold. The heist was not discovered until it was time to open the vault on Monday morning, when bank officials realized the door had been welded shut from the inside. Confirming it as the epitome of a stealth raid, Spaggiari even inscribed on the wall of the vault the words *sans armes, ni haine, ni violence*, or *without weapons, nor hatred, nor violence*.^{7,26}



Figure 5. Entrance to Spaggiari’s tunnel, looking in from the sewer.²⁷

A second category within the Nonviolent Heist class is the **Walk Away** crime. Unlike the Stealth Raid heist, for which thieves actively subvert security measures in order to remain unseen, unheard, and undetected during the commission of the crime, the Walk Away heist is characterized by little or no subversion of physical security measures, but rather by the use of appropriate timing and route planning. Such a heist may involve the crime being committed, but not recognized, in plain sight of security forces operating under normal conditions.

- **Stardust Casino Job.** On September 22, 1992, casino cashier William Brennan took his lunch break at the Stardust Resort and Casino in Las Vegas. As he exited, passing security guards, he was carrying a backpack of cash and chips worth \$800,000 (FY12). Brennan abandoned his Las Vegas apartment after picking up his cat and has not been seen since.^{4,28}

2.2.2. Violent Class of Heists

The final four heist categories (Smash and Grab; Subdue and Seize; Deceive, Subdue, and Seize; and Tiger Kidnapping) are associated with violent heists. With the exception of the Smash and Grab category, all involve some degree of violence against people and the incapacitation or coercion of guards or custodians charged with protecting the targeted high-value items. The Smash and Grab category is distinguished by overt and substantial violence toward property rather than people.

The first category within the Violent Heist class is the *Smash and Grab*. While this category of heist does not involve direct violence toward people, it is characterized by substantial violence toward property. Unlike in a Stealth Raid, the thieves spend little effort avoiding detection; instead, their success relies on the inherent (and sometimes long) delay between detection and security force response. Within the 23 heists considered in this analysis, two fit this description:

- **Vastberga Helicopter Heist.** At 5:15 AM on September 23, 2009, four thieves landed a stolen Bell 206 JetRanger helicopter on the roof of the G4S Cash Depot in Vastberga, Sweden (see Fig. 6). Breaking into the depot through a large pyramid-shaped skylight, the thieves descended via custom-length ladders to the depot's counting room. Breaking through the door using custom-fit explosives, the thieves opened the depot's cash cages with the assistance of a circulating saw. Twenty minutes after they landed, the thieves ascended to the roof and took off with \$6.1 million (FY12) in cash. Thanks to a tip-off from the Serbian foreign ministry, Swedish police had been expecting a helicopter assault on a large cash depot in September, but they were not expecting that the thieves would actively hinder a police response by spreading caltrops across roads near the depot and placing packages resembling bombs outside the police heliport.²⁹⁻³²



Figure 6. Security camera footage of the helicopter on the roof of the G4S Cash Depot. Note the thief in front of the helicopter, preparing to break through the skylight.³²

- **Millennium Dome Raid.** At 9:30 AM on a Tuesday in November 2000, four men on a backhoe (see Fig. 7) smashed into London's Millennium Dome, a 365-meter diameter structure housing a year-long exhibit celebrating the beginning of the third millennium. With dome visitors distracted by smoke bombs, two men in gas masks and body armor then leapt out of the backhoe and within 27 seconds used a nail gun and sledgehammer to smash through the allegedly impregnable glass intended to protect the 203-carat Millennium Star diamond. Fortunately, all



Figure 7. Security camera footage of the backhoe driving through a fence prior to bursting into the Millennium Dome.³⁵

twelve diamonds in the exhibit had been replaced with crystal replicas the previous day, thanks to police efforts anticipating the attack. All the backhoe-riding thieves, as well as a lookout in a van and getaway speedboat pilot, were arrested on the scene before making off with any of the intended \$666.1 million (FY12) loot.³³⁻³⁵

The second category within the Violent Heist class is the *Subdue and Seize* heist, which describes 30% of heists in the database. Each of these heists involves the use of violence intended to incapacitate or coerce of guards or custodians, followed by the seizure of targeted high-value items.

- **Tanzanian Airplane Gold Robbery.** On January 5, 2012, the regularly-scheduled Thursday gold transport airplane was parked at its airstrip near an AngloGold Ashanti mine in Geita, Tanzania. Loaded with \$30.5 million in gold bars weighing nearly 1,300 lbs., the plane came under attack from five men who emerged from the nearby jungle armed with submachine guns, pistols, and hand grenades. Thanks to mine security and police forces, the attack was thwarted. One thief was killed in the firefight.³⁶⁻³⁷

- **Munch Museum Art Heist.** At 11:10 AM on Sunday, August 22, 2004, two armed and masked men entered the Munch Museum in Oslo, Norway. With about 80 visitors in the museum at the time, one thief held visitors and unarmed security guards in the museum's café, while another thief entered a gallery to rip two of Edvard Munch's famous paintings, known as "The Scream" and "Madonna", from the walls. Despite silent alarms on the paintings that alerted police, which had a patrol in the neighborhood, the thieves escaped in minutes (see Fig. 8) and no arrests were made until four months later.³⁸⁻⁴⁰



Figure 8. Thieves making their getaway with "The Scream" and "Madonna" in hand.⁴⁰

- **Carlton Hotel Diamond Heist.** At closing time on a Thursday evening in August 1994, three masked men walked into the jewelry shop within the Carlton Hotel, in Cannes, France. Amidst machine gun fire to threaten employees and customers, the men swept about \$69 million (FY12) in jewels into bags and escaped, never to be seen again. Interestingly, investigations revealed no bullet holes in the jewelry shop; rather, the robbers had been firing blanks.^{1,25}

- **Brink's-Mat Gold Heist.** In November 1983, six armed, masked men entered the Brink's-Mat depot near London's Heathrow Airport ten minutes after its 6:30 AM opening. The six employees present were subdued and bound, and the two employees with vault keys and combinations were called by name, doused with gasoline, and coerced to open the vault doors. Although the thieves were successful at entering the outer vault door (see Fig. 9), the combination-holding employee was so distressed that he could not remember the recently-changed combinations to any of the inner vault doors. Luckily for the thieves, seventy-six boxes of gold bullion worth \$86 million (FY12) sat ready for shipment in the outer chamber of the vault. This gold was loaded into a van and disappeared. It was later revealed that a depot employee, one of the six present at the time of the robbery, provided critical inside information and assistance to the thieves.^{6,41,42}

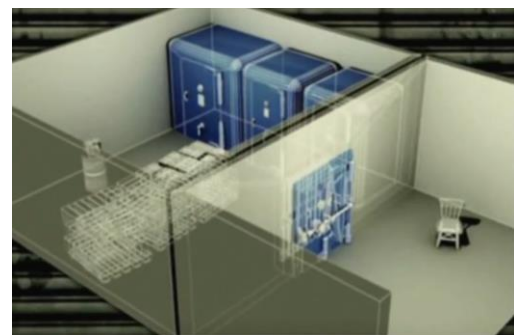


Figure 9. Computer rendering of the interior of the Brink's-Mat inner and outer vaults.⁴¹

- **Lufthansa Heist.** At 3:00 AM one December morning in 1978, seven armed, masked men arrived at the Lufthansa Overseas Cargo Terminal at New York’s John F. Kennedy Airport. Operating in three teams, one man in an automobile waited in the cargo terminal’s parking lot, four men entered the terminal, and the remaining two cut the lock on the security gate, swapped it with a fake replacement, and drove a van to the rear loading areas. Rounding up all ten employees on duty in the terminal, most of whom were on their lunch hour, the thieves forced the supervisor to turn off the facility’s alarms. About 80 minutes after beginning the raid, the thieves left with \$28.2 million (FY12) in cash, gems, and gold. Planning of the heist was made possible by information from a Lufthansa cargo terminal supervisor who was deep in gambling debt to a bookie with mob connections. Reported at the time as the largest cash robbery in U.S. history, the heist helped inspire the popular 1990 film *Goodfellas*. As the movie portrays, however, the criminals’ victory was short-lived: Within a year of the robbery, in an effort to sever connections to the heist, the mob killed all but two of those who had robbed Lufthansa. The remaining two were killed in the mid-1980s.⁴³⁻⁴⁵
- **British Bank of the Middle East Gold Heist.** On January 20, 1976, nine heavily armed soldiers dressed in unmarked military fatigues blasted their way with mortars and grenades into the British Bank of the Middle East in Beirut, Lebanon. Located in a no-man’s land between the Muslim west and Christian east of Beirut during the Lebanese Civil War, the bank was operational only on an ad-hoc basis. Amid the chaos of the war, the force blasted into the bank’s vault and stole an estimated \$204.6 million (FY12) in primarily gold bullion. The identities and affiliations of the perpetrators remains disputed, and little has been publicly documented despite the heist’s fame (see Table 2). The most thorough account found⁴⁶ suggests the heist was perpetrated by a United Kingdom Special Forces unit whose mission was to disguise the seizure of important terrorist group financial documents stored in the bank as a genuine bank robbery.
- **Chase Manhattan Bank Robbery.** At closing time for the Chase Manhattan Bank in New York in August 1972, two ordinary-looking men in the bank produced guns and informed the staff that they were being robbed. Collecting about \$1.2 million (FY12) in cash and traveler’s checks, the two men were impeded in leaving upon the arrival of police, who were informed by a personnel officer at Chase Manhattan’s downtown headquarters that something seemed amiss during a chance phone call he made to the bank manager. Holding the bank staff hostage for some twelve hours, the thieves convince the police to transport them (with their hostages) to an airplane waiting at John F. Kennedy Airport. After arriving at the airport, the Federal Bureau of Investigation (FBI) agent driving the thieves’ limousine, with the assistance of agents in place aside the vehicle, seized an opportunity to shoot and kill one thief and subdue the other.⁴⁷

The third category within the Violent Heist class is termed *Deceive, Subdue, and Seize*, which describes 26% of heists in the database. As the name implies, this heist is defined by a Subdue and Seize event preceded by a deception or diversion, often permitting the thieves access they would not normally have.

- **Mayfair Graff Diamond Heist.** At 4:40 PM on Thursday, August 6, 2009, two men dressed in suits and wearing latex disguises to appear older were let in to the high-end Graff Diamonds shop in London (see Fig. 10). Producing concealed handguns, the men threatened the staff and within two minutes left with \$68.9 million (FY12) in diamonds and



Figure 10. CCTV image of thieves being let in to Graff Diamonds.⁵²

other jewelry – as well as a hostage. Firing warning shots prior to releasing the hostage, the thieves made an initial getaway in a blue BMW fitted with false number plates. The BMW then crashed into a taxi cab, and the jewelry bag was transferred to a man on an orange motorbike. The thieves then switched cars to a waiting silver Mercedes, followed by a second switch to a black vehicle. The first arrests for the crime were not made until nearly two weeks later.⁴⁸⁻⁵⁴

- **Harry Winston Diamond Heist.** At 5:30 PM on Thursday, December 4, 2008, four men, three of whom were dressed as women, requested entry via intercom to the high-end Harry Winston jewelry shop in Paris. Once inside, the men produced a revolver and hand grenade, smashed display cases, and threatened the 15 customers and employees (some of whom were called by name) to assist them in gathering their loot. Within 15 minutes, the thieves calmly drove away from the scene with \$111.3 million (FY12) in diamonds and other jewelry.⁵⁵⁻⁵⁶
- **Schiphol Airport Diamond Heist.** At 10:00 AM on Friday, February 25, 2005, two men dressed in KLM uniforms drove a blue KLM vehicle they had stolen two weeks earlier into the secure freight area at Schiphol Airport in Amsterdam. They then intercepted a truck carrying \$115 million (FY12) worth of diamonds bound for a flight to Antwerp, forcing the two transport guards out of the truck at gunpoint and exiting the security gates by tailgating another truck on its way out. Given the precise timing of the robbery, insider information was suspected but never proven.⁵⁷⁻⁶⁰
- **Swissport Heathrow Heist.** At 9:30 AM on Monday, May 17, 2004, a white delivery van with seemingly legitimate paperwork passed through the security gate at Swissport Cargo Services outside of London’s Heathrow Airport. Unknown to the gate security personnel, the paperwork had been forged with the assistance of an opportunistic insider employed as a delivery driver. Shortly after pulling up to the Swissport warehouse, the van, with eight men on board, backed up and rammed through a rolling door. The gang exited the van and threatened the warehouse staff with at least one firearm as well as knives and clubs. Some thieves began loading into the van the gold bullion that had been delivered to the warehouse some 30 minutes prior, while others approached the cash-containing vault and threatened the custodian in order to obtain his keys. Fortunately for Swissport, Scotland Yard’s Flying Squad had anticipated the attack from prior surveillance of the delivery driver insider, and over 100 police officers were waiting in the vicinity of Heathrow Airport to apprehend the thieves, averting what would likely have been a \$71.1 million (FY12) loss.⁶¹⁻⁶⁴
- **Gardner Museum Art Heist.** At 1:24 AM on Sunday, March 18, 1990, two men posing as Boston Police officers approached the side entrance to the Isabella Stewart Gardner Museum. Claiming to be responding to a disturbance, the officers convinced an on-duty security guard to permit them entrance. To lure the guard away from the panic button at his security booth, the police claimed they had a warrant for his arrest and demanded identification. After the roving guard arrived to assist the guard at the booth, the two men posing as officers handcuffed both guards, wrapped duct tape around their eyes and mouths, and bound them to a steam pipe and workbench in the basement. Over the course of 81 minutes, the thieves made their way through the museum and stole thirteen works of art (see Fig. 11), worth an estimated \$440 million (FY12). Though motion detectors sounded and recorded the movements of the thieves, they transmitted intrusion information only to the guard booth and not to any external force. As a



Figure 11. Empty frames where artwork once stood in the Gardner Museum.⁷⁰

result, the outside world did not know of the heist until the security guards were scheduled to be relieved at 7:00 AM.⁶⁵⁻⁷⁰

- **Knightsbridge Safe Deposit Center Heist.** In July 1987, two men entered the Knightsbridge Safe Deposit Center, the largest safe deposit center in London. One of the men, Valerio Viccei, at that time a client of the center, introduced a friend to the owner, Parvez Latif, who led the two to a private viewing room inside the center's vault. Drawing a pistol, the two men threatened Latif, who was made to request entry into the security guard booth to show the center's security measures. Distracting the security guard, the guard's hand left the panic button and the two thieves subdued him. The front desk security guard was called in to deliver brochures to the owner's office and captured. With both guards subdued, the two thieves attempted to use a two-way radio to call for two waiting accomplices. When the reinforcements failed to answer, Viccei left the safe deposit center and found them nearby, listening to the incorrect radio channel. The thieves used sledgehammers and crowbars to force open 121 of the 5,000 safe deposit boxes in the center (see Fig. 12), making off with an estimated \$130 million (FY12). Thanks to the investigation following the heist, the thieves were eventually captured. Among those sentenced was Parvez Latif himself, who had performed so convincingly during the heist that not even Viccei's hired henchmen knew that he had assisted them by scheduling new guards who would not recognize Viccei and ensuring a technical glitch rendered security cameras useless.^{6,71-72}



Figure 12. Knightsbridge safe deposit boxes in the aftermath of the 1987 heist.⁷¹

The fourth and final category within the Violent Heist class is the *Tiger Kidnapping*, which well describes two heists in the database. Such a heist involves the kidnapping of an individual with critical access privileges as well as, typically, the individual's family. The threat of harm to the kidnapped family is used to coerce the individual to act as an insider.

- **Securitas Cash Depot Heist.** At 6:30 PM on Tuesday, February 21, 2006, the manager of the Securitas Cash Depot some 30 miles southeast of central London was pulled over by two men posing as police officers. Simultaneously, two other men posing as police officers arrived at the manager's residence to inform his wife and child that he had been involved in an accident. In two separate cars, the manager and his family were driven to a farm and held at gunpoint. The thieves told the manager his family would be killed if he did not cooperate, and the manager was brought to the Securitas depot. A thief dressed as a police officer (see Fig. 13) accompanied the manager to the pedestrian entrance, and the manager convinced the control room guard to admit the two and open the main gate, through which three thief vehicles drove. Inside, the thief posing as the police officer subdued the guard, let in his accomplices, subdued the remaining 13 employees inside the depot, and drove away after loading some 6,000 lbs. of cash worth an estimated \$104 million into a truck. Inside information on security measures and procedures



Figure 13. CCTV image of thieves, including one dressed as a police officer, executing the Securitas robbery.⁷⁷

at Securitas had been gathered in advance by Ermir Hysenaj, an Albanian immigrant who was hired as a cash administrator at Securitas two months prior to the robbery.⁷³⁻⁸¹

- **Northern Bank Cash Heist.** At 10:00 PM on Sunday, December 19, 2004, three masked men arrived at the home of Chris Ward, an official of the Northern Bank in Belfast. While two men held hostage Ward's parents, brother, and girlfriend, the third man brought Ward to the home of his supervisor, Kevin McMullan. McMullan and his wife had already been bound by two men who had entered the home posing as police officers. McMullan's wife was taken to an undisclosed location at approximately 11:30 PM. Then, after instructing the two key-holding bank officials on what to do at work the next day, with the consequence of failure being the death of the officials' families, the thieves left the house at 6:30 AM. Returning to work as normal on Monday, Ward and McMullan let the thieves in to the bank once all other employees had left at 6:00 PM. Over the course of two trips with a van, the thieves made off with some \$60.5 million in cash.⁸²⁻⁸⁵

3. ANALYSIS

In this section, data collected for each of the 23 heists in the HMCD are analyzed in order to identify commonalities, trends, and capability envelopes for consideration in security system design and analysis. The analysis is structured as quantitatively as possible but also includes a great deal of qualitative observation. Particular attention is paid to seven focus areas of relevance to security professionals:

- Defeated Security Measures and Devices
- Deception Methods
- Timing and Target Selection
- Weapons Employed
- Resources and Risk Acceptance
- Insiders
- Failures and Mistakes

It is worth noting that complete coverage and analysis of most of these focus areas could easily fill papers of their own. While such studies are under consideration for future work, the present paper highlights the most pertinent findings in each focus area.

3.1. Defeated Security Measures and Devices

*"The vault was reputed to be very nearly impregnable, and it was very difficult to see how anybody could just walk up and go and lift the diamonds out of it."*³⁵

David James
Former Millennium Dome Chairman

The summaries in Section 2.1 highlight the diversity of heists considered within this study. For each heist, one or (usually) more security measures intended to protect high-value items were defeated or rendered ineffective. To the extent that the open and readily available literature allows, this section surveys the security measures that were defeated and the methods that thieves used to defeat them.

3.1.1. Security Measure Defeats

Table 3 contains a summary of security measures and devices that were defeated in the execution of each of the 23 heists in the HMCD. These security measures can be divided into four general categories:

Static barriers are structural or mechanical elements that passively impede the movement of people or objects into or out of a facility. These include fences, walls, windows, and floors, as well as last-line-of-defense barriers dedicated to protecting specific items (e.g., glass cases enclosing jewelry) and anchors dedicated to holding high-value items in place (e.g., steel cables preventing an item from being lifted from its display position). Note that, as tracked in Table 3, the defeat of a static barrier requires destruction of the barrier itself.

Access controls typically secure the access points of a system of static barriers and permit access only to authorized persons. Frequently, these controls take the form of locks that are operated via key or combination. Other access controls encountered in this study are activated via radio frequencies (e.g., garage door openers), access credentials (e.g., badges or paperwork granting access), and recognition of biometric features (automated or otherwise). For the purposes of this study, if unauthorized individuals gain access to an area or assets via the access point, the defeat

of the access point is generally regarded as the defeat of the access control (unless, for example, the control was not active at the time).

Detectors are devices that monitor for unauthorized activity and, often, immediately transmit detections of such activity to security response forces. Detectors encountered in this study include visible-light cameras (often closed-circuit television, or CCTV, cameras), light sensors, infrared sensors, microwave Doppler sensors, and other motion detectors, all of which are aimed at detecting human intrusions into sensitive areas. Less commonly encountered were sensors aimed at detecting physical tampering (such as the detection of the cutting of cables holding a painting to a wall, the smashing of a glass case, or the breaking of a magnetic seal indicating that a door or window is shut).

Security guards are on-premises personnel whose primary duty is to protect the people and property of the facility. In Table 3, guards are distinguished by whether they are armed or unarmed. Note that security guards may serve a variety of purposes, including the assistance of access control, detection, and response, and these duties are frequently not independent of mechanical or information systems.

In Table 3, a bomb (☛) symbol indicates that a given security measure (in the row) was encountered by the thieves and then defeated during a given heist (in the column). In this context, the term “defeat” is intended in the sense of either (1) damage or destruction of a security measure or (2) suppression of a security measure by presenting it with a ruse or with a false or forged authentication. Security measures that were not encountered by the thieves during the heist (whether a result of planning or chance) are not included in this definition of “defeat” as a practical matter, since public information on the full complement of active security measures during heists is not consistently available.

The rightmost column of Table 3 presents a simple count of the number of heists in which each security measure was defeated, and the bottom row presents a simple count of the number of security measures defeated for each heist. Not every security system uses all of the security measures in the table, so a blank cell neither implies that the security system existed nor that it was successful in deterring a given attack. Thus, while low totals in the rightmost column cannot be used to make statements about the general effectiveness of a given security measure, high totals in this column do suggest that certain security measures are commonly defeated. Table 4 adds some detail on *how* each of the defeated security measures in Table 3 was defeated, for heists in which that information could be located. This list is helpful in revealing both common and creative defeat methods.

3.1.1.1. Commonly Defeated Security Measures

As the rightmost column of Table 3 shows, two security measures stand out as very commonly defeated. First, in eleven heists (48% of the database), a keyed lock was ineffective in preventing unauthorized access. For example, in the Antwerp Diamond Heist, thieves defeated keyed locks protecting entry into the Diamond Center from the garage, into a storage room in which the vault key was stored, into the vault door itself, and to individual safe deposit boxes. In defeating each of these keyed locks, the criminals demonstrated a variety of lock defeat techniques: The garage-to-Diamond-Center access was accomplished through use of a custom-made key rake; the storage room lock was defeated via use of a crowbar (the backup plan after a fabricated key failed to work); the key component of the vault door was defeated by use of the key stolen from the storage room; and the individual safe deposit boxes were opened by exploiting a design weakness that allowed a specially designed tool to interface with their keyholes and force their doors open. However, as Table 4 shows, by far the most common method of defeating keyed locks within the heists considered was to threaten a key-holding employee.

Second, unarmed guards were also defeated in eleven heists (48% of the database). As Table 3 shows, these defeats occurred in all Tiger Kidnappings and Deceive, Subdue, and Seize heists. In some cases these defeats made use of a nonviolent deception; for example, criminals in the Swissport Heathrow Heist presented forged papers to gain facility access. In other cases these defeats occurred via an overt threat of violence; for example, a criminal in the Securitas Cash Depot Heist threatened the unarmed security guard with a pistol. Additional discussion on guard forces and deceptions is provided in Sections 3.1.2 and 3.2.

Cameras appear as the third most commonly defeated security measure. Seven heists (30% of the database) exhibit the defeat of a camera system in some manner. It should be noted that this is in some sense an underrepresentation of camera ineffectiveness; because cameras are often used to investigate incidents hours or days after they occur, in several heists the cameras remained fully functional and were thus not defeated, but also did not contribute to stopping the robbery in progress. Some notable camera defeat techniques include exploitation or creation of blind spots, deactivation of the cameras prior to the robbery (e.g., by an insider, as in the case of owner Parvez Latif in the Knightsbridge Safe Deposit Center Heist), and taking control of the camera monitoring station. The latter can be accomplished violently or nonviolently. For example, the Securitas Cash Depot Heist criminals used a pistol to threaten a guard in order to gain control of the guard station. In contrast, it was an insider accomplice who was responsible for monitoring the CCTV camera images at the time of the Brink's-Mat Gold Heist.

Overall, the common defeat of keyed locks, cameras, and unarmed guards may be due in part to the fact that these security measures themselves may be very common, compared to others listed in Table 3. However, the fact remains that they appear to be easily defeated, often through the variety of independent means listed in Table 4. **An important implication of this information is that a security system for high-value items that principally (or solely) relies on keyed locks, cameras, and unarmed guards may be at high risk for exploitation and defeat.**

3.1.1.2. Commonality and Creativity of Defeat Methods

Table 4 contains a wealth of information on the methods criminals used in this study's heists to defeat security measures. **Some methods are simply uses of brute force** (e.g., ramming through fences and walls with a backhoe, as in the Millennium Dome Raid), **while others are highly creative and innovative** (e.g., creating a custom tool to hold together the magnetic contacts of the vault door while they were separated from the door in the Antwerp Diamond Heist). **Interestingly, even among the creative and innovative methods, none makes significant use of high technology. The data in Table 4 also show that no single approach (creative or brute force) clearly dominates. Thieves employ a variety of methods to defeat security measures, and few, if any, can be considered typical.**

However, some defeat methods do appear more frequently than others. In particular, the following defeat methods appear in three or more heists:


- **Threats on guards or on key- or combination-holding employees** is a common defeat method among ten heists (43% of the database). For example, thieves in the Brink's-Mat Gold Heist did not know the combinations to the inner or outer vault doors, but using inside information they learned which employees knew the combinations. Defeating measures the Brink's-Mat warehouse took to ensure that no single employee had all the keys and combinations necessary to open the vault, the thieves identified the individuals who could collectively provide access, doused them with gasoline and threatened to light them on fire, and consequently gained access to some \$86 million (FY12) worth of gold bullion.
- **Using recognized employees to enter and/or vouch for entry** worked to provide unauthorized access in the Knightsbridge Safe Deposit Center, Securitas Cash Depot, and Northern Bank Cash















































































Heists. In the first two cases, the thieves used either coercion or incentive to convince a recognized employee to vouch for their entry into a secure facility, which the thieves then used to subdue the on-duty guard that had granted them entry. In the case of the Northern Bank Cash Heist, the thieves did not enter the secure facility themselves but rather coerced employees to execute the crime on their behalf.

- **Gaining control of CCTV monitoring stations** is another common technique. In some cases, this occurred in the aftermath of using recognized employees to vouch for entry. In another case, an insider employee had control of the CCTV monitoring station.

A common thread among all three of these defeat methods is that they attack segments of the security system in which humans are in the loop. Particularly in the case of the first two methods, the human vulnerability is rooted in the fact that the human has the capability to make decisions in the service of objectives other than facility security. This capability is neither inherently a positive or negative one, and in some situations its use has either (or both) positive and negative outcomes. While this decision capability often resulted in the decidedly negative outcome of loss of millions of dollars to thieves (for example, as a consequence of the on-duty guard at the Securitas depot letting manager Colin Dixon and a purported police officer enter the facility unchallenged), it also resulted in a zero or near-zero casualty rate for the employees present during the robberies. **This malleability of human behavior should be an important consideration in the design of any security system.**

Table 3. Summary of Defeated Security Measures.

 Security Measure was Encountered and Defeated

																							
	Brazil Central Bank Cash Heist	Sumitomo Mitsui Bank Heist	Antwerp Diamond Heist	Museon Jewel Heist	Société Générale Bank Heist	Stardust Casino Job	Vastberga Bank Heist	Millennium Helicopter Heist	Tanzanian Airplane Gold Raid	Munch Museum Art Heist	Carlton Hotel Diamond Heist	Brink's-Mat Gold Heist	Lufthansa Heist	British Bank of the Middle East Gold Heist	Mayfair Manhattan Bank Robbery	Harry Graff Diamond Heist	Schiphol Airport Diamond Heist	Swissport Heathrow Heist	Gardner Museum Art Heist	Knightsbridge Safe Deposit Center Heist	Securitas Cash Depot Heist	Northern Bank Cash Heist	
Static Barriers																							
Fences																							
Walls																							
Windows																							
Floors																							
Target Anchor																							
Target Barrier																							
Access Controls																							
Key																							
Combination																							
Radio Frequency																							
Access Credential																							
Bio Recognition																							
Detectors																							
Cameras																							
Light Sensors																							
Infrared Sensors																							
Microwave Doppler Sensors																							
Unspecified Motion Sensors																							
Physical Tampering Sensors																							
Security Guards																							
Armed																							
Unarmed																							
No. of Entries	3	0	8	5	2	1	3	3	0	2	0	3	3	2	1	2	4	3	3	6	4	4	3




















	1
	5
	3
	1
	1
	3
	11
	4
	1
	2
	5
	7
	1
	3
	1
	3
	1
	1
	11

Table 4. Known Security Measure Defeat Methods. Numbers in parentheses indicate the identification number of the heist to which the defeat method corresponds (see Table 1). An “S” preceding a number indicates that the method is suspected but not known with certainty.

Security Measure	Defeat Method
Static Barriers	
Fences	Ramming with a backhoe (8)
Walls	Power drills, hammers, chisels, and hydraulic jack (5) Heavy knife to slice through canvas wall (7) Ramming with a backhoe (8) or van (19) Mortars and grenades (14)
Windows	Sledgehammer, custom-fit explosives (7) Mortars and grenades (14)
Floors	Possible mechanical or hydraulic jack (1)
Target Anchor	Wire cutters (10)
Target Barrier	Nail gun and sledgehammer (8)
Access Controls	
Key	Custom-made key rake (3) Crowbar (3, 21) Stolen key (3) Custom-made pulling device (3) Plasma cutting torch (5) Custom-fit explosives, circulating saw (7) Threatening key-holding employees (12, 13, 16,18,22,23) Bolt cutters to cut lock (13) Posing as authorities to be let in (20) Sledgehammer (21)
Combination	Video camera to record combination (S3) Custom-made pulling device (3) Threatening combination-holding employees (12, S13, S17)
Radio Frequency	Garage door frequency scanner (3)
Access Credential	Unauthorized use of special entry card (S18) Use of forged shipment paperwork to enter site (19)
Bio Recognition	Posing as typical customers (17) Posing as police officers (20) Using recognized employees to enter and/or vouch for entry (21, 22, 23)
Detectors	
Cameras	Creating camera blind spot via placement of obstacles (1) Placing shroud over camera (3) Confiscating CCTV video recordings (3, 20) Gaining control of CCTV monitoring station (12, 20, 22) Turning cameras away from activity (20, 22) Deactivating video cameras prior to robbery (21)
Light Sensors	Black electrical tape covering (3)
Infrared Sensors	Covering with thin film of hair spray (3)
Microwave Doppler Sensors	Covering with Styrofoam panel (3)
Unspecified Motion Detectors	Gaining control of monitoring station (20)
Physical Tampering Sensors	Separating magnetic tamper detection device from article it protects (3)
Security Guards	
Armed	Surprise assault (13)
Unarmed	Posing as typical employee (6, 23) Threatening with weapons (10, 15, 16, 18, 21, 22) Presenting forged paperwork (19) Subduing with handcuffs after posing as police officers (20)

3.1.1.3. Security Measure Defeats per Heist

The bottom row of Table 3 displays a simple count of the number of security measure types defeated in each heist. Topping the list is the Antwerp Diamond Heist with eight defeated security measure types, solely in categories of access controls and detectors. In this well-documented case, more than two years of thief planning, surveillance, and investigation into the targeted facility's vulnerabilities enabled the defeat of a great many security measure types. Also quite significant were the unsolved Gardner Museum Art Heist in the U.S., where access controls, detectors, and security guards were attacked, as well as the unsolved Museon Jewel Heist in the Netherlands, where static barriers and detectors were defeated by methods that are as yet unclear.

The most interesting observation from this bottom row is that in 18 heists (78% of the database), more than one security measure was defeated.[‡] In fact, the mean number of defeated security measure types is 2.8, and the median is 3.0. This provides clear evidence that **high-value heists typically involve the defeat of multiple security measures**. That is to say, the criminal team committing such a heist will typically possess a diversity of security measure defeat capabilities. This begins to lend evidence, to be augmented in Section 3.5, supporting the characterization of high-value heist criminal teams as sophisticated and well-organized.

3.1.2. Security Forces

The HMCD also records details regarding the security forces in place at the facilities attacked in each of the 23 heists. Supplementing the information in Section 3.1.1, these details include the number and relative activity of personnel defeated, the phases in which knowledge of the heist was attained and response occurred, and the proximity of the facility to external police forces.

Figure 14 indicates the status of guard stations inside target premises during the 23 heists in the database. While 22% of the targeted facilities had no guard stations, it is striking to observe that of the 56% with guard stations, well over three-quarters of these stations were *active* during the heists. Furthermore, Fig. 15 shows that in 65% of the heists in the database, guards were active on the target premises (e.g., on station or patrol, even if there was no central guard station or control room) during the heist.

How are guards in so many heists rendered so ineffective? In general, this occurs either because (1) the thieves take care to avoid being detected by guards (as in the Museon heist), (2) the thieves disguise

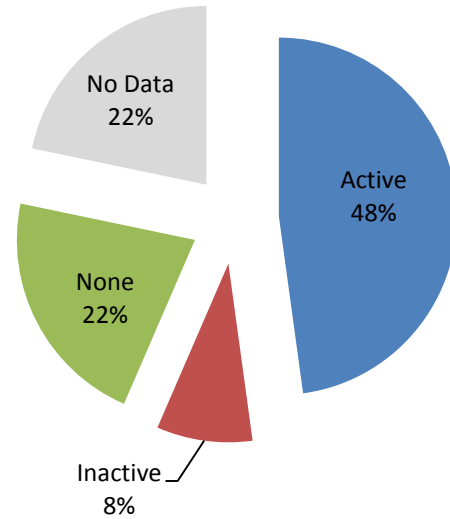


Figure 14. Statuses of Guard Stations at Target Premises during Heists.

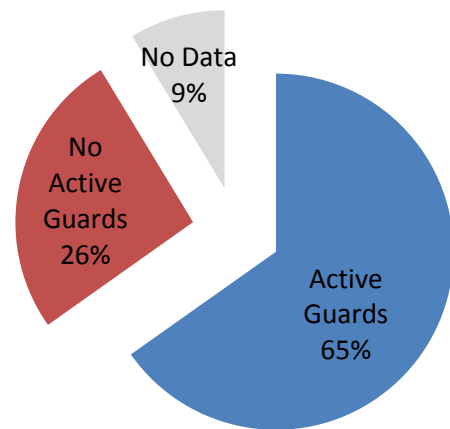


Figure 15. Existence of Active Guards at Target Premises during Heists.

[‡] Furthermore, although the remaining five heists in the database involve either one or zero known security measure defeats, the limited availability of public information for these cases makes it particularly likely that their true numbers of security measure defeats are higher than those reflected by their numbers of *known* defeats.

themselves to appear nonthreatening to guards (as in the Schiphol and Swissport Heathrow heists), or (3) the guards are overpowered and subdued.[§]

These defeat methods suggest that a guard force can exist to fulfill at least two independent roles: Such a force can serve as (1) a sophisticated form of criminal activity sensing and detection and/or (2) an incursion response force.

3.1.2.1. Security Forces as Sensors

The first two of the three methods of defeat relate to ways in which thieves defeat guard forces that are intended for the sensor role. Indeed, the lack of armament among guards of the high-value items in this study suggests that this is the role for which these forces were intended. Interestingly, however, certain heist stories suggest that the guards themselves may not always realize this distinction or may make fundamental decisions regarding their role(s) on the spot during a crisis. For example, in the Mayfair Graff Diamond Heist, a security guard witnessing what appeared to be the kidnapping of a hostage told a court, “I decided that if I was able to tackle them, or at least grab the woman and take her away from them at the price of getting wounded but not killed, it might be worth it.”⁵⁴ This guard was unarmed and, weighing the risks, costs, and benefits, decided to respond (rather than simply observe and report) against two armed men. In another instance, a poorly trained guard at the Isabella Stewart Gardner Museum made the opposite decision: When one of the robbers told him, “Don’t give us any problems, and you won’t get hurt,” he capitulated and responded, “They don’t pay me enough to get hurt.”⁶⁵ Neither guard’s expressed rationale had much to do with his officially recognized duties.

Thus, unlike man-made security devices, a guard force possesses substantial autonomy and ability to make decisions that may not coincide with intended security roles. As a result, even if a thief is certain of the nominal security procedures at a facility, this autonomy introduces substantial uncertainty even for an unarmed guard force. As Fig. 16 shows, the HMCD contains 11 heists (48% of the database) in which armed thieves attacked security personnel, almost all of whom were unarmed. In contrast, only in two cases (the Antwerp Diamond Heist and Gardner Museum Art Heist) did thieves enter unarmed into a facility with security personnel present. In both of these cases, planning is estimated to have initiated 24-30 months prior to the heist (far above the mean planning duration of 9 months and median of 4 months). In combination, these facts suggest that **even unarmed security guards add an element of uncertainty to thieves’ planning,**

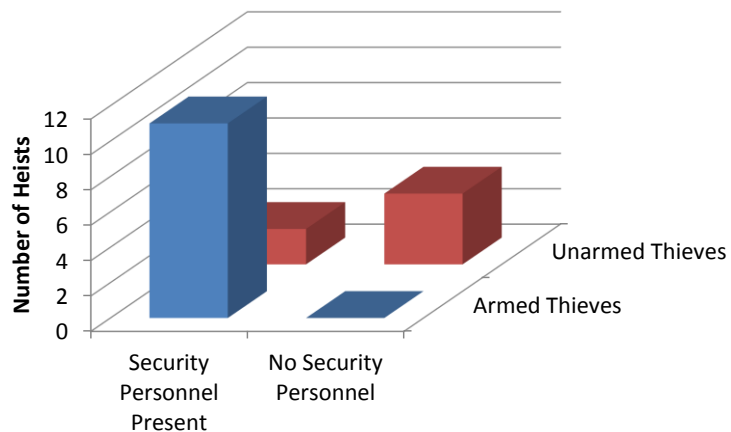


Figure 16. Correlations between the existence of active security personnel and thieves’ use of weapons. Data exists only for 17 of the 23 heists in the HMCD.

[§] Other important techniques not seen in these heists include (1) cutting off guards’ means of communication to outside security forces (rather than subduing them) or (2) emplacing insiders as security guards. A variant of the latter occurred in the Knightsbridge heist: While no security guards were insiders, the owner of the safe deposit center, an insider, scheduled new guards to be on duty during the time of the robbery. Since the theft mastermind, Valerio Viccei, was a tenant of the center and could be recognized by the experienced guards, scheduling these new guards ensured that the robbers would go unrecognized.

encouraging thieves either to arm themselves as a precaution or to buy down the risk with extended planning and intelligence gathering. In the case of the latter, planning may include learning both formal or intended security procedures and the attitudes that guards have toward these procedures.**

In their efforts to judge the likelihood of the security force to respond, thieves also attempt to judge what delay can be realized between the time of heist detection to the time of response. For the heists in this study, Fig. 17 shows on the x-axis the phase in which security forces knew about the heist (Planning, Entry, Theft, Escape, or Aftermath), and the z-axis (into the page) shows the phase in which effective response took place. For brevity, the ordered pair of these two elements will be called the *knowledge-response profile* of a heist. Notably, only in the slight majority of heists (12) did a security response take place in the same phase as heist detection. For the remaining eight heists for which this data was available, response was delayed by between one and three phases. For example, despite the fact that the unarmed security guard on duty in the Securitas Cash Depot became aware of the heist upon the first thief's entry into the guard station, he was held at gunpoint, handcuffed and blindfolded, and could not respond or alert others until after the heist had been completed. **In over one-third of heists in the HMCD, dependence on security guards acting in a sensor role came with a significant delay between detection and response.**

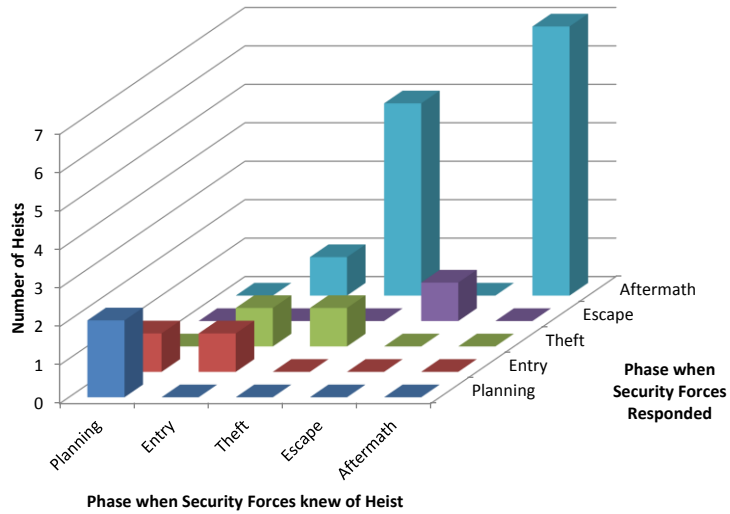


Figure 17. Distribution of Heist Knowledge-Response Profiles. Data exists only for 20 of the 23 heists in the HMCD.

Figure 17 shows that security forces were frequently aware of the heist during the theft phase but were prevented from effectively responding until the aftermath. For example, guards at the Gardner Museum in Boston were not aware that the apparent police officers “arresting” them were actually impostors until after they had been handcuffed and rendered nearly powerless. Not surprisingly, of the five cases in which a theft-phase discovery and aftermath-phase response occurred, four were in the Deceive, Subdue, and Seize category, which itself was comprised of a total of six heists. That is, **an initial deception may not only delay security recognition of a heist (into the theft phase), but it may also enable thieves to delay a security response (into the aftermath phase).**

Disturbingly, Fig. 17 shows that most common knowledge-response profile is an Aftermath detection and Aftermath response. In these cases, security was foiled completely. Every nonviolent heist in the database falls into this category, largely because thieves perpetrating these heists took special care to avoid discovery by existing security measures – including the eyes and ears of guards.

In sum, over half of the heists in the database saw no security response until after the thieves had already escaped from the facility they were robbing. **This is indicative of the dual issues of (1) a security**

** As an example, in the Antwerp Diamond Heist, Diamond Center staff had largely grown complacent.¹ For instance, the concierges responsible for securing the vault each night did not use a security feature built into the vault door's key: The key was designed to be separated into two parts (the pipe and stamp) to be stored separately from each other, but instead the concierges stored both pieces together in a lockbox near the vault.

force's ability to act as a sensor to recognize a heist and (2) a security force's ability to either communicate this information to the appropriate responders or to effectively respond themselves when under duress. Neither issue can be considered in isolation: An excellent detection network can be foiled by a modest number of thieves who prevent the security force from communicating with the outside world or each other. Alternatively, a system with an excellent communications infrastructure can be foiled by a security force that is unable to recognize heists in progress.

3.1.2.2. Security Forces as Responders

In the case of the third method of defeat mentioned earlier during Section 3.1.2, the security forces protecting many of the high-value items within the heists of the HMCD tended to be modest. Figure 18 shows a histogram of the number of security personnel defeated for the heists in the database. As shown, of the heists in which active guard forces were present, 85% employed just one or two guards. The maximum of five guards corresponds to the Brink's-Mat heist, in which all five employees in the depot were classified as guards.^{41,42} The median of the data is one guard, and the mean is 1.5 guards. In the vast majority of these cases, the guards were unarmed. Interestingly, Fig. 19 shows almost no correlation between the size of the on-scene thief force and the number of security personnel ($R^2 = 0.033$), and the same holds between the size of the on-scene thief force and number of non-thief witnesses ($R^2 = 0.002$). **This suggests that, for the heists in the database, the size of the thief force was typically driven by factors other than the size of the security force or witness pool.** For example, the size of the estimated 14-person thief force for the Brazil Central Bank Cash Heist was driven by the need for manpower in quickly passing the stolen cash through the 263-foot-long tunnel under the streets of Fortaleza. In other examples, thief force size was driven by the need for drivers of getaway vehicles or the need for individuals with particular experience or expertise.

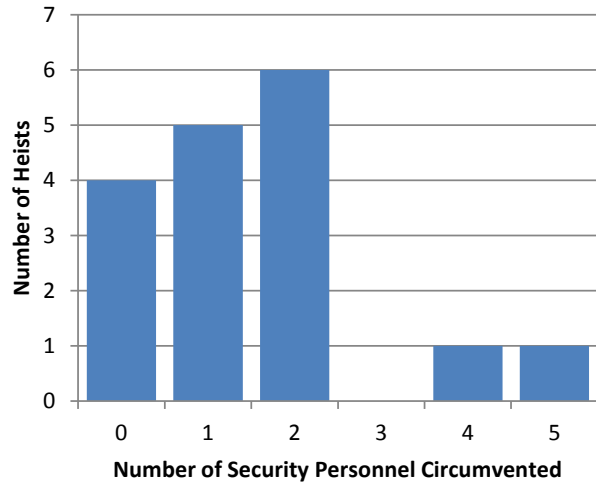


Figure 18. Number of Security Personnel Defeated. Data available for 21 of 23 heists.

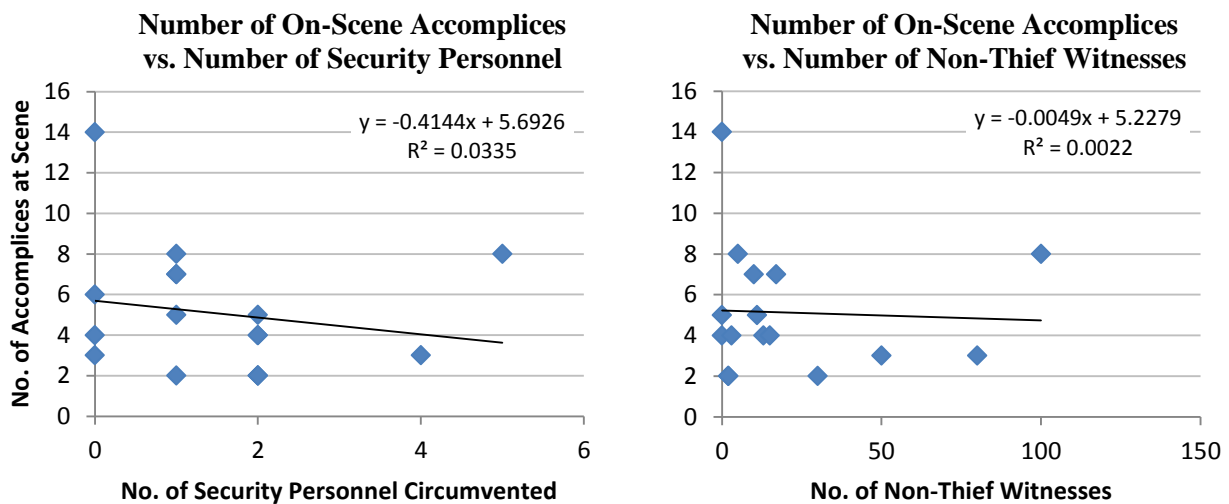


Figure 19. Weak correlations between thief force size and both security force size (left) and number of non-thief witnesses (right). Data available for 17 of 23 heists.

It should further be noted that, as indicated by the histogram in Fig. 20, heists in this study were frequently committed not only under the noses of security guards, but also under the noses of nearby external police forces. On average, such forces were just 0.68 miles away. In three cases (the Antwerp Diamond Heist, the Tanzanian Airplane Gold Robbery, and Harry Winston Diamond Heist), police forces were stationed within 500 feet of the heist. Given a mean heist

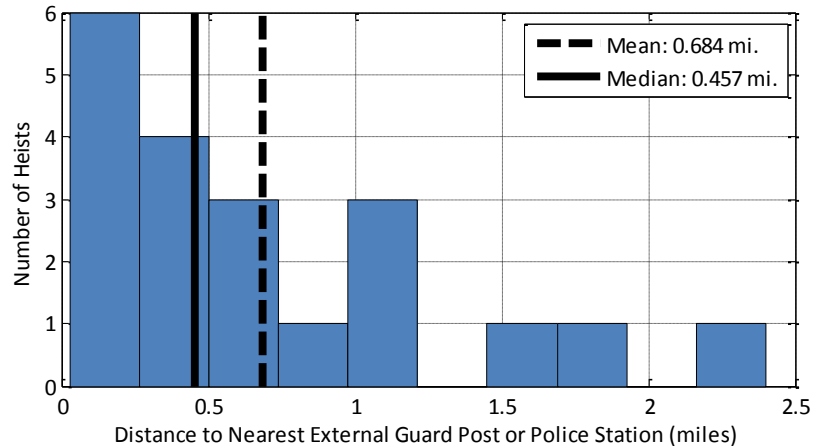


Figure 20. Distances to Nearest External Guard Post or Police Station. Data available for 20 of 23 heists.

duration of 8.3 hours and median of 1.4 hours, this illustrates that **lack of response force proximity is rarely the reason for a lack of security response**. A leisurely 3 mph stroll would allow a security force 0.68 miles away to arrive at a crime scene within 14 minutes; only three of the 23 heists in the database (the Munch Museum Art Heist, Mayfair Graff Diamond Heist, and Schiphol Airport Diamond Heist) took less time than this. In the interesting case of the Vastberga Helicopter Heist, police responded quickly but were deterred from entering the G4S depot by the forethought the thieves demonstrated by placing caltrops on the road near the depot and apparent bombs at the police helicopter hangar. These measures left the police uncertain of what other deterrents or traps could be awaiting them if they continued their approach.

A clear implication of this information is that physical protection by means of guards is often a manageable obstacle for well-prepared thieves. This may be particularly true if guard activities are easily observable, either to outsiders or insiders; as Section 3.6 will show, insiders were present in a substantial majority of heists and fulfilled various roles. Moreover, the example of the Vastberga heist illustrates that, even when acting in a response rather than sensor role, **the effectiveness of security forces can be substantially weakened in the presence of an uncertain but credible threat.**

Nevertheless, the case can be made that the presence of security guards (even unarmed guards) can serve a critical strategic purpose against thieves. While guards themselves may not deter a determined thief, they do add to the amount of time the thief requires to prepare and plan for his heist. The Antwerp Diamond Heist and Securitas Cash Depot Heist serve as two examples illustrating the months or years of planning that thieves may require to learn the details of security practices and procedures at the target facility. In many cases, this preparation calls for the planting or recruitment of an insider. If a facility possesses an effective system for detecting both outside and inside attempts at discovering security practices, the extension of the thief's planning timeline introduced by the use of guards may be used productively toward thwarting heist attempts.

3.2. Deception Methods

*"The criminal plan of the thieves, using the two bogus police officers to enter the Gardner Museum, was quite simple and quite easily executed. The Gardner Museum could have been as secure as Fort Knox, but that does no good if the guard is going to let the thief in."*⁶⁶

*Robert Spiel
Art Theft Investigator*

As highlighted in Section 3.1.2.1, heists involving a deception preceding a subdue and seize event are frequently able to delay recognition of the heist. Typically, a deception, disguise, or diversion allows thieves access to facilities or information critical to implementing their attack plan. While in many cases these facilities or pieces of information could be accessed via violent means, use of a deception spares thieves the expense and risk to life that a violent attack would carry, though often at a higher risk of being detected and captured during the deception. This potential for the employment of deception places a higher burden on security system designers: **Even the most exceptional security response force can be thwarted by a thief who is recognized as an individual with legitimate access.**

Use of deceptions is not limited to those heists in the Deceive, Subdue, and Seize category. Within the database, 91% of heists (all but two) are known to have involved some type of deception, and **use of deception can be considered the norm for large criminal heists.**

To provide more detail on the number and types of deceptions used in such heists, Table 5 summarizes deception methods used in the execution of each of the 23 heists in the HMCD. These deceptions can be divided into three general categories:

Physical disguises are deceptions involving the concealment of a person, place, or object's true identity or purpose via some material means. Types of physical disguises identified in this study include the disguise of thief-possessed buildings or rooms (e.g., presenting materials that allows one to appear as a legitimate and well-meaning tenant), the physical disguise of thefts in progress (e.g., disguising a theft as a routine operation), use of vehicles that blend with surroundings (e.g., using vehicles that appear normal in the setting of the theft), disguised or concealed surveillance equipment (e.g., cameras hidden in clothing), disguised or concealed operations equipment (e.g., concealed weapons or tools), disguise or concealment of loot (e.g., placing loot in nondescript bags or containers), disguised age or gender (e.g., a male thief disguising himself as a woman to give a less threatening impression), or other disguised physical features (e.g., masks or prosthetic facial features to hide identity).

Activity disguises are deceptions involving the concealment of a person, place, or object's true identity or purpose via actions rather than material means. Types of activity disguises identified in this study include disarming personalities or reputations (e.g., charming one's way into obtaining information or averting suspicion), blending in by occupation (e.g., posing as or being a legitimate employee of the organization being robbed), and exertion of perceived legitimate authority (e.g., posing as a police officer to gain an individual's compliance).

Diversions are deceptions meant to draw attention away from a suspicious device or activity. Diversions identified in this study include personal distractions (e.g., welcome or unwelcome wanted advances), relays of stolen goods (e.g., handoffs of loot during a heist to complicate

tracking), decoy vehicles or devices (e.g., fake bombs or vehicles not carrying stolen goods intended to complicate tracking), and exploitation of tensions (e.g., introducing a dispute between two contentious parties to distract from the activities of a third party).

In Table 5, a bomb (💣) symbol indicates that a given deception method (in the row) was known to be employed in a given heist (in the column). The rightmost column of Table 5 presents a simple count of the number of heists in which each deception method was used, and the bottom row presents a simple count of the number of deception methods employed for each heist. Table 6 adds some detail on *how* each of the deception methods in Table 5 was used. This list is helpful in revealing both common and creative deception methods.

3.2.1. Common Deception Methods

As the rightmost column of Table 5 shows, four deception methods stand out as very common, each used in between 11 and 13 (48% and 57%) of heists in the database. The first of these highly common methods is use of vehicles that blend with surroundings. In most cases, this is simple for thieves to achieve: Some 70% of the heists in the database occurred in urban areas, and so almost any commercially available sedan or van blends with urban surroundings. However, there are examples in which the thieves used a backhoe, which did not appear out of the ordinary around the large and recently-completed Millennium Dome; and a KLM airlines vehicle, which was used to inconspicuously enter and lie and wait within the secure freight area at Schiphol Airport in Amsterdam.

The second of these highly common deception methods is the use of disguised or concealed operations equipment. In most cases, this refers to weapons that thieves concealed in their clothing through the entry phase of the robbery. In other cases, operations equipment was concealed inside a thief-possessed building (as in the digging equipment for the Brazil Central Bank Cash Heist) or among the tools that a thief posing as a technician brought to the facility he intended to rob (as in the specialized tool used to maintain the connection between the two tamper-sensing magnets in the Antwerp Diamond Heist).

The third of these common deception methods is disguised physical features, which principally consists of masks to hide thieves' faces from view. These measures are typically aimed at complicating identification of the thieves during post-heist investigations. In some cases, variants on a simple mask have been used, including balaclavas, false mustaches, and prosthetic facial features.

The fourth of these common deception methods is a thief's blending in by occupation. This is perhaps the most interesting of the four common deception methods. This study's heist database is replete with examples of criminals who have deceptively taken on or played the role of a member of a specific organization or occupation. These roles span from customer to owner, either inside or outside the targeted organization. Table 7 summarizes where various heists fall among these two dimensions, with rows representing various roles from customer to owner and columns indicating whether the role was internal or external to the targeted organization. Asterisks indicate heists in which a thief posed in a role that he did not legitimately hold. As Table 7 shows, **thieves or coerced accomplices who blend in by occupation do so more frequently inside than outside the targeted organization. Furthermore, the table shows no clear limitation to what level of occupational role thieves or their coerced accomplices will take; there are virtually equal numbers of examples of inside managers, employees, and customers.** There even exists in the Knightsbridge Safe Deposit Center Heist an instance where an owner used his position to help mask his involvement in the crime.

Speaking generally, a perusal of the methods listed in Table 6 suggests that **the deception methods used in large heists tend not to be particularly high-tech or complex.** Only two heists involved specialized spy equipment (cameras hidden in bags or clothing), and few if any required the level of precision seen in

achieving the silent acrobatics of *Mission Impossible* or navigating complex laser nets like those in the movie *Entrapment*. **The thief's challenge in utilizing deception methods is thus not in executing them so much as it is in planning and selecting the proper deceptions to execute**, since a poor choice could result in detection or suspicion.


3.2.2. Deception Methods per Heist


The bottom row of Table 5 displays a simple count of the number of deception methods used in each heist. Topping the list is the Knightsbridge Safe Deposit Center Heist, which utilized half the list of physical disguises, the entire list of activity disguises, and one diversion. In this heist, the thieves entered the building with a concealed weapon, with the mastermind feigning sickness and covering his face with a handkerchief. During the robbery, the center's owner, who had been befriended by the mastermind weeks earlier and had become an accomplice in the heist, used his authority to order the security guard to open the security booth to him and the thieves, who were posing as prospective safe deposit box customers. Once inside, the criminal mastermind made advances on the guard to distract him and move him out of reach of the panic button. The thieves placed a sign on the center's door to announce that the center was closed for security upgrades, and once the heist was complete they drove off in a nondescript van.

At the bottom of the list with zero known deceptions are the Tanzanian Airplane Gold Robbery and the Museon Jewel Heist. In the case of the Tanzanian heist, the prospective thieves launched an attack on a gold transport airplane with no clear deception tactics; however, information available in public sources regarding this heist attempt is quite limited and may not capture the entirety of the thieves' activities preceding and during the heist. The Museon Jewel Heist remains unsolved and was accomplished so stealthily that the manner in which it was perpetrated remains a mystery; while deceptions are likely to exist for this robbery, so few specifics are known that they cannot be identified.

A key observation to draw from the bottom row of Table 5 is that in all but two heists (i.e., in 91% of the database), at least one deception was used. As stated earlier, **use of deception can be considered the norm for large criminal heists**. Moreover, 83% of heists in the database utilized multiple types of deception, and the average heist employed three deception methods. Thus, just as in the case of defeated security measures, **high value heists typically involve the employment of multiple deception methods**. This fact should not be lost in motivating the thoughtful design of future security systems.

Table 5. Summary of Deception Methods.

 Deception Method was Employed



	Brazil Central Bank Cash Heist	Sumitomo Mitsui Bank Heist	Antwerp Diamond Heist	Museon Jewel Heist	Société Générale Bank Heist	Stardust Casino Job	Vastberga Helicopter Heist	Millennium Dome Heist	Tanzanian Airplane Heist	Munch Museum Art Heist	Carlton Hotel Diamond Heist	Brink's-Mat Gold Robbery	Lufthansa Heist	British Bank of the Middle East Gold Heist	Mayfair Graff Diamond Heist	Harry Winston Diamond Heist	Schiphol Airport Diamond Heist	Swissport Heathrow Heist	Gardner Museum Art Heist	Knightsbridge Safe Deposit Center Heist	Securitas Cash Depot Heist	Northern Bank Cash Heist	No. of Entries
Physical Disguises																							
Disguise of Thief-Possessed Buildings/Rooms	●	●																					2
Disguise of Theft in Progress			●									●								●			2
Vehicles that Blend with Surroundings	●	●	●				●	●	●	●				●	●	●	●			●	●		13
Disguised/Concealed Surveillance Equipment			●																		●		2
Disguised/Concealed Operations Equipment	●	●	●						●					●	●	●				●	●		10
Physical Disguise or Concealment of Loot	●				●										●							●	4
Disguised Age or Gender															●	●							2
Disguised Other Physical Features	●						●	●	●	●	●	●	●				●	●	●	●	●	●	12
Activity Disguises																							
Disarming Personality or Reputation	●		●	●																●			4
Blending in by Occupation	●	●	●	●	●						●	●	●			●	●	●	●	●	●	●	13
Exertion of Perceived Legitimate Authority												●	●		●		●	●	●	●	●	●	8
Diversions																							
Personal Distractions																				●			1
Relay of Stolen Goods		●													●								2
Decoy Vehicle or Device						●						●		●									3
Exploitation of Tensions												●											1
No. of Entries	7	3	6	0	4	2	1	2	0	2	2	3	5	1	2	5	3	4	4	2	8	6	4

Table 6. Known Deception Methods. Numbers in parentheses indicate the identification number of the heist to which the defeat method corresponds (see Table 1). An “S” preceding a number indicates that the method is suspected but not known with certainty.

Category	Specific Deception Method
Physical Disguises	
Disguise of Thief-Possessed Buildings/Rooms	Digging executed from a building rented ostensibly as a synthetic grass manufacturer, complete with a custom awning displaying the company’s logo (1) Thief became a tenant of the facility he intended to rob (3)
Disguise of Theft in Progress	Disguised the lowering of a hydraulic jack into the city sewer as a legitimate construction project (5) Replaced cut lock at security gate with a fake (13) Placed sign on safe deposit center door announcing the facility was closed for the day for security upgrades (21)
Vehicles that Blend with Surroundings	Nondescript commercially available cars, vans, trucks, or motorbikes as getaway or transport vehicles (1,3, 5, 10, 13, 16, 17, 18, 19, 21, 22) Construction vehicle that would not appear unusual in context (8) Stolen airport vehicle that blended in to terminal surroundings (18)
Disguised/Concealed Surveillance Equipment	Video camera concealed in satchel (3) Video camera concealed in belt buckle (22)
Disguised/Concealed Operations Equipment	Concealed digging equipment inside rented storefront (1) Concealed thumb drive (S2) Disguised specialized tampering sensor circumvention tool among tools for installing video surveillance system (3) Concealed weapons (11, 15, 16, 17, 18, 21, 22)
Physical Disguise or Concealment of Loot	Cash hidden inside doors of cars transported via car carrier (1) Cash and chips concealed inside thief’s backpack (6) Loot concealed in garbage bags (16, 23)
Disguised Age or Gender	Prosthetic disguises to appear older (16) Female clothing and wigs (17)
Disguised Other Physical Features	Mastermind used ID card with a photo of him in a hat (1) Masks and/or balaclavas to disguise facial features (7, 8, 10, 11, 12, 13, 19, 22, 23) False mustaches (20) Handkerchief over face, feigning sickness (21) Prosthetic disguises to hide facial features (22)
Activity Disguises	
Disarming Personality or Reputation	Mastermind established good reputation with neighbors and community (1) Insider was open and expressive, smiled, and treated everybody as an old and treasured friend (3) Mastermind known and recognized in town from social

	<p>functions, photography of prominent visitors, and by his elegant style (5)</p> <p>Mastermind was smooth-talking and befriended the safe deposit center owner and his girlfriend (21)</p>
Blending in by Occupation	<p>Thieves set up an inconspicuous storefront for a synthetic grass company in the middle of a major city, complete with a custom awning, promotional hats with the company's logo, and phone book ads (1)</p> <p>Thieves posed as typical law-abiding customers (2, 5, 21)</p> <p>Thief posed as diamond merchant to become a tenant in Diamond Center (3)</p> <p>Thieves lowering hydraulic jack into sewer posed as construction workers (5)</p> <p>Thief or accomplice (willing or coerced) was an employee of the target establishment (2, 6, 12, 13, 21, 22, 23)</p> <p>Thieves dressed in military fatigues typical for individuals in the war zone where the targeted establishment was located (14)</p> <p>Airport cargo thieves posed as airline employees (18)</p> <p>Thieves posed as delivery men, complete with forged paperwork (19)</p>
Exertion of Perceived Legitimate Authority	<p>Bank manager ordered to answer phone calls as usual (15)</p> <p>Posed as legitimate employees (18)</p> <p>Presented apparently legitimate paperwork (19)</p> <p>Posed as police officers (20, 22, 23)</p> <p>Used authority as facility owner or manager (21, 22, 23)</p>
Diversions	
Personal Distractions	<p>Security guard distracted by visiting prospective tenant (and thief's) inappropriate and unwanted advances (21)</p>
Relay of Stolen Goods	<p>Total stolen funds transferred in small amounts to multiple banks to help thwart detection (2)</p> <p>Loot relayed immediately after theft through a series of handoffs among pedestrians and multiple motor vehicles (16)</p>
Decoy Vehicle or Device	<p>Decoy packages with the appearance of bombs placed at police helicopter hangar (7)</p> <p>Decoy cars to complicate possible police chase (13, 16)</p>
Exploitation of Tensions	<p>Mortars fired during a cease-fire to distract and provoke firefight between opposing military forces (14)</p>

Table 7. Summary of roles that heist accomplices (willing or coerced) have taken when blending in by occupation. Asterisks indicate heists in which a thief posed in a role that he did not legitimately hold.

		RELATION TO TARGET ORGANIZATION	
		Inside	Outside
ROLE	Owner	<ul style="list-style-type: none"> • Knightsbridge 	
	Manager	<ul style="list-style-type: none"> • Sumitomo Mitsui • Lufthansa • Securitas • Northern Bank 	
	Employee	<ul style="list-style-type: none"> • Stardust Casino • Brink's-Mat • Securitas • Schiphol Airport* 	<ul style="list-style-type: none"> • Société Générale* • Swissport Heathrow* • British Bank of the Middle East
	Tenant	<ul style="list-style-type: none"> • Antwerp 	<ul style="list-style-type: none"> • Brazil Central Bank
	Customer	<ul style="list-style-type: none"> • Sumitomo Mitsui* • Société Générale • Knightsbridge 	

3.3. Timing and Target Selection

*"Armed with Werner and Gruenwald's plan, Burke and the Robert's Lounge gang hammered out the details: They'd go in late, when only a skeleton crew of ten was on, striking while the graveyard shift was at lunch."*⁴³

Charlie Glaze, Narrator
Daring Capers: Kennedy Airport Caper

The characteristics of this study's 23 heists that are perhaps most quantifiable relate to thief timing and target selection. Timing can be considered both in terms of *absolute timing*, referring to the timing of heists with respect to calendar months, days of the week, or times of day, and *relative timing*, referring to timing with respect to relevant events. While absolute timing data are easily tracked and utilized for statistical analysis (e.g., the dates and times of heists are generally well-known), a thief may decide on the date and time of a heist based on planned or predictable events that will minimize security obstacles or maximize the value of the targeted items. Thus, this analysis considers both absolute and relative timing, taking advantage of the quantifiability of absolute timing and the qualitative insight gained by considering relative timing.

3.3.1. Absolute Timing

To the extent that data is available in the open literature, the dates and times of each of the 23 heists considered in this study are recorded in the HMCD. The absolute timing of these heists is analyzed here on two scales, first on the daily timing (i.e., the time of day at which heists occurred) and second on the monthly and seasonal timing (i.e., the months and seasons during which heists occurred).

3.3.1.1. Time of Day

Beginning with an analysis of absolute timing on the shortest relevant timescales, Fig. 21 shows the distribution of heist initiation timing throughout the day. Within this figure, heists are grouped into categories of Morning (6:00 – 9:00 AM), Work Day (9:00 AM – 5:00 PM)^{††}, Evening (5:00 – 8:00 PM), and Night (8:00 PM – 6:00 AM). For three heists (the Sumitomo Mitsui Bank Heist, Tanzanian Airplane Gold Robbery, and British Bank of the Middle East Gold Heist), the time at which the heist began is unclear from the available open literature.

As Fig. 21 shows, the major heists in the HMCD show no clear preference for daytime versus nighttime initiation. This observation itself deserves some remark, since it suggests that a **continuously vigilant security force for high-value items is essential**.

However, Fig. 22 helps to illustrate that the character of these incidents differs substantially depending on the time of day at which they occurred. In Fig. 22, the duration of each of 16 heists for which data was available is plotted (on a logarithmic scale, to emphasize order-of-magnitude differences in speed for different heists) against the times at which the heists began. Viewing the data from this perspective, most of the heists in the plot can be cleanly categorized into four timing archetypes, as labeled in Fig. 22:

- **Timing Archetype I, the “Early-Bird Heists”** archetype, is characterized by early-morning heists with durations of 1-2 hours. All three heists that fall within this category, the Gardner Museum Art Heist, Lufthansa Heist, and Brink’s-Mat Gold Heist, were characterized by violence. In at least two cases, the thieves executed a well-planned attack against populations of guards and employees substantially smaller than those present during daytime hours. In all three cases, those guards and employees were subdued and unable to call for help. Since the crimes were perpetrated in the early morning when little, if any, business with outside organizations or people was conducted, there was little risk that individuals from the outside would visit the facility and discover the heist in progress. As a result of this timing, these thefts provided the thieves a minimal risk of detection and allowed them to take a substantial amount of time in raiding the facilities.^{‡‡}

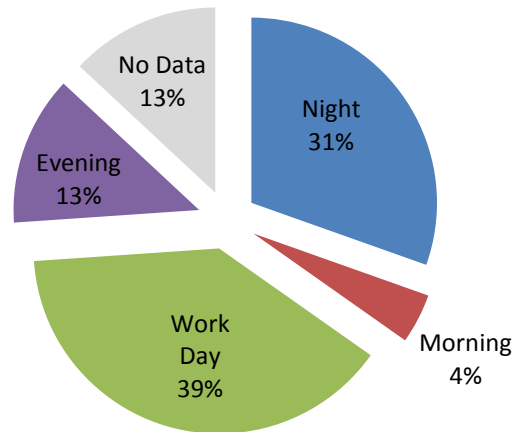


Figure 21. Time of Day Distribution of Heists in the HMCD. Morning is defined as 6-9 AM, Work Day is defined as 9 AM – 5 PM, Evening is defined as 5-8 PM, and Night is defined as 8 PM – 6 AM.

- **Timing Archetype II, the “Broad Daylight Heists”** archetype, is characterized by heists early in the work day that are conducted rapidly, on timescales well under one hour. These timescales are largely a necessity for such heists, and all four in this category (the Swissport Heathrow Heist, Millennium Dome Raid, Schiphol Airport Diamond Heist, and Munch Museum Art Heist)

^{††} Note that the term “Work Day” here is meant only to name the 9:00 AM – 5:00 PM window. Whether the heist occurred on a working day (e.g., Monday through Friday) is not distinguished.

^{‡‡} The duration of the Knightsbridge Safe Deposit Center Heist was quite similar, and the thieves cleverly reduced the risk of detection by outside customers that was inherent in its work day timing by posting a sign indicating that the center was temporarily closed for security system upgrades.

involved use of violence to subdue guards, employees, and bystanders to permit rapid access to the target valuables. However, unlike heists of the Early Bird Heists archetype, response by police forces was unlikely to be prevented, and the thieves needed to work against the clock. While there is no obvious single reason why all four of the heists in this category shared such similar timing, the broad daylight timing for two such heists (the Swissport Heathrow Heist and Schiphol Airport Diamond Heist) was driven by the business-hours timing of large high-value shipments that the thieves were targeting.

- **Timing Archetype III**, the “**Closing Time Heists**” archetype, is similar in duration to the Broad Daylight Heists archetype, but it differs in time of day. These heists occur in the very late afternoon or early evening, as businesses are nearing closing time and employees may be tired, distracted, and somewhat less prepared for a robbery. Both heists in this category, the Harry Winston Diamond Heist and Mayfair Graff Diamond Heist, were complete in just minutes.^{§§}
- **Timing Archetype IV**, the “**Night Raids**” archetype, is characterized not only by heists that begin very late in the day, but also by heists that run the course of several hours. Ironically, the four heists in this category cover some of the least violent and some of the most violent heists in the database. Both tiger kidnappings, the Securitas Cash Depot Heist and Northern Bank Cash Heist, are contained in this category. In both crimes, the kidnappings began in the evening or night, and the ordeals did not end until the following day. At the other end of the spectrum, the stealthy Société Générale Bank Heist and Antwerp Diamond Heist also fall in this category, with both involving undetected vault entries on a Saturday and theft activity not being discovered until staff returned to work the following Monday.^{***} Similar to the Early Bird Heists, the lack of outsider traffic at night allowed these heists to occur without the knowledge of authorities. In part due to the fact that these heists began late in the evening, rather than just before dawn, they are characterized by durations substantially longer than the Early Bird Heists.

While additional archetypes are certainly possible, the four identified here highlight patterns that can be directly supported by the HMCD data. However, perhaps even more interesting than these *observed* correlations between duration and initiation time are those that have remained *unobserved*. For example, long-duration heists (e.g., more than 1-2 hours) have not been observed in early morning hours or in the first half of the work day. This may reflect the fact that such heists would tend to overlap with periods of high activity at each secure facility and make detection of the heist more likely. Conversely, short-duration heists (e.g., under an hour) are almost nonexistent outside of the work day. This further suggests that **thieves have little need to engage in rapid operations when not pressured by the high likelihood of daytime detection that exists at many facilities.**

3.3.1.2. Day of Week

Another aspect of absolute timing is thieves’ selection of the day of the week on which to execute a heist. The distribution of heists in the HMCD among days of the week is shown in Fig. 23. Overall, this distribution is unremarkable, which agrees with data and findings of the 1980 RAND Corporation’s high-value theft analogs study¹². While Wednesday and Friday heists are rare in the HMCD data, statistically this is not significant given the size of the sample; if a uniform distribution of heists across days of the week is hypothesized, the probability that multiple days of the week would be associated with one or fewer heists is substantial, at about 22%.

^{§§} Although clear estimates for the duration of the Carlton Hotel Diamond Heist could not be found, it is likely that this heist, which occurred at the hotel jewelry store’s closing time, would also fit within Timing Archetype III.

^{***} It is worth noting that three of the five Stealth Raid heists were so stealthy that the time of heist initiation and heist duration cannot both be adequately pinpointed in the existing literature to include in the HMCD.

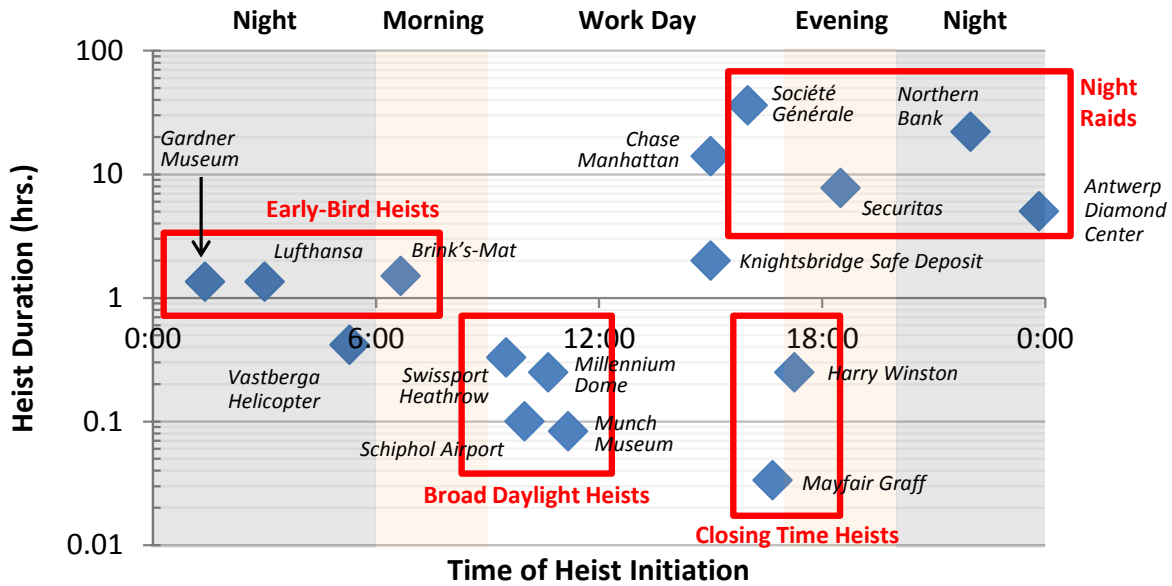


Figure 22. Heist Duration vs. Time of Heist Initiation.
Data shown for 16 heists for which both pieces of data could be obtained.

However, it deserves some note that if the sample of heists is limited only to those in the Stealth Raid category, a clear pattern exists: All but one of the five stealth raids in the HMCD were initiated on a Saturday. The exception of the Museum Jewel Heist was executed on a Monday, a day of the week on which the museum was normally closed. **Thus, while day-of-week patterns are not obvious for the aggregate of all types of high-value heists, stealth raids in particular tend to occur on weekends.**

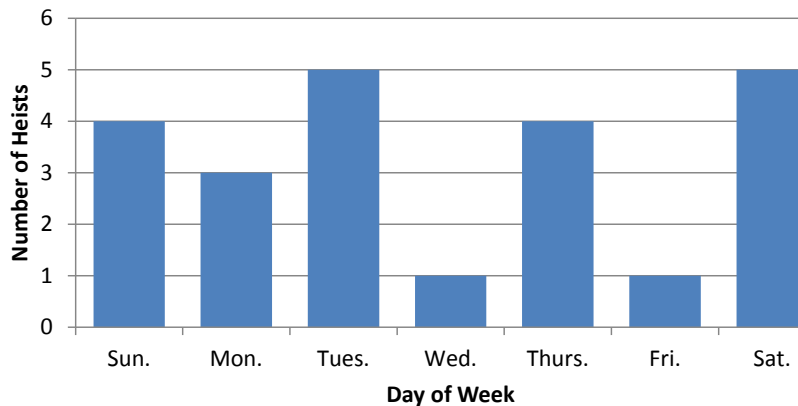


Figure 23. Daily Distribution of Heists in the HMCD.

Reasons for the latter, such as low bystander and security force activity, are discussed in Section 3.3.2.

3.3.1.3. Monthly and Seasonal Timing

A third aspect of interest in terms of absolute timing is monthly and seasonal timing. The present section presents observations regarding the nonuniformity of the monthly and seasonal occurrences of major heists in the HMCD.

Figure 24 displays the distribution of the 23 heists in the HMCD by the month of their occurrence. The distribution is nonuniform, with local peaks in February, August, and December. The most notable peak is the month of August, during which 22% of all heists in the database occurred. In contrast, the four months of March through June account for less than 9% of the heists in the database.

This observation is more clearly described by Fig. 25, which shows the distribution of heists by local season (i.e., whether the season was winter, spring, summer, or fall at the location where the heist took place). Of particular note is the dearth of spring heists (the only such heist was the Swissport Heathrow Heist). This finding is statistically significant; had a uniform distribution across seasons been expected among the 23 heists in the database, the probability of one or fewer

heists occurring in a season purely due to random variation is less than 5%.

Unfortunately, the reason for these significantly nonuniform distributions is not obvious. Crime data in general is known to have seasonal trends,⁸⁶ with peaks typically during summer months. Seasonal crime trend explanations from Ref. 86 include possible associations with vacations and with times of year (e.g., summertime) when doors and windows are less likely to be locked. However, the relevance of these mechanisms to explaining high-

value heist seasonality is unclear. The distributions in Figs. 24 and 25 are also not in clear agreement with the “thermic law” of crime, introduced by Quetelet, which observes the increase in property crimes during winter and the increase in crimes against persons during summer.⁸⁷⁻⁸⁹

Perhaps the most logical hypothesis for a springtime lull in high-value heists is that using the spring to conduct planning, rather than thefts, permits thieves the maximum possible time for conducting surveillance and practice runs (discussed in Section 3.5.2) for outdoor portions of the heist in relevant or hospitable environments. The one- to two-season planning duration suggested by this hypothesis is supported by the data presented in Section 3.5.1, which shows that about half of the heists for which planning time data exists executed involved 1-5 months of planning. Further, it may be hypothesized that thieves perceive some advantages to defeating security at the end of summer or during the winter holiday season, when less experienced security forces may be on duty while their more senior and highly experienced counterparts may be inclined to capitalize on accrued vacation time.

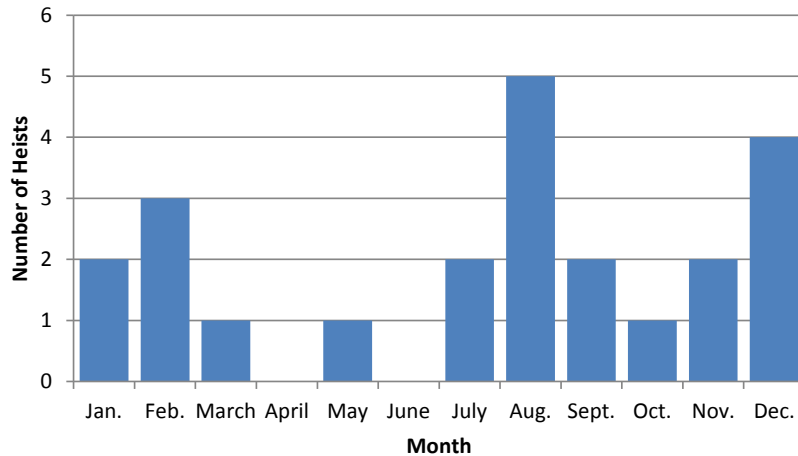


Figure 24. Monthly Distribution of Heists in the HMCD.

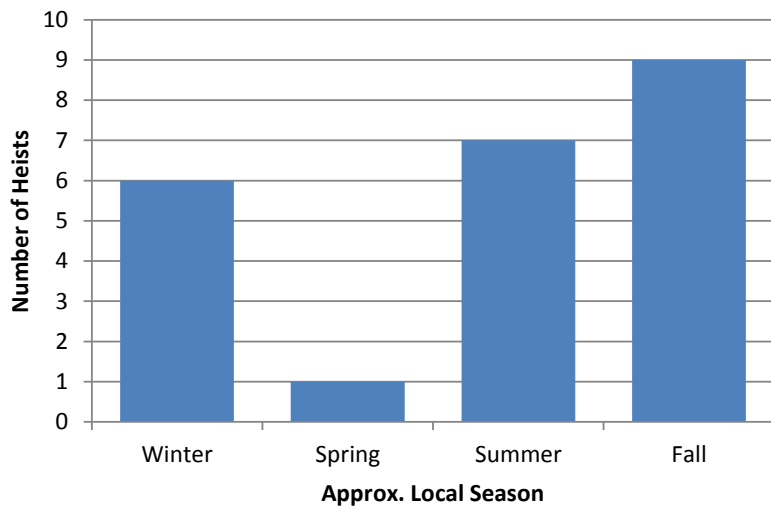


Figure 25. Seasonal Distribution of Heists in the HMCD.

3.3.2. Relative Timing

A less quantifiable but perhaps more important investigation of thief timing is a characterization of the events relative to which thieves planned their heists. Among the heists in the HMCD, three qualitative factors relating to relative timing, some of which have already been indicated in absolute timing discussions, are particularly common:

First, thieves frequently choose to commit large heists at times of low bystander activity. By minimizing the probability that a bystander will exist in the area of the heist, the thieves help to reduce the probability that unusual activity will be reported. All else being equal, this would drive thieves to frequently choose times outside of core business hours. Examples include the late-night Valentine's Day weekend theft at the Antwerp Diamond Center and the yet-unsolved 4:00 AM theft from the Museon science museum.

Second, thieves frequently choose to commit large heists at times of low employee or security activity. Like the first factor, this factor helps minimize the probability of unanticipated detection. Moreover, though, often thieves choose to commit large heists at times of low employee or security activity because it minimizes the difficulty of defeating *anticipated* detection. This factor too tends to drive thieves to choose times outside of core business hours for the targeted entity. Examples include the 3:00 AM assault on the small graveyard shift at the Kennedy Airport Lufthansa Cargo Terminal and the 1:30 AM attack on the Gardner Museum, which was protected only by an overnight force of two unarmed guards.

Third, thieves frequently choose to commit large heists at times of high target value. Given that thieves typically have only one opportunity to attack before a target's security systems are substantially upgraded, they aim to maximize the amount of loot they can carry away, frequently by selecting attack times when an abnormally large amount of loot is available to be stolen. Thieves' ability to execute timing in this way depends on the quality of information they can obtain on the movement of valuables in and out of the target facility. The highest quality information typically comes from insiders. For example, the Lufthansa Heist was expedited as soon as a Lufthansa cargo supervisor and insider informed a preassembled Mafia gang that an unusually large shipment of cash was being stored in the Lufthansa Cargo Terminal over the weekend. On the other hand, outsider observations can be effective as well. The Tanzanian Airplane Gold Robbery, for example, was perpetrated against a weekly shipment from the AngloGold Ashanti gold mine.

Additional notable but uncommon timing factors found in the heists of the HMCD include:

Knowledge of personnel location vs. time. In the case of the Antwerp Diamond Heist, for example, the thieves aimed to penetrate the vault two stories below ground in the B block of the Antwerp Diamond Center. They likely knew that the concierge on duty over the chosen weekend of the robbery stayed in an apartment on the fourth floor of the neighboring C block, rather than the alternative concierge, who stayed on the second floor of the B block.

Physics-based timing. In the case of the Millennium Dome Raid, the thieves planned to escape via boat. However, this necessitated timing the heist to coincide properly with ocean tides so that the boat could pull up to receive the fleeing criminals.

3.3.3. Target Selection

While the previous two sections have considered temporal patterns among heists, spatial, environmental, and functional factors also play an important part in thieves' selection of a target. These characteristics are the subject of the present discussion.

Within the HMCD, the primary targets of each set of thieves are categorized by (1) the type of targeted valuables and (2) the target setting. Six different types of valuables are identified: cash, electronic funds, gold, diamonds and other jewelry, artwork, and miscellaneous stored valuables^{†††}. Five different settings are identified: museum, retail^{‡‡‡}, transport, depot, and vault. As written in the lists above, the valuable types are in an order intended to represent increasing difficulty to fence, starting with cash (which is already in a spendable form) and progressing through electronic funds, gold (which must often be melted down to remove distinguishing marks), diamonds (which must often be recut), artwork (which is often so distinguishable that finding a buyer may be impossible), and miscellaneous stored valuables (which can consist a combination of any of the other categories of items). Similarly, the settings are written in an order intended to represent an increasing difficulty to penetrate, beginning with museums (typically some of the lowest security budgets and least secured settings for valuables) and ending with vaults.

Table 8 identifies the distribution of heists in this study among these two dimensions of targeted valuables and target settings. As a result of the ordering of valuables and settings, valuables that are easy to fence and stored in facilities that are easy to penetrate (and thus likely low-hanging fruits to a potential criminal) are indicated in the top left corner of the table, while valuables that are difficult to fence and stored in difficult-to-penetrate facilities (and thus likely unattractive targets to a potential thief) are in the bottom right corner of the table.

Interestingly, most of the heists examined in this study fall along the bottom-left-to-top-right diagonal of Table 8. In a sense, each of the heists on this diagonal pose a similar desirability to thieves but via different trades between asset liquidity (or “fence-ability”) and target penetrability. **This helps to illustrate rationality in the decision-making preferences of the criminals involved in these heists.** Outliers toward the top left of the table include the Stardust Casino Job and Chase Manhattan Bank Robbery, though these were both smaller-scale robberies on the order of \$1 million (FY12). Substantially larger yield targets toward the top left of this table are likely few and far between, and may not even exist. Outliers toward the bottom right of the table include the Antwerp, Société Générale, and Knightsbridge heists, which were all thefts from safe deposit boxes and required the thieves, at a minimum, to sort through a hodgepodge of items found upon opening the deposit boxes. All three targets were difficult to penetrate, and the heists averaged about 1.5 years of planning apiece; however, they were also some of the highest-yield heists in the database, averaging a take of \$170 million (FY12) apiece.^{§§§}

^{†††} This latter category is typical of safe deposit box centers, where individuals may choose to store any items of value to them.

^{‡‡‡} The term retail is here meant quite broadly, encompassing venues where public sale or any consumer good or service occurs. For the purposes of this categorization, this includes not only public shops (such as jewelry stores), but also banks and casinos.

^{§§§} It may be reasonably noted that, even though the Antwerp, Société Générale, and Knightsbridge heists involved theft from safe deposit boxes, the contents of which the thieves would not have known with certainty in advance, the thieves may have avoided the task of fencing more difficult items by leaving them behind at the crime scene. In this case, these outlying heists may belong somewhat higher in Table 8 (in easier-to-fence rows) and further support the rationality hypothesis. For this reason (that is, since targets of miscellaneous stored valuables may be more closely associated with another target type rather than a true mix of all target types), the Miscellaneous Stored Valuables row in Table 8 is shaded gray.

Table 8. Distribution of Heists in the HMCD among Targeted Valuables and Settings.

		TARGET SETTING					Total No.
		Easy to Penetrate		Hard to Penetrate			
		Museum	Retail	Transport	Depot	Vault	
TARGETED VALUABLES	Easy to Fence	Cash	• Stardust Casino • Chase Manhattan		• Vastberga • Brink's-Mat • Lufthansa • Securitas	• Brazil Central Bank • Northern Bank	8
	Electronic Funds		• Sumitomo Mitsui				1
	Gold			• Tanzanian Airplane	• Swissport Heathrow	• British Bank of the Middle East	3
	Diamonds and other Jewelry	• Museon	• Carlton Hotel • Mayfair Graff • Harry Winston	• Schiphol Airport	• Millennium Dome		6
	Artwork	• Munch Museum • Gardner Museum					2
	Hard to Fence	Misc. Stored Valuables				• Antwerp • Société Générale • Knightsbridge	3
Total No.		3	6	2	6	6	23

Another interesting point revealed by data on these heists is that the complete theft of all (or even most) valuables at a target is rare. Figure 26 illustrates. Here, each heist is categorized by whether it resulted (or, in the case of failed heists, was intended to result) in the theft of all (100%), a vast majority (90-100%), majority (50-90%), minority (10-50%), or small minority (0-10%) of locally accessible valuables. Only in 22% of heists in the database (specifically, the Millennium Dome Raid, British Bank of the Middle East Heist, Chase Manhattan Bank Robbery, Harry Winston Diamond Heist, and Schiphol Airport Diamond Heist) did thieves steal or intend to steal more than 50% of the valuables at a target. In the remainder of heists for which this information was found, thieves were highly selective in what they removed from the target facility (for example, the Société Générale thieves brought with them an appraiser for real-time advice on the most valuable items to take^{****}). In a number of cases, including the Antwerp Diamond Heist, Northern Bank Cash Heist, and Securitas Cash Depot Heist, this selectivity was influenced by limitations in transportation capacity.

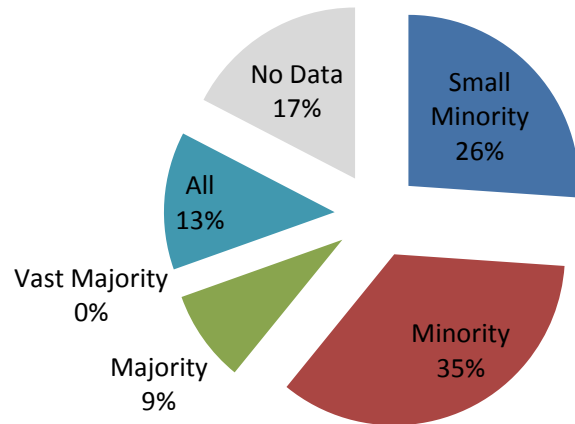


Figure 26. Fraction of Local Accessible Valuables Stolen among Heists in the HMCD.

**** In addition to the appraiser, the criminals brought wine, cheese, soup, sausage, and pâté⁹¹ to celebrate and sustain themselves during the 36-hour-long heist. While plundering the vault's safe deposit boxes, the thieves had further reason to celebrate when a late-night casino cash drop from a local casino, worth hundreds of thousands of dollars, came barreling down into the vault.^{26,91}

In terms of target environments, Fig. 27 illustrates a clear bias toward urban areas in the commission of these high-value heists. Besides the 70% of heists in urban areas, an additional 17% occurred in the vicinity of airports (e.g., the Schiphol Airport Diamond Heist, Brink’s-Mat Gold Heist and Swissport Heathrow Heist, both at Heathrow Airport, and the Lufthansa Heist at Kennedy Airport). Urban areas present both opportunities and challenges for thieves. If disguised properly, the large amount of activity in an urban area can complicate tracking of a thief, before, during, or after a heist. However, the availability of numerous and specialized security forces in a city can also be a detriment for a thief that is not well-disguised (as the criminals in both the Millennium Dome Raid and Swissport Heathrow Heist learned, when confronted with a 100-officer Metropolitan Police operation designed to foil their heist). It is probable, instead, that the primary reason for the observed urban bias is that many high-value targets are located in cities.

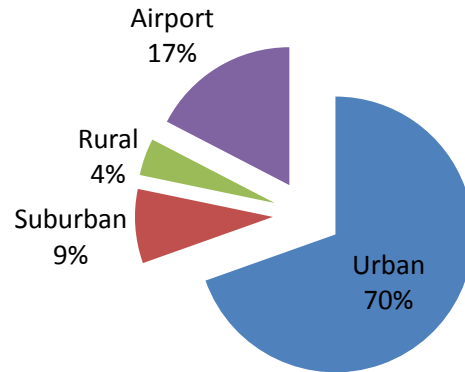


Figure 27. Target Environments among Heists in the HMCD.

A final observation regarding the heists in this study is a clear bias toward European crimes. Figure 28 shows that 70% of the heists in the database were committed in Europe; half of these were committed in the United Kingdom. An additional 18% were committed in North America, specifically in the United States. The remaining 12% comprises the Brazil Central Bank Cash Heist (South America), Tanzanian Airplane Gold Robbery (Africa), and British Bank of the Middle East Gold Heist (Asia). For reference, the estimated latitude/longitude coordinates of the locations for each heist are provided in Table 9.^{†††} Since the lists of major heists from which the database’s 23 were derived were of Western origin, a Western bias in Fig. 28 is not entirely surprising. However, the fact that European heists have much greater representation than North American heists among Western sources is not well explained. For example, is Europe simply the home of more centers of high-value goods, or are European thieves more interested in engaging in this type of criminal activity? It is also surprising that Eastern Europe, Russia, South Asia, East Asia, and Australia have no representation among lists of major heists. Major heists in these regions of the world may prove to be a subject of important insight and worthy of future investigation.

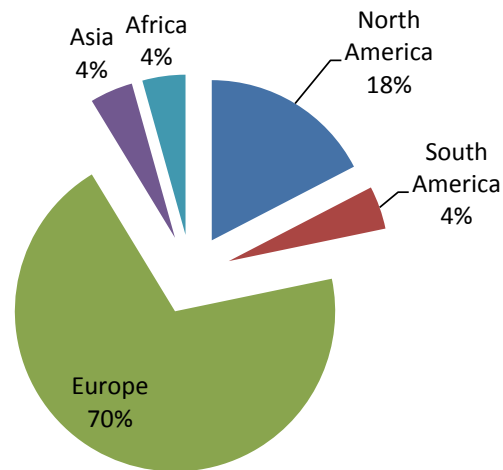


Figure 28. Continental Distribution among Heists in the HMCD.

^{†††} A Google Map locating each of the 23 heists in the database, plus several for which complete data entries could not be made in time for the writing of this paper, is available at <https://www.google.com/maps/ms?msid=206565135619449682207.0004be5da3a6089e3d9c5&msa=0>.

Table 9. Estimated Latitude/Longitude Coordinates of Heists in the HMCD.

ID	Name	City	Estimated Target Location	
			Latitude (deg.)	Longitude (deg.)
1	Brazil Central Bank Cash Heist	Fortaleza, Brazil	-3.734031	-38.522260
2	Sumitomo Mitsui Bank Heist	London, UK	51.511694	-0.097418
3	Antwerp Diamond Heist	Antwerp, Belgium	51.213927	4.418049
4	Museon Jewel Heist	The Hague, Netherlands	52.088960	4.279991
5	Société Générale Bank Heist	Nice, France	43.699004	7.269326
6	Stardust Casino Job	Las Vegas, USA	36.133282	-115.166900
7	Vastberga Helicopter Heist	Stockholm, Sweden	59.298020	18.012890
8	Millennium Dome Raid	London, UK	51.502986	0.003150
9	Tanzanian Airplane Gold Robbery	Geita, Tanzania	-2.810833	32.174170
10	Munch Museum Art Heist	Oslo, Norway	59.916849	10.774734
11	Carlton Hotel Diamond Heist	Cannes, France	43.549166	7.027150
12	Brink's-Mat Gold Heist	London, UK	51.469836	-0.404799
13	Lufthansa Heist	New York, USA	40.662117	-73.787440
14	British Bank of the Middle East Gold Heist	Beirut, Lebanon	33.896677	35.503097
15	Chase Manhattan Bank Robbery	New York, USA	40.608935	-73.970650
16	Mayfair Graff Diamond Heist	London, UK	51.509821	-0.141851
17	Harry Winston Diamond Heist	Paris, France	48.866493	2.304736
18	Schiphol Airport Diamond Heist	Amsterdam, Netherlands	52.304106	4.758053
19	Swissport Heathrow Heist	London, UK	51.454331	-0.456367
20	Gardner Museum Art Heist	Boston, USA	42.338768	-71.098860
21	Knightsbridge Safe Deposit Center Heist	London, UK	51.498765	-0.166361
22	Securitas Cash Depot Heist	Tonbridge, UK	51.191098	0.277652
23	Northern Bank Cash Heist	Belfast, UK	54.596244	-5.932016

3.4. Weapons Employed

*"When they threaten the guards with a gun there is not much to be done."*⁴⁰

*Jorunn Christofferson
Munch Museum Press Officer*

Among the tools that criminals frequently have at their disposal in the commission of a high-value heist are weapons. These tools are particularly unique in that they are almost always intended as a device for defeating human elements of security systems. As Fig. 16 in Section 3.1.2.1 illustrated, the HMCD shows a strong apparent correlation between the existence of security personnel and whether the criminals arrived at the heist armed. This section takes a brief look at some of the weapons that thieves have used to achieve their objectives.

Table 10 provides a summary of the types of weapons know to be used among the 23 heists in the HMCD. **A variety of weaponry has been employed in the commission of large heists**, and these weapons can be divided into four categories:

Conventional firearms tend to be the most frequently used weapons and include a variety of handguns, shotguns, machine guns, and rifles. Examples particularly abound in which firearms were used purely in a threatening manner with no shots actually fired.^{****} For example, guns were used to threaten Securitas manager Colin Dixon that his family would be killed if he did not comply and lead them into the Securitas cash depot. In the interesting example of the Carlton Hotel Diamond Heist, thieves fired machine guns as they entered the hotel's jewelry store. However, upon investigation of the crime, police found that the thieves had been firing blanks.

Explosives and incendiaries include weapons such as grenades, mortars, plastic explosives, and bombs. This category also includes the combination of gas and matches, which was used to threaten employees in the Brink's-Mat Gold Heist. In this heist, the two combination-holding employees^{§§§§} were doused with gasoline, and thieves threatened to light them on fire if they did not comply. They complied.^{*****}

Bladed weapons were rarely used in the HMCD heists. The only known examples involved knives used to threaten staff at the Swissport Cargo Warehouse at Heathrow Airport and to slice through the canvas wall of a commercial helicopter hangar in the Vastberga Helicopter Heist.

Blunt weapons were similarly rare among the HMCD heists. The only known examples in this category involved thieves wielding hockey sticks, clubs, and lumps of wood to threaten staff at the Swissport Cargo Warehouse.

In Table 10, a bomb (☛) symbol indicates that a given weapon (in the row) was known to be employed in a given heist (in the column). The rightmost column of Table 10 presents a simple count of the number of heists in which each weapon type was used, and the bottom row presents a simple count of the number of weapon types employed for each heist. A couple notes are worth discussion in both of these areas:

First, by far the most commonly used type of weapon was the handgun. This class of weapon is both deadly and easily concealed, permitting thieves to enter a facility and invite little scrutiny from security personnel or bystanders. The Harry Winston and Mayfair Graff diamond heists, both Timing Archetype III (Closing Time) heists, demonstrated skillful execution using this characteristic of handguns. Also somewhat common is use of shotguns and assault rifles. For certain heists, the type of firearm used was not ascertainable from public sources, and these were noted under the category of unspecified firearms. It is worth noting that, overall, 15 of the 23 (65% of) heists in the database are known to have used some sort of conventional firearm in execution of the crime.

Second, an interesting observation can be made from the bottom row of Table 10. While 70% of heists involved use of some weapon, it is worth noting that 7 heists (30%) involved no known use of weapons. These heists include both of the nonviolent heist categories (i.e., the Stealth Raid and Walk Away categories) plus the Gardner Museum Art Heist. Strikingly, these weaponless heists account for three of

^{****} Whether the thieves *would have* fired these weapons in the event of victim noncompliance is an open question. On one hand, failure to fire in such an event would cast doubt on the thieves' sincerity. On the other hand, killing the employee with the vault combination would do little to facilitate the thieves' success.

^{§§§§} This facility's security measures included a system of dual control, in which the opening of vault doors required two individuals with separate keys and combinations. The cooperation of *both* individuals was required to gain entry to the vaults.

^{*****} Wouldn't you?

the top four valued heists in the HMCD.^{††††} **This prompts the observation that an unarmed adversary is not an unimportant adversary.** Indeed, the unarmed adversary may be the most important adversary, if measured by the monetary value of the theft. Albert Spaggiari, the mastermind of the Société Générale Bank Heist, summarized the philosophy of such criminals well when he famously wrote on the wall of the vault that he robbed, “Sans arme, ni haine, ni violence,” or “Without weapons, nor hatred, nor violence.”

3.5. Resources and Risk Acceptance

*"It's like a big challenge, like Olympic games. You train for most part of your life, and go that day hoping to have an opportunity."*⁷²

*Valerio Viccei, Criminal
Knightsbridge Safe Deposit Center Heist*

The end of Section 3.1.1 mentioned that the diversity of security measure defeat capabilities observed in major heists supports a description of high-value heist criminal teams as sophisticated and well-organized. This section expands substantially on this characterization, delving into the resources that thieves bring to bear on attacking high-value targets and the risk that the criminals have historically accepted. In essence, this section shows the degree of ambition, discipline, and overall project management skill that these criminals often possess.

3.5.1. Planning Time and Schedule

Figure 29 depicts the distribution of estimated planning times for the heists in the HMCD. Within the data available for the figure (15 of the 23 heists), most heists involved known planning times of less than 30 weeks (7 months). The mean among this group of shorter planning times was 13 weeks (3 months). A prime example of one of these heists is the Brazil Central Bank Cash Heist, which commenced digging from the rented Grama Sintética storefront some three months prior to the robbery itself.

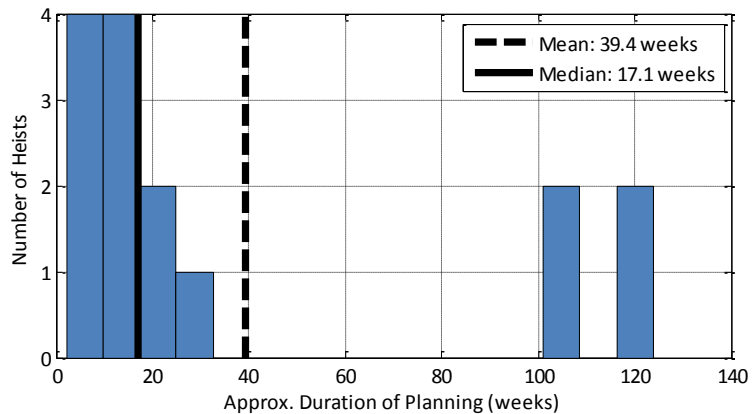
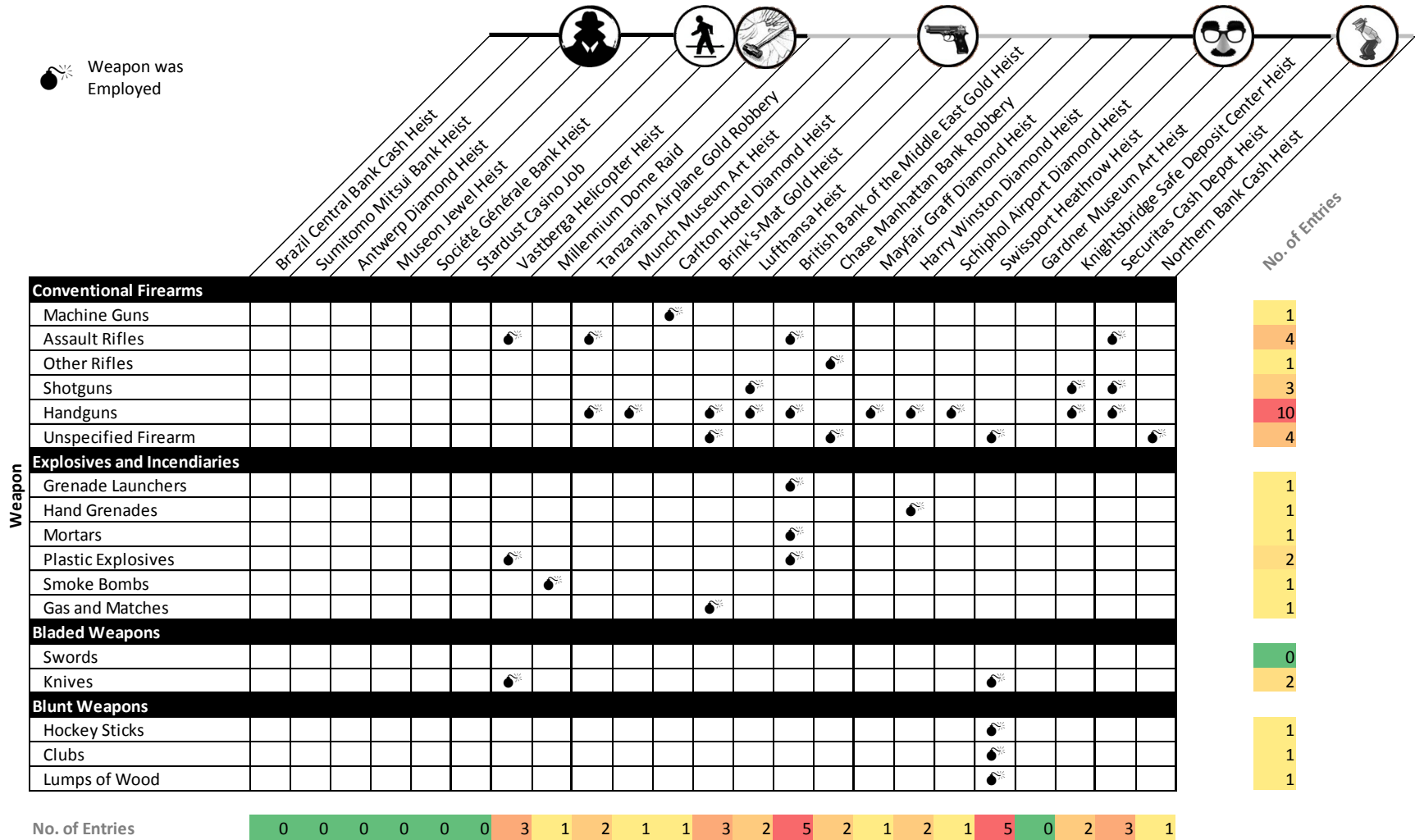


Figure 29. Distribution of Heist Planning Times.
Data available for 15 of 23 heists.

^{††††} The other heist on this top-four list was the Millennium Dome Raid, which used smoke bombs mainly to distract and confuse bystanders and security forces, rather than cause bodily harm.

Table 10. Summary of Weapons Used by Thieves.



A second region of interest in Fig. 29 exists for the four heists with planning times of more than 100 weeks. Included among these heists is the Antwerp Diamond Heist, with the longest estimated planning time of 2.4 years; it was in the autumn of 2000 that Leonardo Notarbartolo, the mastermind of the Antwerp Diamond Heist, began renting an office in the Antwerp Diamond Center in preparation for the eventual February 2003 heist. In another example, two years prior to the Société Générale Bank Heist, Albert Spaggiari rented a bank safe deposit box shortly after he heard from a neighbor and bank manager that the bank's vault was not alarmed. As well, in the case of the Gardner Museum Art Heist, one of the suspects in the crime admitted that he had scoped out the museum's security measures years earlier. On one visit in particular, he unlocked a window in the facility. Visiting again every few months, he found that the window remained unlocked and used this as a partial gauge of the attentiveness and thoroughness of the security force.

An important fact that this information elucidates is that **thieves do their homework, typically taking months or years to plan a high-value heist.** This clearly indicates that the thieves take the time to develop execution plans of high quality, though it also suggests that security forces have time on their side if they are able to effectively recognize the planning activities of a prospective thief.

3.5.2. Practice Runs and Testing

Figure 30 indicates the distribution of the approximate number of practice or reconnaissance runs thieves made to their targeted facility in advance of the heist itself. The figure shows two distinct types of practice and reconnaissance behavior: About two-thirds of the heists for which this data is available likely involved a handful of (less than six) practice runs. The remainder involved over twenty, and in some cases, over 100 practice or reconnaissance runs. This latter case describes heists executed by criminal teams with inside access, for example with an employee insider who is able to observe security procedures and other relevant details at work on a daily basis. Examples of this are well summarized in Table 7. **Most importantly, Fig. 30 illustrates that the majority of heists involved at least one practice or reconnaissance run. This reinforces the point made in Section 3.5.1 that thieves of high-value items indeed do their homework and are well-prepared to execute the theft.**

In addition to practice runs to the target facility itself, there exists one heist in which external vulnerability investigation and practice took place: In the planning of the Antwerp Diamond Heist, reconnaissance from the Antwerp Diamond Center revealed the brand of locks used for the doors, vault, and safe deposit boxes of the center. Since the heist planning team included a locksmith company owner, locks of the same brand could be ordered without raising suspicion, and vulnerabilities could be identified through experimentation.

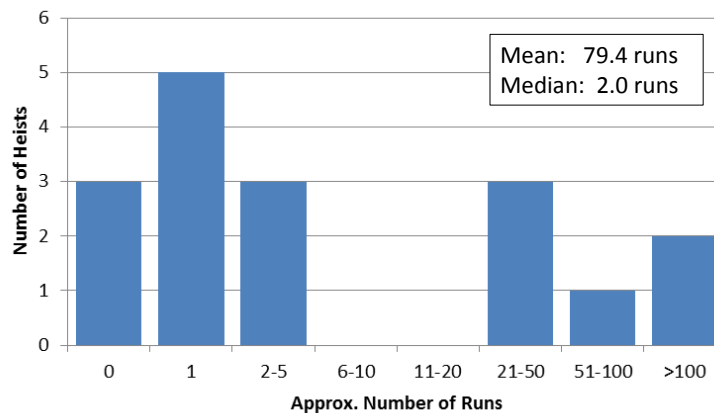


Figure 30. Distribution of Number of Practice and Reconnaissance Runs. Data available for 17 of 23 heists.

3.5.3. Transportation Capabilities

In planning for high-value heists, thieves must be confident that they can transport the stolen loot away from the crime scene. In many cases, as mentioned in the discussion of Fig. 26, it is not the amount of loot available at the target facility, but rather the capacity of the thieves' transportation vehicle(s) that limits the amount of loot the criminals can steal.

For each of the 23 heists in the HMCD, estimates were generated for the total weight of items stolen. Figure 31 shows the distribution of these results on a roughly logarithmic scale. In the first category are total weights of less than 5 lbs., such as the targeted diamonds from the Millennium Dome and gems from the Museon science museum. Also in this category are the electronic (and therefore weightless) funds of the attempted Sumitomo Mitsui Bank Heist. Goods of this small size can be easily carried out of a facility in a small bag or in a thief's pockets. In the middle of the graph lie items 50-500 lbs. in weight, such as the cash of the Vastberga Helicopter Heist and safe deposit box contents of the Antwerp Diamond Heist. These takes require backpack-class containers, possibly carried by multiple team members. At the far right extreme are loads of loot weighing more than 5,000 lbs. Examples here include loads of cash and/or gold from the Brazil Central Bank Cash Heist, Brink's-Mat Gold Heist, and Securitas Cash Depot Heist. These extremely heavy loads require the capacity of a sizable truck (see Fig. 32 for the truck used in the Securitas heist).

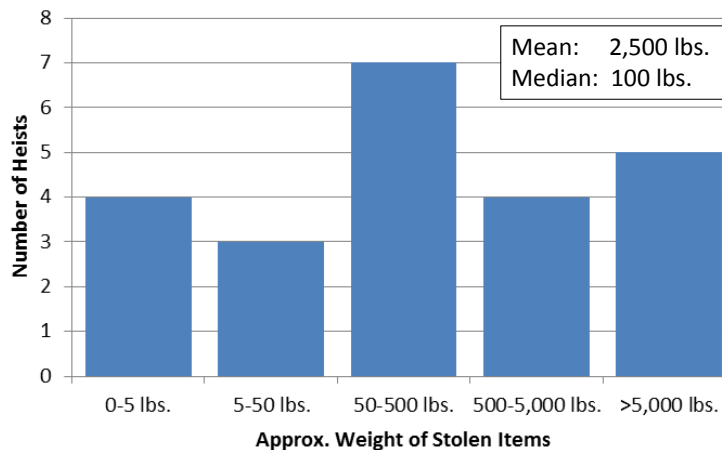


Figure 31. Weight of Stolen Items for HMCD Heists.



Figure 32. Renault truck recovered in connection with the Securitas Cash Depot Heist.⁷⁶

In selecting the size of the getaway vehicle, thieves must often choose between increasing the amount of loot (and thus money) they can transport from the target facility and decreasing their exposure and traceability. A larger getaway vehicle will translate into more wealth for the criminals but at a higher risk of discovery, either before the robbery (since renting or buying a truck is more noticeable than using the thieves' existing cars), during the robbery (since it takes more time to load the larger vehicle), immediately after the robbery (since it is easier to notice and harder to maneuver a large truck through city streets), or long after the robbery (since a greater amount of loot generally translates into a greater chance that it will be recognized as stolen when traded or spent). These factors, and different criminals' preferences for wealth over risk of capture, may be responsible for the broad variation of stolen item weight seen in Fig. 31. **However, the fact remains that thieves have demonstrated capabilities to steal anything from briefcases to trucks full of loot in the commission of high-value heists.**

3.5.4. Human Resources

In addition to time and transportation resources, a key component in the planning of a major heist is the management of human resources. This includes decisions regarding the number and size of teams as well as the characteristics of individual team members.

3.5.4.1. Number and Size of Teams

As Fig. 33 shows, solo heists are exceedingly rare; the only heist in the database that fits this criterion is the Stardust Casino Job. However, heists consisting of crime-scene teams of more than eight are also exceedingly rare. On average, for the heists in the HMCD, 4-5 willing accomplices were on-scene and responsible for the success of the theft. This number of accomplices appears to be large enough to allow the team of thieves to possess a diversity of skills and sufficient manpower to complete required tasks, but also small enough to avoid the introduction of undue risk of detection.

Figure 34 tracks the distribution of the number of on-scene teams among the heists in the database. Here, there exists a clear preference for single-team operations, which tend to be less complex; just over half of the heists in the database involved a single team in the crime scene vicinity. The number of heists with two, three, and four teams decreases almost geometrically. The four-team example in the database was the Mayfair Graff Diamond Heist, which involved a complex relay of the stolen goods among the occupants of different motor vehicles.

Figure 35 illustrates the discrepancy and magnification that exists when comparing the number of accomplices at the crime scene to the number of total accomplices for a given heist. The data from the HMCD suggest that for every accomplice at the scene of a heist, there are typically 1.26 total accomplices; in other words, for every four criminals present at a heist, about one additional willing accomplice has assisted in planning and preparation.

A key lesson from this discussion of team number and size is that, in the planning and execution of a heist,

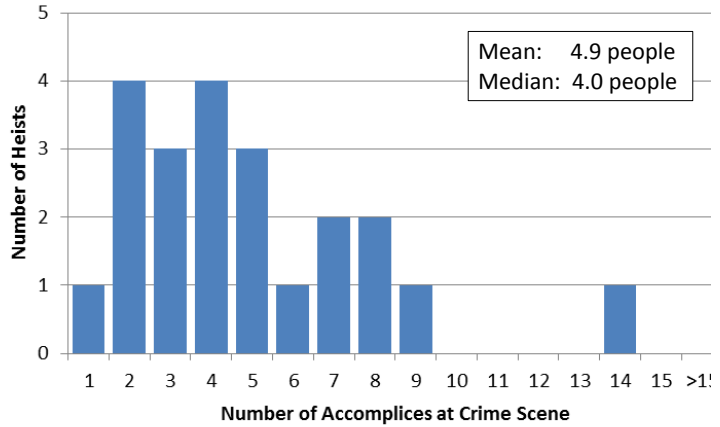


Figure 33. Number of Willing Accomplices at Crime Scene. Data available for 22 of 23 heists.

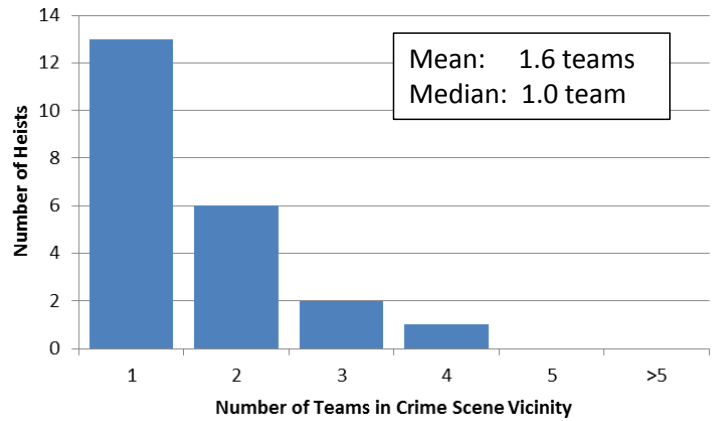


Figure 34. Number of Teams in Crime Scene Vicinity. Data available for 22 of 23 heists.

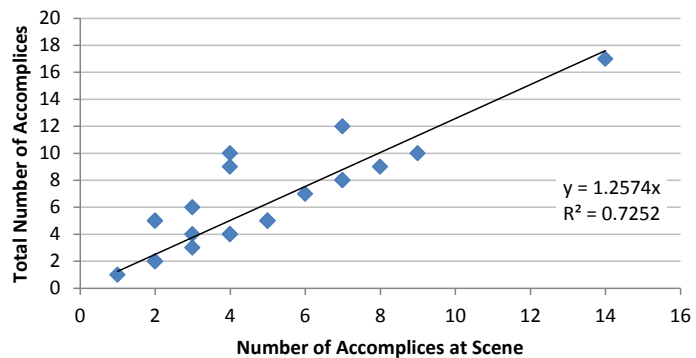


Figure 35. Crime Scene Participation Rate. Data available for 22 of 23 heists.

thieves almost always work in small teams. Furthermore, while much of the planning team is also involved in the physical execution of the heist, **the criminal team commonly extends beyond those who physically commit the crime.**

3.5.4.2. Typical Criminal Profiles

Among the data compiled in the HMCD are basic age, gender, and nationality profile data for criminals that have been identified as responsible for each of the 23 heists. These data provide the basis for three interesting observations:

First, all of the 133 criminals in the database for whom gender was known^{****} were male. This is a clear deviation from the demographic of the general population.

Second, the distribution of ages for the 83 criminals in the database for whom age (at the time of the crime) was known, provided in Fig. 36, shows an unusually high mean when compared to typical robbery or burglary criminals. The mean age of the high-value heist criminal was 36.1 years. In contrast, the average ages of typical robbers, burglars, and motor vehicle and other property thieves vary only between 24 and 27 years,⁹⁰ a good decade younger than

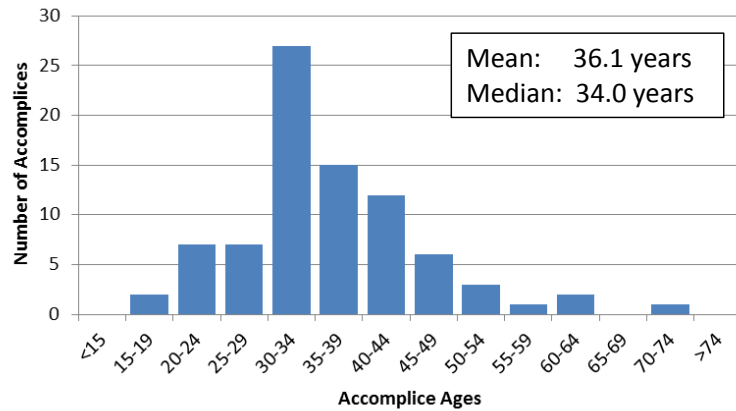


Figure 36. Distribution of Accomplice Ages (n = 83).

those observed committing high-value heists. Interestingly, the average age of high-value heist criminals appears more akin to those responsible for deceit crimes such as forgery, counterfeiting, and fraud, which have average ages between 30 and 33 years.

Third, Fig. 37 illustrates that in 74% of heists in the database, the criminal teams were native to the country in which the heist took place. In 16% of heists, the criminal team included both foreign and native citizens, and in only 10% of heists (specifically, the Antwerp Diamond Heist and British Bank of the Middle East Gold Heist) were the teams thought to consist entirely of citizens from foreign nations.

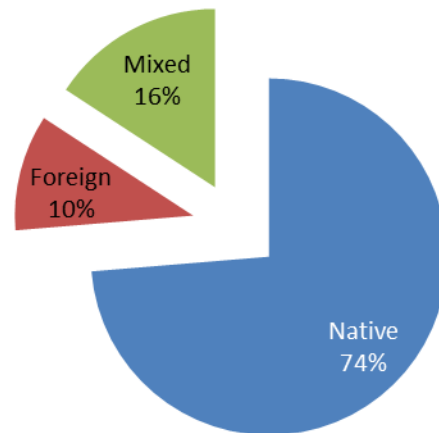


Figure 37. Criminal Team Nationality.
Data available for 19 of 23 heists.

Additionally, an effort was made to characterize the occupations of the thieves in the heist database. A list of the occupations recorded in the database is shown in Table 11, divided into categories of employees, managers, business owners, illicit, and other. The table shows a diversity of occupations for criminals categorized as having simple employee occupations, though most are not occupations requiring high levels of education or skill. Managerial occupations are notably few on the list, especially when compared to the diversity of business owners. However, a fact that does not

^{****} In a small minority of cases, involvement of additional accomplices was very strongly suspected, but their identity and gender remains unknown.

appear prominently in Table 11 is the predominance of the illicit career criminal occupation. In fact, among the business owners on this list are some of the more famous masterminds behind the heists in the database (e.g., Notarbartolo, the Antwerp mastermind, owned his own jewelry design business, and Spaggiari, the Société Générale mastermind, was a camera store owner), and in many cases those with occupations in the employee category were brought in to the planning or execution of the heist for their specialized skills or because of the plan's simple need for unskilled labor (e.g., for tunnel digging in the example of the Brazil Central Bank Cash Heist). As a result, many of the occupations on this list existed for appearances, and the men themselves could be more accurately understood as career criminals.

Summarizing, a reasonably accurate profile of the average high-value heist criminal is that of a 36-year-old man who is a career criminal (but with a front occupation for appearances) and is native to the country that is home to the valuables he aims to steal.

Table 11. List of Occupations for High-Value Heist Accomplices.

Employees	Managers	Business Owners	Illicit	Other
Appraiser	Airline Cargo Supervisor	Adult Store Owner	Career Criminal	Cage Fighter
Cashier	Security Chief	Bar Owner	Drug Dealer	Soldier
Construction Worker	TV Producer	Camera Store Owner	Gang Leader	Unemployed
Delivery Driver	Youth Club Leader	Coffee Shop Owner	Hacker	
Doorman		Garage Owner	Petty Thief	
Electrician		Jewelry Designer		
Electronics & Alarms Expert		Minicab Agency Owner		
Engineer		Safe Deposit Center Owner		
Gardener				
Journalist				
Musician				
Pizzeria Worker				
Postal Worker				
Roofer				
Security Guard				
Used Car Salesman				

3.5.5. Financial Risks and Returns

As with any major undertaking, lawful or criminal, the thieves of high-value heists must place at risk some financial resources. Equipment must be purchased, getaway vehicles must be procured, reconnaissance trips must be funded, and insiders may need to be incentivized. For 20 of the 23 heists in the HMCD, rough order of magnitude estimates were made of thieves' total expenditures, with the distribution of results shown in Fig. 38. Placed into bins by approximate order of magnitude, the results span a wide range of financial investment.

At the lower end of Fig. 38 are heists like the Sumitomo Mitsui Bank Heist, which required little more than a thumb drive and the setup of a several bank accounts to which funds could be deposited. Similarly, the Stardust Casino Job required little financial investment other than, perhaps, the

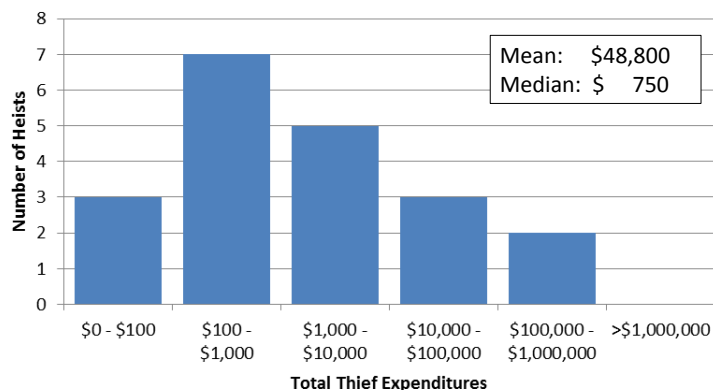


Figure 38. Estimated Thief Expenditures.
Estimates available for 20 of 23 heists.

purchase of a backpack with which to carry the stolen money out of the casino.

At the other extreme of Fig. 38 is the Brazil Central Bank Cash Heist, which included renting a storefront, advance payment of about \$3,000 to members of the tunnel-digging crew, a \$100,000 bribe to a bank security guard, and the purchase of about 10 cars in which to hide portions of the loot.

As a complement to Fig. 38, Fig. 39 shows the distribution of the ratio of return (measured by the value of the loot stolen or intended to be stolen) to investment (measured by the total thief expenditures) for 19 of the 23 heists in the database. The results are striking, and they pose a compellingly rational explanation for the commission of these crimes: The potential returns on investment are enormous. The *minimum* return on investment ratio in the data was 110, corresponding to the high-cost Brazil Central Bank Cash Heist. Return on investment ratios in the database span several orders of magnitude above this (consider, for example, the Sumitomo Mitsui Bank Heist, which would have had a cost in the tens of dollars but netted over \$400 million); the arithmetic mean ratio is about 1.5 million, and the median is 39,000. Thus, even in the worst case, these high-value heists have the potential for orders of magnitude returns on investment. **With enormous potential financial return, it is not surprising that thieves are willing to devote large amounts of time and money to the planning and execution of such thefts.**

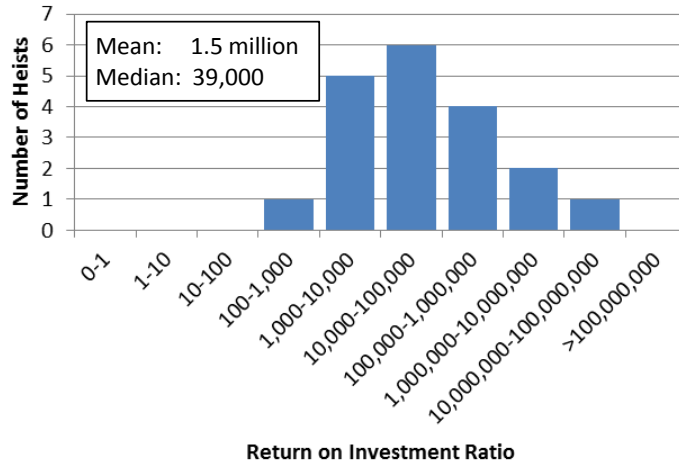


Figure 39. Estimated Thief Return on Investment Ratio.
Estimates available for 19 of 23 heists.

3.5.6. Risk Acceptance

While Section 3.5.5 showed that the heists in this study all had the potential to bear enormous financial return, the criminals took a substantial risk in executing their crimes. However, the **thieves' acceptance of risk was frequently a carefully calculated and rational decision.** The following qualitative analysis of the risks that the thieves undertook should help to shed light on some of the thieves' decisions:

The thieves who perpetrated these heists likely considered the distinction between the risk of capture and risk of death as a result of a heist. For many high-value targets, the risk of both of these events can be quite high if an attack is executed with no reconnaissance or planning; however, as Section 3.5.1 illustrated, in most cases the thieves planned for months prior to the execution of a heist. In doing so, they made reconnaissance and practice runs, frequently recruited or planted insiders, and learned what security measures were in place. Through these actions, the thieves reduced their risks substantially.

Furthermore, in cases of an unarmed attack (e.g., a Stealth Raid), the thieves would have realized that the risk of death would be quite low since it is unlikely that unarmed intruders would be fired upon by any armed security force (and certainly not by the much more common unarmed security force). Since they were unarmed, even if caught (as many of the perpetrators were, after having escaped with and hidden much of the loot) their prison sentences would not be particularly long. In the case of the Antwerp Diamond Heist, those convicted were sentenced to 5-10 years in prison. Considering that they all had sufficient time to hide the loot after the heist, many would consider this duration of prison time a fair trade for a life supported by tens or hundreds of millions of dollars' worth of hidden loot for the remainder of one's life.

The case of an armed attack poses a more substantial risk of death, which is an event that occurred in the cases of two armed thieves in the Chase Manhattan Bank Robbery and Tanzanian Airplane Gold Robbery. Nevertheless, the fact that only two criminal deaths occurred in the execution of the 16 armed heists in this database, which in total involved about 80 on-scene accomplices, puts the probability of death at about the same order of magnitude as an astronaut would accept to fly on the Space Shuttle. If committed in a European country in which conventional police do not carry guns, risk of death is further reduced. §§§§§ The consequences of capture in the case of an armed attack would be substantially higher than those of an unarmed attack, but they would likely be mitigated if nobody was physically harmed (e.g., if the thieves make sure only to *threaten* violence).

Perhaps the greatest risks are less intuitive. First, any except for the most stealthy heist attempts will very likely bring about their own obsolescence. That is, once a heist plan is executed, it can be used only once. If the plan fails, it will likely result in the security forces' discovery (and, hopefully, repair) of the security vulnerabilities that the criminals attempted to exploit. If the plan succeeds, it will result in the discovery (and, hopefully, repair) of the vulnerabilities that the criminals exploited. In either case, deciding to plan and execute a heist brings about a substantial risk that the next several months of planning will be a wholly wasted effort (i.e., if the heist fails). Further, the more effort that a criminal puts into planning with the intent of increasing his probability of success, the greater the (sunk cost) consequence of failure.

Second, a much more important risk consideration for prospective thieves is the post-heist risk of death. In three heists within this database, specifically the Brazil Central Bank Cash Heist, Lufthansa Heist, and Brink's-Mat Gold Heist, heist-related killings have occurred in the aftermath of the robbery itself. The most famous of these examples is the Lufthansa Heist: Following the heist, one thief neglected to fulfill his duty of bringing the van used during the heist to a junkyard to be compacted and destroyed. Instead, it had been parked in a no-parking zone and discovered by police two days after the robbery. Fingerprints found inside the van began leading police toward the thieves. To avoid being arrested and sent to prison for his involvement, the mob boss responsible who received most of the stolen cash from the heist began ordering the killing of those involved. Within one year of the heist, seven of the Lufthansa accomplices disappeared. Within another eight years, the entire crew that executed the heists had been either reported missing or found murdered. *****

§§§§§ This may be an additional factor explaining the prevalence of European heists noted in Section 3.3.3.

***** Another example of note is the kidnapping and murder of the alleged financier of the Brazil Central Bank Cash Heist, Luis Fernando Ribeiro. Ribeiro was kidnapped two months after the robbery and held for ransom. Though the ransom was paid, Ribeiro's bullet-ridden corpse was found in farm country several hundred miles from São Paulo two weeks later. Information was later uncovered to suggest that members of the state police had executed the kidnapping and murder for their own financial gain.²⁰

3.6. Insiders

"They knew so much. To be honest, I could have written down the combination numbers, given them the keys, and sat upstairs and had a cup of tea. They told me how to get into my own vault."⁴¹

Mike Scouse
Brink's-Mat Security Supervisor

Sections 3.2.1 and 3.5.4.2 discussed instances in which thieves have deceptively blended in to society or a specific organization by intentionally taking on an occupation that provides them cover or provides them access that they would not normally garner. The latter is so common among large heists that this section is dedicated to a discussion of such insiders. As Figure 40 suggests, **insider involvement is exceedingly common in the planning and execution of high-value heists.**

For the purposes of this work, an insider is defined as a person recognized or accepted as a member of a group or organization who has authorized access to restricted areas, equipment, or information. As the HMCD data has shown, insiders come in a wide variety of forms. In all cases, they can be characterized by at least three dimensions: Degree of Access, Origin, and Role.

The Degree of Access dimension can be largely characterized by the position that the insider holds in the target organization. As characterized earlier in Table 7, insiders have spanned almost every basic role in a target organization, from customer through owner. Insiders at different such levels in an organization's hierarchy often have different types of access, and gain it via different means. For example, customers and tenants often have the most restricted access to sensitive areas, equipment, or information, but becoming a customer or tenant is often a simple matter of putting forward the right amount of money. Figure 41 provides some examples of individuals that this database has considered insiders, but who have operated with varying degrees of inside access. Owners (e.g., Parvez Latif in the Knightsbridge Safe Deposit Center Heist), managers (e.g., Louis Werner in the Lufthansa Heist), and employees (e.g., Ermir Hysenaj in the Securitas Cash Depot Heist) fall into the clear category of being a "full" insider with a high degree of inside access. Customers (e.g., Albert Spaggiari in the Société Générale Bank Heist) and tenants (e.g., Leonardo Notarbolo in the Antwerp Diamond Heist) had less access to inside areas, equipment, and information. Because they were outsiders who purchased their way into the organization they were aiming to rob, by some standards they might be considered "partial" insiders (though they are still considered as insiders for the purposes of this study).

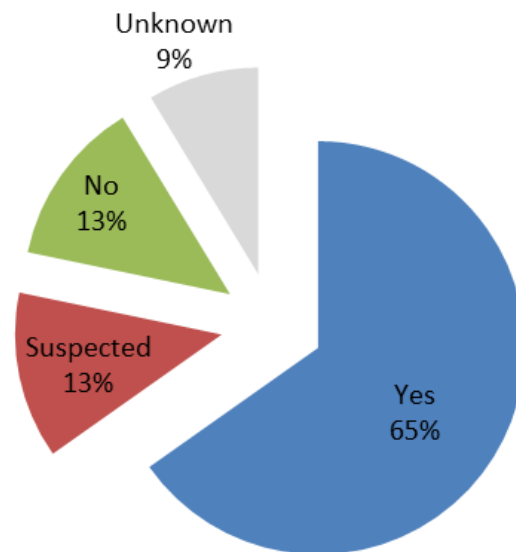


Figure 40. Was an insider used?
Results from all 23 heists.

The Insider Spectrum



Figure 41. Examples of insiders, ordered by their degree of inside access.

Origin refers to the means by which the insiders of a heist became insiders. For the heists of the HMCD, the Origin dimension is well summarized by five categories:

Planted insiders are individuals who become part of an organization with the intent of robbing it. Because it typically takes a significant amount of time to be promoted through the ranks of an organization, these insiders are typically limited to the easy-to-access lower levels in the organizational hierarchy. The most famous examples of Spaggiari, Viccei, and Notarbartolo in Fig. 41 were all planted insiders at the customer or tenant level. The example of Ermir Hysenaj, an Eastern European immigrant and the inside employee in the Securitas Cash Depot Heist, also encountered notoriously easy path to access: Hysenaj's interview for the job lasted just ten minutes, and he was on the job six days later.

Recruited insiders are individuals who are part of an organization and, typically as a result of their existing access and influence, are asked to join a heist plot. Recruitment is a risky tactic for a thief to employ, since the individual being recruited may refuse and subsequently alert authorities. Consequently, recruited insiders are uncommon in the database. There exist just three examples: the owner of the Knightsbridge Safe Deposit Center, an employee of the Brink's-Mat depot, and a security guard at Brazil's Central Bank in Fortaleza.

Opportunistic insiders are individuals who become part of an organization and subsequently realize that they can use their access to achieve substantial personal gain. Examples in this category also tend to be uncommon, but those that do exist include the security supervisor at the Sumitomo Mitsui Bank and cargo supervisor at the Lufthansa Overseas Cargo Terminal (interestingly, both in management roles) as well as the lone thief in the Stardust Casino Job.

Unwitting insiders are individuals who are not aware that they are being used to gather inside information, equipment, or area access in support of a crime. Coverage of unwitting insiders is sparse in the literature, and it is likely that the number of unwitting insiders involved in the heists of the HMCD is underestimated. However, prominent examples include the building manager who provided blueprints to the Antwerp Diamond Heist mastermind and the neighbor of Albert Spaggiari who let it slip that the Société Générale's vault was not alarmed.

Coerced insiders are by far the most numerous in the database, accounting for 11 of the 27 (41% of) identified insiders. At the time of the heist, these individuals are most often presented with threats on their lives or, in some cases, their loved ones lives. As a result, these individuals are compelled to use their inside access (especially keys and combinations) to comply with thieves' demands and assist in the robbery.

Role refers to the type of actions that an insider takes in the commission of a heist. For the heists of the HMCD, the Role dimension is well summarized by three categories:

Active violent insiders use or credibly threaten violence during a heist. Insiders in this role are exceedingly rare in the database, and only one example has been identified: Valerio Viccei, a customer of the Knightsbridge Safe Deposit Center, entered the center with another accomplice and wielded a gun to subdue the owner and guards.^{†††††}

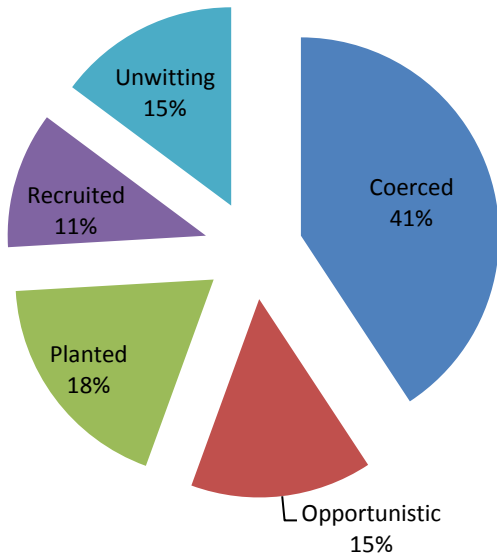
Active nonviolent insiders take part in the execution of a heist but do not threaten or use violence. This is the most common insider role in the database, describing 74% of insiders. This stands in some contrast with the fact that 16 of the 23 heists in the database (70%) involved armed thieves. That is, even in violent thefts, insiders rarely play violent roles.

Passive insiders do not take an active role in the execution of the heist. This role is largely associated with unwitting insiders, but it also includes opportunistic and recruited insiders whose sole role is to provide information about security vulnerabilities (e.g., the recruited security guard in the Brazil Central Bank Cash Heist and opportunistic cargo supervisor in the Lufthansa Heist).

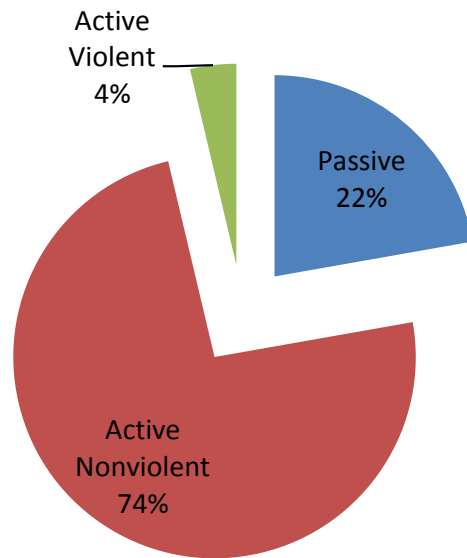
Figure 42 summarizes the distribution of insiders in the HMCD among different origins and roles. The top of the figure summarizes the distribution of insiders among origin and role individually, reflecting the discussions of origins and roles above. The bottom of the figure summarizes the joint distribution. The most striking characteristic about this joint distribution is that the database contains nearly three times as many examples of coerced, active nonviolent insiders as any other type of insider. In other words, **the most common inside help that thieves receive during a high-value heist comes from unwilling participants**. This is simultaneously troubling and promising. It is troubling in that it suggests executing a heist is not simply about bypassing networks of alarms and sensors, but very frequently about subverting human will and manipulating individuals to take actions that they do not wish to take. It is promising in the sense that, for these coerced insiders, the will to subvert the security system never existed. If security system designers can provide these potentially coerced insiders with tactics to free themselves from such coercion when it occurs, the insider problem may be substantially mitigated. For example, in the Securitas Cash Depot Heist, the security booth contained a sign that advised staff: "Don't Be a Hero" While sound advice aimed at saving the lives of employees, the same advice invites attacks by criminals who know the staff will surrender at the sight of a weapon (even if the thief has no intention of using it). An important consideration in security system design is whether tactics can be devised that simultaneously preserve human life and undermine the plans of thieves.

^{†††††} The owner, Parvez Latif, was also an accomplice, but Viccei kept that information secret from his other accomplices. Thus, to reduce suspicion, during the heist Latif played the part of a victim and surprised owner, and Viccei's accomplices remained clueless about Latif's involvement until their trials.

Insider Origin



Insider Role



Distribution of Insiders over Origins and Roles

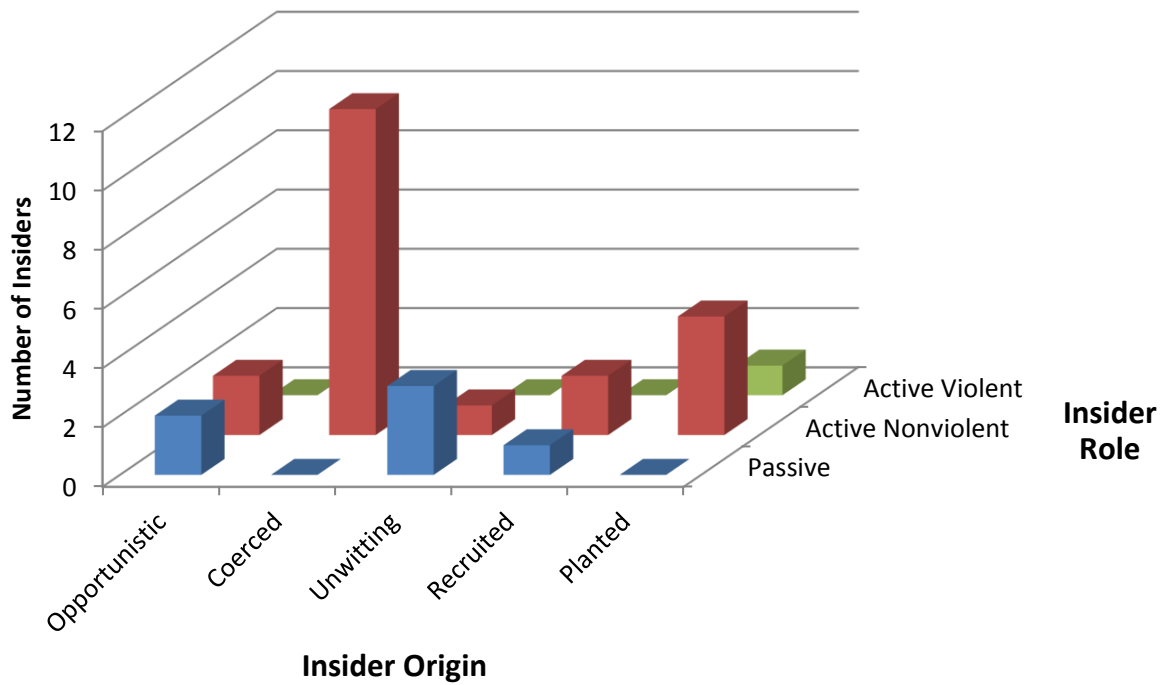


Figure 42. Summary of Activity among Insiders within the HMCD.

A final set of observations regarding insiders is illustrated through Fig. 43, which shows the distribution of numbers of insiders of different origins over the set of heists in the HMCD. First, the left plot shows that the number of *willing* insiders was limited to one in all but one of the heists in the database; the exception was the Knightsbridge Safe Deposit Center Heist, in which both the owner (Parvez Latif) and a safe deposit box renter (Valerio Viccei) colluded to perpetrate the heist. The second, center plot indicates that heists with *coerced* insiders are rarer than heists with willing insiders but involve more insiders per incident. An example of collusion among unwilling insiders occurred in the Northern Bank Cash Heist, in which the families of two bank employees, Chris Ward and Kevin McMullan, were held hostage while Ward and McMullan assisted thieves in robbing the bank.^{*****} The final plot on the right illustrates the aggregate number of insiders per heist. Among the observations that can be made is that multiple-insider heists are actually more common than single-insider heists in the database. That is, **not only are insiders common among high-value heists, but clear threats also originate from multiple insiders, both unwillingly and willingly colluding.** Insights such as this could prove particularly useful in the design and operation of human components of security systems.

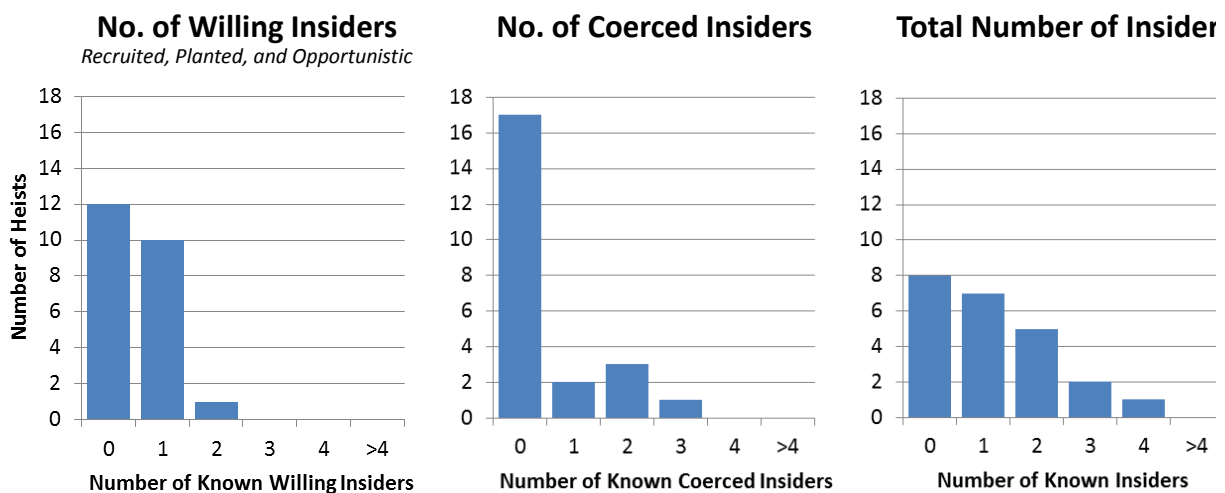


Figure 43. Distributions of Insider Numbers across Heists.

3.7. Failures and Mistakes

"I mean, there is no security system that can't be bypassed, because there always is a human mind and a human hand activating them."⁷²

*Valerio Viccei, Criminal
Knightsbridge Safe Deposit Center Heist*

This final focus area examines some failures that have happened in association with the heists in the HMCD, both on the side of the security forces and on the side of the thieves. Some failures were the

^{*****} Ward was tried for colluding with the thieves but was cleared of wrongdoing. During the trial, Justice Richard McLaughlin asked assistant manager Kevin McMullan, "It's not like the movies, you don't need dynamite?" McMullan responded, "You just need to take someone's wife away from them."

consequence of risks that were well-known and, for one reason or another, accepted by the responsible party. Others were the result of risks not recognized in advance.

3.7.1. Security Failures

This study's database is replete with examples of security procedures that failed to protect the assets they were intended to protect. **In most cases, the failure of these security procedures was that they were sufficient to deter opportunity theft or a hastily planned attack but insufficient to protect against an attack by a knowledgeable, patient, and determined criminal.** In a few cases, however, the thieves utilized attack modes that were almost certainly beyond the imagination of the security system designers:

The **Vastberga Helicopter Heist** is perhaps the most obvious such attack. Rather than enter the G4S depot from the ground level, or even by an ascent to the top of the building to break in via the pyramid skylight, the thieves recruited a helicopter pilot to land them on the roof. It can hardly be imagined that helicopters were included on the list of potential threats against which the depot's security was designed to protect. Still, even if they had, a local police force was equipped with a helicopter and could pursue if necessary. However, the thieves were able to preclude the use of this option by placing packages with the appearance of bombs outside the police heliport.

A second, less dramatic example is the **Munch Museum Art Heist**. In this heist, armed thieves entered the museum and stole two pieces of art while holding guards and visitors at gunpoint. Such a heist was unexpected and was not well-protected against in the design of the museum's security; this was reportedly the very first armed art heist in Norway.

In contrast, in a few cases the thieves were far from imaginative. Instead, with enough reconnaissance, they attacked vulnerabilities that the facilities had already recognized as weak points:

In the case of the **Antwerp Diamond Heist**, the targeted Diamond Center was not insured. In fact, the building managers would not consent to an insurance evaluation, possibly because they were aware of several clear security vulnerabilities.¹ For example, motion detectors were not anti-masking, CCTV recordings were stored via on-site videotapes, one side of the facility was accessible from outside the Secure Antwerp Diamond Area (SADA), and the garage door facing the street outside of the SADA was controlled by an old single-code door opener whose code could be identified with a frequency scanner. Moreover, the center did not perform background or reference checks on tenants. These vulnerabilities piqued the interest of the criminal Ferdinando Finotto when he was in Antwerp to perpetrate another crime years earlier, and the information was passed on to the eventual Antwerp mastermind, Leonardo Notarbartolo.

In the **Gardner Museum Art Heist**, an independent security evaluation conducted two years prior to the robbery had recommended an enclosed security station and protective second door for the museum's side entrance. Additionally, the director of security had lobbied the museum's board of trustees for more security funding so that he could attract security guards more qualified and experienced than local college students. However, the museum was in financial trouble, and the funds never came.

3.7.2. Thief Failures

When discussing failures, it is important to remember that **mistakes and unplanned events occur for criminals as well as security forces.** Clearly, in the five failed heists in this database, events transpired poorly for the thieves:

In the **Sumitomo Mitsui Bank Heist**, an improperly completed interbank communications form stood in the way of the \$480 million fund transfer. Bank employees called the authorities after

returning to work on a Monday and noticing the attempted transactions and severed network cables.

In both the **Millennium Dome Raid** and **Swissport Heathrow Heist**, intelligence gathered by the Metropolitan Police well in advance resulted in 100-officer operations to foil the robberies, with police forces lying in wait on the days of the heists.

The **Tanzanian Airplane Gold Robbery** was thwarted thanks to strong mine security and police forces. One thief was killed and one security guard injured in the firefight.

The **Chase Manhattan Bank Robbery** was foiled by a disguised phone communication between bank managers during the initial stages of the heist. As a result, the bank manager off-scene alerted police and a standoff resulted. Some 14 hours later, one of the robbers was captured and another killed while waiting for their getaway airplane in a limousine driven by an FBI agent.

Beyond these failed heists, however, there are numerous examples of unplanned events having significant effects on thieves' plans. In many cases, such events required the thieves to alter their plans mid-heist. **Of the 23 heists in the database, at least 13 (57%) experienced such events. Still, in all but the five failed cases above, these unexpected events were overcome and resulted in a successful heist.** Examples include:

In the violent **Brink's-Mat Gold Heist**, the employee responsible for holding the combinations to the inner vault doors was so distressed (after being drenched in gasoline) that he could not remember his recently-changed combinations. The inner vaults contained between \$3.4 million and \$10.3 million (FY12). Fortunately for the thieves, stored in the outer vault on that particular day was \$85.9 million (FY12) in gold bullion.

During the **Knightsbridge Safe Deposit Center Heist**, mastermind Valerio Viccei used a radio to call for his help on the outside once the center's owner and guards had been subdued. However, Viccei received no reply. He had to physically leave the safe deposit center during the robbery to find his henchmen,^{§§§§§§} who were waiting nearby as planned – with their radios tuned to the wrong channel.

During the **Société Générale Bank Heist**, the thieves saw both pleasant and unpleasant surprises. Pleasantly, in the middle of the night, a local casino dropped a cash deposit into the night deposit box and, in effect, into the thieves' waiting arms. Less pleasantly, a storm arrived during the heist and threatened to flood the thieves' sewer exit route, prompting a premature end to the thieves' time in the vault. No doubt after finishing the last of the celebratory feast of wine, cheese, soup, sausage, and pâté they had brought to the robbery, the thieves fled with \$40.4 million (FY12) in hand.⁹¹

^{§§§§§§} At the time when this occurred, police were out in force in the area, searching for a kidnapped child.⁷²

4. CONCLUSIONS

This paper has extensively surveyed 23 sophisticated and high-value heists, with particular emphasis on those that have occurred over the past three decades. The results of this survey have been compiled in a Heist Methods and Characteristics Database (HMCD) and analyzed qualitatively and quantitatively, with the goals of (1) characterizing the range and diversity of criminal methods and (2) identifying characteristics that are common (or uncommon) in high-value heists. The analysis has been structured into seven focus areas:

- Defeated Security Measures and Devices
- Deception Methods
- Timing and Target Selection
- Weapons Employed
- Resources and Risk Acceptance
- Insiders
- Failures and Mistakes

In the analysis process, which has been the subject of the bulk of this paper, some 44 key lessons have been emphasized and are summarized in Section 4.2. Perhaps even more interesting, however, are some generalizations profiling the types of criminals and criminal teams that perpetrate the types of high-value heists seen throughout this study. The latter is the subject of Section 4.1.

4.1. Who is the adversary?

While no two perpetrators of high value heists are the same, this study has revealed both commonalities and ranges to their characteristics and the characteristics of their methods and teams.

The typical high-value heist criminal is a man in his thirties: Just over half of the criminals in the HMCD were 30-39 years old at the time of their crimes, and the mean age is 36.1 years. All criminals in the database were men, and nearly three-quarters were natives of the country whose valuables they were targeting. While there is no typical occupation, these criminals gravitate toward either being employees or business owners (often of front companies), but infrequently toward middle management. Regardless of their officially stated occupation, however, they are often career criminals.

The typical criminal team consists of 2-10 (mean of 6.4, maximum of 17 observed) total accomplices, with 2-8 (mean of 4.9, maximum of 14 observed) typically being present at the crime scene. Most commonly, they will perpetrate the robbery as a single team, although multiple teams (up to four) are not uncommon. It is not uncommon for members of the team to each have specialized roles in preparing for or executing the heist. Use of weapons, particularly firearms, is typical but in many cases not required for the success of a heist.

Given the enormous payoffs in heists of this class, thieves are willing to devote substantial time and resources to planning. Commonly, thieves of high-value items have been observed to plan for about three months prior to a robbery, though a number of cases have involved planning over a period of two years. Thieves are willing to spend hundreds of thousands of dollars on planning if necessary, though in many cases this level of expenditure is unnecessary to circumvent a facility's security measures. Knowing that transportation capabilities limit the amount of loot they can steal (single-trip heists are preferred), thieves have demonstrated the ability to load and transport thousands of pounds of stolen valuables away from the crime scene without being chased or stopped.

Thieves are frequently thorough and innovative in their planning. This applies to their development of novel methods for defeating security measures and especially to their development of clever deception methods. Rarely, however, do these innovations require or involve the use of advanced, high technology. Security defeat and deception methods are often physically very simple, but they are highly targeted toward vulnerabilities the thieves have identified in advance of the heist. In the identification and exploitation of these vulnerabilities, deceptions and insiders almost always play a role. Additionally, thieves frequently identify and exploit vulnerabilities that allow them to avoid, rather than engage, a well-equipped security force response.

Finally, it is extremely common for a high-value heist to involve the use of an insider. Thieves may plant themselves as insiders, typically as customers or tenants of the organizations they intend to rob. Alternatively, thieves may occasionally recruit an insider from anywhere among the ranks of the organization. Criminal insiders may also arise from employees who see an opportunity for financial gain, or from employees who unwittingly provide critical information. However, by far the most common type of insider is the coerced insider who unwillingly assists in the crime, often upon threat of losing his own life or the lives of his family members.

4.2. Lessons Learned

For convenience, the following list is a compilation of major lessons learned that have been highlighted individually (in bold) in each of the focus area sections of this paper:

Section 3.1: Defeated Security Measures and Devices

1. A security system for high-value items that principally or solely relies on keyed locks, cameras, and unarmed guards may be at high risk for exploitation and defeat.
2. While some security measure defeat methods employed in high-value heists are simply uses of brute force, others are highly creative and innovative.
3. Even among the creative and innovative security measure defeat methods observed in high-value heists, none make significant use of high technology.
4. No single approach (whether creative or brute force) to defeating security measures clearly dominates thieves' practice. Thieves employ a variety of methods to defeat security measures, and few, if any, can be considered typical.
5. A common thread among the three most common security measure defeat methods is that they all attack segments of the security system in which humans are in the loop.
6. The malleability of human behavior should be an important consideration in the design of any security system.
7. High-value heists typically involve the defeat of multiple security measures.
8. Even unarmed security guards can add an element of uncertainty to thieves' planning, encouraging thieves either to arm themselves as a precaution or to buy down the risk with extended planning and intelligence gathering.

9. In over one-third of heists in the HMCD, dependence on security guards acting in a sensor role came with a significant delay between detection and response.
10. Heists involving a deception prior to a subdue and seize event are often able to delay both security recognition of the heist and a security response to the heist.
11. To be effective, an on-scene security force must be able to (1) act as a sensor to recognize a heist in progress and (2) either communicate this information to the appropriate responders or effectively respond themselves when under duress.
12. For the heists in the database, the size of the thief force was typically driven by factors other than the size of the security force.
13. Lack of response force proximity is rarely the reason for a lack of security response.
14. Physical protection by means of guards is often a manageable obstacle for well-prepared thieves.
15. The effectiveness of security forces can be substantially weakened in the presence of an uncertain but credible threat.

Section 3.2: Deception Methods

16. Even the most exceptional security response force can be thwarted by a thief who is recognized as an individual with legitimate access.
17. Use of deception is a standard element of large criminal heists.
18. Thieves or coerced accomplices who blend in by occupation exist more frequently inside than outside the targeted organization.
19. There is no clear limitation to what level of an occupational role thieves or their coerced accomplices will take; the database contains virtually equal numbers of examples of inside managers, employees, and customers.
20. Deception methods used in large heists tend not to be particularly high-tech or complex.
21. The thief's challenge in utilizing deception methods is not in executing them so much as it is in planning and selecting the proper deceptions to execute.
22. High value heists typically involve the employment of multiple deception methods.

Section 3.3: Timing and Target Selection

23. A continuously vigilant security force for high-value items is essential.
24. Thieves have little need to engage in rapid operations when not pressured by the high likelihood of daytime detection that exists at many facilities.
25. While day-of-week patterns are not obvious for the aggregate of all types of high-value heists, stealth raids in particular tend to occur on weekends.

26. In selecting targets according to their penetrability ease of asset liquidation (“fence-ability”), criminals demonstrate rationality in their decision-making preferences.
27. The complete theft of all (or even most) valuables at a target is rare.
28. There exists a clear bias toward urban environments in the commission of these high-value heists.

Section 3.4: Weapons Employed

29. A variety of weaponry has been utilized in the commission of large heists.
30. An unarmed adversary is not an unimportant adversary.

Section 3.5: Resources and Risk Acceptance

31. Thieves do their homework, typically taking months or years to plan a high-value heist.
32. The majority of heists involve at least one practice or reconnaissance run.
33. Thieves have demonstrated capabilities to steal anything from briefcases to trucks full of loot in the commission of high-value heists.
34. In the planning and execution of a heist, criminals almost always work in small teams.
35. While much of the theft planning team is also involved of the physical execution of the heist, the team commonly extends beyond those who physically commit the crime.
36. A reasonably accurate profile of the average high-value heist criminal is that of a 36-year-old man who is a career criminal (but with a front occupation for appearances) and is native to the country that is home to the valuables he aims to steal.
37. Seen through the lens of financial return and return on investment, it is not surprising that thieves are willing to devote large amounts of time and money to the planning and execution of high-value thefts.
38. Thieves’ acceptance of risk is frequently a carefully calculated and rational decision.

Section 3.6: Insiders

39. Insider involvement is exceedingly common in the planning and execution of high-value heists.
40. The most common inside help that thieves receive during a high-value heist comes from unwilling participants (coerced, active nonviolent insiders).
41. Not only are insiders common among high-value heists, but clear threats also originate from multiple insiders, both unwillingly and willingly colluding.

Section 3.7: Failures and Mistakes

42. In most cases, the failure of security procedures was that they were sufficient to deter opportunity theft or a hastily planned attack but insufficient to protect against an attack by a knowledgeable, patient, and determined criminal.
43. Mistakes and unplanned events occur for criminals as well as security forces.
44. Unplanned events do not always result in failure. Despite the fact that thieves in over half of the heists in the database experienced unexpected and plan-altering events, less than one-quarter of the heists in the database failed.

4.3. Future Work

Certainly, the survey and analysis presented in this paper has only scratched the surface of security insights that may be gained through the study of high-value heists and related crimes. Future work is recommended in a variety of areas. First, expansion of the HMCD to encompass additional heists is an obvious future work item. This expansion might continue to track down details of thefts that commonly make published lists of top heists, or it might take the direction of purposefully widening the scope geographically (e.g., to include heists in Russia, South Asia, East Asia, and Australia) and temporally (e.g., to include heists prior to the 1970s, perhaps as far back as the early 1900s, or farther back to the 1800s or even 1700s) to ensure the representation of a greater diversity of criminal methods and techniques in the data.

Additionally, it would be of some interest to explicitly compare criminal methods for high-value heists with those for smaller-value heists (for which much more data should be available) to understand areas of similarities and differences. Similarly, investigations into illicit tunneling activities, high-firepower criminal raids, and prison breaks might also yield comparative insights. Studies into the criminal methods exploited in fictional novel and motion picture heists may also yield insights into what is possible, if nothing else, in the criminal imagination.

Finally, a more extensive categorization of insiders is well worth future consideration. For example, at what threshold barrier to entry does an outside customer become an insider? Also, at what threshold of legitimacy should an individual posing as an industry or organization insider be considered an insider rather than an impostor? Do historical examples exist to help draw these lines? While these questions are at first glance questions of semantics, a more extensive characterization of the types and categories of insiders can help ensure that future security analyses consider as complete a set of threats as possible.

Ultimately, the insights from studies such as this are aimed at assisting the security systems design and operations communities to more fully protect against the threats they face and, at a minimum, ensure that the methods thieves have cleverly used in the past are no longer available or effective toward their future plans.

5. REFERENCES

- ¹ Selby, S.A. and Campbell, G., *Flawless: Inside the Largest Diamond Heist in History*, Sterling, New York, 2010.
- ² Time Staff, “Top 10 Brazen Heists,” *Time*, 4 Aug. 2011, Available: http://www.time.com/time/specials/packages/article/0,28804,1865132_1865133_2086915,00.html [8 Aug. 2012].
- ³ British Broadcasting Corporation, “High-profile heists,” *BBC News*, 11 Aug. 2009, Available: http://news.bbc.co.uk/2/hi/uk_news/7019889.stm [14 Aug. 2012].
- ⁴ Discovery Communications, “Top 10 Heists,” *Investigation Discovery*, 2012, Available: <http://investigation.discovery.com/investigation/crime-countdowns/heists/heists.html> [8 Aug. 2012].
- ⁵ Shaw Media, “Top Ten Heists of All Time,” *History Television*, 2012, Available: <http://www.history.ca/content/contentdetail.aspx?contentid=226> [8 Aug. 2012].
- ⁶ Wilson, C., Schott, I., Shedd, E., Wilson, D., and Wilson, R. (Eds.), *The World’s Greatest True Crime Stories*, Barnes & Noble, New York, 2004.
- ⁷ Cummins, J., *Heists: Gripping Exposés of the World’s Most Notorious Robberies*, Pier 9, Millers Point, 2011.
- ⁸ Rafter, N., *Shots in the Mirror: Crime Films and Society*, Oxford University Press, New York, 2006, chs. 1, 7.
- ⁹ McDowall, D., “The Present and Possible Future of Quantitative Criminology,” *Journal of Quantitative Criminology*, Vol. 26, No. 4, Dec. 2010, pp. 429-435.
- ¹⁰ Bitzer, E.G. III and Hoffman, A., “Psychology in the Study of Physical Security,” *Journal of Physical Security*, Vol. 2, No. 1, 2007, Paper 4.
- ¹¹ Warner, J.S., “What’s with All This Peer-Review Stuff Anyway?,” *Journal of Physical Security*, Vol. 4, No. 1, 2010, Paper 3.
- ¹² Reinstedt, R.N. and Westbury, J., “Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs,” RAND Note N-1498-SL, April 1980.
- ¹³ Schuller, C.R. and Ford, J.L., “Demand Side Analysis of Theft of Nuclear Materials – Some Insights from the Study of Complex Crime,” Conference on Physical Protection of Nuclear Materials – Experience in Regulation, Implementation, and Operations, *Proceeding Series of the International Atomic Energy Agency*, Vienna, 10-14 Nov. 1997, pp. 385-393.
- ¹⁴ Bunn, M., *Guardians at the Gates of Hell: Estimating the Risk of Nuclear Theft and Terrorism – and Identifying the Highest-Priority Risks of Nuclear Theft*, Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, Jan. 2007, Ch. 4.
- ¹⁵ Bunn, M., *Securing the Bomb 2010: Securing all Nuclear Materials in Four Years*. Cambridge: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative, April 2010, p. 95.
- ¹⁶ Bunn, M. and Glynn, K.M., “Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries.” *Journal of Nuclear Materials Management*, Vol. 41, No. 3, June 2013, pp. 4-16.
- ¹⁷ British Broadcasting Corporation, “‘Record’ bank robbery in Brazil,” *BBC News*, 8 Aug. 2005, Available: <http://news.bbc.co.uk/2/hi/americas/4133388.stm> [11 Oct. 2012].
- ¹⁸ The Sydney Morning Herald, “Gardener who became Brazil’s biggest bank robber,” *The Sydney Morning Herald*, 10 Aug. 2005, Available: <http://www.smh.com.au/news/world/gardener-who-became-brazils-biggest-bank-robber/2005/08/10/1123353368764.html> [11 Oct. 2012].
- ¹⁹ Caminada, C. and Walter, M., “Brazil Central Bank Robbed of \$67 Million in Currency (Update5),” *Bloomberg*, 8 Aug. 2005, Available: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=auuqiUfRM060&refer=news_index [11 Oct. 2012].
- ²⁰ Erskine, J., *Gold Diggers: The World’s Biggest Bank Robbery*, Discovery Communications, 2006.
- ²¹ British Broadcasting Corporation, “The big heist that came so close,” *BBC News*, 4 March 2009, Available: http://news.bbc.co.uk/2/hi/uk_news/7909595.stm [12 Oct. 2012].

- ²² Incisive Media Investments Limited, “Foiling a thoroughly modern bank heist,” *computing.co.uk*, 19 March 2009, Available: <http://www.computing.co.uk/ctg/analysis/1858212/foiling-thoroughly-modern-bank-heist#> [12 Oct. 2012].
- ²³ Davis, J., “The Untold Story of the World’s Biggest Diamond Heist,” *Wired Magazine*, 12 March 2009, Available: http://www.wired.com/politics/law/magazine/17-04/ff_diamonds?currentPage=all [13 Oct. 2012].
- ²⁴ Henley, J., “Museum gem theft dazzles Dutch police,” *The Guardian*, 3 Dec. 2002, Available: <http://www.guardian.co.uk/world/2002/dec/03/internationaleducationnews.education> [15 Oct. 2012].
- ²⁵ Layton, J. and Chandler, N., “10 Largest Diamond Heists,” *HowStuffWorks.com*, 23 April 2008, Available: <http://people.howstuffworks.com/five-largest-diamond-heists.htm> [15 Oct. 2012].
- ²⁶ Rothery, C., *Masterminds: The Riviera Job*, Red Apple Entertainment, 2004.
- ²⁷ Mondy, C., “Des égouts à la salle des coffres: "casse" parfait à la Société Générale de Nice,” *Live2Times*, 10 Aug. 2010, Available: <http://www.live2times.com/1976-casse-du-siecle-a-la-societe-generale-de-nice-e--9960/> [25 Oct. 2012].
- ²⁸ Mead Publishing, “Theft nets \$500,000 from Stardust Hotel,” *Loose Change*, Vol. 15, No. 1, Nov. 1992, p. 13.
- ²⁹ Simpson, P.V., “Helicopter robbery – how it happened,” *The Local*, 24 Sept. 2009, Available: <http://www.thelocal.se/22260/20090924/> [28 Oct. 2012].
- ³⁰ “Stockholm cash depot hit by helicopter heist,” *The Local*, 23 Sept. 2009, Available: <http://www.thelocal.se/22234/20090923/> [28 Oct. 2012].
- ³¹ Ratliff, E., *Lifted*, Atavist, New York, Available: <https://www.atavist.com/stories/lifted/> [28 Oct. 2012].
- ³² “Seven convicted of spectacular helicopter heist,” *The Telegraph*, 7 Oct. 2010, Available: <http://www.telegraph.co.uk/news/newsvideo/8049390/Seven-convicted-of-spectacular-helicopter-heist.html> [28 Oct. 2012].
- ³³ Steele, J. and Foster, P., “Police foil smash and grab raid on Dome’s £350m diamonds,” *The Telegraph*, 8 Nov. 2000, Available: <http://www.telegraph.co.uk/news/uknews/1373643/Police-foil-smash-and-grab-raid-on-Domes-350m-diamonds.html> [29 Oct. 2012].
- ³⁴ “Great Dome robbery foiled,” *BBC News*, 7 Nov. 2000, Available: http://news.bbc.co.uk/2/hi/uk_news/1010974.stm [29 Oct. 2012].
- ³⁵ *Dome Raiders*, BBC, 2002.
- ³⁶ Bariyo, N., “Police Foil Gold Heist in Tanzania,” *The Wall Street Journal*, 6 Jan. 2012, Available: <http://online.wsj.com/article/SB10001424052970203471004577144354040588404.html> [30 Oct. 2012].
- ³⁷ White, G., “Tanzanian police foil \$30m ‘Great Plane Robbery’ gold heist,” *The Telegraph*, 6 Jan. 2012, Available: <http://www.telegraph.co.uk/finance/personalfinance/investing/gold/8998263/Tanzanian-police-foil-30m-Great-Plane-Robbery-gold-heist.html> [30 Oct. 2012].
- ³⁸ Gibbs, W. and Vogel, C., “Munch's 'Scream' Is Stolen From a Crowded Museum in Oslo,” *The New York Times*, 23 Aug. 2004, Available: <http://www.nytimes.com/2004/08/23/world/munch-s-scream-is-stolen-from-a-crowded-museum-in-oslo.html> [31 Oct. 2012].
- ³⁹ Gibbs, W., “3 Convicted, 3 Acquitted in Theft of Munch's Art,” *The New York Times*, 3 May 2006, Available: <http://www.nytimes.com/2006/05/03/arts/design/03scre.html> [31 Oct. 2012].
- ⁴⁰ “Scream stolen from Norway museum,” *BBC News*, 22 Aug. 2004, Available: <http://news.bbc.co.uk/2/hi/europe/3588282.stm> [1 Nov. 2012].
- ⁴¹ Ali, M., *Britain’s Biggest Heists: The Brink’s Mat Robbery*, Crime and Investigation Network, 2009.
- ⁴² “Brinks Mat gold: The unsolved mystery,” *BBC News*, 15 April 2000, Available: http://news.bbc.co.uk/2/hi/uk_news/714289.stm [18 May 2013].
- ⁴³ Naughton, T., “Kennedy Airport Caper,” *Daring Capers*, New Dominion Pictures, 2009, DVD Disc 1.
- ⁴⁴ May, A., “The Lufthansa Heist Revisited,” *Crime Library: Criminal Minds and Methods*, Available: http://www.trutv.com/library/crime/gangsters_outlaws/gang/heist/1.html [14 Jan. 2013].
- ⁴⁵ Pileggi, N., *Wise Guy*, Pocket Books, New York, 1985.

- ⁴⁶ Lewis, D., "Soldiers of Fortune," *Daily Mail*, 2 June 2007, Available: <http://www.dailymail.co.uk/home/moslive/article-459185/Soldiers-Fortune.html> [14 Jan. 2013].
- ⁴⁷ Kluge, P.F. and Moore, T., "The Boys in the Bank," *Life*, Vol. 73, No. 12, 22 Sept. 1972, pp. 66-74.
- ⁴⁸ "Graff jewel raid: Police make two arrests," *The Telegraph*, 19 Aug. 2009, Available: <http://www.telegraph.co.uk/news/uknews/law-and-order/6058277/Graff-jewel-raid-Police-make-two-arrests.html> [14 Jan. 2013].
- ⁴⁹ Edwards, R., "Graff jewel heist: robbers found guilty of £40m raid," *The Telegraph*, 6 July 2010, Available: <http://www.telegraph.co.uk/news/uknews/crime/7874965/Graff-jewel-heist-robbers-found-guilty-of-40m-raid.html> [14 Jan. 2013].
- ⁵⁰ Edwards, R., "Graff jewel heist: police recover loaded gun," *The Telegraph*, 13 Aug. 2009, Available: <http://www.telegraph.co.uk/news/uknews/law-and-order/6023817/Police-investigating-the-40m-jewel-heist-from-Graff-in-Londons-Mayfair-have-recovered-a-loaded-gun-connected-to-the-robbery..html> [14 Jan. 2013].
- ⁵¹ Edwards, R., "Graff jewel heist: 'Stig' robber escaped with £40m haul," *The Telegraph*, 6 July 2010, Available: <http://www.telegraph.co.uk/news/uknews/crime/7875649/Graff-jewel-heist-Stig-robber-escaped-with-40m-haul.html> [14 Jan. 2013].
- ⁵² "Graff jewel heist: third man arrested," *The Telegraph*, 20 Aug. 2009, Available: <http://www.telegraph.co.uk/news/uknews/law-and-order/6062617/Graff-jewel-heist-third-man-arrested.html> [14 Jan. 2013].
- ⁵³ "Fifth man guilty of Graff robbery," Metropolitan Police, 4 March 2011, Available: <http://content.met.police.uk/News/Fifth-man-guilty-of-Graff-robbery/1260268631105/1257246745756> [14 Jan. 2013].
- ⁵⁴ "Graff guard 'feared for his life' in London robbery," BBC News, 19 April 2010, Available: http://news.bbc.co.uk/2/hi/uk_news/england/london/8652119.stm [16 Jan. 2014].
- ⁵⁵ Carvajal, D., "The Heist at Harry's," *The New York Times*, 12 Dec. 2008, Available: http://www.nytimes.com/2008/12/14/fashion/14heist.html?_r=2& [14 Jan. 2013].
- ⁵⁶ Schpoliansky, C., "Daring Diamond Heist in Downtown Paris," ABC News, 5 Dec. 2008, Available: <http://abcnews.go.com/International/story?id=6400551&page=1> [14 Jan. 2013].
- ⁵⁷ Cowan, R. and Bowcott, O., "Up to £52m in gems stolen in airport raid," *The Guardian*, 25 Feb. 2005, Available: <http://www.guardian.co.uk/world/2005/feb/26/ukcrime.uk> [14 Jan. 2013].
- ⁵⁸ "KLM errors 'led to diamond heist'," Expatica News, 2 March 2005, Available: http://www.expatica.com/nl/news/local_news/klm-errors-led-to-diamond-heist-17534.html [14 Jan. 2013].
- ⁵⁹ "Police suspect diamond gang 'had inside help'," Expatica News, 28 Feb. 2005, Available: http://www.expatica.com/nl/news/local_news/police-suspect-diamond-gang-had-inside-help-17437.html?ppager=1 [14 Jan. 2013].
- ⁶⁰ "Dutch seek clues to jewel heist," BBC News, 26 Feb. 2005, Available: <http://news.bbc.co.uk/2/hi/europe/4300741.stm> [14 Jan. 2013].
- ⁶¹ Wright, G., "Police foil £40m Heathrow robbery," *The Guardian*, 17 May 2004, Available: <http://www.guardian.co.uk/uk/2004/may/17/ukcrime.georgewright> [14 Jan. 2013].
- ⁶² "Flying Squad foils £80m robbery," BBC News, 18 May 2004, Available: http://news.bbc.co.uk/2/hi/uk_news/3723839.stm [14 Jan. 2013].
- ⁶³ Cowan, R., "Police foil £80m Heathrow heist," *The Guardian*, 17 May 2004, Available: <http://www.guardian.co.uk/uk/2004/may/18/ukcrime.rosiecowan> [14 Jan. 2013].
- ⁶⁴ Young, K., *Crimewatch Solved*, BBC One, 6 Jan. 2009.
- ⁶⁵ Boser, U., *The Gardner Heist*, HarperCollins, New York, 2009.
- ⁶⁶ Naughton, T., "Art Attack," *Daring Capers*, New Dominion Pictures, 2009, DVD Disc 1.
- ⁶⁷ Kurkjian, S., "Secrets behind the largest art theft in history," *The Boston Globe*, 13 March 2005, Available: http://www.boston.com/news/specials/gardner_heist/heist/ [14 Jan. 2013].

- ⁶⁸ Boser, U., "Revisiting the Gardner Heist," Boston Common Magazine, Available: <http://bostoncommon-magazine.com/culture/articles/connecting-clues-in-the-gardner-museum-heist?page=1> [14 Jan. 2013].
- ⁶⁹ Ashbrook, T., "The Gardner Heist and Stolen Art," On Point with Tom Ashbrook, 24 Feb. 2010, Available: <http://onpoint.wbur.org/2010/02/24/stolen-art> [14 Jan. 2013].
- ⁷⁰ Quijano, E., "Possible new lead in largest art heist ever," CBS This Morning, 11 May 2012, Available: http://www.cbsnews.com/8301-505263_162-57432400/possible-new-lead-in-largest-art-heist-ever/ [14 Jan. 2013].
- ⁷¹ Naughton, T., "The Knightsbridge Heist," *Daring Capers*, New Dominion Pictures, 2009, DVD Disc 3.
- ⁷² *Great Bank Robberies*, Crime and Investigation Network.
- ⁷³ Sounes, H., *Heist: The True Story of the World's Biggest Cash Robbery*, Simon & Schuster, London, 2009.
- ⁷⁴ Austin, M., "Britain's Biggest Heist," *Real Crime*, ITV Studios, 2010.
- ⁷⁵ "Securitas robbery: how it happened," BBC News, 27 Feb. 2006, Available: http://news.bbc.co.uk/2/hi/uk_news/england/kent/4754786.stm [14 Jan. 2013].
- ⁷⁶ "Securitas robbery: the investigation," BBC News, 6 March 2006, Available: http://news.bbc.co.uk/2/hi/uk_news/england/kent/4742972.stm [14 Jan. 2013].
- ⁷⁷ Campbell, D., "Caught on video: UK's biggest cash robbery," The Guardian, 1 Aug. 2007, Available: <http://www.guardian.co.uk/uk/2007/aug/02/ukcrime.topstories3> [14 Jan. 2013].
- ⁷⁸ "Profile: Ermir Hysenaj," BBC News, 28 Jan. 2008, Available: http://news.bbc.co.uk/2/hi/uk_news/6945994.stm [14 Jan. 2013].
- ⁷⁹ Summers, C., "What happened to the Securitas cash?" BBC News, 28 Jan. 2008, Available: http://news.bbc.co.uk/2/hi/uk_news/6245404.stm [14 Jan. 2013].
- ⁸⁰ Summers, C., "The role of the 'inside man'," BBC News, 28 Jan. 2008, Available: http://news.bbc.co.uk/2/hi/uk_news/7154191.stm [14 Jan. 2013].
- ⁸¹ "Cage-fighter jailed over £53m Kent Securitas raid," BBC News, 1 June 2010, Available: <http://www.bbc.co.uk/news/10209285> [14 Jan. 2013].
- ⁸² "Northern Bank Robbery," Crime File, Crime and Investigation Network, Available: <http://www.crimeandinvestigation.co.uk/crime-files/northern-bank-robbery/crime.html> [14 Jan. 2013].
- ⁸³ McDonald, H., "Employee cleared of £26.5m Northern Bank robbery," The Guardian, 9 Oct. 2008, Available: <http://www.guardian.co.uk/uk/2008/oct/09/northern.bank.robbery1> [14 Jan. 2013].
- ⁸⁴ "Timeline: Northern Bank robbery," BBC News, 7 Jan. 2005, Available: http://news.bbc.co.uk/2/hi/uk_news/northern_ireland/4117219.stm [14 Jan. 2013].
- ⁸⁵ Bell, R., "Belfast's Northern Bank Robbery," Crime Library: Criminal Minds and Methods, Available: http://www.trutv.com/library/crime/gangsters_outlaws/outlaws/major_heists/index.html [14 Jan. 2013].
- ⁸⁶ Dodge, R.W. and Lentzner, H.R., "Crime and Seasonality," U.S. Department of Justice Bureau of Justice Statistics, National Crime Survey Report SD-NCS-N-15, NCJ-64818, May 1980.
- ⁸⁷ Hagan, F.E., *Crime Types and Criminals*, SAGE, Los Angeles, 2010, ch. 3.
- ⁸⁸ Fox, V., *Introduction to Criminology*, 2nd ed., Prentice-Hall, 1985, ch. 16.
- ⁸⁹ Quetelet, M.A., *A Treatise on Man and the Development of his Faculties*, William and Robert Chambers, Edinburgh, 1842.
- ⁹⁰ "Age-Specific Arrest Rates and Race-Specific Arrest Rates for Selected Offenses 1993-2001," Uniform Crime Reports, U.S. Department of Justice Federal Bureau of Investigation, Nov. 2003.
- ⁹¹ Naughton, T., "Plunder Under Nice," *Daring Capers*, New Dominion Pictures, 2009, DVD Disc 1.

6. APPENDIX: COMPILED HEIST DETAILS

Most of the heists captured in this study's database are so well known and rich in captivating detail that full-length books, documentaries, and even motion pictures have been produced to convey their stories. The summaries in Section 2.2 are, therefore, highly abbreviated. However, throughout this paper these summaries have been supplemented through the mention of specific details as these details have become relevant in the discussion of a given focus area. The intent of this appendix is to list all of these details in one place for each heist.

This appendix is divided into 23 sections, one for each heist. Each section begins with a summary of the heist based on Section 2.2. Following the summary is a list of statements made about the specific heist throughout the rest of the report.

6.1. Nonviolent Heists

6.1.1. Brazil Central Bank Cash Heist



6.1.1.1. Synopsis

Over a period of three months, more than a dozen men posing as employees of a synthetic grass company (see Fig. 3) dug a 656-foot-long tunnel 13 feet under Fortaleza, Brazil, in order to access the vault of the local branch of the Brazil Central Bank. On Saturday, August 6, 2005, the thieves transferred over 7,700 lbs. of cash worth \$81.9 million (FY12 equivalent) out of the bank through their elaborate electrically-lit, air-conditioned, and structurally reinforced tunnel.¹⁵⁻²⁰

6.1.1.2. Additional Details

- **From §3.1.2.2:** The size of the estimated 14-person thief force for the Brazil Central Bank Cash Heist was driven in part by the need for manpower in quickly passing the stolen cash through the 263-foot-long tunnel under the streets of Fortaleza.
- **From §3.2.1:** In the Brazil Central Bank Cash Heist, digging equipment was concealed inside a thief-possessed building.
- **From §3.5.1:** Within the 15 heists for which planning time data was available, most involved known planning times of less than 30 weeks (7 months). The mean among this group of shorter planning times was 13 weeks (3 months). A prime example of one of these heists is the Brazil Central Bank Cash Heist, which commenced digging from the rented Grama Sintética storefront some three months prior to the robbery itself.
- **From §3.5.3:** Examples of loot weighing more than 5,000 lbs. include loads of cash and/or gold from the Brazil Central Bank Cash Heist, Brink's-Mat Gold Heist, and Securitas Cash Depot Heist.
- **From §3.5.4.2:** Criminals with legitimate occupations other than manager or business owner were often brought in to the planning or execution of the heist for their specialized skills or because of the plan's simple need for unskilled labor (e.g., for tunnel digging in the example of the Brazil Central Bank Cash Heist).
- **From §3.5.5:** The Brazil Central Bank Cash Heist involved significant investment, which included renting a storefront, advance payment of about \$3,000 to members of the tunnel-digging crew, a \$100,000 bribe to a bank security guard, and the purchase of about 10 cars in which to hide portions of the loot. This reduced this heist's ratio of return (measured by the value of the

loot stolen or intended to be stolen) to investment (measured by the total thief expenditures), becoming the minimum return on investment ratio in the database at 110.

- **From §3.5.6:** One example of post-heist death is the kidnapping and murder of the alleged financier of the Brazil Central Bank Cash Heist, Luis Fernando Ribeiro. Ribeiro was kidnapped two months after the robbery and held for ransom. Though the ransom was paid, Ribeiro's bullet-ridden corpse was found in farm country several hundred miles from São Paulo two weeks later. Information was later uncovered to suggest that members of the state police had executed the kidnapping and murder for their own financial gain.²⁰
- **From §3.6:** Recruited insiders are uncommon in the heist database. There exist just three examples: the owner of the Knightsbridge Safe Deposit Center, an employee of the Brink's-Mat depot, and a security guard at Brazil's Central Bank in Fortaleza. In the case of the Brazil Central Bank security guard, he did not take an active role in the execution of the heist and is considered a passive insider in the database.

6.1.2. Sumitomo Mitsui Bank Heist

*Stealth
Raid*



6.1.2.1. Synopsis

On September 16, 2004, two computer hackers in collusion with the security chief of the Sumitomo Mitsui Bank in London installed keylogging software on fund transfer computer terminals. Just over two weeks later, on a weekend, the thieves returned to use this data to attempt \$478.5 million (FY12) in fraudulent transfers to twenty bank accounts in ten countries. To reduce the likelihood that the thieves could be identified, the security chief had dialed down the sensitivity of most of the bank's motion-sensor-triggered cameras. The thieves' plans were foiled only by their improper completion of an interbank communications form. Bank employees called the authorities after returning to work on a Monday and noticing the attempted transactions and severed network cables.²¹⁻²²

6.1.2.2. Additional Details

- **From §3.3.1.1:** For three heists, including the Sumitomo Mitsui Bank Heist, the time at which the heist began is unclear from the available open literature.
- **From §3.5.3:** Included in the category of targeted valuables weighing less than 5 lbs. are the electronic (and therefore weightless) funds of the attempted Sumitomo Mitsui Bank Heist.
- **From §3.5.5:** At the lower end of financial investment are heists like the Sumitomo Mitsui Bank Heist, which required little more than a thumb drive and the setup of a several bank accounts to which funds could be deposited. Within the database, the minimum return on investment ratio for a heist was 110. Return on investment ratios span several orders of magnitude above this. Consider, for example, the Sumitomo Mitsui Bank Heist, which would have had a cost in the tens of dollars but netted over \$400 million.
- **From §3.6:** Opportunistic insiders are uncommon in the HMCD; one example is the security supervisor at the Sumitomo Mitsui Bank.
- **From §3.7.2:** In the Sumitomo Mitsui Bank Heist, an improperly completed interbank communications form stood in the way of the \$480 million fund transfer. Bank employees called the authorities after returning to work on a Monday and noticing the attempted transactions and severed network cables.

6.1.3. Antwerp Diamond Heist



6.1.3.1. Synopsis

On the morning of Monday, February 17, 2003, concierge Jorge Dias De Souza descended two levels beneath Antwerp's Diamond Center. Expecting to open the center's vault for a normal day of business for its wealthy diamantaire customers, he was astonished to discover the lights on, the vault door open, and 109 of the center's 189 safe deposit boxes wide open, with millions of dollars' worth of discarded contents littering the floor (see Fig. 4). What was not on the floor was what the thieves *could* carry with them: between \$108 million and \$432 million worth of diamonds, gold, cash, and other valuables. The theft was later dubbed the heist of the century.¹

Located within the Secure Antwerp Diamond Area, the Diamond Center had been thought to be among the most fortified businesses in the world. Entry into the center's vault required a controlled access card to enter the building, a two-story descent underground to a guard-controlled gate, and both a key and one of 100 million possible combinations to open the foot-thick steel vault door. If a person somehow entered the vault unauthorized, he would be detected by a broken magnetic seal on the vault door as well as a microwave Doppler motion detector, infrared energy detector, and light detector within the vault itself. If he tried to tunnel his way in, he would be detected by seismic sensors. With a police station not more than 200 feet from the Diamond Center's front entrance – and a police kiosk even closer – any detected thief would be captured in minutes. Since all the detectors were silent alarms, the thief wouldn't know he had been detected until he was surrounded by security forces. Remarkably, the Antwerp thieves discovered how to defeat *all* of these measures.¹

The mastermind of the heist was Leonardo Notarbartolo, a career criminal posing as a diamond merchant who planted himself as a tenant at the Diamond Center more than two years in advance of the robbery in order to conduct reconnaissance and discover security vulnerabilities.

6.1.3.2. Additional Details

- **From §3.1.1.1:** In the Antwerp Diamond Heist, thieves defeated keyed locks protecting entry into the Diamond Center from the garage, into a storage room in which the vault key was stored, into the vault door itself, and to individual safe deposit boxes. In defeating each of these keyed locks, the criminals demonstrated a variety of lock defeat techniques: The garage-to-Diamond-Center access was accomplished through use of a custom-made key rake; the storage room lock was defeated via use of a crowbar (the backup plan after a fabricated key failed to work); the key component of the vault door was defeated by use of the key stolen from the storage room; and the individual safe deposit boxes were opened by exploiting a design weakness that allowed a specially designed tool to interface with their keyholes and force their doors open.
- **From §3.1.1.2:** Some security measure defeat methods are uses of brute force while others are highly creative and innovative (e.g., creating a custom tool to hold together the magnetic contacts of the vault door while they were separated from the door in the Antwerp Diamond Heist).
- **From §3.1.1.3:** Topping the list of security measure types defeated in each heist is the Antwerp Diamond Heist with eight defeated security measure types, solely in categories of access controls and detectors. In this well-documented case, more than two years of thief planning, surveillance, and investigation into the targeted facility's vulnerabilities enabled the defeat of a great many security measure types.
- **From §3.1.2.1:** The HMCD contains 11 heists (48% of the database) in which armed thieves attacked security personnel, almost all of whom were unarmed. In contrast, only in two cases (the Antwerp Diamond Heist and Gardner Museum Art Heist) did thieves enter unarmed into a facility with security personnel present. In both of these cases, planning is estimated to have

initiated 24-30 months prior to the heist (far above the mean planning duration of 9 months and median of 4 months).

- **From §3.1.2.1:** In the Antwerp Diamond Heist, Diamond Center staff had largely grown complacent.¹ For instance, the concierges responsible for securing the vault each night did not use a security feature built into the vault door's key: The key was designed to be separated into two parts (the pipe and stamp) to be stored separately from each other, but instead the concierges stored both pieces together in a lockbox near the vault.
- **From §3.1.2.2:** Heists in this study were frequently committed not only under the noses of security guards, but also under the noses of nearby external police forces. In three cases (the Antwerp Diamond Heist, the Tanzanian Airplane Gold Robbery, and Harry Winston Diamond Heist), police forces were stationed within 500 feet of the heist.
- **From §3.1.2.2:** While guards themselves may not deter a determined thief, they do add to the amount of time the thief requires to prepare and plan for his heist. The Antwerp Diamond Heist and Securitas Cash Depot Heist serve as two examples illustrating the months or years of planning that thieves may require to learn the details of security practices and procedures at the target facility.
- **From §3.2.1:** In some cases, operations equipment was concealed inside a thief-possessed building or among the tools that a thief posing as a technician brought to the facility he intended to rob (as in the specialized tool used to maintain the connection between the two tamper-sensing magnets in the Antwerp Diamond Heist).
- **From §3.3.1.1:** The "Night Raids" timing archetype is characterized not only by heists that begin very late in the day, but also by heists that run the course of several hours. The stealthy Société Générale Bank Heist and Antwerp Diamond Heist fall in this category, with both involving undetected vault entries on a Saturday and theft activity not being discovered until staff returned to work the following Monday.
- **From §3.3.2:** Thieves frequently choose to commit large heists at times of low bystander activity. All else being equal, this would drive thieves to frequently choose times outside of core business hours. Examples include the late-night Valentine's Day weekend theft at the Antwerp Diamond Center and the yet-unsolved 4:00 AM theft from the Museon science museum.
- **From §3.3.2:** As an example of a heist in which knowledge of personnel location vs. time contributed to timing decisions, in the case of the Antwerp Diamond Heist, the thieves aimed to penetrate the vault two stories below ground in the B block of the Antwerp Diamond Center. They likely knew that the concierge on duty over the chosen weekend of the robbery stayed in an apartment on the fourth floor of the neighboring C block, rather than the alternative concierge, who stayed on the second floor of the B block.
- **From §3.3.3:** The Antwerp, Société Générale, and Knightsbridge heists were all thefts from safe deposit boxes and required the thieves, at a minimum, to sort through a hodgepodge of items found upon opening the deposit boxes. All three targets were difficult to penetrate, and the heists averaged about 1.5 years of planning apiece; however, they were also some of the highest-yield heists in the database, averaging a take of \$170 million (FY12) apiece.
- **From §3.3.3:** In most heists in the database, thieves were highly selective in what they removed from the target facility. In a number of cases, including the Antwerp Diamond Heist, Northern Bank Cash Heist, and Securitas Cash Depot Heist, this selectivity was influenced by limitations in transportation capacity.

- **From §3.5.1:** Four heists in the database involved planning times of more than 100 weeks. Included among them is the Antwerp Diamond Heist, with the longest estimated planning time of 2.4 years; it was in the autumn of 2000 that Leonardo Notarbartolo, the mastermind of the Antwerp Diamond Heist, began renting an office in the Antwerp Diamond Center in preparation for the eventual February 2003 heist.
- **From §3.5.2:** In the planning of the Antwerp Diamond Heist, reconnaissance from the Antwerp Diamond Center revealed the brand of locks used for the doors, vault, and safe deposit boxes of the center. Since the heist planning team included a locksmith company owner, locks of the same brand could be ordered without raising suspicion, and vulnerabilities could be identified through experimentation.
- **From §3.5.4.2:** In only 10% of heists (specifically, the Antwerp Diamond Heist and British Bank of the Middle East Gold Heist) were the criminal teams thought to consist entirely of citizens from foreign nations.
- **From §3.5.4.2:** Career criminals frequently mask their true careers under an innocuous façade. For example, some of the more famous masterminds behind the heists in the database were business owners (e.g., Notarbartolo, the Antwerp mastermind, owned his own jewelry design business).
- **From §3.5.6:** The prison sentences of unarmed thieves tend not to be particularly long. In the case of the Antwerp Diamond Heist, those convicted were sentenced to 5-10 years in prison.
- **From §3.6:** Coverage of unwitting insiders is sparse in the available literature, and it is likely that the number of unwitting insiders involved in the heists of the HMCD is underestimated. However, prominent examples include the building manager who provided blueprints to the Antwerp Diamond Heist mastermind.
- **From §3.7.1:** In the case of the Antwerp Diamond Heist, the targeted Diamond Center was not insured. In fact, the building managers would not consent to an insurance evaluation, possibly because they were aware of several clear security vulnerabilities.¹ For example, motion detectors were not anti-masking, CCTV recordings were stored via on-site videotapes, one side of the facility was accessible from outside the Secure Antwerp Diamond Area (SADA), and the garage door facing the street outside of the SADA was controlled by an old single-code door opener whose code could be identified with a frequency scanner. Moreover, the center did not perform background or reference checks on tenants. These vulnerabilities piqued the interest of the criminal Ferdinando Finotto when he was in Antwerp to perpetrate another crime years earlier, and the information was passed on to the eventual Antwerp mastermind, Leonardo Notarbartolo.

6.1.4. Museon Jewel Heist



6.1.4.1. Synopsis

At 4:00 AM on December 2, 2002, thieves gained entry to a popular Dutch science museum, the Museon, which was hosting a diamond exhibit. The thieves circumvented 24-hour camera surveillance, motion detection, infrared sensors, and security guards to steal approximately \$15.4 million (FY12) worth of diamonds and other jewelry from six of the 28 exhibit reinforced-glass display cabinets. Outside of the missing jewelry, the only evidence of a break-in the thieves left behind was the smashed window through which they entered.²⁴⁻²⁵

6.1.4.2. Additional Details

- **From §3.1.1.3:** One particularly significant heist from a security measure defeat standpoint is the unsolved Gardner Museum Art Heist, where access controls, detectors, and security guards were attacked.
- **From §3.1.2:** One technique thieves use toward rendering guard security ineffective is simply to avoid being detected by guards (as in the Museon heist).
- **From §3.2.2:** At the bottom of the list with zero known deceptions are the Tanzanian Airplane Gold Robbery and the Museon Jewel Heist. The Museon Jewel Heist remains unsolved and was accomplished so stealthily that the manner in which it was perpetrated remains a mystery; while deceptions are likely to exist for this robbery, so few specifics are known that they cannot be identified.
- **From §3.3.1.2:** All but one of the five stealth raids in the HMCD were initiated on a Saturday. The exception of the Museon Jewel Heist was executed on a Monday, a day of the week on which the museum was normally closed.
- **From §3.3.2:** Thieves frequently choose to commit large heists at times of low bystander activity. All else being equal, this would drive thieves to frequently choose times outside of core business hours. Examples include the late-night Valentine’s Day weekend theft at the Antwerp Diamond Center and the yet-unsolved 4:00 AM theft from the Museon science museum.
- **From §3.5.3:** In the category of stolen good weights of less than 5 lbs. are the targeted diamonds from the Millennium Dome and gems from the Museon science museum.

6.1.5. Société Générale Bank Heist



6.1.5.1. Synopsis

In the afternoon of Saturday, July 17, 1976, several men under the leadership of Albert Spaggiari, a French army paratrooper-turned-criminal, finished a two-month job of tunneling 60 feet from the city sewers into the underground vault of the Société Générale Bank in Nice, France (see Fig. 5). In a heist lasting 36 uninterrupted hours, the criminals stole \$40.4 million (FY12) in contents from 400 of the 4,000 safe deposit boxes within the bank’s vault, as well as from the bank’s own supply of cash and gold. The heist was not discovered until it was time to open the vault on Monday morning, when bank officials realized the door had been welded shut from the inside. Confirming it as the epitome of a stealth raid, Spaggiari even inscribed on the wall of the vault the words *sans armes, ni haine, ni violence, or without weapons, nor hatred, nor violence.*^{7,26}

6.1.5.2. Additional Details

- **From §3.3.1.1:** The “Night Raids” timing archetype is characterized not only by heists that begin very late in the day, but also by heists that run the course of several hours. The stealthy Société Générale Bank Heist and Antwerp Diamond Heist fall in this category, with both involving undetected vault entries on a Saturday and theft activity not being discovered until staff returned to work the following Monday.
- **From §3.3.3:** The Antwerp, Société Générale, and Knightsbridge heists were all thefts from safe deposit boxes and required the thieves, at a minimum, to sort through a hodgepodge of items found upon opening the deposit boxes. All three targets were difficult to penetrate, and the heists averaged about 1.5 years of planning apiece; however, they were also some of the highest-yield heists in the database, averaging a take of \$170 million (FY12) apiece.

- **From §3.3.3:** In most heists in the database, thieves were highly selective in what they removed from the target facility. For example, the Société Générale thieves brought with them an appraiser for real-time advice on the most valuable items to take. (In addition to the appraiser, the criminals brought wine, cheese, soup, sausage, and pâté⁹¹ to celebrate and sustain themselves during the 36-hour-long heist. While plundering the vault’s safe deposit boxes, the thieves had further reason to celebrate when a late-night casino cash drop from a local casino, worth hundreds of thousands of dollars, came barreling down into the vault.^{26,91})
- **From §3.4:** An unarmed adversary is not an unimportant adversary. Indeed, the unarmed adversary may be the most important adversary, if measured by the monetary value of the theft. Albert Spaggiari, the mastermind of the Société Générale Bank Heist, summarized the philosophy of such criminals well when he famously wrote on the wall of the vault that he robbed, “Sans arme, ni haine, ni violence,” or “Without weapons, nor hatred, nor violence.”
- **From §3.5.1:** Four heists in the database involved planning times of more than 100 weeks. In one example, two years prior to the Société Générale Bank Heist, Albert Spaggiari rented a bank safe deposit box shortly after he heard from a neighbor and bank manager that the bank’s vault was not alarmed.
- **From §3.5.4.2:** Career criminals frequently mask their true careers under an innocuous façade. For example, some of the more famous masterminds behind the heists in the database were business owners (e.g., Spaggiari, the Société Générale mastermind, was a camera store owner).
- **From §3.7.2:** During the Société Générale Bank Heist, the thieves saw both pleasant and unpleasant surprises. Pleasantly, in the middle of the night, a local casino dropped a cash deposit into the night deposit box and, in effect, into the thieves’ waiting arms. Less pleasantly, a storm arrived during the heist and threatened to flood the thieves’ sewer exit route, prompting a premature end to the thieves’ time in the vault. No doubt after finishing the last of the celebratory feast of wine, cheese, soup, sausage, and pâté they had brought to the robbery, the thieves fled with \$40.4 million (FY12) in hand.⁹¹

6.1.6. Stardust Casino Job



6.1.6.1. Synopsis

On September 22, 1992, casino cashier William Brennan took his lunch break at the Stardust Resort and Casino in Las Vegas. As he exited, passing security guards, he was carrying a backpack of cash and chips worth \$800,000 (FY12). Brennan abandoned his Las Vegas apartment after picking up his cat and has not been seen since.^{4,28}

6.1.6.2. Additional Details

- **From §3.3.3:** Outliers in terms of their targeted facility’s ease of penetration and targeted valuables’ ease of fencing include the Stardust Casino Job and Chase Manhattan Bank Robbery, though these were both smaller-scale robberies on the order of \$1 million (FY12).
- **From §3.5.4.1:** Solo heists are exceedingly rare; the only heist in the database that fits this criterion is the Stardust Casino Job.
- **From §3.5.5:** The Stardust Casino Job required little financial investment other than, perhaps, the purchase of a backpack with which to carry the stolen money out of the casino.
- **From §3.6.5:** Opportunistic insiders are uncommon in the HMCD; one example is the lone thief in the Stardust Casino Job.

6.2. Violent Heists

6.2.1. Vastberga Helicopter Heist



6.2.1.1. Synopsis

At 5:15 AM on September 23, 2009, four thieves landed a stolen Bell 206 JetRanger helicopter on the roof of the G4S Cash Depot in Vastberga, Sweden (see Fig. 6). Breaking into the depot through a large pyramid-shaped skylight, the thieves descended via custom-length ladders to the depot's counting room. Breaking through the door using custom-fit explosives, the thieves opened the depot's cash cages with the assistance of a circulating saw. Twenty minutes after they landed, the thieves ascended to the roof and took off with \$6.1 million (FY12) in cash. Thanks to a tip-off from the Serbian foreign ministry, Swedish police had been expecting a helicopter assault on a large cash depot in September, but they were not expecting that the thieves would actively hinder a police response by spreading caltrops across roads near the depot and placing packages resembling bombs outside the police heliport.²⁹⁻³²

6.2.1.2. Additional Details

- **From §3.1.2.2:** In the interesting case of the Vastberga Helicopter Heist, police responded quickly but were deterred from entering the G4S depot by the forethought the thieves demonstrated by placing caltrops on the road near the depot and apparent bombs at the police helicopter hangar. These measures left the police uncertain of what other deterrents or traps could be awaiting them if they continued their approach. This heist illustrates that the effectiveness of security forces can be substantially weakened in the presence of an uncertain but credible threat.
- **From §3.4:** Bladed weapons were rarely used in the HMCD heists. One of the only two examples involved knives to slice through the canvas wall of a commercial helicopter hangar in the Vastberga Helicopter Heist.
- **From §3.5.3:** Included in the category of stolen goods weighing 50-500 lbs. is the cash of the Vastberga Helicopter Heist.
- **From §3.7.1:** In a few heists, the thieves utilized attack modes that were almost certainly beyond the imagination of the security system designers. The Vastberga Helicopter Heist is perhaps the most obvious such attack. Rather than enter the G4S depot from the ground level, or even by an ascent to the top of the building to break in via the pyramid skylight, the thieves recruited a helicopter pilot to land them on the roof. It can hardly be imagined that helicopters were included on the list of potential threats against which the depot's security was designed to protect. Still, even if they had, a local police force was equipped with a helicopter and could pursue if necessary. However, the thieves were able to preclude the use of this option by placing packages with the appearance of bombs outside the police heliport.

6.2.2. Millennium Dome Raid



6.2.2.1. Synopsis

At 9:30 AM on a Tuesday in November 2000, four men on a backhoe (see Fig. 7) smashed into London's Millennium Dome, a 365-meter diameter structure housing a year-long exhibit celebrating the beginning of the third millennium. With dome visitors distracted by smoke bombs, two men in gas masks and body armor then leapt out of the backhoe and within 27 seconds used a nail gun and sledgehammer to smash through the allegedly impregnable glass intended to protect the 203-carat Millennium Star diamond. Fortunately, all twelve diamonds in the exhibit had been replaced with crystal replicas the previous day,

thanks to police efforts anticipating the attack. All the backhoe-riding thieves, as well as a lookout in a van and getaway speedboat pilot, were arrested on the scene before making off with any of the intended \$666.1 million (FY12) loot.³³⁻³⁵

6.2.2.2. Additional Details

- **From §3.1.1.2:** Some security measure defeat methods are uses of brute force (e.g., ramming through fences and walls with a backhoe, as in the Millennium Dome Raid), while others are highly creative and innovative.
- **From §3.2.1:** Some 70% of the heists in the database occurred in urban areas, and almost any commercially available sedan or van blends with urban surroundings. However, to illustrate a less typical of a vehicle blending with surroundings, in the Millennium Dome Raid the thieves used a backhoe, which did not appear out of the ordinary around the large and recently-completed Millennium Dome.
- **From §3.3.1.1:** The “Broad Daylight Heists” timing archetype is characterized by heists early in the work day that are conducted rapidly, on timescales well under one hour. These timescales are largely a necessity for such heists, and all four in this category (the Swissport Heathrow Heist, Millennium Dome Raid, Schiphol Airport Diamond Heist, and Munch Museum Art Heist) involved use of violence to subdue guards, employees, and bystanders to permit rapid access to the target valuables.
- **From §3.3.2:** In the case of the Millennium Dome Raid, the thieves planned to escape via boat. However, this necessitated timing the heist to coincide properly with ocean tides so that the boat could pull up to receive the fleeing criminals.
- **From §3.3.3:** Only in 22% of heists in the database (specifically, the Millennium Dome Raid, British Bank of the Middle East Heist, Chase Manhattan Bank Robbery, Harry Winston Diamond Heist, and Schiphol Airport Diamond Heist) did thieves steal or intend to steal more than 50% of the valuables at a target.
- **From §3.3.3:** The availability of numerous and specialized security forces in a city can be a detriment for a thief that is not well-disguised (as the criminals in both the Millennium Dome Raid and Swissport Heathrow Heist learned, when confronted with a 100-officer Metropolitan Police operation designed to foil their heist).
- **From §3.4:** The only heist on the top-four highest-valued heists list that employed weapons was the Millennium Dome Raid, which used smoke bombs. However, these bombs were primarily intended to distract and confuse bystanders and security forces, rather than cause bodily harm.
- **From §3.5.3:** Included in the category of targeted valuables weighing less than 5 lbs. are the targeted diamonds from the Millennium Dome.
- **From §3.7.2:** In both the Millennium Dome Raid and Swissport Heathrow Heist, intelligence gathered by the Metropolitan Police well in advance resulted in 100-officer operations to foil the robberies, with police forces lying in wait on the days of the heists.

6.2.3. Tanzanian Airplane Gold Robbery

*Subdue
& Seize*



6.2.3.1. Synopsis

On January 5, 2012, the regularly-scheduled Thursday gold transport airplane was parked at its airstrip near an AngloGold Ashanti mine in Geita, Tanzania. Loaded with \$30.5 million in gold bars weighing nearly 1,300 lbs., the plane came under attack from five men who emerged from the nearby jungle armed with submachine guns, pistols, and hand grenades. Thanks to mine security and police forces, the attack was thwarted. One thief was killed in the firefight.³⁶⁻³⁷

6.2.3.2. Additional Details

- **From §3.1.2.2:** Heists in this study were frequently committed not only under the noses of security guards, but also under the noses of nearby external police forces. In three cases (the Antwerp Diamond Heist, the Tanzanian Airplane Gold Robbery, and Harry Winston Diamond Heist), police forces were stationed within 500 feet of the heist.
- **From §3.2.2:** At the bottom of the list with zero known deceptions are the Tanzanian Airplane Gold Robbery and the Museon Jewel Heist. In the case of the Tanzanian heist, the prospective thieves launched an attack on a gold transport airplane with no clear deception tactics; however, information available in public sources regarding this heist attempt is quite limited and may not capture the entirety of the thieves' activities preceding and during the heist.
- **From §3.3.1.1:** For three heists, including the Tanzanian Airplane Gold Robbery, the time at which the heist began is unclear from the available open literature.
- **From §3.3.2:** Outsider observations aimed at discovering times of high target value can be effective. The Tanzanian Airplane Gold Robbery, for example, was perpetrated against a weekly shipment from the AngloGold Ashanti gold mine.
- **From §3.5.6:** Compared to the case of unarmed thieves, an armed attack poses a more substantial risk of death to participants, which occurred in the cases of two armed thieves in the Chase Manhattan Bank Robbery and Tanzanian Airplane Gold Robbery.
- **From §3.7.2:** The Tanzanian Airplane Gold Robbery was thwarted thanks to strong mine security and police forces. One thief was killed and one security guard injured in the firefight.

6.2.4. Munch Museum Art Heist

*Subdue
& Seize*



6.2.4.1. Synopsis

At 11:10 AM on Sunday, August 22, 2004, two armed and masked men entered the Munch Museum in Oslo, Norway. With about 80 visitors in the museum at the time, one thief held visitors and unarmed security guards in the museum's café, while another thief entered a gallery to rip two of Edvard Munch's famous paintings, known as "The Scream" and "Madonna", from the walls. Despite silent alarms on the paintings that alerted police, which had a patrol in the neighborhood, the thieves escaped in minutes (see Fig. 8) and no arrests were made until four months later.³⁸⁻⁴⁰

6.2.4.2. Additional Details

- **From §3.1.2.2:** Only three of the 23 heists in the database (the Munch Museum Art Heist, Mayfair Graff Diamond Heist, and Schiphol Airport Diamond Heist) took less than 14 minutes.
- **From §3.3.1.1:** The "Broad Daylight Heists" timing archetype is characterized by heists early in the work day that are conducted rapidly, on timescales well under one hour. These timescales are

largely a necessity for such heists, and all four in this category (the Swissport Heathrow Heist, Millennium Dome Raid, Schiphol Airport Diamond Heist, and Munch Museum Art Heist) involved use of violence to subdue guards, employees, and bystanders to permit rapid access to the target valuables.

- **From §3.7.1:** In the Munch Museum Art Heist, armed thieves entered the museum and stole two pieces of art while holding guards and visitors at gunpoint. Such a heist was unexpected and was not well-protected against in the design of the museum's security; this was reportedly the very first armed art heist in Norway.

6.2.5. Carlton Hotel Diamond Heist

*Subdue
& Seize*



6.2.5.1. Synopsis

At closing time on a Thursday evening in August 1994, three masked men walked into the jewelry shop within the Carlton Hotel, in Cannes, France. Amidst machine gun fire to threaten employees and customers, the men swept about \$69 million (FY12) in jewels into bags and escaped, never to be seen again. Interestingly, investigations revealed no bullet holes in the jewelry shop; rather, the robbers had been firing blanks.^{1,25}

6.2.5.2. Additional Details

- **From §3.3.1.1:** Although clear estimates for the duration of the Carlton Hotel Diamond Heist could not be found, it is likely that this heist, which occurred at the hotel jewelry store's closing time, would also fit within Timing Archetype III.
- **From §3.4:** In the example of the Carlton Hotel Diamond Heist, thieves fired machine guns as they entered the hotel's jewelry store. However, upon investigation of the crime, police found that the thieves had been firing blanks.

6.2.6. Brink's-Mat Gold Heist

*Subdue
& Seize*



6.2.6.1. Synopsis

In November 1983, seven armed, masked men entered the Brink's-Mat depot near London's Heathrow Airport ten minutes after its 6:30 AM opening. The six employees present were subdued and bound, and the two employees with vault keys and combinations were called by name and coerced at gunpoint to open the vault doors. Although the thieves were successful at entering the outer vault door (see Fig. 9), the combination-holding employee was so distressed that he could not remember the recently-changed combinations to any of the inner vault doors. Luckily for the thieves, seventy-six boxes of gold bullion worth \$86 million (FY12) sat ready for shipment in the outer chamber of the vault. This gold was loaded into a van and disappeared. It was later revealed that a depot employee, one of the six present at the time of the robbery, provided critical inside information and assistance to the thieves.^{6,41}

6.2.6.2. Additional Details

- **From §3.1.1.1:** One notable camera defeat technique is for thieves to gain control of the camera monitoring station. This can be accomplished violently or nonviolently. As an example of the latter, it was an insider accomplice who was responsible for monitoring the CCTV camera images at the time of the Brink's-Mat Gold Heist.

- **From §3.1.1.2:** Threats on guards or on key- or combination-holding employees is a common defeat method among ten heists (43% of the database). For example, thieves in the Brink’s-Mat Gold Heist did not know the combinations to the inner or outer vault doors, but using inside information they learned which employees knew the combinations. Defeating measures the Brink’s-Mat warehouse took to ensure that no single employee had all the keys and combinations necessary to open the vault, the thieves identified the individuals who could collectively provide access, doused them with gasoline and threatened to light them on fire, and consequently gained access to some \$86 million (FY12) worth of gold bullion.
- **From §3.1.2.2:** Among heists in which active guard forces were present, 85% employed just one or two guards. The maximum of five guards corresponds to the Brink’s-Mat heist, in which all five employees in the depot were classified as guards.^{41,42}
- **From §3.3.1.1:** The “Early-Bird Heists” timing archetype is characterized by early-morning heists with durations of 1-2 hours. All three heists that fall within this category, the Gardner Museum Art Heist, Lufthansa Heist, and Brink’s-Mat Gold Heist, were characterized by violence. In all three cases, those guards and employees were subdued and unable to call for help. Since the crimes were perpetrated in the early morning when little, if any, business with outside organizations or people was conducted, there was little risk that individuals from the outside would visit the facility and discover the heist in progress.
- **From §3.4:** At the Brink’s-Mat depot near Heathrow Airport in 1983, the facility’s security measures included a system of dual control, in which the opening of vault doors required two individuals with separate keys and combinations. Thus, the cooperation of *both* individuals was required to gain entry to the vaults. During the Brink’s Mat Gold Heist, the two combination-holding employees were doused with gasoline, and thieves threatened to light them on fire if they did not comply. They complied (wouldn’t you?).
- **From §3.5.3:** Examples of loot weighing more than 5,000 lbs. include loads of cash and/or gold from the Brazil Central Bank Cash Heist, Brink’s-Mat Gold Heist, and Securitas Cash Depot Heist.
- **From §3.5.6:** An important risk consideration for prospective thieves is the post-heist risk of death. In three heists within this database, specifically the Brazil Central Bank Cash Heist, Lufthansa Heist, and Brink’s-Mat Gold Heist, heist-related killings occurred after the robbery itself.
- **From §3.6:** Recruited insiders are individuals who are part of an organization and, typically as a result of their existing access and influence, are asked to join a heist plot. Recruitment is a risky tactic for a thief to employ, and consequently, recruited insiders are uncommon in the HMCD. There exist just three examples: the owner of the Knightsbridge Safe Deposit Center, an employee of the Brink’s-Mat depot, and a security guard at Brazil’s Central Bank in Fortaleza.
- **From §3.7.2:** In the violent Brink’s-Mat Gold Heist, the employee responsible for holding the combinations to the inner vault doors was so distressed (after being drenched in gasoline) that he could not remember his recently-changed combinations. The inner vaults contained between \$3.4 million and \$10.3 million (FY12). Fortunately for the thieves, stored in the outer vault on that particular day was \$85.9 million (FY12) in gold bullion.

6.2.7. Lufthansa Heist

*Subdue
& Seize*



6.2.7.1. Synopsis

At 3:00 AM one December morning in 1978, seven armed, masked men arrived at the Lufthansa Overseas Cargo Terminal at New York's John F. Kennedy Airport. Operating in three teams, one man in an automobile waited in the cargo terminal's parking lot, four men entered the terminal, and the remaining two cut the lock on the security gate, swapped it with a fake replacement, and drove a van to the rear loading areas. Rounding up all ten employees on duty in the terminal, most of whom were on their lunch hour, the thieves forced the supervisor to turn off the facility's alarms. About 80 minutes after beginning the raid, the thieves left with \$28.2 million (FY12) in cash, gems, and gold. Planning of the heist was made possible by information from a Lufthansa cargo terminal supervisor who was deep in gambling debt to a bookie with organized crime connections.⁴³⁻⁴⁵

6.2.7.2. Additional Details

- **From §3.3.1.1:** The “Early-Bird Heists” timing archetype is characterized by early-morning heists with durations of 1-2 hours. All three heists that fall within this category, the Gardner Museum Art Heist, Lufthansa Heist, and Brink's-Mat Gold Heist, were characterized by violence. In all three cases, those guards and employees were subdued and unable to call for help. Since the crimes were perpetrated in the early morning when little, if any, business with outside organizations or people was conducted, there was little risk that individuals from the outside would visit the facility and discover the heist in progress.
- **From §3.3.2:** Thieves frequently choose to commit large heists at times of low employee or security activity because it minimizes the difficulty of defeating *anticipated* detection. This factor tends to drive thieves to choose times outside of core business hours for the targeted entity. One example is the 3:00 AM assault on the small graveyard shift at the Kennedy Airport Lufthansa Cargo Terminal.
- **From §3.3.2:** Thieves also frequently choose to commit large heists at times of high target value. Thieves' ability to execute timing in this way depends on the quality of information they can obtain on the movement of valuables in and out of the target facility. The highest quality information typically comes from insiders. For example, the Lufthansa Heist was expedited as soon as a Lufthansa cargo supervisor and insider informed a preassembled Mafia gang that an unusually large shipment of cash was being stored in the Lufthansa Cargo Terminal over the weekend.
- **From §3.5.6:** In three heists within the heist database, heist-related killings have occurred in the aftermath of the robbery itself. The most famous of these examples is the Lufthansa Heist: Following the heist, one thief neglected to fulfill his duty of bringing the van used during the heist to a junkyard to be compacted and destroyed. Instead, it had been parked in a no-parking zone and discovered by police two days after the robbery. Fingerprints found inside the van began leading police toward the thieves. To avoid being arrested and sent to prison for his involvement, the mob boss responsible who received most of the stolen cash from the heist began ordering the killing of those involved. Within one year of the heist, seven of the Lufthansa accomplices disappeared. Within another eight years, the entire crew that executed the heists had been either reported missing or found murdered.
- **From §3.6:** Insiders within this study have operated with varying degrees of inside access. Owners, managers (e.g., Louis Werner in the Lufthansa Heist), and employees fall into the clear category of being a “full” insider with a high degree of inside access.

- **From §3.6:** Opportunistic insiders are uncommon in the HMCD; one example is the cargo supervisor at the Lufthansa Overseas Cargo Terminal. However, since he did not take an active role in the execution of the heist, he is a passive opportunistic insider.

6.2.8. British Bank of the Middle East Gold Heist

*Subdue
& Seize*



6.2.8.1. Synopsis

On January 20, 1976, nine heavily armed soldiers dressed in unmarked military fatigues blasted their way with mortars and grenades into the British Bank of the Middle East in Beirut, Lebanon. Located in a no-man's land between the Muslim west and Christian east of Beirut during the Lebanese Civil War, the bank was operational only on an ad-hoc basis. Amid the chaos of the war, the force blasted into the bank's vault and stole an estimated \$204.6 million (FY12) in primarily gold bullion. The identities and affiliations of the perpetrators remains disputed, and little has been publicly documented despite the heist's fame (see Table 2). The most thorough account found⁴⁶ suggests the heist was perpetrated by a United Kingdom Special Forces unit whose mission was to disguise the seizure of important terrorist group financial documents stored in the bank as a genuine bank robbery.

6.2.8.2. Additional Details

- **From §3.3.1.1:** For three heists, including the British Bank of the Middle East Gold Heist, the time at which the heist began is unclear from the available open literature.
- **From §3.3.3:** Only in 22% of heists in the database (specifically, the Millennium Dome Raid, British Bank of the Middle East Heist, Chase Manhattan Bank Robbery, Harry Winston Diamond Heist, and Schiphol Airport Diamond Heist) did thieves steal or intend to steal more than 50% of the valuables at a target.
- **From §3.5.4.2:** In only 10% of heists (specifically, the Antwerp Diamond Heist and British Bank of the Middle East Gold Heist) were the criminal teams thought to consist entirely of citizens from foreign nations.

6.2.9. Chase Manhattan Bank Robbery

*Subdue
& Seize*



6.2.9.1. Synopsis

At closing time for the Chase Manhattan Bank in New York in August 1972, two ordinary-looking men in the bank produced guns and informed the staff that they were being robbed. Collecting about \$1.2 million (FY12) in cash and traveler's checks, the two men were impeded in leaving upon the arrival of police, who were informed by a personnel officer at Chase Manhattan's downtown headquarters that something seemed amiss during a chance phone call he made to the bank manager. Holding the bank staff hostage for some twelve hours, the thieves convince the police to transport them (with their hostages) to an airplane waiting at John F. Kennedy Airport. After arriving at the airport, the Federal Bureau of Investigation (FBI) agent driving the thieves' limousine, with the assistance of agents in place aside the vehicle, seized an opportunity to shoot and kill one thief and subdue the other.⁴⁷

6.2.9.2. Additional Details

- **From §3.3.3:** Outliers in terms of their targeted facility's ease of penetration and targeted valuables' ease of fencing include the Stardust Casino Job and Chase Manhattan Bank Robbery, though these were both smaller-scale robberies on the order of \$1 million (FY12).

- **From §3.3.3:** Only in 22% of heists in the database (specifically, the Millennium Dome Raid, British Bank of the Middle East Heist, Chase Manhattan Bank Robbery, Harry Winston Diamond Heist, and Schiphol Airport Diamond Heist) did thieves steal or intend to steal more than 50% of the valuables at a target.
- **From §3.7.2:** The Chase Manhattan Bank Robbery was foiled by a disguised phone communication between bank managers during the initial stages of the heist. As a result, the bank manager off-scene alerted police and a standoff resulted. Some 14 hours later, one of the robbers was captured and another killed while waiting for their getaway airplane in a limousine driven by an FBI agent.

6.2.10. Mayfair Graff Diamond Heist



6.2.10.1. Synopsis

At 4:40 PM on Thursday, August 6, 2009, two men dressed in suits and wearing latex disguises to appear older were let in to the high-end Graff Diamonds shop in London (see Fig. 10). Producing concealed handguns, the men threatened the staff and within two minutes left with \$68.9 million (FY12) in diamonds and other jewelry – as well as a hostage. Firing warning shots prior to releasing the hostage, the thieves made an initial getaway in a blue BMW fitted with false number plates. The BMW then crashed into a taxi cab, and the jewelry bag was transferred to a man on an orange motorbike. The thieves then switched cars to a waiting silver Mercedes, followed by a second switch to a black vehicle. The first arrests for the crime were not made until nearly two weeks later.⁴⁸⁻⁵⁴

6.2.10.2. Additional Details

- **From §3.1.2.1:** Interestingly, certain heist stories suggest that guards may make fundamental decisions regarding their role(s) as sensors or responders on the spot during a crisis. For example, in the Mayfair Graff Diamond Heist, a security guard witnessing what appeared to be the kidnapping of a hostage told a court, “I decided that if I was able to tackle them, or at least grab the woman and take her away from them at the price of getting wounded but not killed, it might be worth it.”⁵⁴ This guard was unarmed and, weighing the risks, costs, and benefits, decided to respond (rather than simply observe and report) against two armed men.
- **From §3.1.2.2:** Only three of the 23 heists in the database (the Munch Museum Art Heist, Mayfair Graff Diamond Heist, and Schiphol Airport Diamond Heist) took less than 14 minutes.
- **From §3.3.1.1:** Heists of the “Closing Time Heists” timing archetype occur in the very late afternoon or early evening, as businesses are nearing closing time and employees may be tired, distracted, and somewhat less prepared for a robbery. Both heists in this category, the Harry Winston Diamond Heist and Mayfair Graff Diamond Heist, were complete in just minutes.
- **From §3.4:** By far the most commonly used type of weapon was the handgun. This class of weapon is both deadly and easily concealed, permitting thieves to enter a facility and invite little scrutiny from security personnel or bystanders. The Harry Winston and Mayfair Graff diamond heists, both Closing Time heists, demonstrated skillful execution using this characteristic of handguns.
- **From §3.5.4.1:** The only example of a four-team operation was the Mayfair Graff Diamond Heist, which involved a complex relay of the stolen goods among the occupants of different motor vehicles.

6.2.11. Harry Winston Diamond Heist

*Deceive,
Subdue
& Seize*



6.2.11.1. Synopsis

At 5:30 PM on Thursday, December 4, 2008, four men, three of whom were dressed as women, requested entry via intercom to the high-end Harry Winston jewelry shop in Paris. Upon inside, the men produced a revolver and hand grenade, smashed display cases, and threatened the 15 customers and employees (some of whom were called by name) to assist them in gathering \$111.3 million (FY12) in diamonds and other jewelry. Within 15 minutes, the thieves calmly drove away from the scene.⁵⁵⁻⁵⁶

6.2.11.2. Additional Details

- **From §3.1.2.2:** Heists in this study were frequently committed not only under the noses of security guards, but also under the noses of nearby external police forces. In three cases (the Antwerp Diamond Heist, the Tanzanian Airplane Gold Robbery, and Harry Winston Diamond Heist), police forces were stationed within 500 feet of the heist.
- **From §3.3.1.1:** Heists of the “Closing Time Heists” timing archetype occur in the very late afternoon or early evening, as businesses are nearing closing time and employees may be tired, distracted, and somewhat less prepared for a robbery. Both heists in this category, the Harry Winston Diamond Heist and Mayfair Graff Diamond Heist, were complete in just minutes.
- **From §3.3.3:** Only in 22% of heists in the database (specifically, the Millennium Dome Raid, British Bank of the Middle East Heist, Chase Manhattan Bank Robbery, Harry Winston Diamond Heist, and Schiphol Airport Diamond Heist) did thieves steal or intend to steal more than 50% of the valuables at a target.
- **From §3.4:** By far the most commonly used type of weapon was the handgun. This class of weapon is both deadly and easily concealed, permitting thieves to enter a facility and invite little scrutiny from security personnel or bystanders. The Harry Winston and Mayfair Graff diamond heists, both Closing Time heists, demonstrated skillful execution using this characteristic of handguns.

6.2.12. Schiphol Airport Diamond Heist

*Deceive,
Subdue
& Seize*



6.2.12.1. Synopsis

At 10:00 AM on Friday, February 25, 2005, two men dressed in KLM uniforms drove a blue KLM vehicle they had stolen two weeks earlier into the secure freight area at Schiphol Airport in Amsterdam. They then intercepted a truck carrying \$115 million (FY12) worth of diamonds bound for a flight to Antwerp, forcing the two transport guards out of the truck at gunpoint and exiting the security gates by tailgating another truck on its way out. Given the precise timing of the robbery, insider information was suspected but never proven.⁵⁷⁻⁶⁰

6.2.12.2. Additional Details

- **From §3.1.2:** One technique thieves use toward rendering guard security ineffective is to disguise themselves to appear nonthreatening to guards (as in the Schiphol and Heathrow heists).
- **From §3.1.2.2:** Only three of the 23 heists in the database (the Munch Museum Art Heist, Mayfair Graff Diamond Heist, and Schiphol Airport Diamond Heist) took less than 14 minutes.

- **From §3.2.1:** Some 70% of the heists in the database occurred in urban areas, and almost any commercially available sedan or van blends with urban surroundings. However, to illustrate a less typical of a vehicle blending with surroundings, in the Schiphol Airport Diamond Heist the thieves used a KLM airlines vehicle, which was used to inconspicuously enter and lie and wait within the secure freight area at Schiphol Airport in Amsterdam.
- **From §3.3.1.1:** The “Broad Daylight Heists” timing archetype is characterized by heists early in the work day that are conducted rapidly, on timescales well under one hour. These timescales are largely a necessity for such heists, and all four in this category (the Swissport Heathrow Heist, Millennium Dome Raid, Schiphol Airport Diamond Heist, and Munch Museum Art Heist) involved use of violence to subdue guards, employees, and bystanders to permit rapid access to the target valuables. However, unlike heists of the Early Bird Heists archetype, response by police forces was unlikely to be prevented, and the thieves needed to work against the clock. While there is no obvious single reason why all four of the heists in this category shared such similar timing, the broad daylight timing for two such heists (the Swissport Heathrow Heist and Schiphol Airport Diamond Heist) was driven by the business-hours timing of large high-value shipments that the thieves were targeting.
- **From §3.3.3:** Only in 22% of heists in the database (specifically, the Millennium Dome Raid, British Bank of the Middle East Heist, Chase Manhattan Bank Robbery, Harry Winston Diamond Heist, and Schiphol Airport Diamond Heist) did thieves steal or intend to steal more than 50% of the valuables at a target.

6.2.13. Swissport Heathrow Heist

*Deceive,
Subdue
& Seize* 

6.2.13.1. Synopsis

At 9:30 AM on Monday, May 17, 2004, a white delivery van with seemingly legitimate paperwork passed through the security gate at Swissport Cargo Services outside of London’s Heathrow Airport. Unknown to the gate security personnel, the paperwork had been forged with the assistance of an opportunistic insider employed as a delivery driver. Shortly after pulling up to the Swissport warehouse, the van, with eight men on board, backed up and rammed through a rolling door. The gang exited the van and threatened the warehouse staff with at least one firearm as well as knives and clubs. Some thieves began loading into the van the gold bullion that had been delivered to the warehouse some 30 minutes prior, while others approached the cash-containing vault and threatened the custodian in order to obtain his keys. Fortunately for Swissport, Scotland Yard’s Flying Squad had anticipated the attack from prior surveillance of the delivery driver insider, and over 100 police officers were waiting in the vicinity of Heathrow Airport to apprehend the thieves, averting what would likely have been a \$71.1 million (FY12) loss.⁶¹⁻⁶⁴

6.2.13.2. Additional Details

- **From §3.1.1.1:** In some cases, defeat of an unarmed guard security measure took the form of a nonviolent deception; for example, criminals in the Swissport Heathrow Heist presented forged papers to gain facility access.
- **From §3.1.2:** One technique thieves use toward rendering guard security ineffective is to disguise themselves to appear nonthreatening to guards (as in the Schiphol and Swissport Heathrow heists).
- **From §3.3.1.1:** The “Broad Daylight Heists” timing archetype is characterized by heists early in the work day that are conducted rapidly, on timescales well under one hour. These timescales are

largely a necessity for such heists, and all four in this category (the Swissport Heathrow Heist, Millennium Dome Raid, Schiphol Airport Diamond Heist, and Munch Museum Art Heist) involved use of violence to subdue guards, employees, and bystanders to permit rapid access to the target valuables. However, unlike heists of the Early Bird Heists archetype, response by police forces was unlikely to be prevented, and the thieves needed to work against the clock. While there is no obvious single reason why all four of the heists in this category shared such similar timing, the broad daylight timing for two such heists (the Swissport Heathrow Heist and Schiphol Airport Diamond Heist) was driven by the business-hours timing of large high-value shipments that the thieves were targeting.

- **From §3.3.1.3:** The Swissport Heathrow Heist is the only springtime heist in the database.
- **From §3.3.3:** The availability of numerous and specialized security forces in a city can be a detriment for a thief that is not well-disguised (as the criminals in both the Millennium Dome Raid and Swissport Heathrow Heist learned, when confronted with a 100-officer Metropolitan Police operation designed to foil their heist).
- **From §3.4:** Bladed weapons were rarely used in the HMCD heists. One of the only two examples involved knives to threaten staff at the Swissport Cargo Warehouse at Heathrow Airport. Blunt weapons were similarly rare. The only known examples in this category involved thieves wielding hockey sticks, clubs, and lumps of wood to threaten staff at the Swissport Cargo Warehouse.
- **From §3.7.2:** In both the Millennium Dome Raid and Swissport Heathrow Heist, intelligence gathered by the Metropolitan Police well in advance resulted in 100-officer operations to foil the robberies, with police forces lying in wait on the days of the heists.

6.2.14. Gardner Museum Art Heist

*Deceive,
Subdue
& Seize* 

6.2.14.1. Synopsis

At 1:24 AM on Sunday, March 18, 1990, two men posing as Boston Police officers approached the side entrance to the Isabella Stewart Gardner Museum. Claiming to be responding to a disturbance, the officers convinced an on-duty security guard to permit them entrance. To lure the guard away from the panic button at his security booth, the police claimed they had a warrant for his arrest and demanded identification. After the roving guard arrived to assist the guard at the booth, the two men posing as officers handcuffed both guards, wrapped duct tape around their eyes and mouths, and bound them to a steam pipe and workbench in the basement. Over the course of 81 minutes, the thieves made their way through the museum and stole thirteen works of art (see Fig. 11), worth an estimated \$440 million (FY12). Though motion detectors sounded and recorded the movements of the thieves, they transmitted intrusion information only to the guard booth and not to any external force. As a result, the outside world did not know of the heist until the security guards were scheduled to be relieved at 7:00 AM.⁶⁵⁻⁷⁰

6.2.14.2. Additional Details

- **From §3.1.1.3:** One particularly significant heist from a security measure defeat standpoint is the unsolved Museon Jewel Heist in the Netherlands, where static barriers and detectors were defeated by methods that are as yet unclear.
- **From §3.1.2.1:** Interestingly, certain heist stories suggest that guards may make important decisions regarding their roles on the spot during a crisis. In one instance, a guard at the Isabella Stewart Gardner Museum decided that his salary was not high enough to merit resisting the thieves who had just handcuffed him: When one of the robbers told him, “Don’t give us any

problems, and you won't get hurt," he capitulated and responded, "They don't pay me enough to get hurt." ⁶⁵

- **From §3.1.2.1:** The HMCD contains 11 heists (48% of the database) in which armed thieves attacked security personnel, almost all of whom were unarmed. In contrast, only in two cases (the Antwerp Diamond Heist and Gardner Museum Art Heist) did thieves enter unarmed into a facility with security personnel present. In both of these cases, planning is estimated to have initiated 24-30 months prior to the heist (far above the mean planning duration of 9 months and median of 4 months).
- **From §3.1.2.1:** Within the heists examined in this study, security forces were frequently aware of the heist during the theft phase but were prevented from effectively responding until the aftermath. For example, guards at the Gardner Museum in Boston were not aware that the apparent police officers "arresting" them were actually impostors until after they had been handcuffed and rendered nearly powerless.
- **From §3.3.1.1:** The "Early-Bird Heists" timing archetype is characterized by early-morning heists with durations of 1-2 hours. All three heists that fall within this category, the Gardner Museum Art Heist, Lufthansa Heist, and Brink's-Mat Gold Heist, were characterized by violence. In all three cases, those guards and employees were subdued and unable to call for help. Since the crimes were perpetrated in the early morning when little, if any, business with outside organizations or people was conducted, there was little risk that individuals from the outside would visit the facility and discover the heist in progress.
- **From §3.3.2:** Thieves frequently choose to commit large heists at times of low employee or security activity because it minimizes the difficulty of defeating *anticipated* detection. This factor tends to drive thieves to choose times outside of core business hours for the targeted entity. One example is the 1:30 AM attack on the Gardner Museum, which was protected only by an overnight force of two unarmed guards.
- **From §3.4:** While 70% of heists involved use of some weapon, it is worth noting that 7 heists (30%) involved no known use of weapons. These heists include both of the nonviolent heist categories (i.e., the Stealth Raid and Walk Away categories) plus the Gardner Museum Art Heist.
- **From §3.5.1:** In the case of the Gardner Museum Art Heist, one of the suspects in the crime admitted that he had scoped out the museum's security measures years earlier. On one visit in particular, he unlocked a window in the facility. Visiting again every few months, he found that the window remained unlocked and used this as a partial gauge of the attentiveness and thoroughness of the security force.
- **From §3.7.1:** In the Gardner Museum Art Heist, an independent security evaluation conducted two years prior to the robbery had recommended an enclosed security station and protective second door for the museum's side entrance. Additionally, the director of security had lobbied the museum's board of trustees for more security funding so that he could attract security guards more qualified and experienced than local college students. However, the museum was in financial trouble, and the funds never came.

6.2.15. Knightsbridge Safe Deposit Center Heist

6.2.15.1. Synopsis

In July 1987, two men entered the Knightsbridge Safe Deposit Center, the largest safe deposit center in London. One of the men, Valerio Viccei, at that time a client of the center, introduced a friend to the

*Deceive,
Subdue
& Seize*



owner, Parvez Latif, who led the two to a private viewing room inside the center's vault. Drawing a pistol, the two men threatened Latif, who was made to request entry into the security guard booth to show the center's security measures. Distracting the security guard, the guard's hand left the panic button and the two thieves subdued him. The front desk security guard was called in to deliver brochures to the owner's office and captured. With both guards subdued, the two thieves attempted to use a two-way radio to call for two waiting accomplices. When the reinforcements failed to answer, Viccei left the safe deposit center and found them nearby, listening to the incorrect radio channel. The thieves used sledgehammers and crowbars to force open 121 of the 5,000 safe deposit boxes in the center (see Fig. 12), making off with an estimated \$130 million (FY12). Thanks to the investigation following the heist, the thieves were eventually captured. Among those sentenced was Parvez Latif himself, who had performed so convincingly during the heist that not even Viccei's hired henchmen knew that he had assisted them by scheduling new guards who would not recognize Viccei and ensuring a technical glitch rendered security cameras useless.^{6,71-72}

6.2.15.2. Additional Details

- **From §3.1.1.1:** One notable camera defeat technique is deactivation of the cameras prior to the robbery as was done by an insider, safe deposit center owner Parvez Latif, in the Knightsbridge Safe Deposit Center Heist.
- **From §3.1.1.2:** Using recognized employees to enter and/or vouch for entry worked to provide unauthorized access in the Knightsbridge Safe Deposit Center, Securitas Cash Depot, and Northern Bank Cash Heists. In the first two cases, the thieves used either coercion or incentive to convince a recognized employee to vouch for their entry into a secure facility, which the thieves then used to subdue the on-duty guard that had granted them entry.
- **From §3.1.2:** One important security guard defeat technique not seen in the heists in the HMCD is the emplacement of insiders as security guards. However, a variant of the latter occurred in the Knightsbridge heist: While no security guards were insiders, the owner of the safe deposit center, an insider, scheduled new guards to be on duty during the time of the robbery. Since the theft mastermind, Valerio Viccei, was a tenant of the center and could be recognized by the experienced guards, scheduling these new guards ensured that the robbers would go unrecognized.
- **From §3.2.1:** The HMCD shows no clear limitation to what level of occupational role thieves or their coerced accomplices will take; there are virtually equal numbers of examples of inside managers, employees, and customers. There even exists in the Knightsbridge Safe Deposit Center Heist an instance where an owner used his position to help mask his involvement in the crime.
- **From §3.2.2:** The top number of deception methods employed for a heists within the HMCD is associated with the Knightsbridge Safe Deposit Center Heist, which utilized half the list of physical disguises in Table 5, the entire list of activity disguises, and one diversion. In this heist, the thieves entered the building with a concealed weapon, with the mastermind feigning sickness and covering his face with a handkerchief. During the robbery, the center's owner, who had been befriended by the mastermind weeks earlier and had become an accomplice in the heist, used his authority to order the security guard to open the security booth to him and the thieves, who were posing as prospective safe deposit box customers. Once inside, the criminal mastermind made advances on the guard to distract him and move him out of reach of the panic button. The thieves placed a sign on the center's door to announce that the center was closed for security upgrades, and once the heist was complete they drove off in a nondescript van.

- **From §3.3.1.1:** The duration of the Knightsbridge Safe Deposit Center Heist was quite similar to that of an Early-Bird Heist, and the thieves cleverly reduced the risk of detection by outside customers by posting a sign indicating that the center was temporarily closed for security system upgrades.
- **From §3.3.3:** The Antwerp, Société Générale, and Knightsbridge heists were all thefts from safe deposit boxes and required the thieves, at a minimum, to sort through a hodgepodge of items found upon opening the deposit boxes. All three targets were difficult to penetrate, and the heists averaged about 1.5 years of planning apiece; however, they were also some of the highest-yield heists in the database, averaging a take of \$170 million (FY12) apiece.
- **From §3.6:** Insiders within this study have operated with varying degrees of inside access. Owners (e.g., Parvez Latif in the Knightsbridge Safe Deposit Center Heist), managers, and employees fall into the clear category of being a “full” insider with a high degree of inside access.
- **From §3.6:** Recruited insiders are individuals who are part of an organization and, typically as a result of their existing access and influence, are asked to join a heist plot. Recruitment is a risky tactic for a thief to employ, and consequently, recruited insiders are uncommon in the HMCD. There exist just three examples: the owner of the Knightsbridge Safe Deposit Center, an employee of the Brink’s-Mat depot, and a security guard at Brazil’s Central Bank in Fortaleza.
- **From §3.6:** Active violent insiders use or credibly threaten violence during a heist. Insiders in this role are exceedingly rare in the database, and only one example has been identified: Valerio Viccei, a customer of the Knightsbridge Safe Deposit Center, entered the center with another accomplice and wielded a gun to subdue the owner and guards. (The owner, Parvez Latif, was also an accomplice, but Viccei kept that information secret from his other accomplices. Thus, to reduce suspicion, during the heist Latif played the part of a victim and surprised owner, and Viccei’s accomplices remained clueless about Latif’s involvement until their trials.)
- **From §3.6:** Within the HMCD, the number of *willing* insiders was limited to one in all but one of the heists; the exception was the Knightsbridge Safe Deposit Center Heist, in which both the owner (Parvez Latif) and a safe deposit box renter (Valerio Viccei) colluded to perpetrate the heist.
- **From §3.7.2:** During the Knightsbridge Safe Deposit Center Heist, mastermind Valerio Viccei used a radio to call for his help on the outside once the center’s owner and guards had been subdued. However, Viccei received no reply. He had to physically leave the safe deposit center during the robbery to find his henchmen, who were waiting nearby as planned – with their radios tuned to the wrong channel (To exacerbate the risk, at the time when this occurred, police were out in force in the area, searching for a kidnapped child.⁷²)

6.2.16. Securitas Cash Depot Heist



6.2.16.1. Synopsis

At 6:30 PM on Tuesday, February 21, 2006, the manager of the Securitas Cash Depot some 30 miles southeast of central London was pulled over by two men posing as police officers. Simultaneously, two other men posing as police officers arrived at the manager’s residence to inform his wife and child that he had been involved in an accident. In two separate cars, the manager and his family were driven to a farm and held at gunpoint. The thieves told the manager his family would be killed if he did not cooperate, and the manager was brought to the Securitas depot. A thief dressed as a police officer (see Fig. 13) accompanied the manager to the pedestrian entrance, and the manager convinced the control room guard to admit the two and open the main gate, through which three thief vehicles drove. Inside, the thief

posing as the police officer subdued the guard, let in his accomplices, subdued the remaining 13 employees inside the depot, and drove away after loading some 6,000 lbs. of cash worth an estimated \$104 million into a truck.⁷³⁻⁸¹

6.2.16.2. Additional Details

- **From §3.1.1.1:** In some cases, defeat of a guard took the form of an overt threat of violence; for example, a criminal in the Securitas Cash Depot Heist threatened the unarmed security guard with a pistol.
- **From §3.1.1.1:** One notable camera defeat technique is for thieves to gain control of the camera monitoring station. This can be accomplished violently or nonviolently. As an example of the former, the Securitas Cash Depot Heist criminals used a pistol to threaten a guard in order to gain control of the guard station.
- **From §3.1.1.2:** Using recognized employees to enter and/or vouch for entry worked to provide unauthorized access in the Knightsbridge Safe Deposit Center, Securitas Cash Depot, and Northern Bank Cash Heists. In the first two cases, the thieves used either coercion or incentive to convince a recognized employee to vouch for their entry into a secure facility, which the thieves then used to subdue the on-duty guard that had granted them entry.
- **From §3.1.1.2:** A complication introduced when using humans in the loop for security systems is the fact that the human has the capability to make decisions in the service of objectives other than facility security. While this decision capability often resulted in the decidedly negative outcome of loss of millions of dollars to thieves (for example, as a consequence of the on-duty guard at the Securitas depot letting manager Colin Dixon and a purported police officer enter the facility unchallenged), it also resulted in a zero or near-zero casualty rate for the employees present during the robberies.
- **From §3.1.2.1:** For eight heists in the database, response was delayed by between one and three phases (of the sequence Planning, Entry, Theft, Escape, and Aftermath). For example, despite the fact that the unarmed security guard on duty in the Securitas Cash Depot became aware of the heist upon the first thief's entry into the guard station, he was held at gunpoint, handcuffed and blindfolded, and could not respond or alert others until after the heist had been completed.
- **From §3.1.2.2:** While guards themselves may not deter a determined thief, they do add to the amount of time the thief requires to prepare and plan for his heist. The Antwerp Diamond Heist and Securitas Cash Depot Heist serve as two examples illustrating the months or years of planning that thieves may require to learn the details of security practices and procedures at the target facility.
- **From §3.3.1.1:** The "Night Raids" timing archetype is characterized not only by heists that begin very late in the day, but also by heists that run the course of several hours. Ironically, the four heists in this category cover some of the least violent and some of the most violent heists in the database. Both tiger kidnappings, the Securitas Cash Depot Heist and Northern Bank Cash Heist, are contained in this category. In both crimes, the kidnappings began in the evening or night, and the ordeals did not end until the following day.
- **From §3.3.3:** In most heists in the database, thieves were highly selective in what they removed from the target facility. In a number of cases, including the Antwerp Diamond Heist, Northern Bank Cash Heist, and Securitas Cash Depot Heist, this selectivity was influenced by limitations in transportation capacity.
- **From §3.4:** Conventional firearms tend to be the most frequently used weapons among heists in the HMCD. Examples particularly abound in which firearms were used purely in a threatening

manner with no shots actually fired. For example, guns were used to threaten Securitas manager Colin Dixon that his family would be killed if he did not comply and lead them into the Securitas cash depot.

- **From §3.5.3:** Examples of loot weighing more than 5,000 lbs. include loads of cash and/or gold from the Brazil Central Bank Cash Heist, Brink's-Mat Gold Heist, and Securitas Cash Depot Heist. These extremely heavy loads require the capacity of a sizable truck (see Fig. 32 for the truck used in the Securitas heist).
- **From §3.6:** Insiders within this study have operated with varying degrees of inside access. Owners, managers, and employees (e.g., Ermir Hysenaj in the Securitas Cash Depot Heist) fall into the clear category of being a "full" insider with a high degree of inside access.
- **From §3.6:** Planted insiders are individuals who become part of an organization with the intent of robbing it. Because it typically takes a significant amount of time to be promoted through the ranks of an organization, these insiders are typically limited to the easy-to-access lower levels in the organizational hierarchy. The example of Ermir Hysenaj, an Eastern European immigrant and the inside employee in the Securitas Cash Depot Heist, also encountered notoriously easy path to access: Hysenaj's interview for the job lasted just ten minutes, and he was on the job six days later.
- **From §3.6:** If security system designers can provide these potentially coerced insiders with tactics to free themselves from such coercion when it occurs, the insider problem has largely been solved. For example, in the Securitas Cash Depot Heist, the security booth contained a sign that advised staff: "Don't Be a Hero" While sound advice aimed at saving the lives of employees, the same advice invites attacks by criminals who know the staff will surrender at the sight of a weapon (even if the thief has no intention of using it). An important consideration in security system design is whether tactics can be devised that simultaneously preserve human life and undermine the plans of thieves.

6.2.17. Northern Bank Cash Heist



6.2.17.1. Synopsis

At 10:00 PM on Sunday, December 19, 2004, three masked men arrived at the home of Chris Ward, an official of the Northern Bank in Belfast. While two men held hostage Ward's parents, brother, and girlfriend, the third man brought Ward to the home of his supervisor, Kevin McMullan. McMullan and his wife had already been bound by two men who had entered the home posing as police officers. McMullan's wife was taken to an undisclosed location at approximately 11:30 PM. Then, after instructing the two key-holding bank officials on what to do at work the next day, with the consequence of failure being the death of the officials' families, the thieves left the house at 6:30 AM. Returning to work as normal on Monday, Ward and McMullan let the thieves in to the bank once all other employees had left at 6:00 PM. Over the course of two trips with a van, the thieves made off with some \$60.5 million in cash.⁸²⁻⁸⁵

6.2.17.2. Additional Details

- **From §3.1.1.2:** Using recognized employees to enter and/or vouch for entry worked to provide unauthorized access in the Knightsbridge Safe Deposit Center, Securitas Cash Depot, and Northern Bank Cash Heists. In the first two cases, the thieves used either coercion or incentive to convince a recognized employee to vouch for their entry into a secure facility, which the thieves then used to subdue the on-duty guard that had granted them entry.

- **From §3.3.1.1:** The “Night Raids” timing archetype is characterized not only by heists that begin very late in the day, but also by heists that run the course of several hours. Ironically, the four heists in this category cover some of the least violent and some of the most violent heists in the database. Both tiger kidnappings, the Securitas Cash Depot Heist and Northern Bank Cash Heist, are contained in this category. In both crimes, the kidnappings began in the evening or night, and the ordeals did not end until the following day.
- **From §3.3.3:** In most heists in the database, thieves were highly selective in what they removed from the target facility. In a number of cases, including the Antwerp Diamond Heist, Northern Bank Cash Heist, and Securitas Cash Depot Heist, this selectivity was influenced by limitations in transportation capacity.
- **From §3.6:** An example of collusion among unwilling insiders occurred in the Northern Bank Cash Heist, in which the families of two bank employees, Chris Ward and Kevin McMullan, were held hostage while Ward and McMullan assisted thieves in robbing the bank. Ward was later tried for colluding with the thieves but was cleared of wrongdoing. During the trial, Justice Richard McLaughlin asked assistant manager Kevin McMullan, “It’s not like the movies, you don’t need dynamite?” McMullan responded, “You just need to take someone’s wife away from them.”

DISTRIBUTION

1	MS0757	Gregory Wyss	6612 (electronic copy)
1	MS0757	John Clem	6612 (electronic copy)
1	MS0780	Bradley Norman	6523 (electronic copy)
1	MS0781	Jennifer Nelson	6520 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)
1	MS1234	Adam Williams	6812 (electronic copy)
1	MS9004	Duane Lindner	8100 (electronic copy)
1	MS9004	Heidi Ammerlahn	8110 (electronic copy)
1	MS9031	Patricia Koning	8521 (electronic copy)
1	MS9033	Justin Pack	0021 (electronic copy)
1	MS9406	Todd West	8114 (electronic copy)
1	MS9406	Paul Nielan	8118 (electronic copy)
1	MS9407	Jason Reinhardt	8111 (electronic copy)
1	MS9407	Nathaniel Gleason	8116 (electronic copy)
1	MS9407	Matthew Sumner	8116 (electronic copy)
1	MS9407	William Rorke	8118 (electronic copy)



Sandia National Laboratories

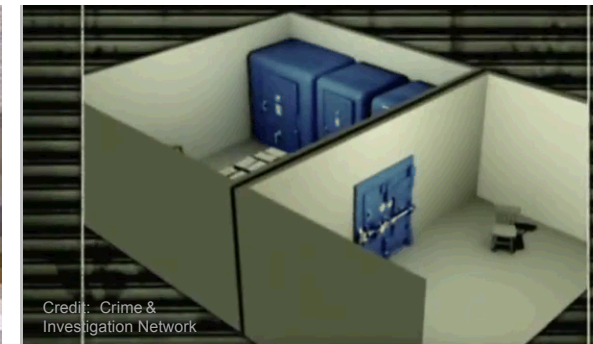
Exceptional service in the national interest



Credit: Google



Credit: The Guardian
Kent Police



Credit: Crime & Investigation Network

The Perfect Heist

Recipes from Around the World

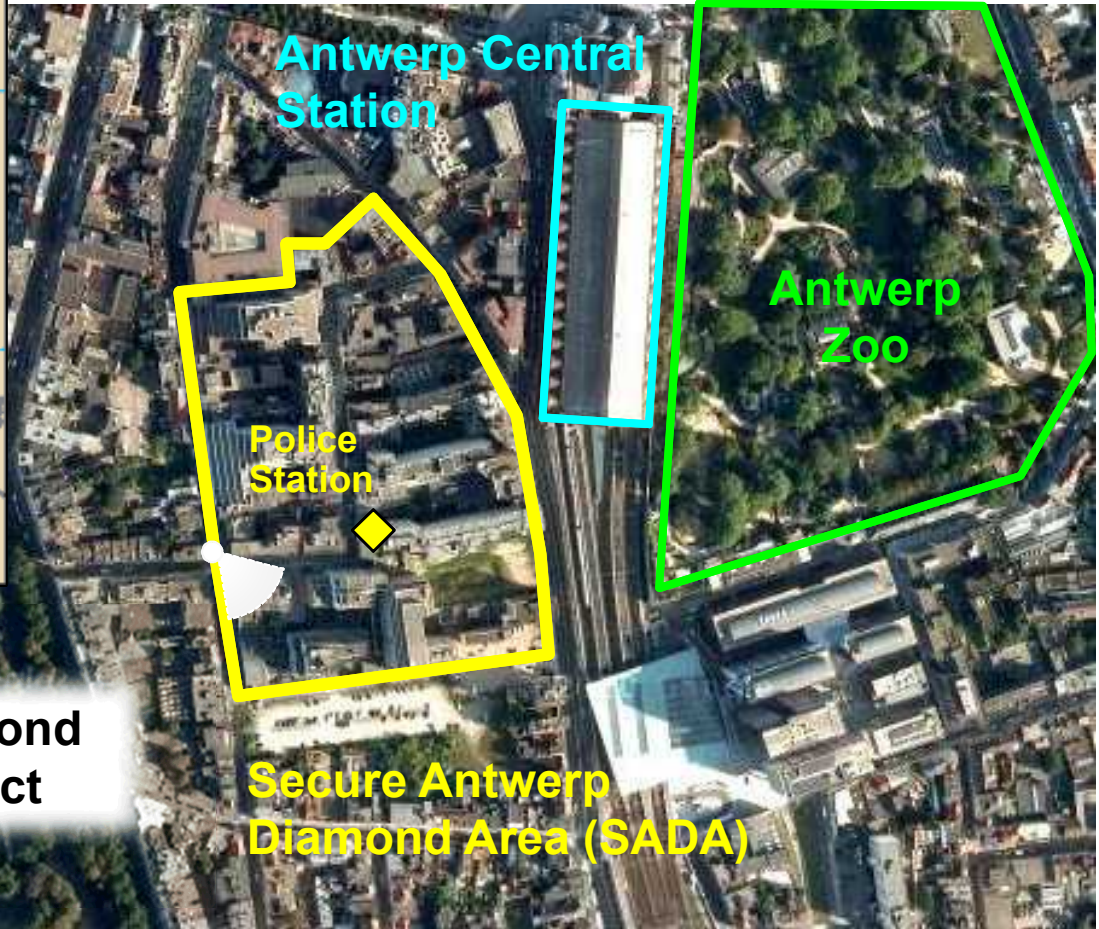
Jarret Lafleur, Luke Purvis, Alex Roesler, and Paul Westland
Sandia Systems Analysis and Engineering
June 1, 2015



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Antwerp: Feb. 2003



Diamond District

Secure Antwerp Diamond Area (SADA)



Antwerp: Feb. 2003

SADA Security Measures:
Vehicle Barricades
Police Stations
Uniformed and Plainclothes Police Patrols





Antwerp: Feb. 2003

*Can you spot the
CCTV cameras?*

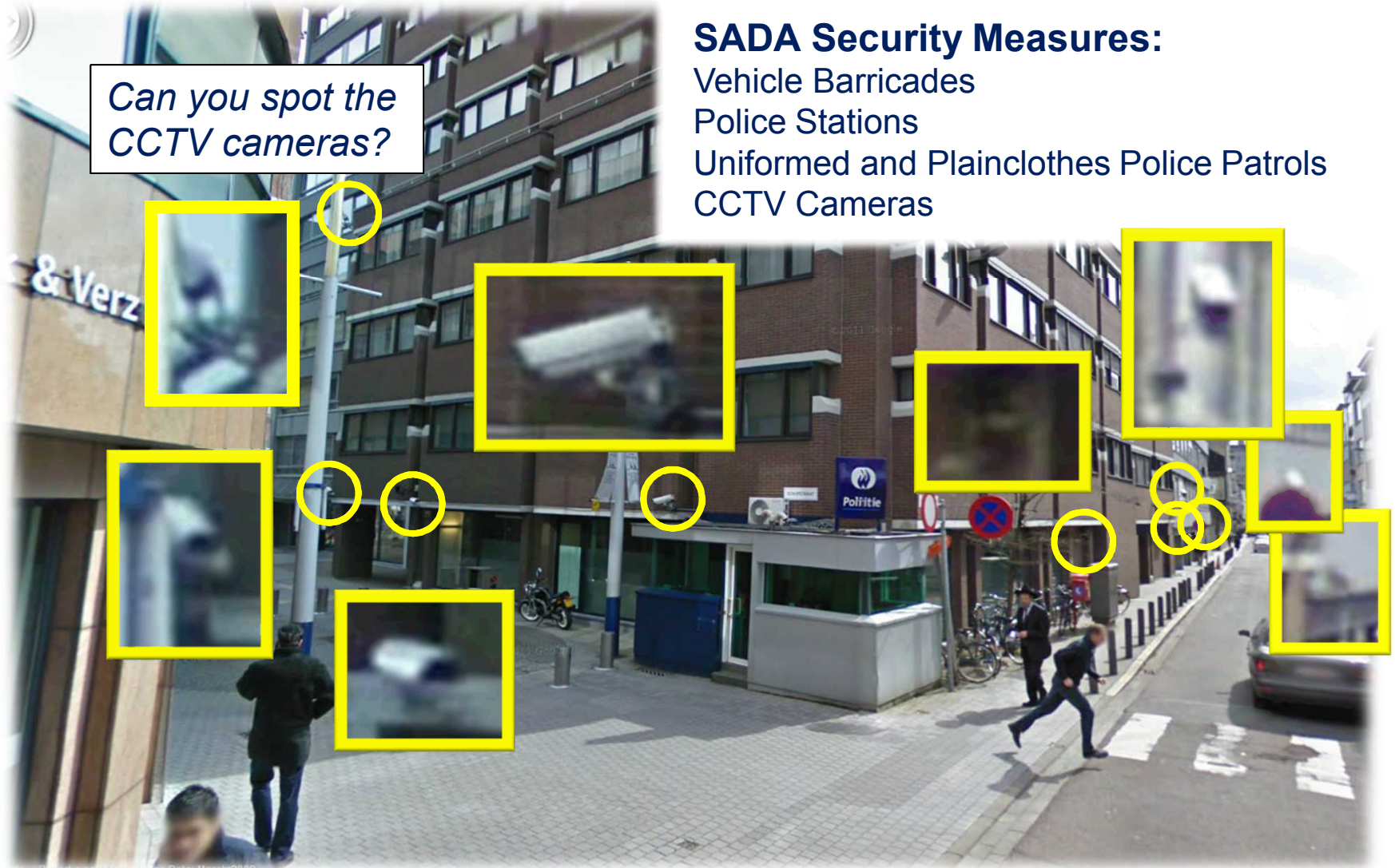
SADA Security Measures:

Vehicle Barricades

Police Stations

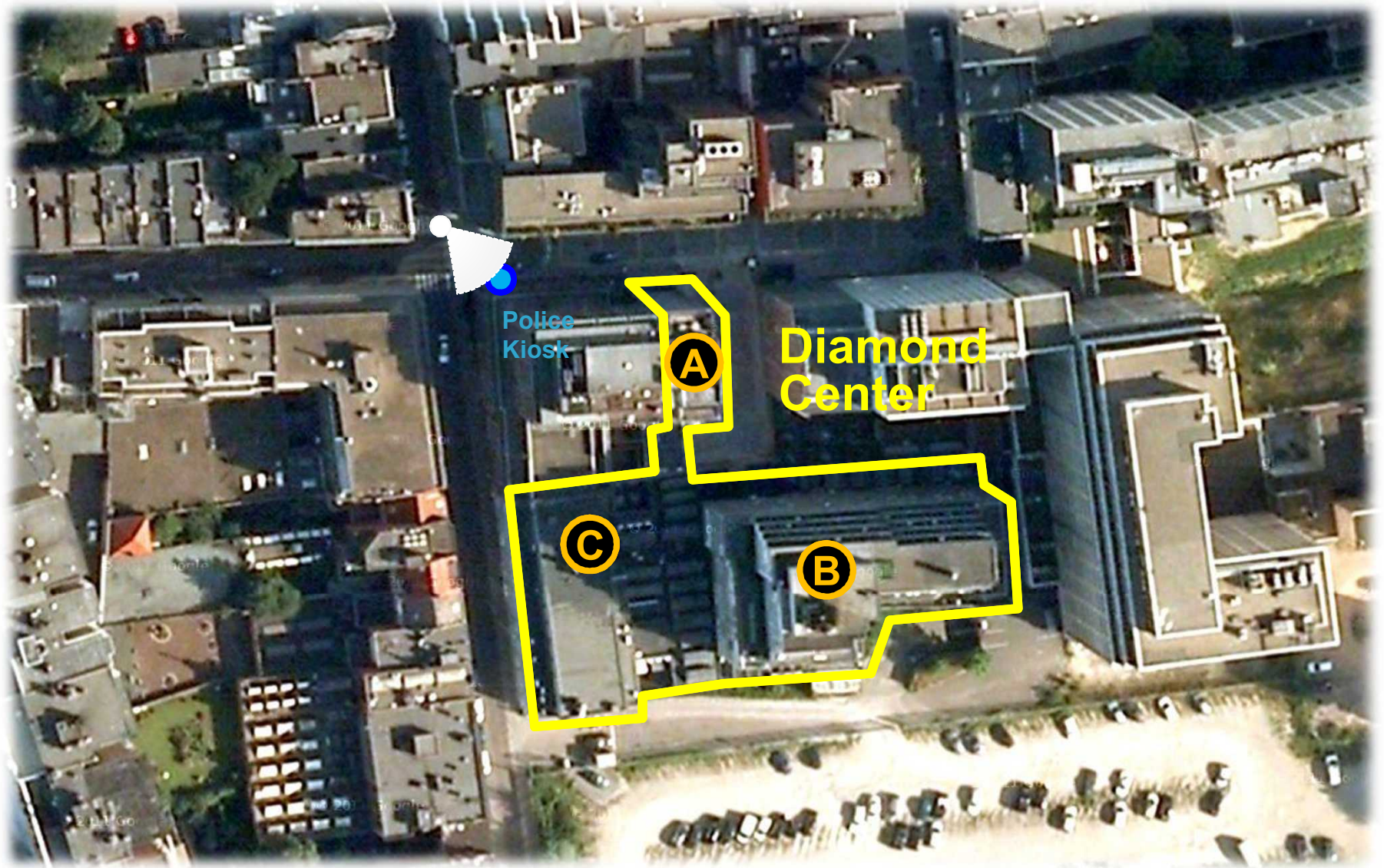
Uniformed and Plainclothes Police Patrols

CCTV Cameras





Antwerp: Feb. 2003





Antwerp: Feb. 2003

Saturday, Feb. 15
23:50

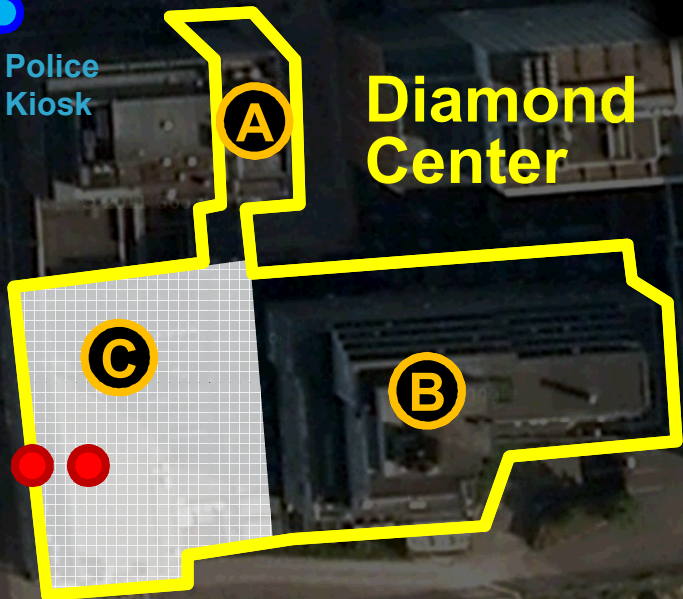
- Entry via garage doors, avoiding Schupstraat police and cameras.
- Interior door access via custom key rake



Police
Kiosk



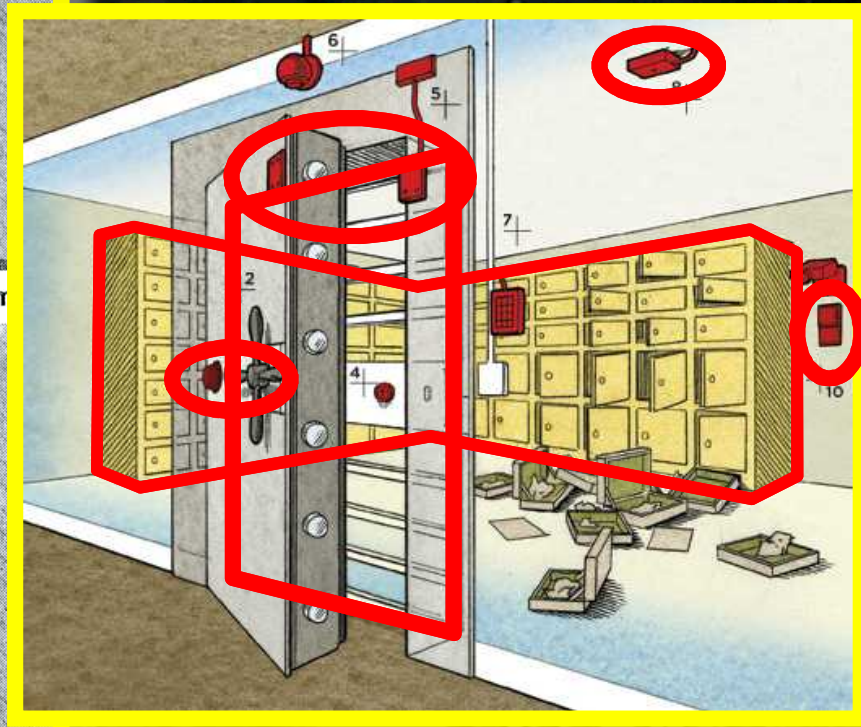
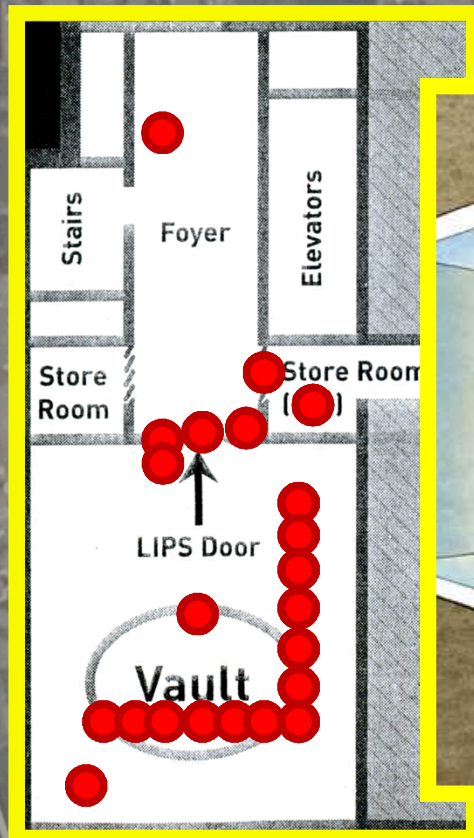
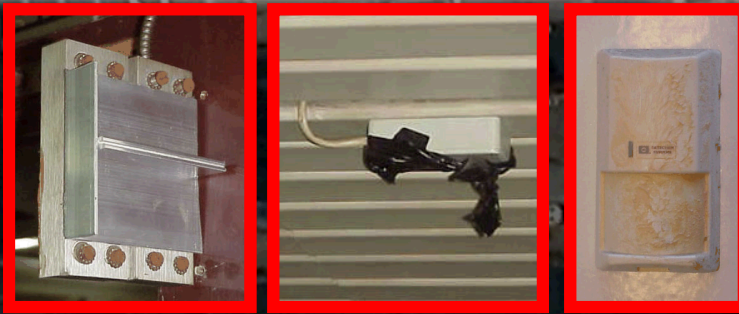
Diamond
Center





Antwerp: Feb. 2003

Sunday, Feb.
0:00 (approx.)



- Shrouded CCTV camera
- Tore away door-sealing magnets
- Recovered fiber-optic camera from ceiling tile
- Broke into store room and internal lock box with crowbar to obtain vault key (pipe and stamp)
- Opened vault door
- Pried open day gate
- Covered light sensor with electrical tape
- Covered Doppler motion sensor with styrofoam (IR sensor already blocked with hairspray)
- Forced open 109 plastic-backed deposit boxes



Antwerp: Feb. 2003

Sunday, Feb. 16
5:00 (approx.)





Antwerp: Feb. 2003

Sunday, Feb. 16
5:00 (approx.)

- Entry into security booth to steal CCTV tapes
- Exit via garage



Police Kiosk

A

Diamond Center

C

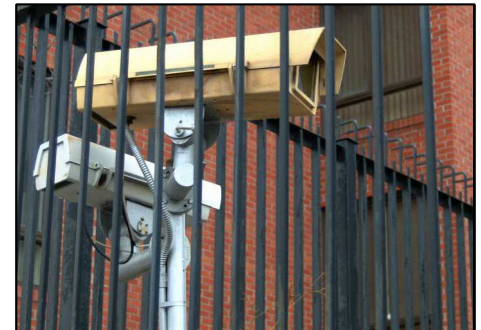
B



\$108 to \$432 million
in Diamonds, Gold, Cash, and other Stored Valuables

Why should DOE care?

- DOE and partnering national security agencies are responsible for analysis, design, and implementation of complex physical security systems to protect high-value assets
- **Are we considering the right threats?**
 - Relying on historical attacks can be problematic if there is a low incidence of such attacks
 - **Are there lessons to be learned from major criminal heists** that will help us protect against future adversaries?



Lesson #1:

There's more than one way to steal \$100 million

Nonviolent Classes



Stealth Raid

Thieves actively circumvent security measures without the knowledge of security forces.



Walk Away

Thieves passively circumvent security measures without the knowledge of security forces.

Violent Classes



Smash and Grab

Employing violence toward property rather than people, thieves seize valuables by relying on the delay between theft detection and security force response.



Subdue and Seize

Via violent means, individuals and/or security systems are controlled or incapacitated prior to seizure of valuables.



Deceive, Subdue, and Seize

A Subdue and Seize event is preceded by a deception or diversion, typically permitting the thieves access that they would not normally have.

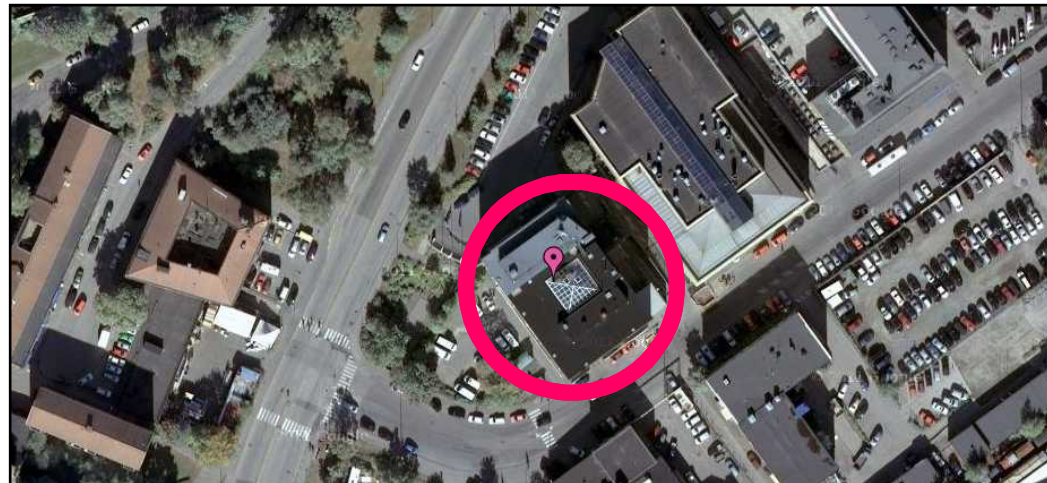


Tiger Kidnapping

A Subdue and Seize event is preceded by a kidnapping, typically of an individual with access and his family, coercing a person with access the thieves need to act as an insider.



Stockholm: September 2009





Stockholm: September 2009





Stockholm: September 2009

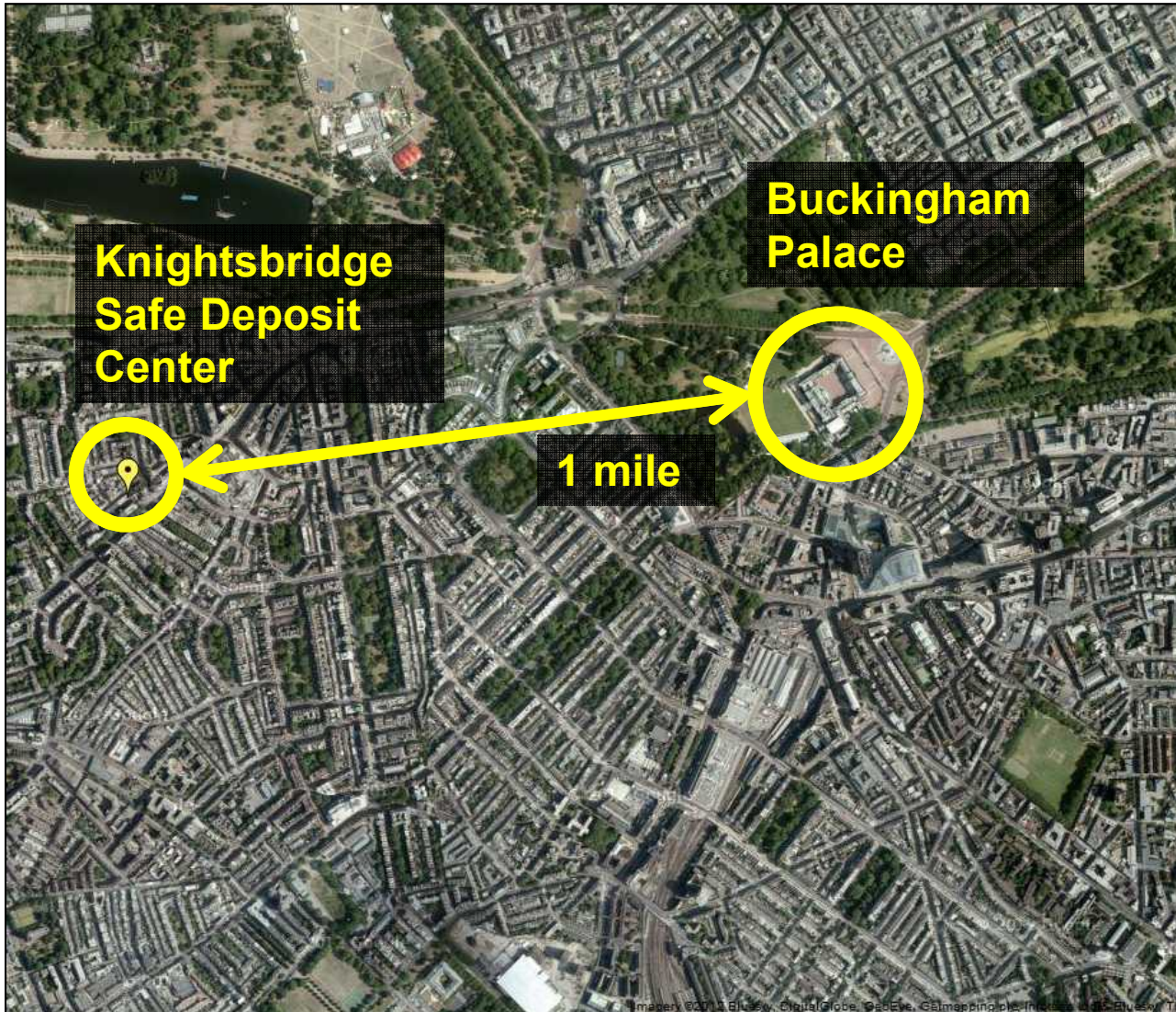


See CCTV footage at:

<http://www.telegraph.co.uk/news/newsvideo/8049390/Seven-convicted-of-spectacular-helicopter-heist.html>



London: July 1987





London: July 1987





London: July 1987

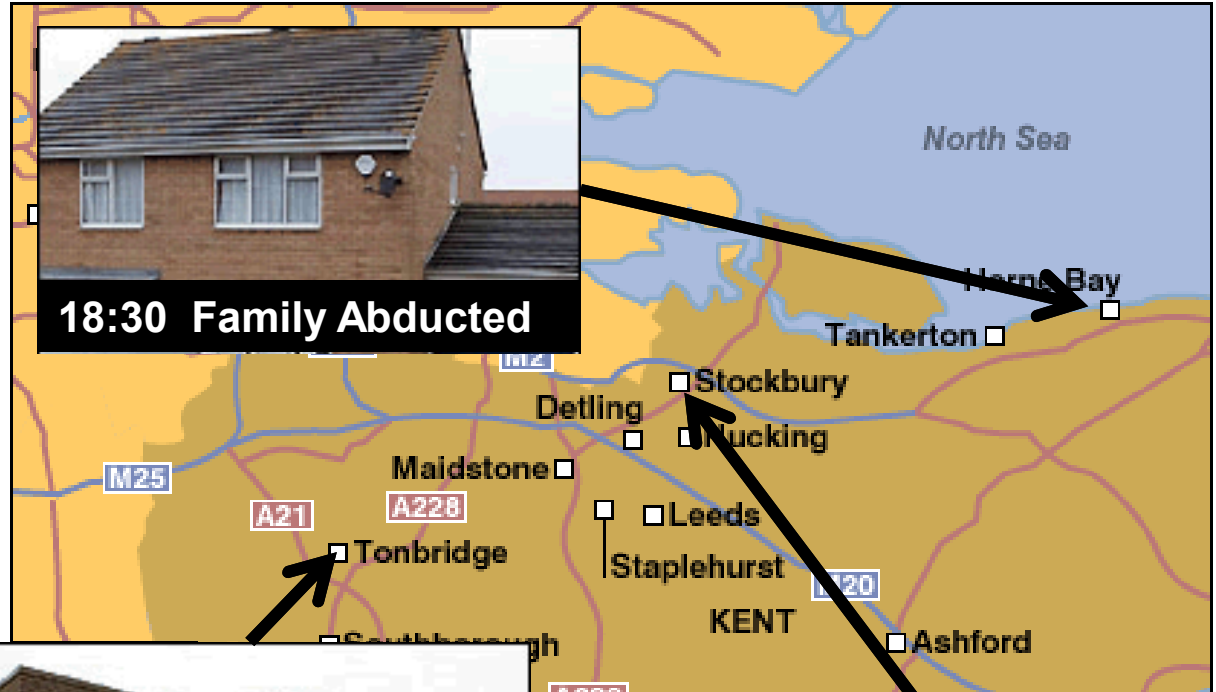


\$130 million

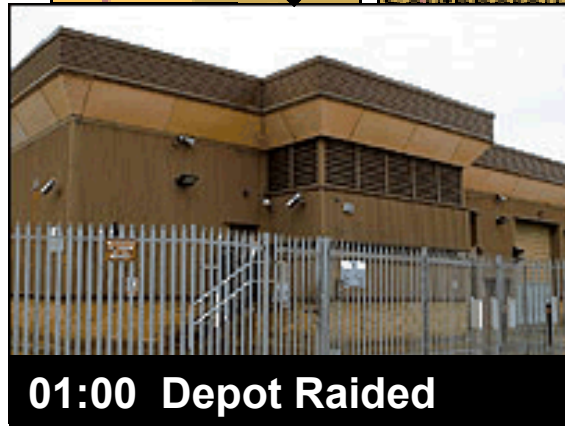
in Diamonds, Gems, Cash, and other Stored Valuables



Tonbridge: February 2006



18:30 Family Abducted



01:00 Depot Raided



18:30 Manager Abducted



Tonbridge: February 2006





Tonbridge: February 2006





Tonbridge: February 2006



6,000 lbs.
of loot

😊 **\$104 million**
in Cash

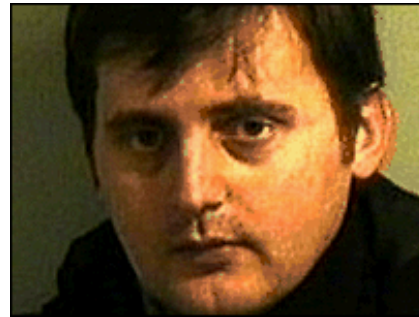




Tonbridge: February 2006

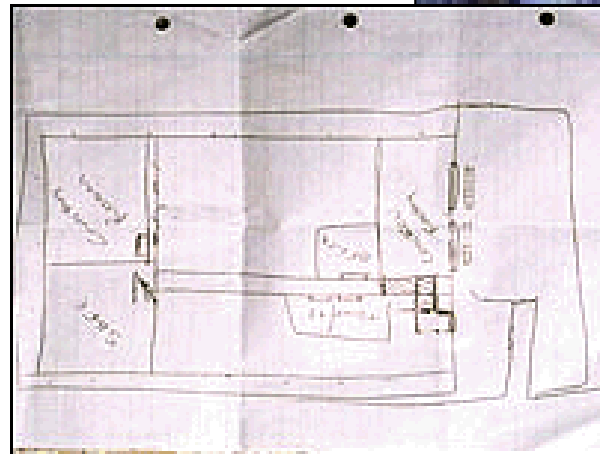


The Inside Man: Ermir Hysenaj



Hysenaj conducting surveillance in plain sight

Hand-drawn plan of the Securitas Depot



Hysenaj uncharacteristically tucked in his shirt on this day to allow unobstructed video footage from his belt camera.

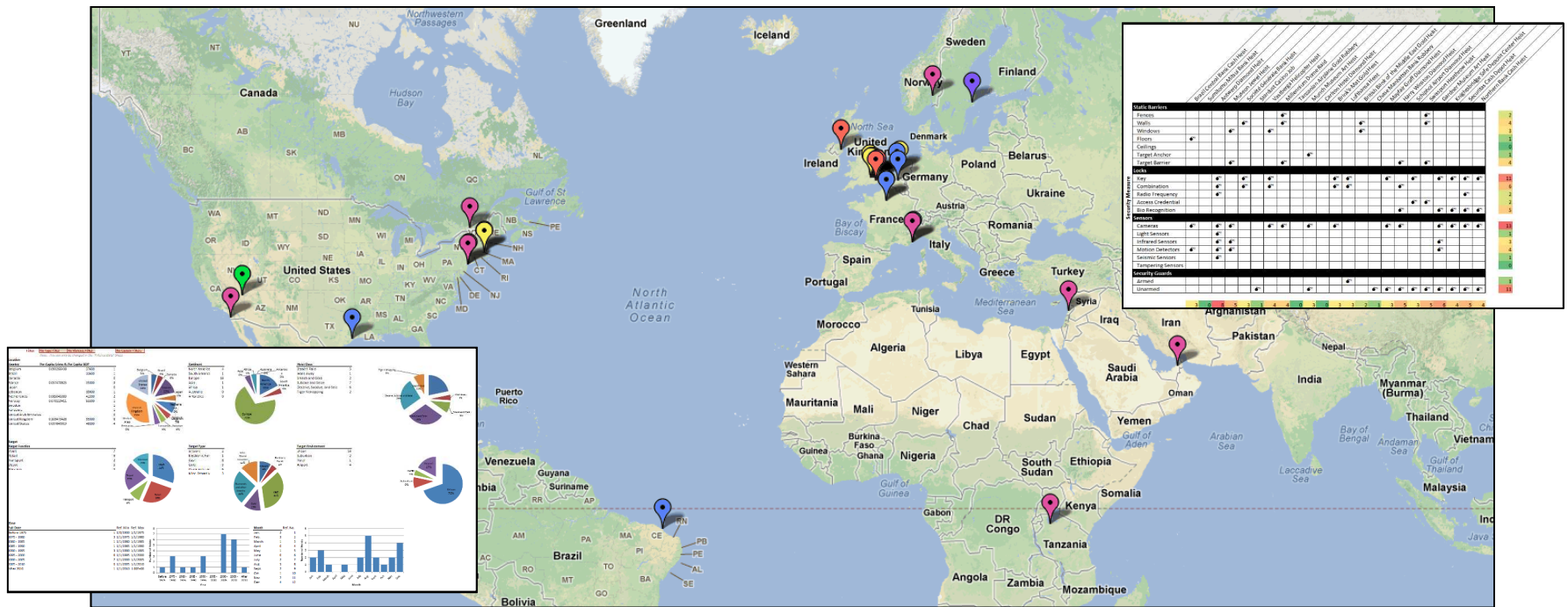
The Heist Database

ID	Name	Date	Location	Category	Success?	Approx. Value of Items Stolen* (\$FY12M)
1	Brazil Central Bank Cash Heist	Sat., Aug. 6, 2005	Fortaleza, Brazil	Stealth Raid	✓	81.9
2	Sumitomo Mitsui Bank Heist	Sat., Oct. 2, 2004	London, UK	Stealth Raid	✓	478.5
3	Antwerp Diamond Heist	Sat., Feb. 15, 2003	Antwerp, Belgium	Stealth Raid	✓	332.1
4	Museon Jewel Heist	Mon., Dec. 2, 2002	The Hague, Netherlands	Stealth Raid	✓	15.4
5	Société Générale Bank Heist	Sat., July 17, 1976	Nice, France	Stealth Raid	✓	40.4
6	Stardust Casino Job	Tues., Sept. 22, 1992	Las Vegas, USA	Walk Away	✓	0.8
7	Vastberga Helicopter Heist	Wed., Sept. 23, 2009	Stockholm, Sweden	Smash and Grab	✓	6.1
8	Millennium Dome Raid	Tues., Nov. 7, 2000	London, UK	Smash and Grab	✓	666.1
9	Tanzanian Airplane Gold Robbery	Thurs., Jan. 5, 2012	Geita, Tanzania	Subdue and Seize	✓	30.5
10	Munch Museum Art Heist	Sun., Aug. 22, 2004	Oslo, Norway	Subdue and Seize	✓	137.9
11	Carlton Hotel Diamond Heist	Thurs., Aug. 11, 1994	Cannes, France	Subdue and Seize	✓	69.3
12	Brink's-Mat Gold Heist	Sat., Nov. 26, 1983	London, UK	Subdue and Seize	✓	85.9
13	Lufthansa Heist	Mon., Dec. 11, 1978	New York, USA	Subdue and Seize	✓	28.2
14	British Bank of the Middle East Gold Heist	Tues., Jan. 20, 1976	Beirut, Lebanon	Subdue and Seize	✓	204.6
15	Chase Manhattan Bank Robbery	Tues., Aug. 22, 1972	New York, USA	Subdue and Seize	✓	1.2
16	Mayfair Graff Diamond Heist	Thurs., Aug. 6, 2009	London, UK	Deceive, Subdue, and Seize	✓	68.9
17	Harry Winston Diamond Heist	Thurs., Dec. 4, 2008	Paris, France	Deceive, Subdue, and Seize	✓	111.3
18	Schiphol Airport Diamond Heist	Fri., Feb. 25, 2005	Amsterdam, Netherlands	Deceive, Subdue, and Seize	✓	115.8
19	Swissport Heathrow Heist	Mon., May 17, 2004	London, UK	Deceive, Subdue, and Seize	✓	71.1
20	Gardner Museum Art Heist	Sun., March 18, 1990	Boston, USA	Deceive, Subdue, and Seize	✓	440.0
21	Knightsbridge Safe Deposit Center Heist	Sun., July 12, 1987	London, UK	Deceive, Subdue, and Seize	✓	130.0
22	Securitas Cash Depot Heist	Tues., Feb. 21, 2006	Tonbridge, UK	Tiger Kidnapping	✓	104.0
23	Northern Bank Cash Heist	Sun., Dec. 19, 2004	Belfast, UK	Tiger Kidnapping	✓	60.5



The Heist Database

- Heist Methods & Characteristics Database (HMCD) consists of:
 - 152 data fields per heist
 - 23 heists completely characterized heists (3,496 entries)
 - 11 additional heists partially characterized (excluded from this analysis)



<https://www.google.com/maps/ms?msid=206565135619449682207.0004be5da3a6089e3d9c5&msa=0>

Study Objectives

- Through qualitative and quantitative analysis, characterize the landscape of high-value criminal heists
 - Describe the **range and diversity of criminal methods** utilized in large heists, both qualitatively and quantitatively
 - Identify **characteristics that are common** (or uncommon) to large heists
- In framing the problem and discussion, focus on:
 - Defeated security measures and devices
 - Deception methods
 - Timing and target selection
 - Weapons employed
 - Resources and risk acceptance
 - Insider information and actions
 - Failures and mistakes

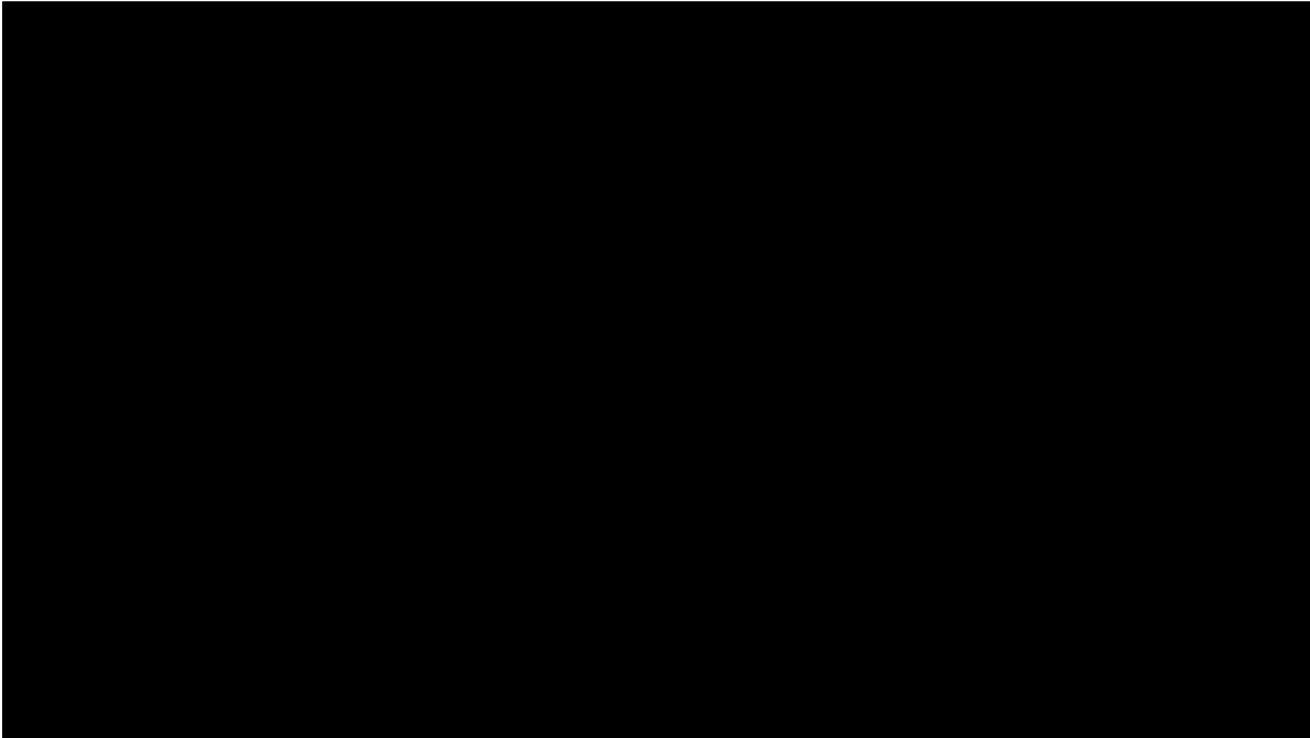
**Today's
Presentation**

DEFEATED SECURITY MEASURES AND DEVICES

The vault was reputed to be very nearly impregnable, and it was very difficult to see how anybody could just walk up and go and lift the diamonds out of it.

David James
Former Millennium Dome Chairman

DEFEATED SECURITY MEASURES AND DEVICES

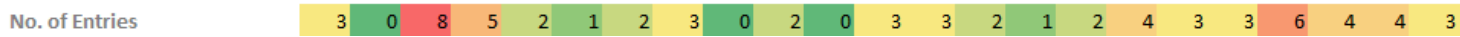
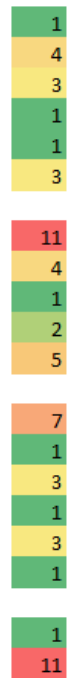
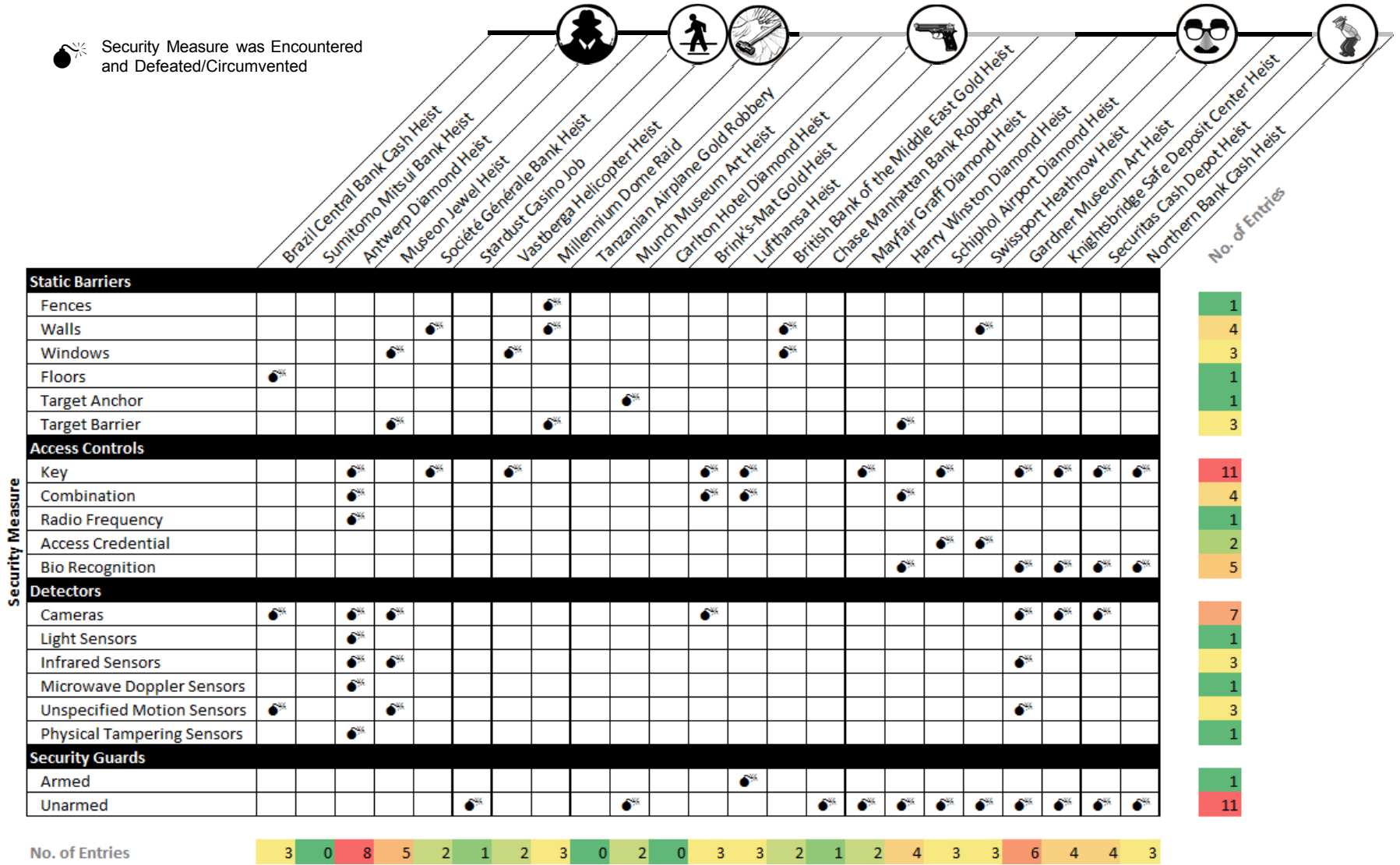


How
e

James
Irman

Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented



Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented

- Brazil Central Bank Cash Heist
- Sumitomo Mitsui Bank Heist
- Antwerp Diamond Heist
- Museon Jewel Heist
- Soci t  G n rale Bank Heist
- Stardust Casino Job
- Vastberga Helicopter Heist
- Millennium Dome
- Tanzania

SMASH AND GRAB

Failed

Millennium Dome Raid

Tues., Nov. 7, 2000, at 10:38
London, United Kingdom
51.50299°N, 0.00315°E

Target: The Millennium Dome
Stolen: \$666.1 million in diamonds (attempted)
Heist Duration: 15 min.

Static Barriers									
Fences									
Walls									
Windows									
Floors									
Target Anchor									
Target Barrier									

Security Measure

Access Controls									
Key									
Combination									
Radio Frequency									
Access Credential									
Bio Recognition									
Detectors									
Cameras									
Light Sensors									
Infrared Sensors									
Microwave Doppler Sensor									
Unspecified Motion Sensor									
Physical Tampering Sensor									
Security Guards									
Armed									
Unarmed									

STEALTH RAID

Successful

Brazil Central Bank Cash Heist

Sat., Aug. 6, 2005, at 04:00
Fortaleza, Brazil
3.734031°S, 38.522256°W

Target: Central Bank Vault
Stolen: \$81.9 million in cash
Heist Duration: Up to 30 hrs.

					11
					4
					1
					2
					5
					7
					1
					3
					1
					3
					1
					11

No. of Entries

3 6 4 4 3

Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented



Security Measure

Static Barriers		Access Controls		Detectors		Security Guards	
Fences							
Walls							
Windows							
Floors							
Target Anchor							
Target Barrier							
Key							
Combination							
Radio Frequency							
Access Credential							
Bio Recognition							
Cameras							
Light Sensors							
Infrared Sensors							
Microwave Doppler Sensors							
Unspecified Motion Sensors							
Physical Tampering Sensors							
Armed							
Unarmed							

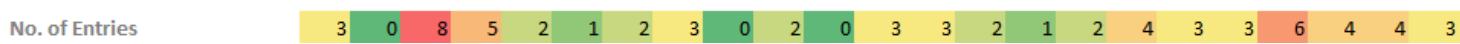
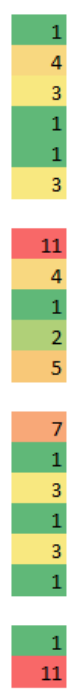
STEALTH RAID

Successful

Antwerp Diamond Heist

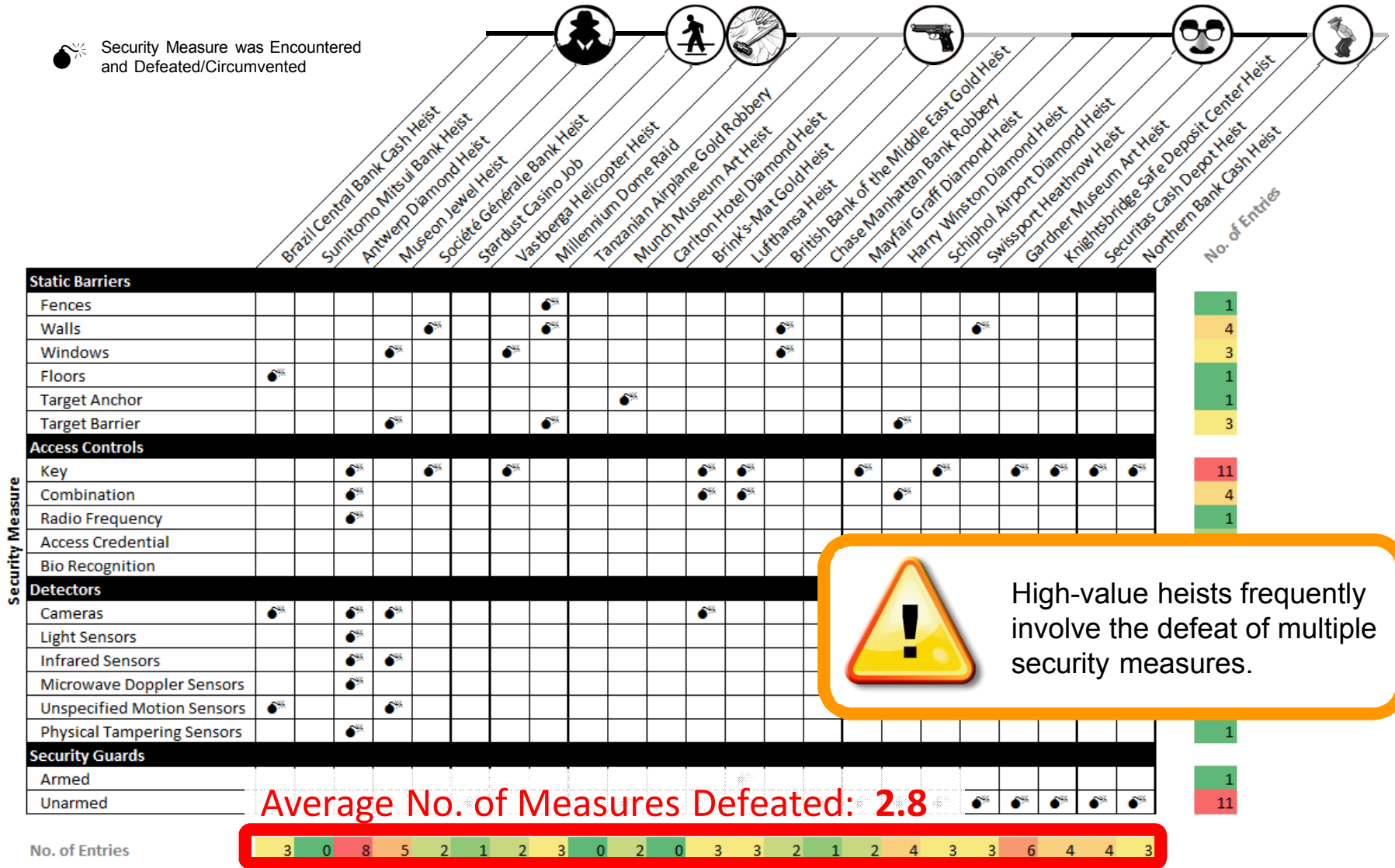
Sat., Feb. 15, 2003, at 23:50
Antwerp, Belgium
51.51393°N, 4.41805°E

Target: Diamond Center Vault
Stolen: \$332.1 million in diamonds and stored valuables
Heist Duration: 5 hrs. (approx.)



Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented

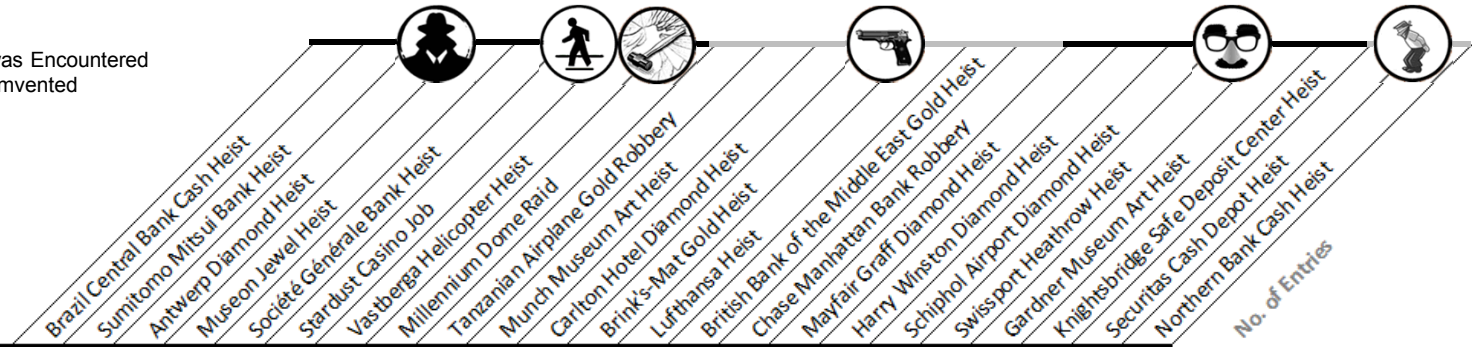


High-value heists frequently involve the defeat of multiple security measures.

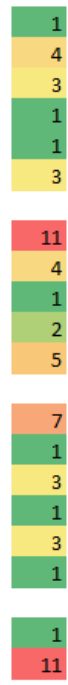
Average No. of Measures Defeated: 2.8

Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented



Security Measure	Brazil Central Bank Cash Heist	Sumitomo Mitsui Bank Heist	Antwerp Diamond Heist	Museon Jewel Heist	Societe Generale Bank Heist	Stardust Casino Job	Vastberga Helicopter Heist	Millennium Dome Heist	Tanzanian Airplane Gold Heist	Munich Museum Art Heist	Carlton Hotel Diamond Heist	Brink's-Mat Gold Heist	Lufthansa Heist	British Heist	Chase Manhattan Bank Robbery	Mayfair Graff Diamond Heist	Harry Winston Bank Robbery	Schiphol Airport Diamond Heist	Swissport Airport Diamond Heist	Gardner Heathrow Heist	Knightsbridge Safe Heist	Securitas Cash Depot Heist	Northern Bank Cash Heist	
Static Barriers																								
Fences																								
Walls																								
Windows																								
Floors																								
Target Anchor																								
Target Barrier																								
Access Controls																								
Key																								
Combination																								
Radio Frequency																								
Access Credential																								
Bio Recognition																								
Detectors																								
Cameras																								
Light Sensors																								
Infrared Sensors																								
Microwave Doppler Sensors																								
Unspecified Motion Sensors																								
Physical Tampering Sensors																								
Security Guards																								
Armed																								
Unarmed																								

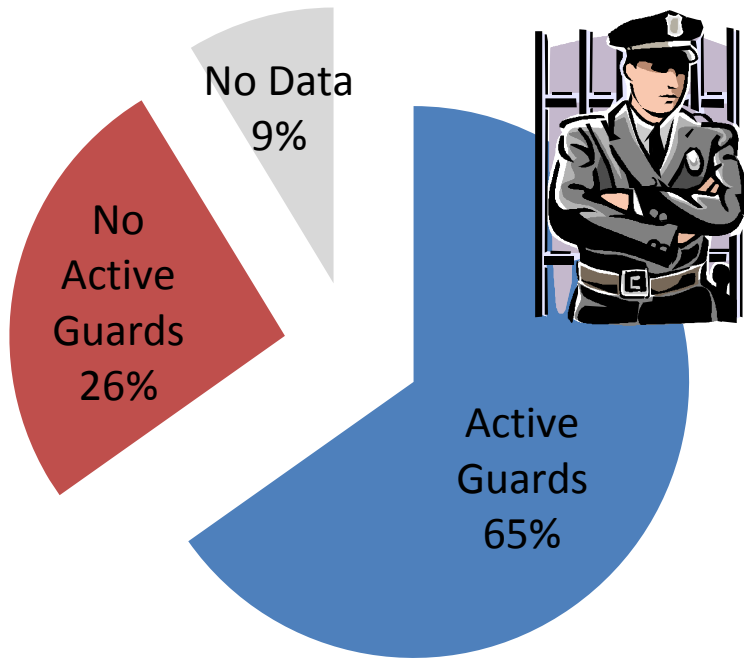


No. of Entries: 3 0 8 5 2 1 2 3 0 2 0 3 3 2 1 2 4 3 3 6 4 4 4 3

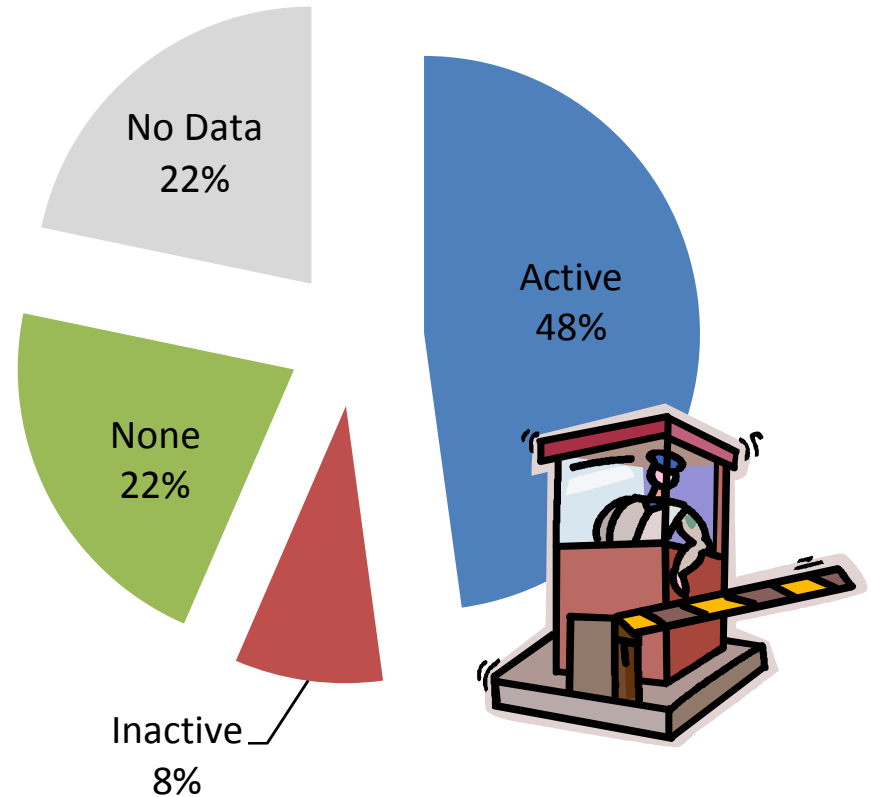
Defeated Security Measures

Security Guards

Existence of Active Guards at Target Premises During Heists



Status of Guard Stations at Target Premises During Heists



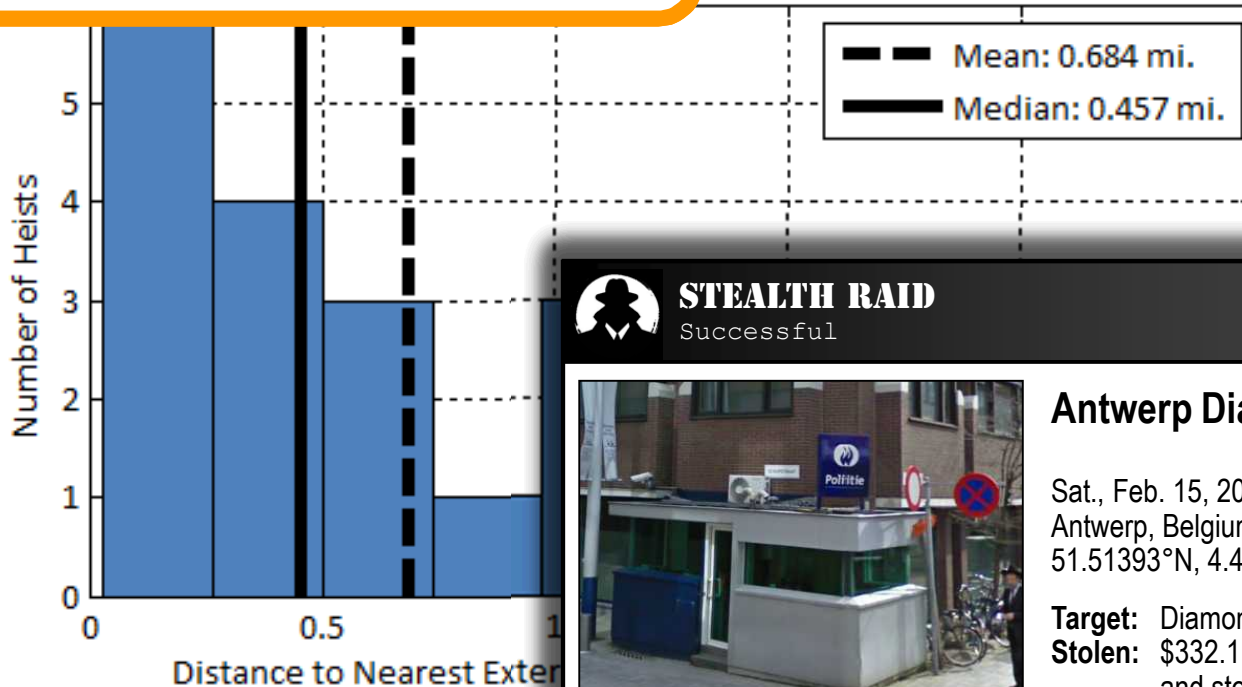
Defeated Security Measures

Security Guards



Close proximity of security forces is not a sufficient condition for protecting high-value assets.

Nearest or Police Station



STEALTH RAID
Successful

Antwerp Diamond Heist

Sat., Feb. 15, 2003, at 23:50
Antwerp, Belgium
51.51393°N, 4.41805°E

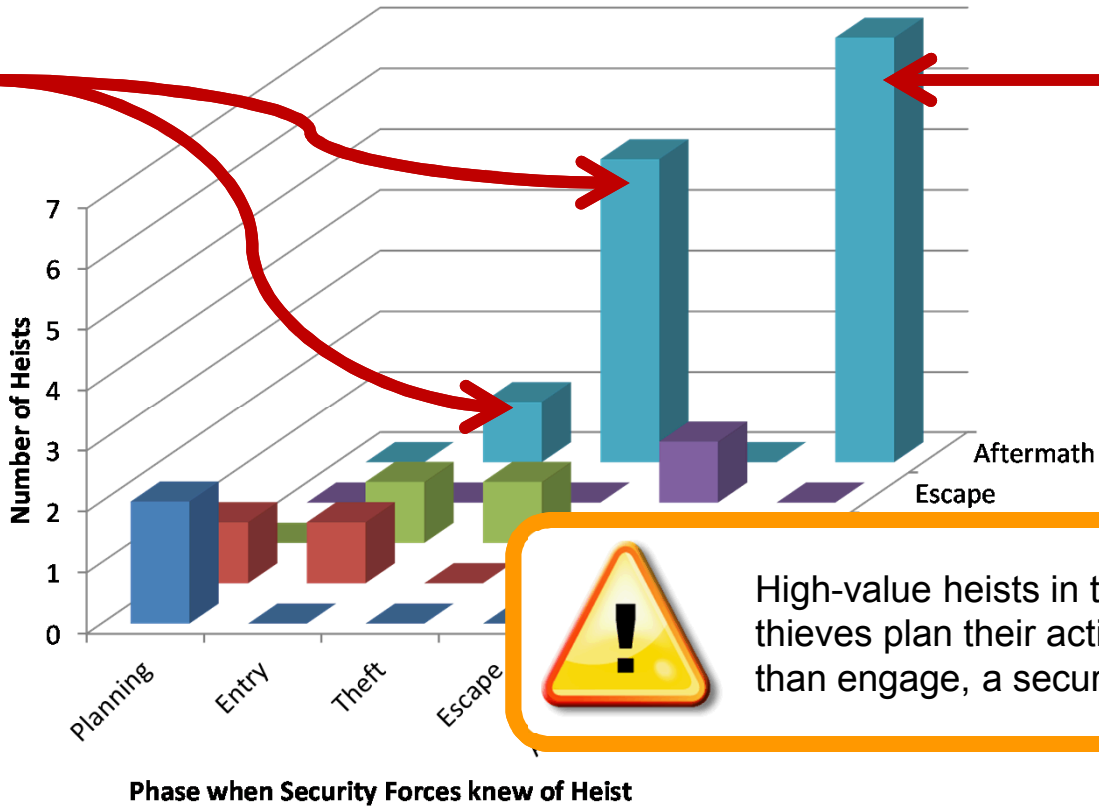
Target: Diamond Center Vault
Stolen: \$332.1 million in diamonds and stored valuables
Heist Duration: 5 hrs. (approx.)

Defeated Security Measures

Security Guards



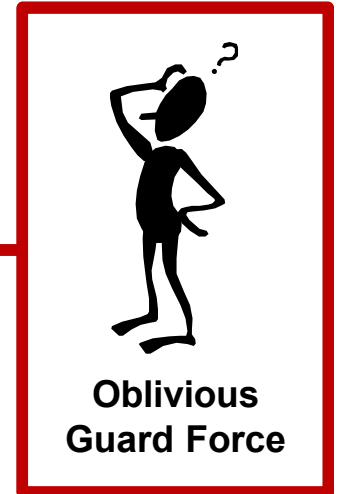
Distribution of Heist Knowledge-Response Profiles



High-value heists in the database suggest thieves plan their activities to avoid, rather than engage, a security response.

Defeated Security Measures

Security Guards

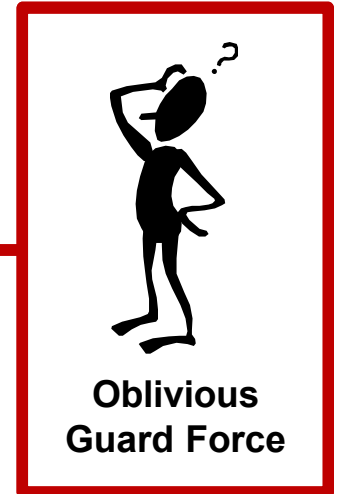


ermath

ts in the database suggest
ir activities to avoid, rather
security response.

Defeated Security Measures

Security Guards



rmath

s in the database suggest
r activities to avoid, rather
security response.

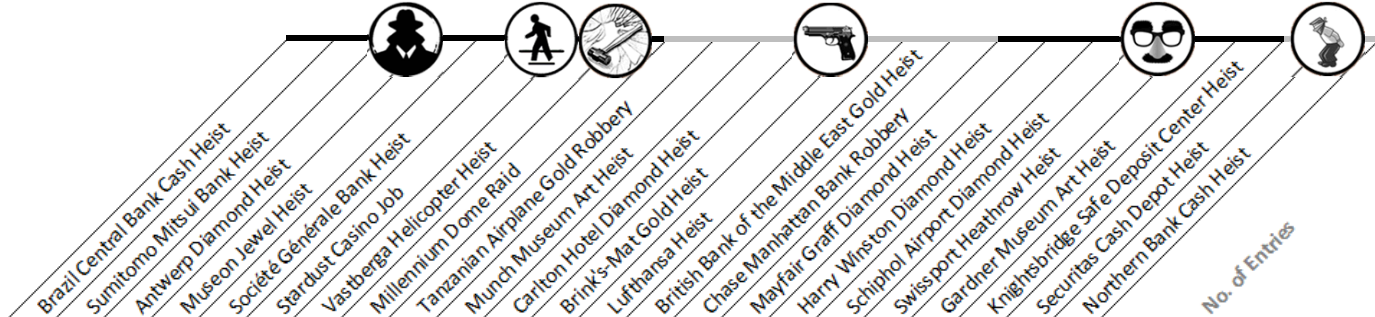
DECEPTION METHODS

The criminal plan of the thieves, using the two bogus police officers to enter the Gardner Museum, was quite simple and quite easily executed. The Gardner Museum could have been as secure as Fort Knox, but that does no good if the guard is going to let the thief in.

Robert Spiel
Art Theft Investigator

Deception Methods

Deception Method was Employed



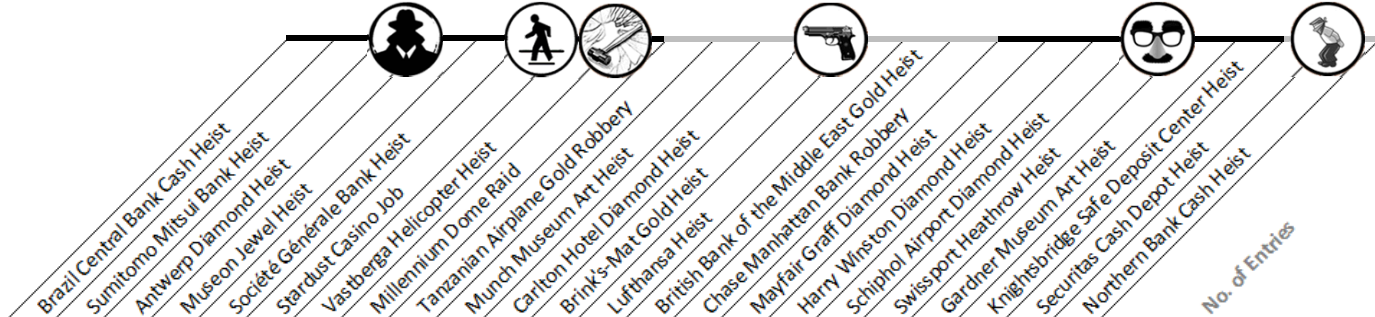
Deception Methods	No. of Entries																						
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20			
Physical Disguises																							
Disguise of Thief-Possessed Buildings/Rooms	●	●																					
Disguise of Theft in Progress				●									●						●				
Vehicles that Blend with Surroundings	●	●	●			●		●		●	●			●	●	●	●		●	●			
Disguised/Concealed Surveillance Equipment		●																	●				
Disguised/Concealed Operations Equipment	●	●	●						●				●	●	●	●			●	●			
Physical Disguise or Concealment of Loot	●					●								●						●			
Disguised Age or Gender														●	●								
Disguised Other Physical Features	●					●	●		●	●	●	●					●	●	●	●			
Activity Disguises																							
Disarming Personality or Reputation	●		●	●															●				
Blending in by Occupation	●	●	●	●	●						●	●	●				●	●	●	●			
Exertion of Perceived Legitimate Authority												●	●		●		●	●	●	●			
Diversions																							
Personal Distractions																			●				
Relay of Stolen Goods		●													●								
Decoy Vehicle or Device						●						●			●								
Exploitation of Tensions												●											
No. of Entries																							
	7	3	6	0	4	2	1	2	0	2	2	3	5	1	2	5	3	4	4	2	8	6	4

Color-coded legend for No. of Entries:

- 2 (Green)
- 3 (Yellow)
- 13 (Red)
- 2 (Light Green)
- 10 (Orange)
- 4 (Yellow)
- 2 (Light Green)
- 12 (Red)
- 4 (Yellow)
- 13 (Red)
- 8 (Orange)
- 1 (Green)
- 2 (Light Green)
- 3 (Yellow)
- 1 (Green)

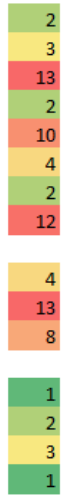
Deception Methods

Deception Method was Employed



Deception Methods

Deception Method	Brazil Central Bank Cash Heist	Sumitomo Mitsui Bank Heist	Antwerp Diamond Heist	Museon Jewel Heist	Société Générale Bank Heist	Stardust Casino Job	Vastberga Helicopter Heist	Millennium Dome Raid	Tanzanian Airplane Gold Heist	Munich Museum Art Heist	Carlton Hotel Diamond Heist	Brink's-Mat Gold Heist	Lufthansa Heist	British Bank of the Middle East Gold Heist	Chase Manhattan Bank Robbery	Mayfair Graff Diamond Heist	Harry Winston Bank Robbery	Schiphol Airport Diamond Heist	Swissport Airport Diamond Heist	Gardner Heathrow Heist	Knightsbridge Safe Heist	Securitas Cash Depot Heist	Northern Bank Cash Heist	
Physical Disguises																								
Disguise of Thief-Possessed Buildings/Rooms																								
Disguise of Theft in Progress																								
Vehicles that Blend with Surroundings																								
Disguised/Concealed Surveillance Equipment																								
Disguised/Concealed Operations Equipment																								
Physical Disguise or Concealment of Loot																								
Disguised Age or Gender																								
Disguised Other Physical Features																								
Activity Disguises																								
Disarming Personality or Reputation																								
Blending in by Occupation																								
Exertion of Perceived Legitimacy																								
Diversions																								
Personal Distractions																								
Relay of Stolen Goods																								
Decoy Vehicle or Device																								
Exploitation of Tensions																								



No. of Entries



STEALTH RAID
Successful



Brazil Central Bank Cash Heist

Sat., Aug. 6, 2005, at 04:00
Fortaleza, Brazil
3.734031°S, 38.522256°W

Target: Central Bank Vault
Stolen: \$81.9 million in cash
Heist Duration: Up to 30 hrs.

Deception Methods

Deception Method was Employed

Physical Disguises

- Disguise of Thief-Possessed Buildings/Rooms
- Disguise of Theft in Progress
- Vehicles that Blend with Surroundings
- Disguised/Concealed Surveillance Equipment
- Disguised/Concealed Operations Equipment
- Physical Disguise or Concealment of Loot
- Disguised Age or Gender
- Disguised Other Physical Features

Activity Disguises

- Disarming Personality or Reputation
- Blending in by Occupation
- Exertion of Perceived Legitimacy

Diversions

- Personal Distractions
- Relay of Stolen Goods
- Decoy Vehicle or Device
- Exploitation of Tensions

Deception Methods

No. of Entries

TIGER KIDNAPPING

Successful

Securitas Cash Depot Heist

Tues., Feb. 21, 2006, at 18:30
 Tonbridge, United Kingdom
 51.191098°N, 0.277652°E

Target: Securitas Depot
Stolen: \$104 million in cash
Heist Duration: 7.8 hours

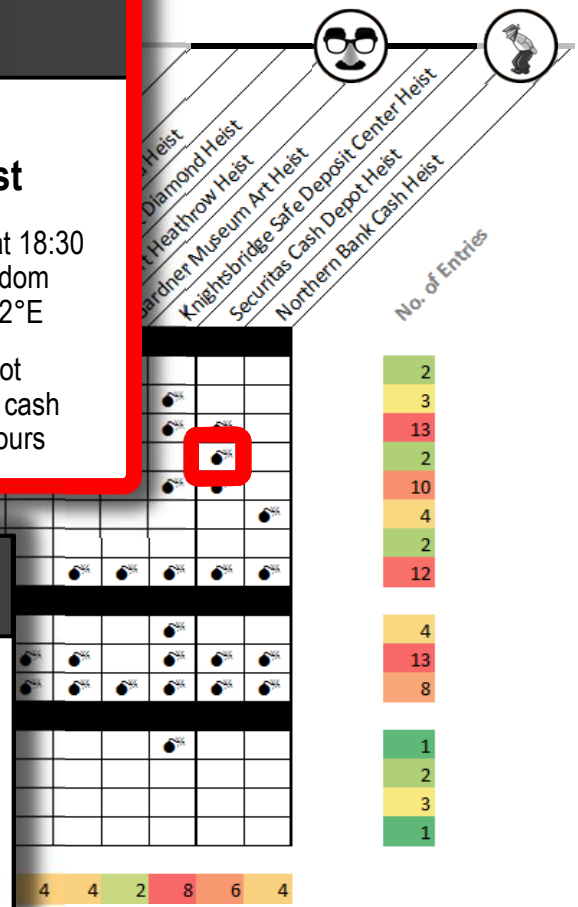
STEALTH RAID

Successful

Brazil Central Bank Cash Heist

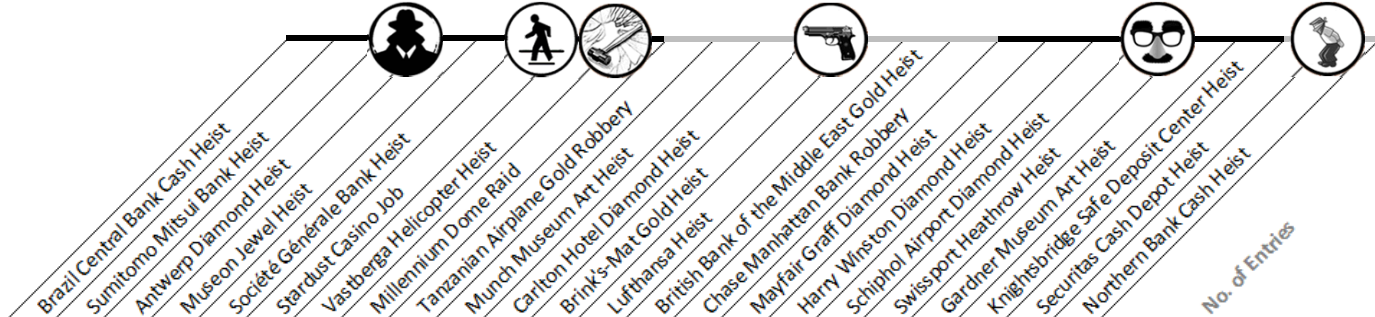
Sat., Aug. 6, 2005, at 04:00
 Fortaleza, Brazil
 3.734031°S, 38.522256°W

Target: Central Bank Vault
Stolen: \$81.9 million in cash
Heist Duration: Up to 30 hrs.

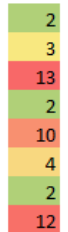


Deception Methods

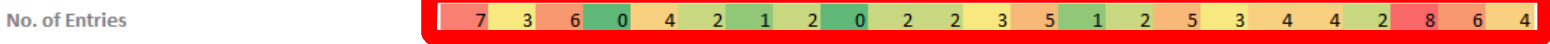
Deception Method was Employed



Deception Methods	No. of Entries															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Physical Disguises																
Disguise of Thief-Possessed Buildings/Rooms	●	●														
Disguise of Theft in Progress				●						●					●	
Vehicles that Blend with Surroundings	●	●	●		●	●				●	●	●	●		●	●
Disguised/Concealed Surveillance Equipment		●													●	
Disguised/Concealed Operations Equipment	●	●	●				●			●	●	●	●		●	●
Physical Disguise or Concealment of Loot	●				●					●						●
Disguised Age or Gender										●	●					
Disguised Other Physical Features	●				●	●		●	●	●				●	●	●
Activity Disguises																
Disarming Personality or Reputation	●		●	●												
Blending in by Occupation	●	●	●	●	●											
Exertion of Perceived Legitimate Authority																
Diversions																
Personal Distractions																
Relay of Stolen Goods		●														
Decoy Vehicle or Device					●											
Exploitation of Tensions																



Almost all heists (91%) involved some identifiable use of deception. Many (83%) utilized multiple types of deceptions.



RESOURCES AND RISK ACCEPTANCE



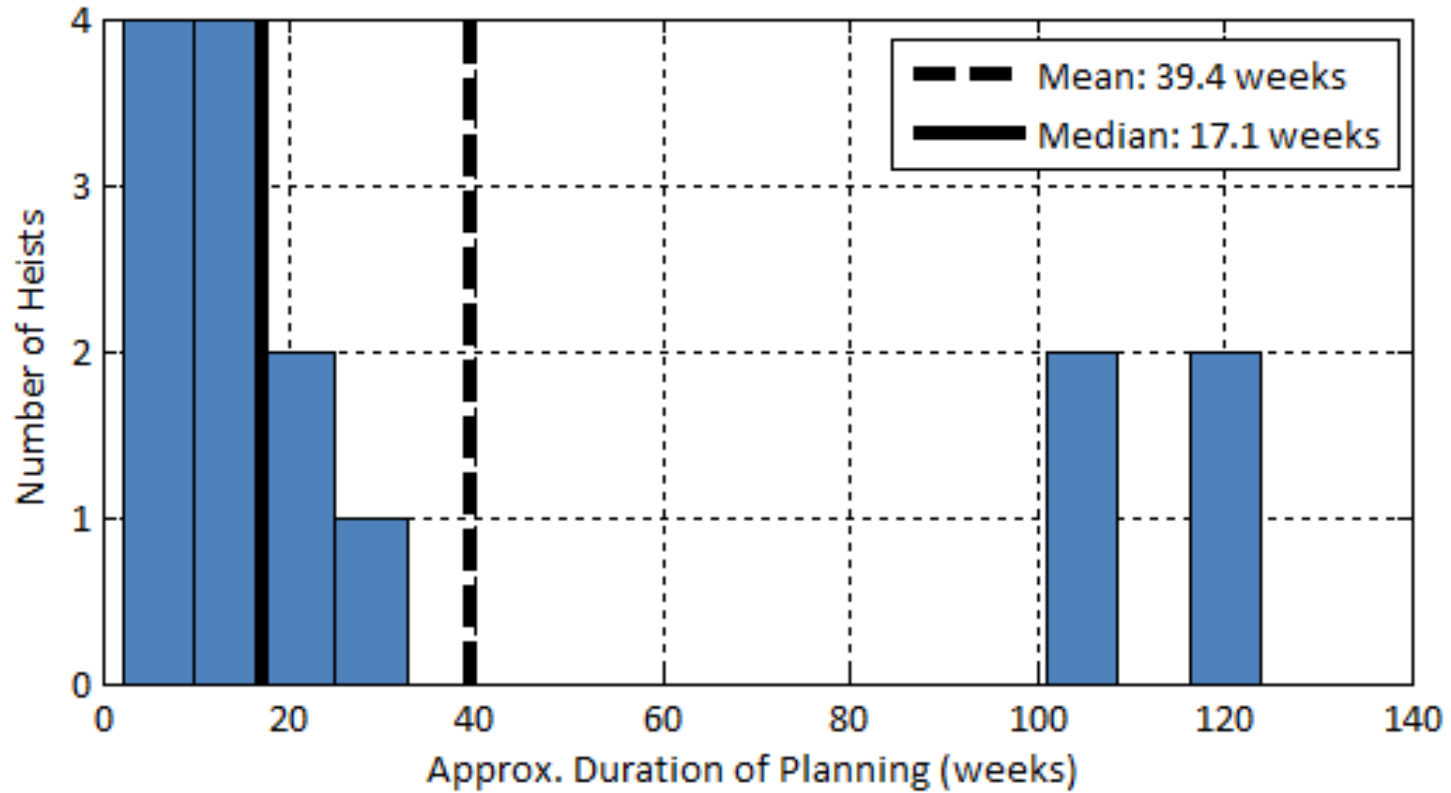
Thieves of high-value items are often a lot like us: Ambitious, disciplined, and good systems engineers and project managers.

It's like a big challenge, like Olympic games. You train for most part of your life, and go that day hoping to have an opportunity.

Valerio Viccei, Criminal
Knightsbridge Safe Deposit Center Heist

Resources and Risk Acceptance Schedule

Thief Planning Time



Resources and Risk Acceptance Schedule



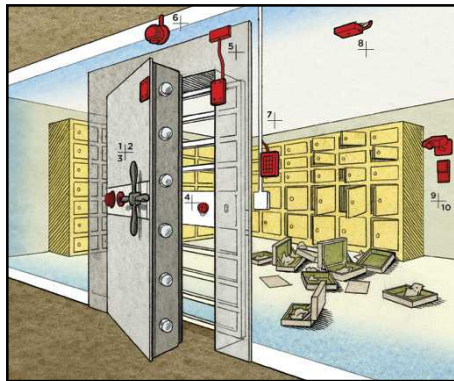
Thieves do their homework and typically take months or years to plan a high-value heist.

Planning Time



STEALTH RAID
Successful

123 weeks



Antwerp Diamond Heist

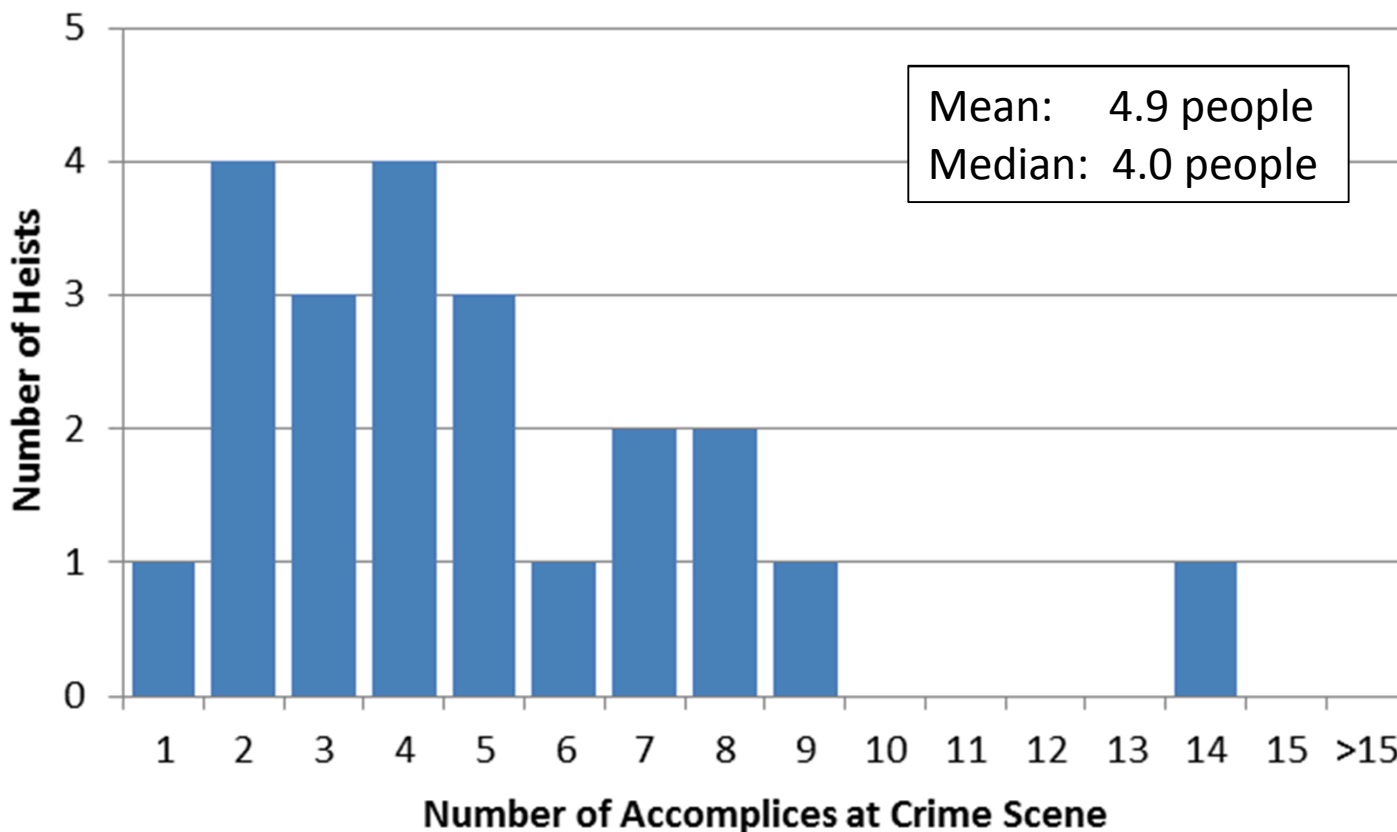
Sat., Feb. 15, 2003, at 23:50
Antwerp, Belgium
51.51393°N, 4.41805°E

Target: Diamond Center Vault
Stolen: \$332.1 million in diamonds and stored valuables
Heist Duration: 5 hrs. (approx.)

Resources and Risk Acceptance

Human Resources

Accomplices at Crime Scene



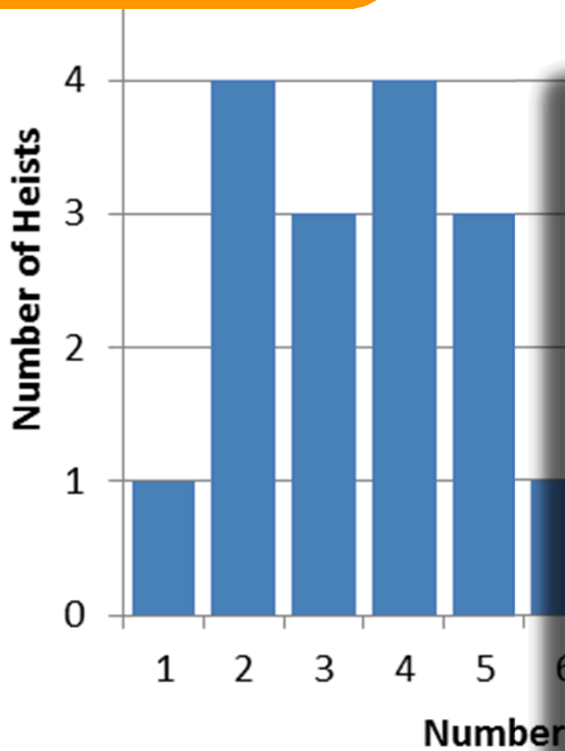
Resources and Risk Acceptance

Human Resources

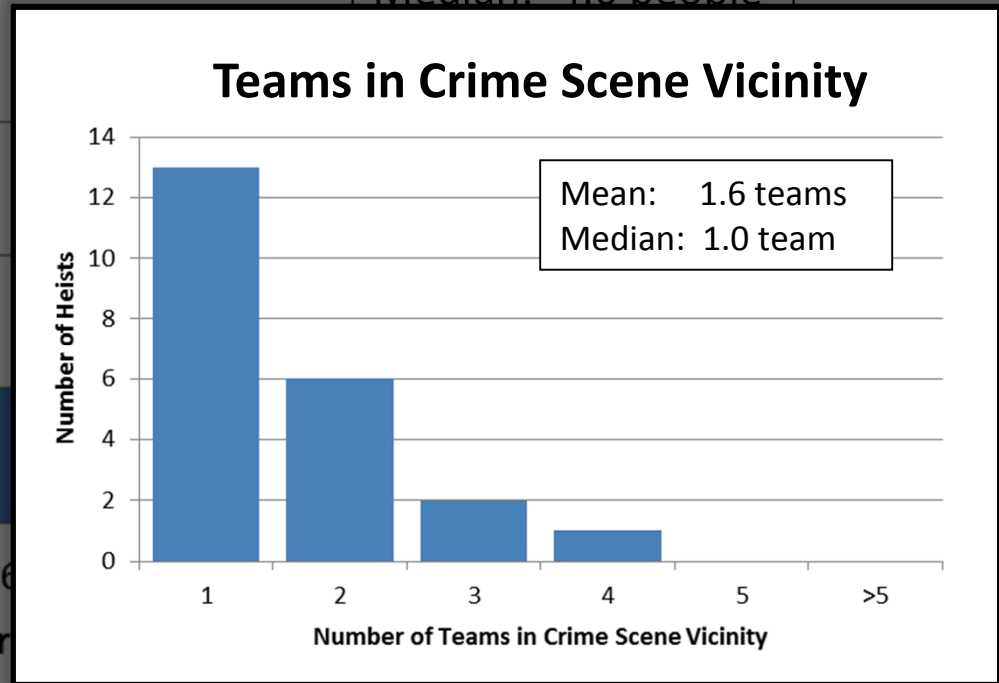


Thieves need the ability to work well in small teams.

Accomplices at Crime Scene



Mean: 4.9 people
Median: 4.0 people

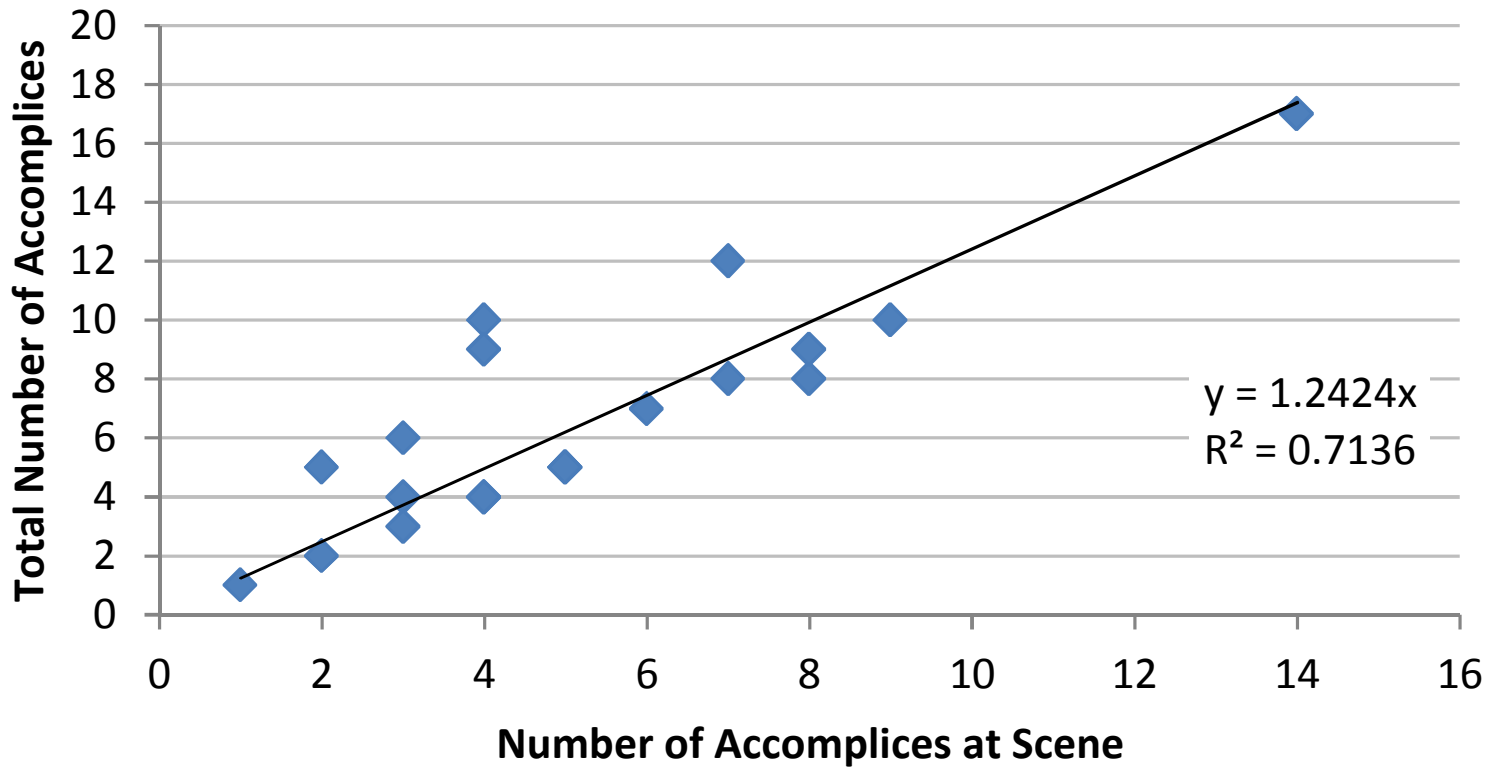


Mean: 1.6 teams
Median: 1.0 team

Resources and Risk Acceptance

Human Resources

Crime Scene Participation Rate



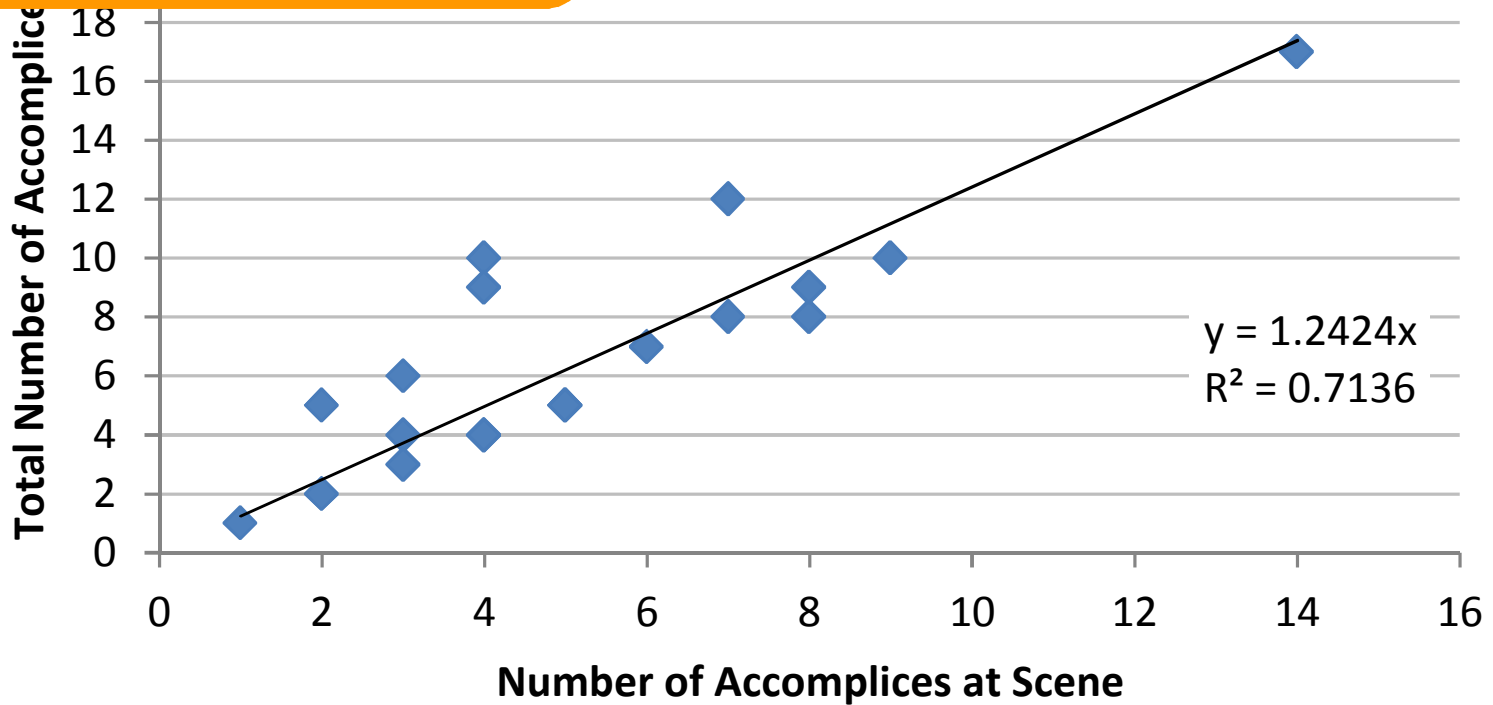
Resources and Risk Acceptance

Human Resources



Thief operations are almost always supported by a larger team effort.

Scene Participation Rate



Resources and Risk Acceptance

Human Resources

Thief Level of Effort

A Back of the Envelope Calculation

- 39.4 weeks planning time (average)
- × 7.0 days/week
- × 4.9 accomplices at scene (average)
- × 1.2 total accomplices / accomplice at scene (average)
- ÷ 365 days/year

4.4 person-years of effort



Thieves put substantial effort into planning high-value heists.

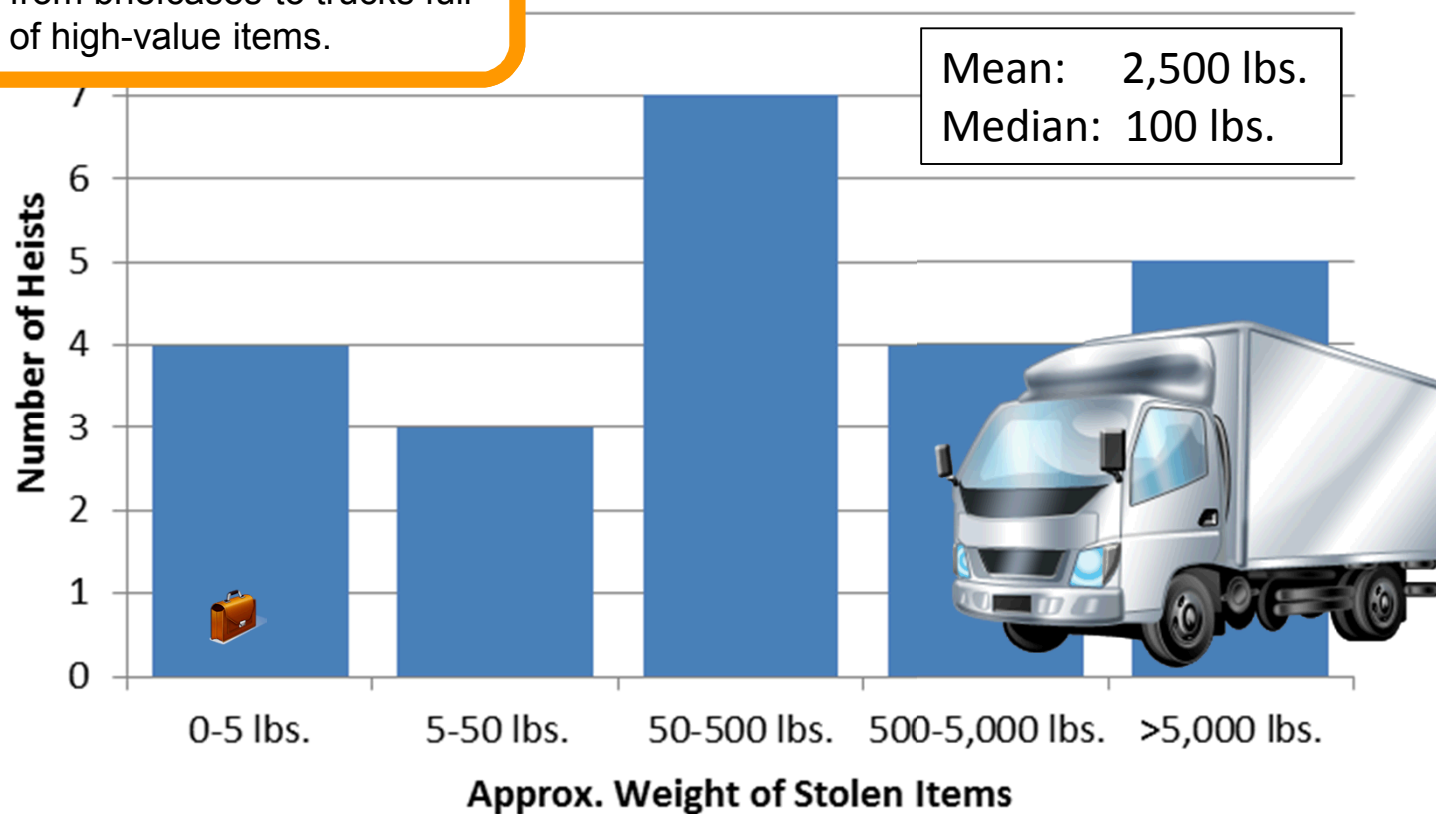
Resources and Risk Acceptance

Mass Properties



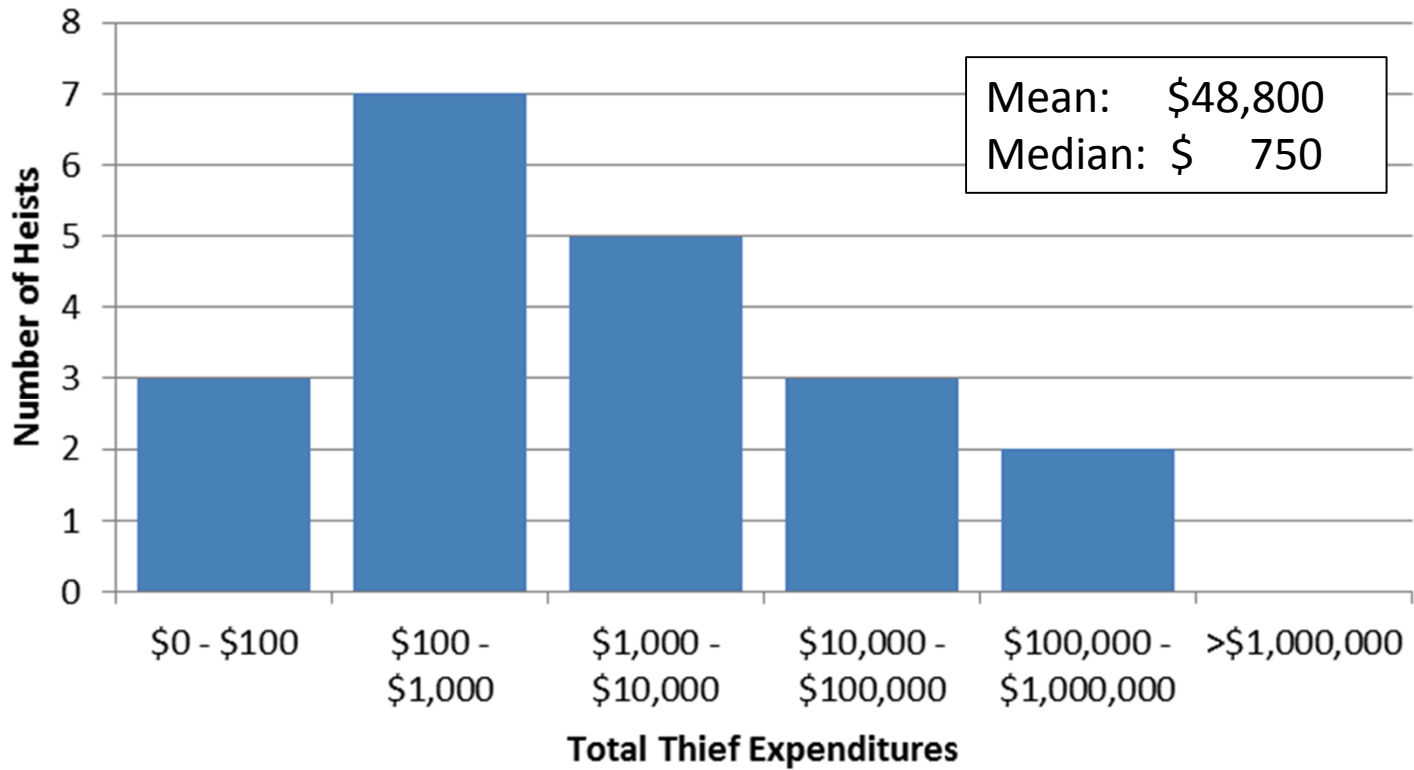
Thieves have demonstrated capabilities to steal anything from briefcases to trucks full of high-value items.

Weight of Stolen Items




Resources and Risk Acceptance Budget

Estimated Thief Expenditures



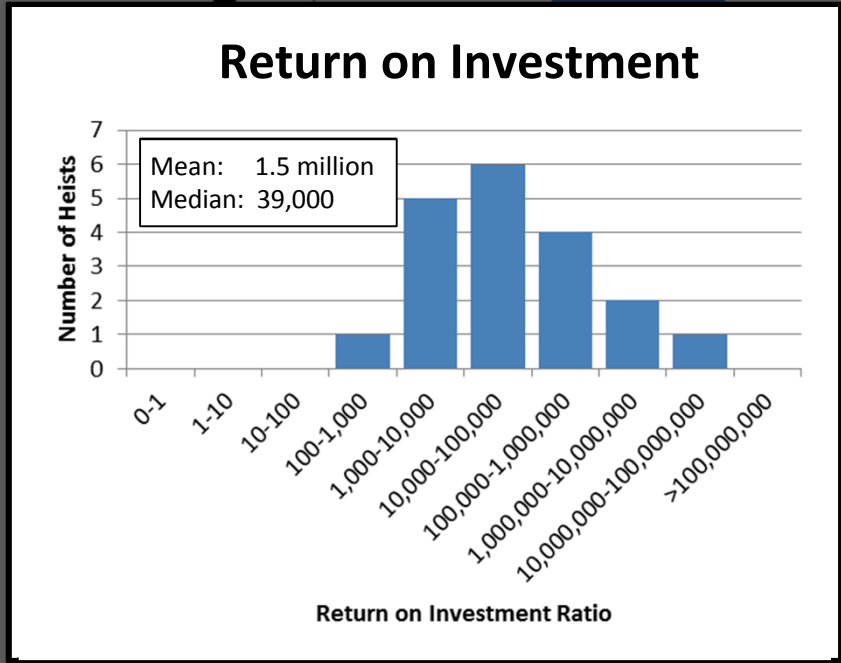
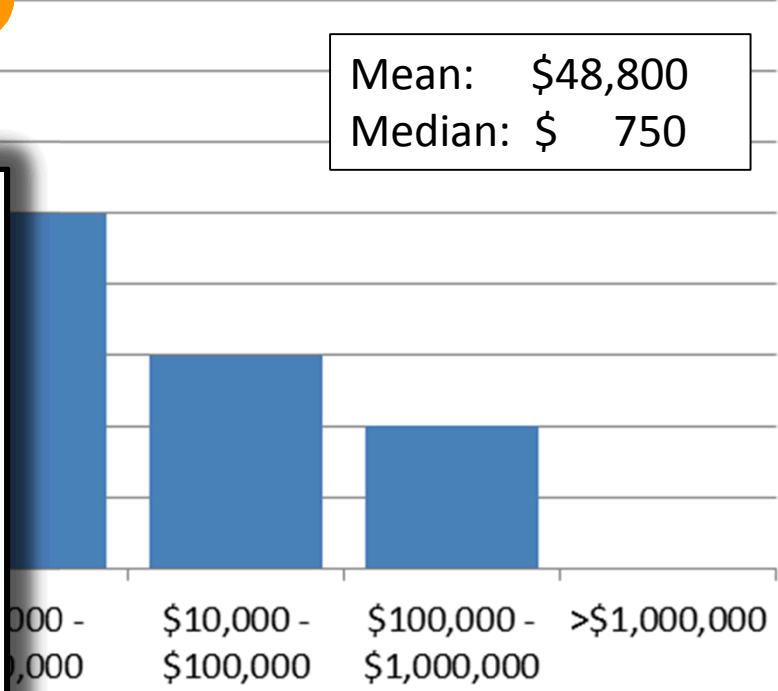
Resources and Risk Acceptance Budget



Thieves are willing to invest large amounts of money in planning and preparation, justified in part by the probable financial returns.

Thief Expenditures

Mean: \$48,800
Median: \$ 750

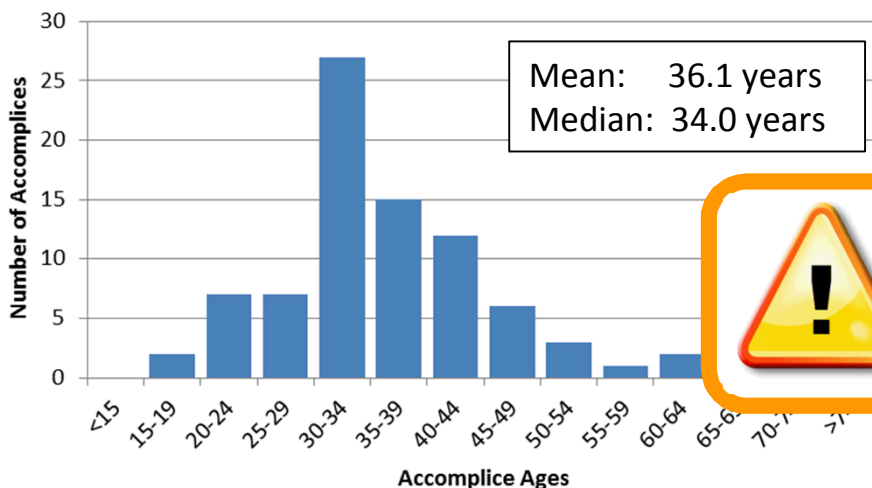


Thief Expenditures

Resources and Risk Acceptance

Recruiting

Accomplice Age



Accomplice Gender

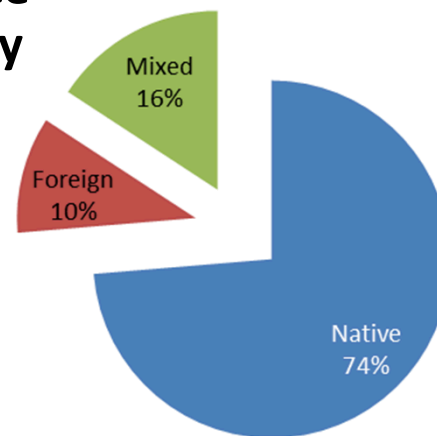
n = 133

Female
0%



The typical high-value item thief is a 36-year-old man who is native to the country that is home to the asset he intends to steal.

Accomplice Nationality



Comparing to the general population:

U.S. Arrestee Average Ages, 2001:

Motor Vehicle Theft:	24.4
Robbery:	25.3
Burglary:	25.3
Stolen Property:	26.9
Weapons Violations:	27.0
Violent Crime:	29.6
Forgery/Counterfeiting:	30.6
Fraud:	32.3

Average high-value heist criminal is closer in age to that of the average fraud or forgery, rather than robbery or burglary, criminal.

Resources and Risk Acceptance

Risk Assessment

- Risks of capture and death to a thief can be quite high for an attack executed with minimal planning, but can be bought down with:
 - Reconnaissance, often with insiders
 - Detailed planning (for months or years prior to heist)
- For an unarmed attack:
 - Risk of death generally low (unarmed intruders unlikely to be fired upon)
 - If captured, consequences are relatively minor (e.g., 5-10 years for Antwerp)
- For an armed attack:
 - Risk of death higher but not unfathomable (2 deaths out of 80 violent heist on-scene accomplices in database), and much lower risk if security forces are unarmed
 - Consequences of capture higher, but mitigated if nobody was harmed (i.e., if thieves plan only to *threaten* violence)
- Less intuitive risks:
 - Risk of attack plan obsolescence (as soon as attack plan is executed, targeted security force will quickly adapt)
 - Risk of post-heist death (examples: Brazil Central Bank Heist, Lufthansa Heist)

INSIDER INFORMATION AND ACTIONS



They knew so much. To be honest I could have written down the combination numbers, given them the keys, and sat upstairs and had a cup of tea. They told me how to get into my own vault.

Mike Scouse
Brink's-Mat Security Supervisor

Insider Information and Actions

Working Definition for **Insider**:

A person recognized or accepted as a member of a group or organization who has authorized access to restricted areas, equipment, or information.

The Insider Spectrum

“Partial” Insider

Spaggiari (Société Générale)



Hearing a rumor that the Société Générale vault was not alarmed, Spaggiari rented a safe deposit box and investigated.

Viccei (Knightsbridge)



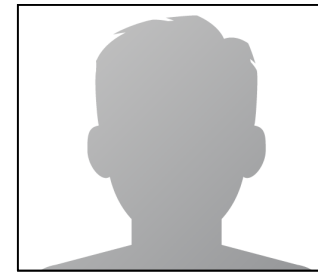
Rented a safe deposit box in the Knightsbridge center, built up a rapport, and learned through the owner's girlfriend that the owner was in financial trouble (and recruitable).

Notarbartolo (Antwerp)



Became a tenant of the Antwerp Diamond Center two years before the heist to gain access to the vault and identify security procedures and weaknesses.

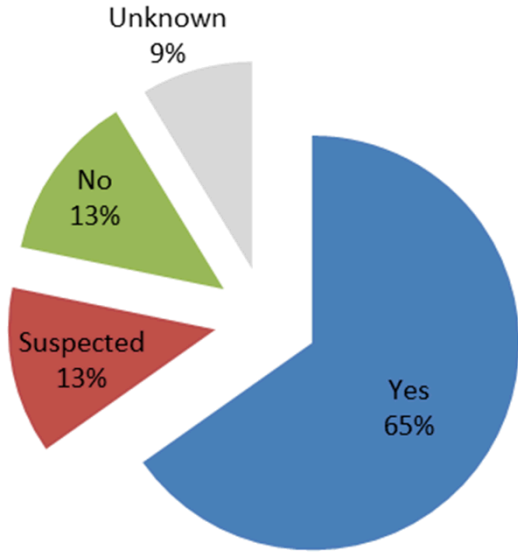
Latif (Knightsbridge)



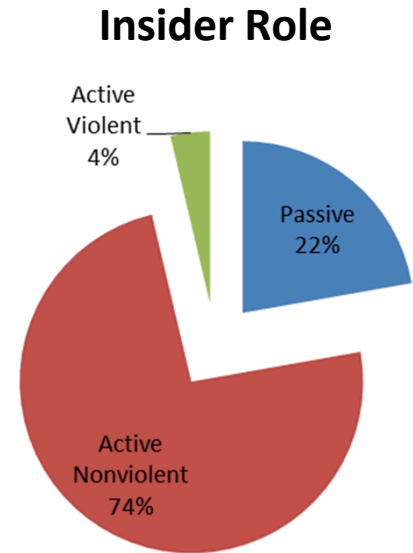
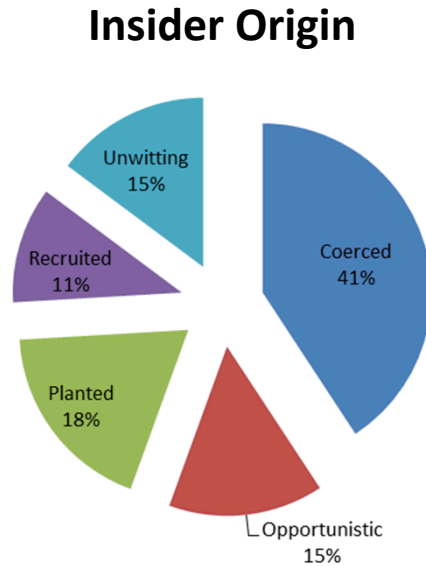
In financial trouble, this owner of the Knightsbridge Safe Deposit Center had the good fortune to be recruited by Viccei to help rob his own facility.


Insider Information and Actions

Was an insider used?
among heists in the database



What types of insiders were used?
among heists in the database

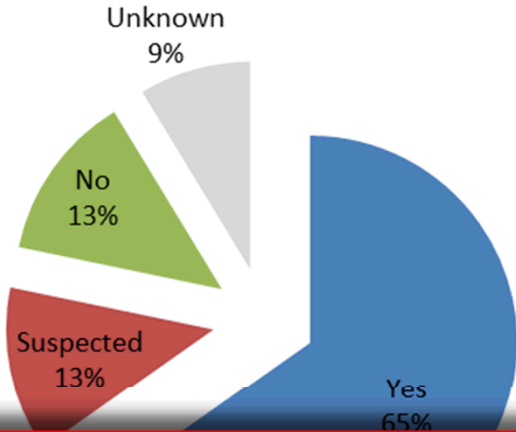




Insider involvement is exceedingly common in the planning and execution of high-value heists.

Insider Information and Actions

Was an insider used?
among heists in the database

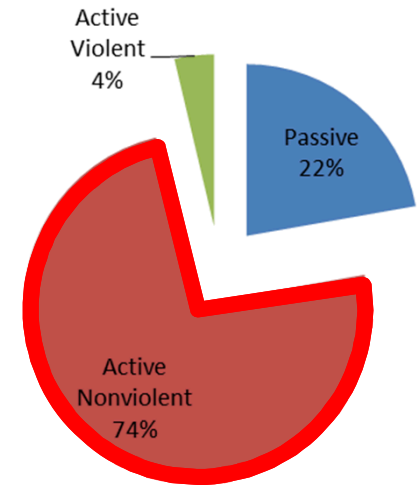



What types of insiders were used?
among heists in the database

Insider Origin




Insider Role





STEALTH RAID
Successful

Planted, Active
Nonviolent Insider



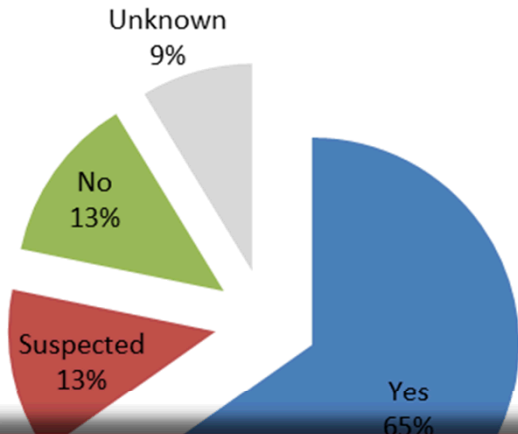
Antwerp Diamond Heist

Sat., Feb. 15, 2003, at 23:50
Antwerp, Belgium
51.51393°N, 4.41805°E

Target: Diamond Center Vault
Stolen: \$332.1 million in diamonds and stored valuables
Heist Duration: 5 hrs. (approx.)

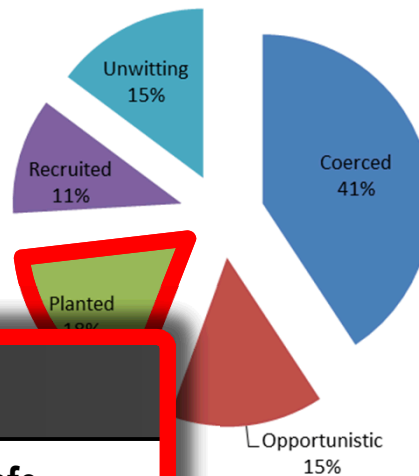
Insider Information and Actions

Was an insider used?
among heists in the database

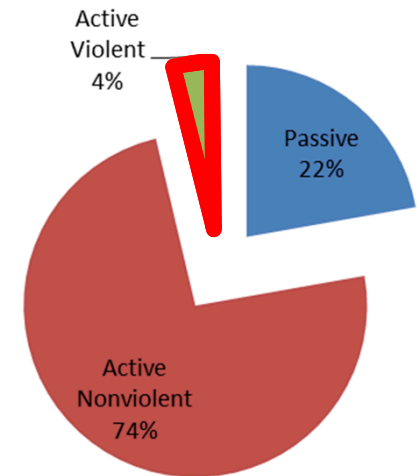


What types of insiders were used?
among heists in the database

Insider Origin



Insider Role



DECEIVE, SUBDUE, AND SEIZE

Successful



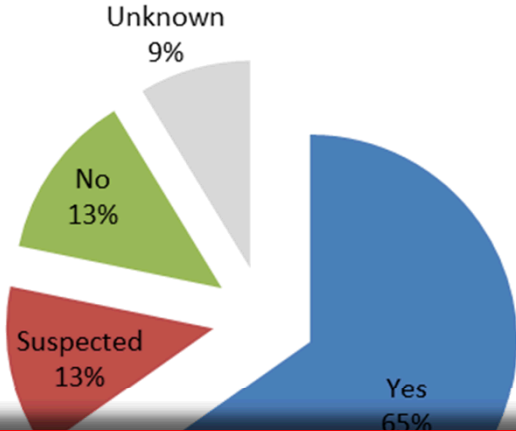
Knightsbridge Safe Deposit Center Heist

Sun., July 12, 1987, at 15:00
London, United Kingdom
51.498765°N, 0.166361°W

Target: Safe Deposit Center
Stolen: \$130 million in cash, gems, and stored valuables
Heist Duration: 2 hours

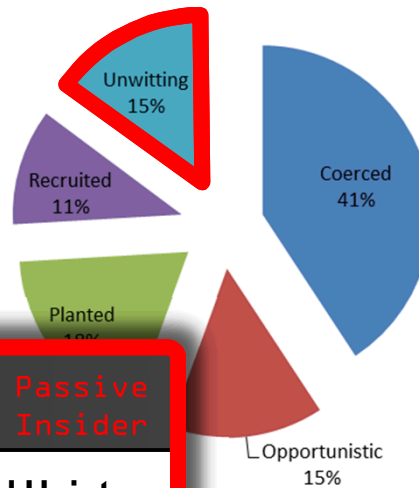
Insider Information and Actions

Was an insider used?
among heists in the database

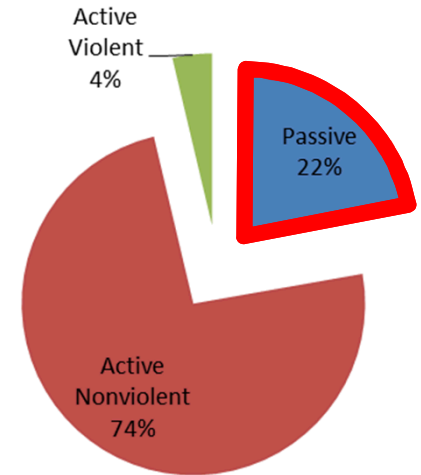


What types of insiders were used?
among heists in the database

Insider Origin



Insider Role



STEALTH RAID
Successful

Unwitting, Passive
Insider

Julie Boost CPP , CFM
Inspector / Expert Nuclear Security at FANC - Federaal Agentschap voor Nucleaire Controle
Antwerp Area, Belgium | Security and Investigations

[Join LinkedIn and access Julie Boost CPP , CFM's full profile](#)

As a LinkedIn member, you'll join 175 million other professionals who are sharing connections, ideas, and opportunities. And it's free! You'll also be able to:

- See who you and **Julie Boost CPP , CFM** know in common
- Get introduced to **Julie Boost CPP , CFM**
- Contact **Julie Boost CPP , CFM** directly

[View Full Profile](#)

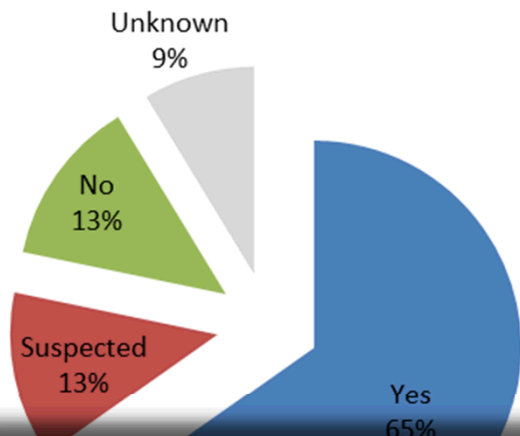
Antwerp Diamond Heist

Sat., Feb. 15, 2003, at 23:50
Antwerp, Belgium
51.51393°N, 4.41805°E

Target: Diamond Center Vault
Stolen: \$332.1 million in diamonds and stored valuables
Heist Duration: 5 hrs. (approx.)

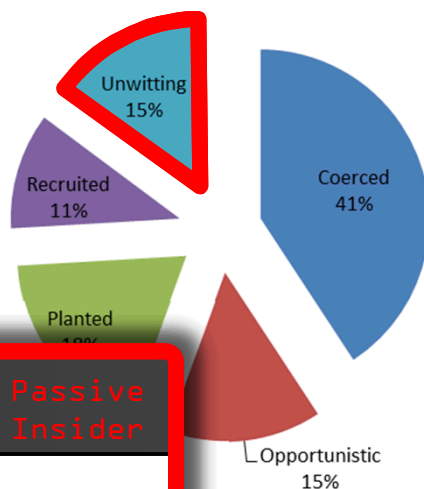
Insider Information and Actions

Was an insider used?
among heists in the database

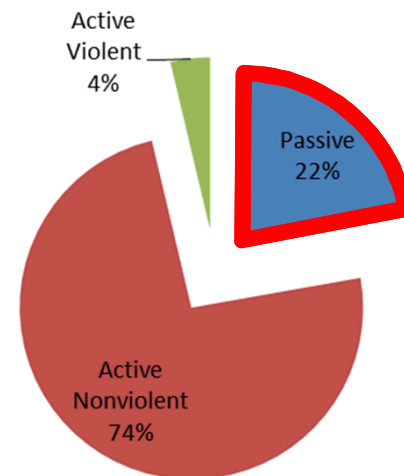


What types of insiders were used?
among heists in the database

Insider Origin



Insider Role





STEALTH RAID
Successful

Unwitting, Passive
Insider



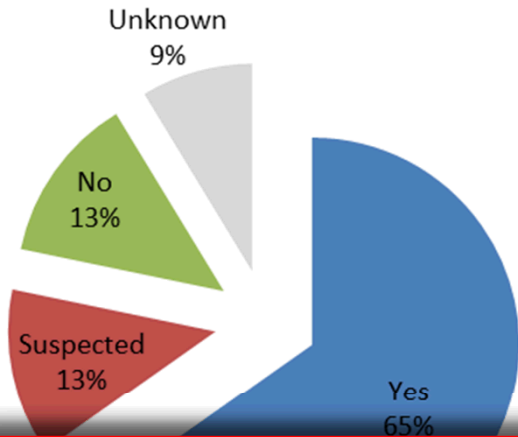
Société Générale Bank Heist

Sat., July 17, 1976, at 16:00
Nice, France
43.69900°N, 7.26933°E

Target: Société Générale Vault
Stolen: \$40.4 million in cash, gold, and stored valuables
Heist Duration: 36 hrs. (approx.)

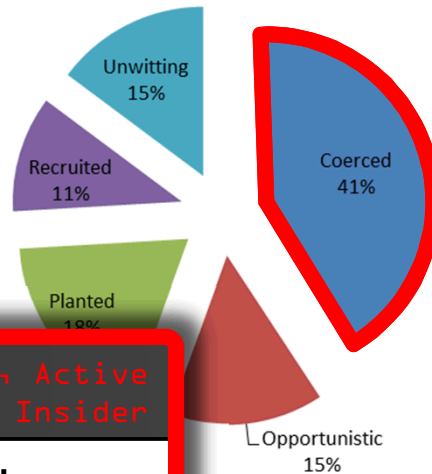
Insider Information and Actions

Was an insider used?
among heists in the database

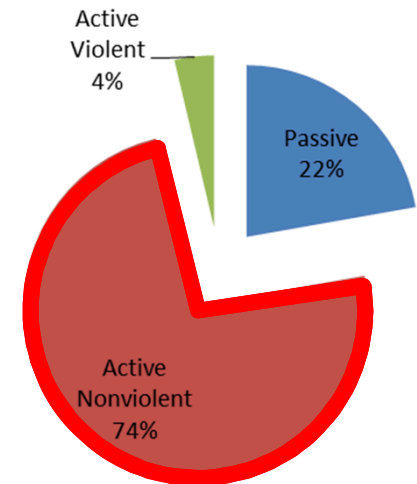


What types of insiders were used?
among heists in the database

Insider Origin



Insider Role



TIGER KIDNAPPING
Successful

Coerced, Active
Nonviolent Insider

Northern Bank Cash Heist

Sun., Dec. 19, 2004, at 22:00
Belfast, United Kingdom
54.596244°N, 5.932016°W

Target: Northern Bank
Stolen: \$60.5 million in cash
Heist Duration: 22 hours

Insider involvement can take a variety of forms, spanning various origins and various roles.

Who is the adversary?

- Experienced, 30-40 year old native citizens and career criminals (male)
- Typical teams
 - Total Size: 2-8 people
 - Breaking up into 1-4 teams during heist
- Resources
 - Planning time: 2 weeks to 2 years
 - Willing to spend tens of thousands of dollars or more, given the return on investment
 - Able to transport thousands of pounds of loot
- Innovative, esp. in terms of:
 - Security circumvention Measures
 - Deceptions
 - Getaway methods
- Use (or become) insiders to assist in planning and execution

Rodley (Sumitomo Mitsui)



Notarbartolo (Antwerp)



Spaggiari (Société Générale)



Viccei (Knightsbridge)



Allen (Securitas)



Sergio (Central Bank)

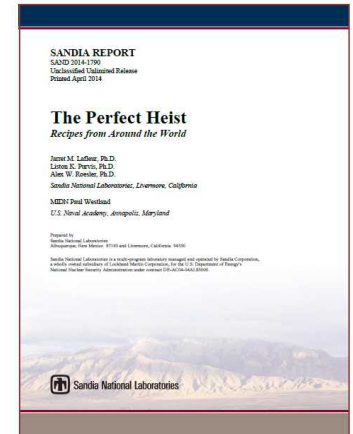


Some Lessons Learned

- Security circumvention techniques are often **innovative and novel** (e.g., helicopters, tunnels, and backhoes) but often **not high-tech**
- Thieves of high-value items typically plan to **avoid, rather than engage**, a security response
- Almost all large heists involve some use of **deception**
- Thieves have **great timing** (i.e., attack at times of low activity and high target value)
- An **unarmed adversary is not an unimportant adversary**
- Thieves demonstrate great **project management** skills
- **Insider involvement** is exceedingly common in heist planning and execution
- Insiders can have a **variety of origins and roles.**

Follow-on Work

- Documentation
 - SAND Report of Overall Study
 - Conference Paper and/or Journal Article on Overall Study
 - Numerous Presentations in California, New Mexico, and the Washington, DC area
- Summer Military Academic Collaboration Projects
 - Trading Centralization vs. Distribution of Security Access Privileges
 - The Perfect Heist: Recipes from the Silver Screen
 - The Double-Edged Sword of Redundancy in Security System Design
- Future Research Areas
 - Analysis of Clandestine Tunneling Operations
 - Comparison of Heist Lessons Learned to Defined Threats
 - Outreach to other Security-Focused Government Agencies



Follow-on Work: Cyber Heists

Cyber Heists

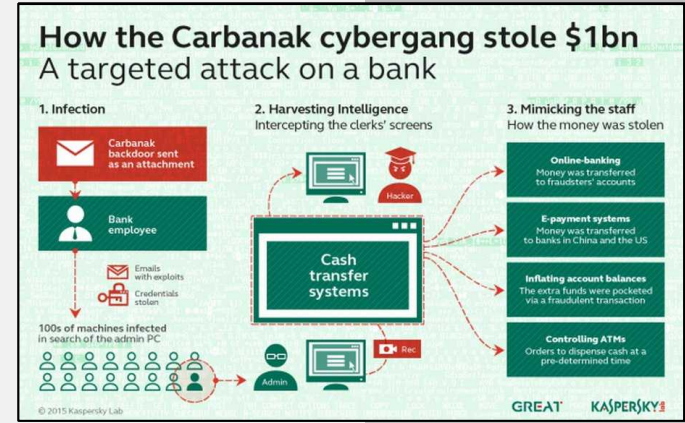
Defeat of security measures and theft itself occurs in cyberspace



Target Credit Card Breach, Nov. 2013



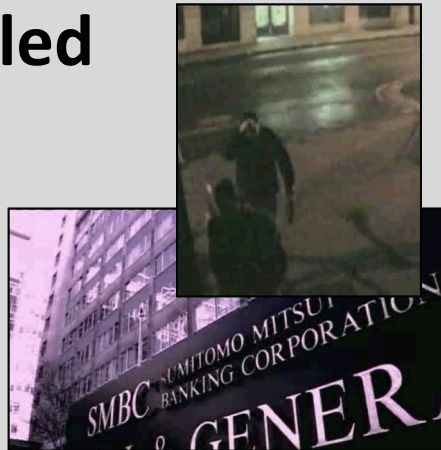
JPMorgan Breach, Aug. 2014



Carbanak Cybergang Heist, Feb. 2015

Physical-Enabled Cyber Heists

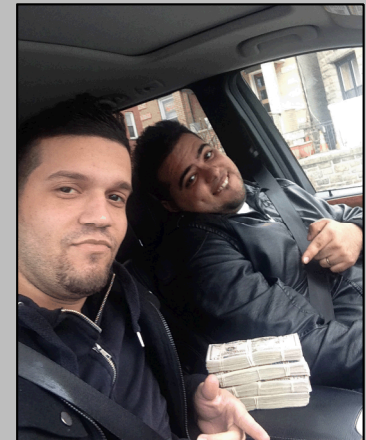
Defeat of security measures occurs or is assisted in physical space, while theft itself occurs in cyberspace



Sumitomo Mitsui Bank Heist, 2004

Cyber-Enabled Physical Heists

Defeat of security measures occurs or is assisted in cyberspace, while theft itself occurs in physical space



Global ATM Heist, Feb. 2013

Follow-on Work: Cyber Heists

Research and Discussion Questions

- What diversity of criminal methods is employed among large cyber heists? What criminal methods are common?
- What characteristics of large cyber heists are common between cyber and physical-only heists?
- If we apply the original heist study's database-driven methodology:
 - What specific cyber heist examples should we track?
 - What characteristics should we track?
 - Defeated security measures and devices
 - Deception methods
 - Timing and target selection
 - Weapons employed
 - Resources and risk acceptance
 - Insider information and actions
 - Failures and mistakes
- Are there other methodologies we should consider?

Questions?

Primary Point of Contact:

Jarret M. Lafleur, Ph.D.

Homeland Security and Defense Systems Center

Sandia National Laboratories

P.O. Box 969, MS 9407

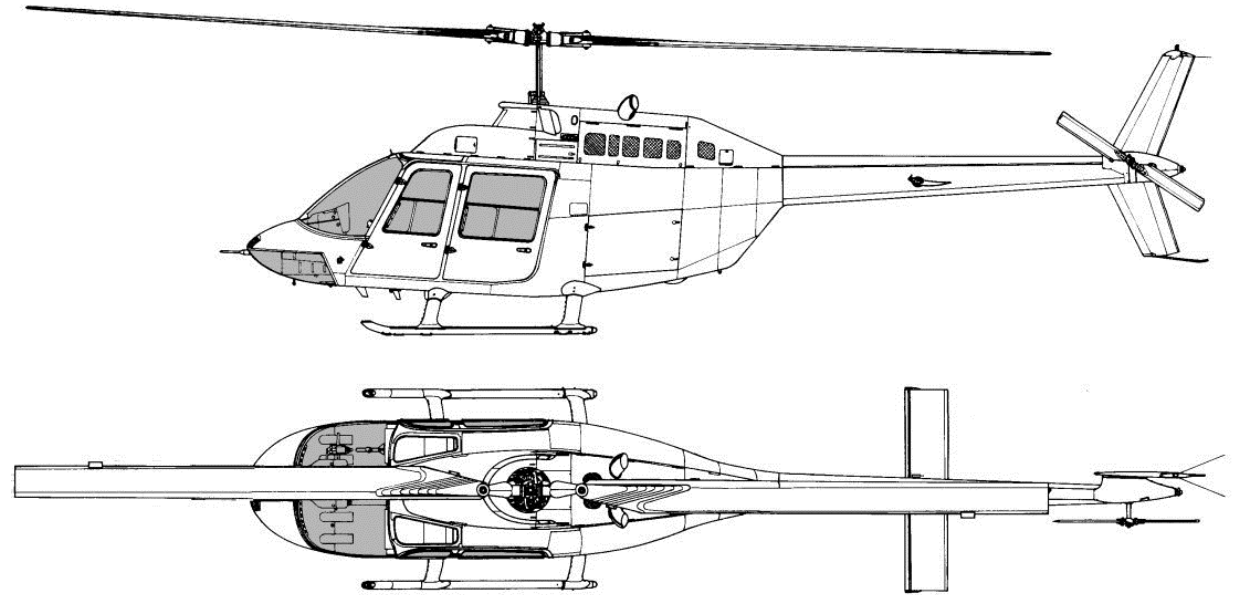
Livermore, CA 94550

E-mail: jarret.lafleur@sandia.gov

Phone: (925) 294-3449



Stockholm: September 2009



Bell 206 JetRanger

Role: Multipurpose Utility Helicopter

Capacity: 1 pilot, 4 passengers

Max Speed: 139 mph

Range: 430 miles

Ceiling: 13,500 ft.



New York: December 1978





New York: December 1978



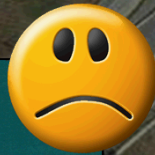


New York: December 1978

Monday, Dec. 11
03:00

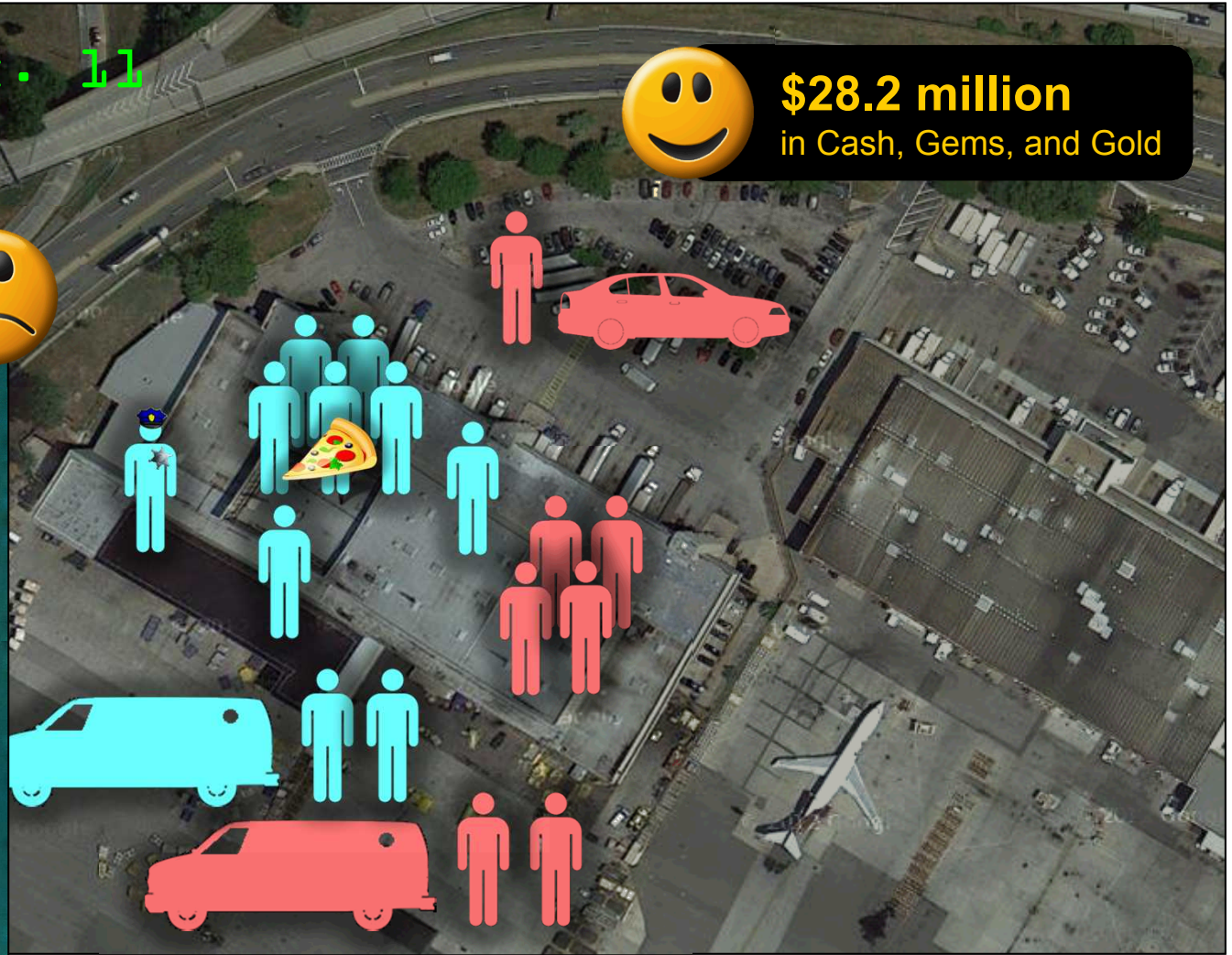


\$28.2 million
in Cash, Gems, and Gold



PEOPLE MURDERED BY THE LUCCHESE CRIME FAMILY

MURDER VICTIMS RELATED TO THE LUFTHANSA HEIST, MARTIN KRUGMAN, ROBERT MCMAHON, LOUIS CAFORA, JOE MANRI, RICHARD EATON, PARNELL EDWARDS, MICHAEL "SPIDER" GIANCO, PAOLO LICASTRI, THERESA FERRARA, TOM MONTELEONE, JOSEPH PINZOLO, RONALD JEROTHE





Tonbridge: February 2006



Real police officer with recovered Ford Transit van from kidnappings



Phony police officer ushering criminals into Securitas Cash Depot

Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented

Brazil Central Bank Cash Heist
 Sumitomo Mitsui Bank Heist
 Antwerp Diamond Heist
 Museon Jewel Heist
 Soci t  G n rale Bank Heist
 Stardust Casino Job
 Vastberga Helicopter Heist
 Millennium Dome
 Tanzania

SMASH AND GRAB Failed



Millennium Dome Raid

Tues., Nov. 7, 2000, at 10:38
 London, United Kingdom
 51.50299°N, 0.00315°E

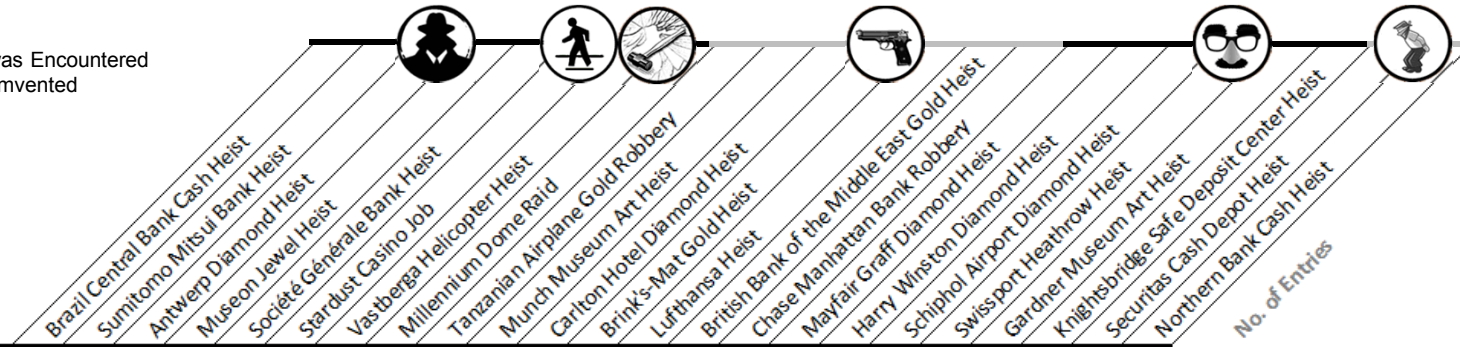
Target: The Millennium Dome
Stolen: \$666.1 million in diamonds (attempted)
Heist Duration: 15 min.

Security Measure	Brazil Central Bank Cash Heist	Sumitomo Mitsui Bank Heist	Antwerp Diamond Heist	Museon Jewel Heist	Soci�t� G�n�rale Bank Heist	Stardust Casino Job	Vastberga Helicopter Heist	Millennium Dome	Tanzania
Static Barriers									
Fences									
Walls									
Windows									
Floors									
Target Anchor									
Target Barrier									
Access Controls									
Key									
Combination									
Radio Frequency									
Access Credential									
Bio Recognition									
Detectors									
Cameras									
Light Sensors									
Infrared Sensors									
Microwave Doppler Sensors									
Unspecified Motion Sensors									
Physical Tampering Sensors									
Security Guards									
Armed									
Unarmed									

No. of Entries: 3 0 8 5 2 1 2 3 0 2

Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented

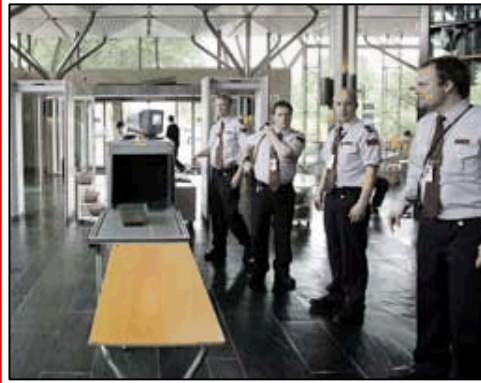


Security Measure	Heist Events															No. of Entries
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Static Barriers																
Fences																
Walls																
Windows																
Floors																
Target Anchor																
Target Barrier																
Access Controls																
Key																
Combination																
Radio Frequency																
Access Credential																
Bio Recognition																
Detectors																
Cameras																
Light Sensors																
Infrared Sensors																
Microwave Doppler Sensors																
Unspecified Motion Sensors																
Physical Tampering Sensors																
Security Guards																
Armed																
Unarmed																



SUBDUE AND SEIZE

Successful



Munch Museum Art Heist

Sun., Aug. 22, 2004, at 11:10
Oslo, Norway
59.91685°N, 10.77473°E

Target: Munch Museum
Stolen: \$137.9 million in artwork
Heist Duration: 5 minutes

No. of Entries: 3 0 8 5 2 1 2 3 0 2 0 3 3 2 1 2 4 3 3 6 4 4 3

Defeated Security Measures

Lessons Learned

- High-value heists typically involve the defeat of **multiple security measures**
- Keyed locks, cameras, and unarmed guards are very commonly defeated
- Even among the creative and innovative security measure defeat methods, **none make significant use of high technology**
- Lack of response force proximity is rarely the reason for a lack of security response
- Security systems relying on a small on-duty guard force to detect incursions are **highly susceptible to well-planned adversary attacks** designed to prevent the guards from acting as effective sensors or responders
- Thieves of high-value items **typically plan to avoid, rather than engage, a security response**

Deception Methods

Lessons Learned

- **Almost all large heists involve some use of deception**
- Frequently, deceptions are physically **simple and inexpensive** (e.g., sign indicating security upgrades are occurring, police jacket and cap, promotional baseball hats)
- However, effective deceptions are highly dependent on context and **may require time and inside information to develop** (e.g., creating false paperwork for authorized access, learning the occupational jargon of the targeted industry)
- Most frequently, thieves (1) use getaway vehicles that do not draw attention, (2) conceal equipment, (3) disguise or mask their physical features, and **(4) avoid attention by blending in to normal occupational activities.**
 - Thieves or coerced accomplices that blend in by occupation exist more frequently inside than outside the targeted organization
 - There is no clear limitation to what level (e.g., manager, employee, customer) of occupational role thieves or their coerced accomplices will take

TIMING AND TARGET SELECTION

Armed with Werner and Gruenwald's plan, Burke and the Robert's Lounge gang hammered out the details: They'd go in late, when only a skeleton crew of ten was on, striking while the graveyard shift was at lunch.

Charlie Glaze, Narrator
Daring Capers: Kennedy Airport Caper

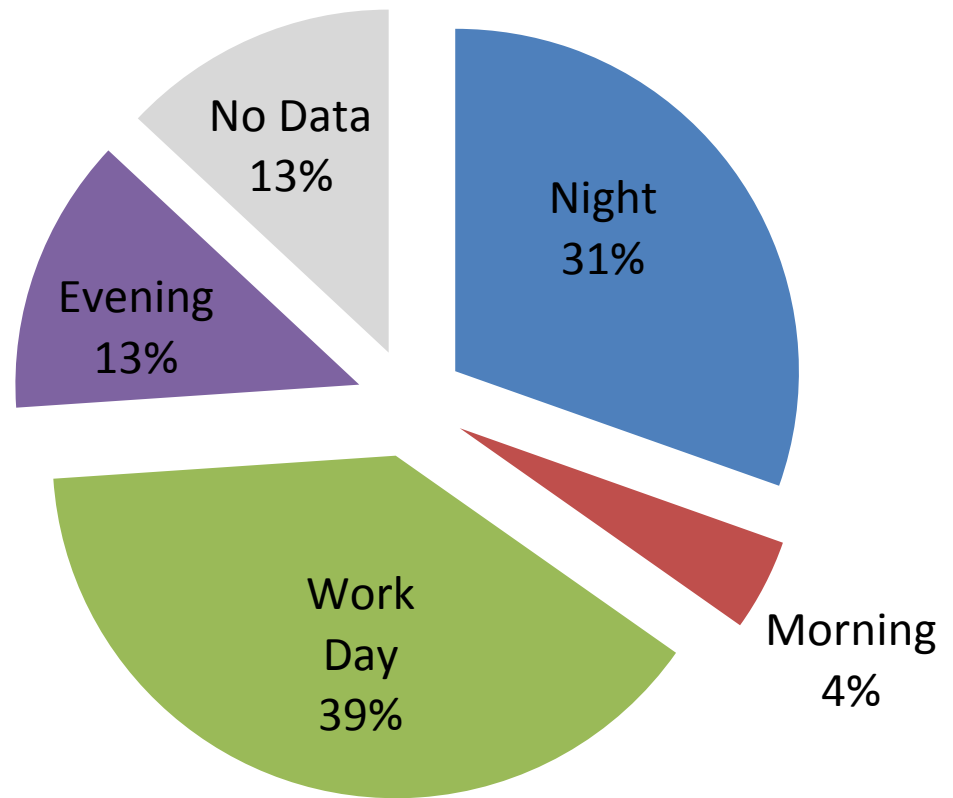
Timing and Target Selection

Absolute Timing

Term Definitions

Term	Time Range
Morning	6:00 AM – 9:00 AM
Work Day	9:00 AM – 5:00 PM
Evening	5:00 PM – 8:00 PM
Night	8:00 PM – 6:00 AM

Time of Day Distribution for Heists in the Database



Thieves of high-value items have no clear preference for a particular time of day at which to strike.

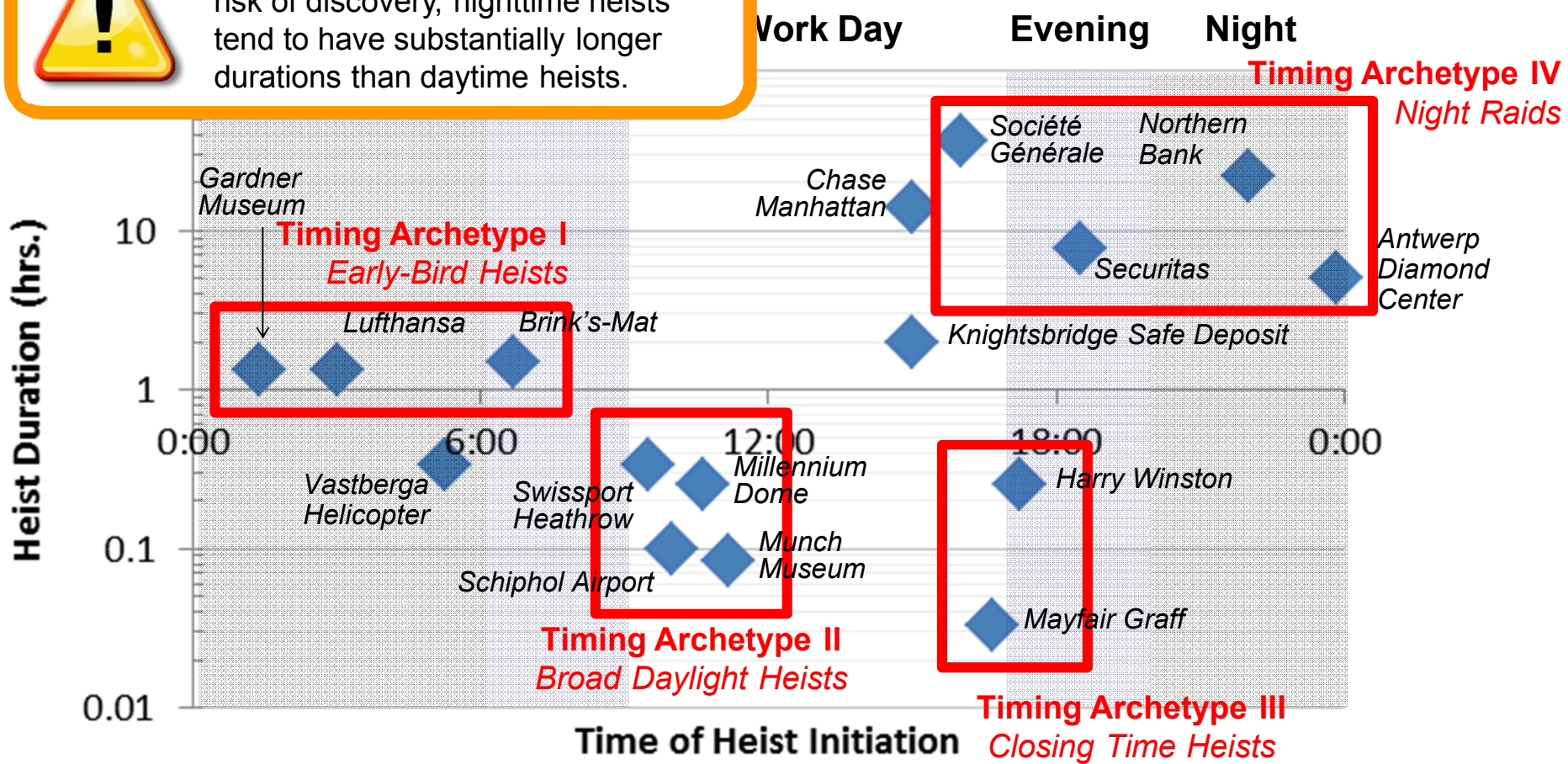
Timing and Target Selection

Absolute Timing



With lower surrounding activity and risk of discovery, nighttime heists tend to have substantially longer durations than daytime heists.

s. Time of Initiation



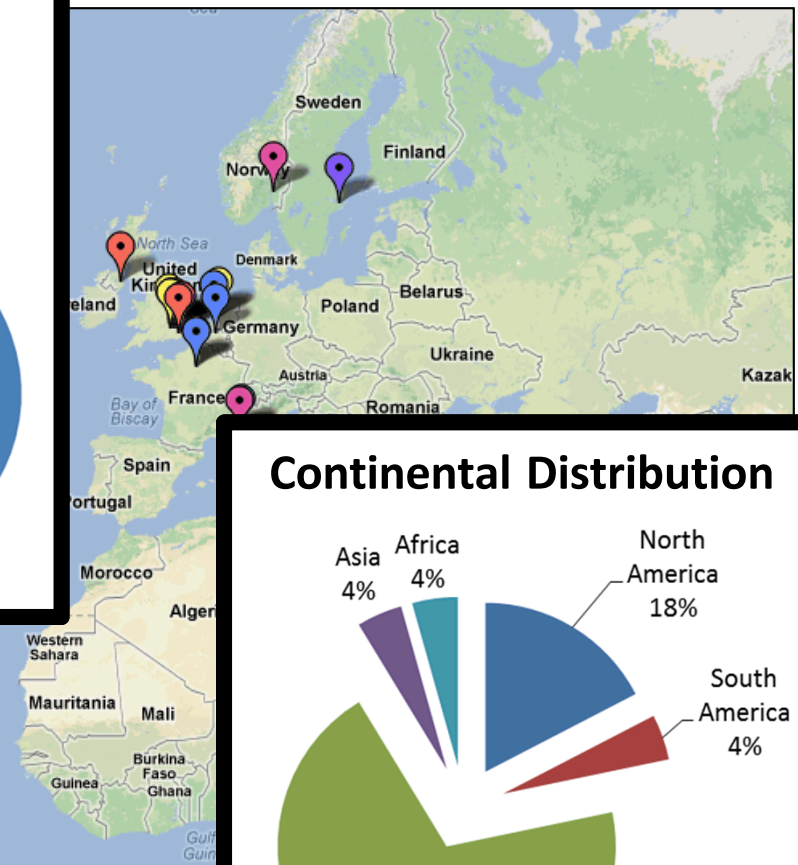
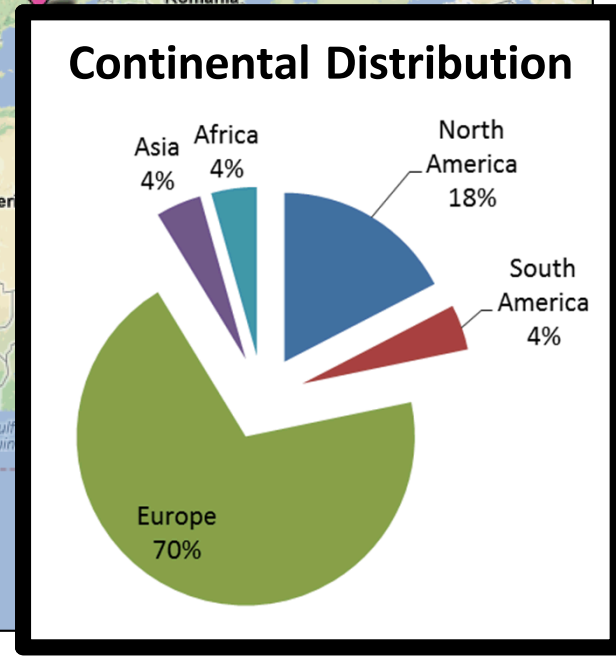
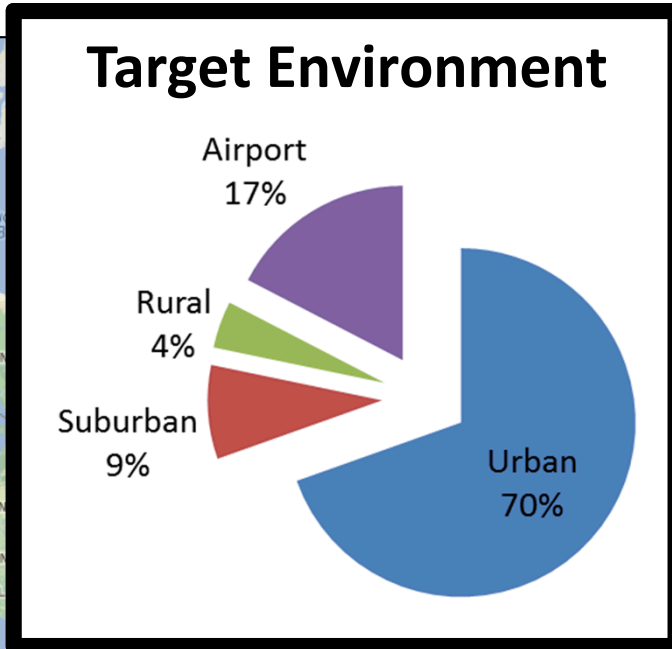

Timing and Target Selection

Relative Timing

- Common Factors
 - Low bystander activity, typically resulting in:
 - **Low likelihood of unexpected detection**
 - Timing outside of core business hours (nights, weekends, holidays)
 - Low employee or security activity, typically resulting in:
 - **Ease of defeating expected detection**
 - Timing outside of core business hours (nights, weekends, holidays)
 - High target value, with regular or irregular timing known through:
 - Inside information
 - Outside observation or inference
- Uncommon Factors
 - Direct knowledge of personnel location vs. time
 - Physics-related timing (e.g., tides enabling escape)

Timing and Target Selection

Target Environments

Historically, high-value heists in the West have predominantly taken place in areas with high amounts of daily activity (e.g., airports and urban areas).

Timing and Target Selection

Lessons Learned

- Timing
 - Absolute Timing
 - **Thieves can – and do – strike at any time of day**
 - **Night heists typically do not demand rapid operations** and tend to have substantially longer durations than daytime heists
 - Relative Timing
 - **Times of low bystander, employee, and security activity** (nights, weekends, holidays) offer thieves a low likelihood of unexpected detection and ease of defeating any expected detection
 - **High available target value**, often known through inside information
- Target Selection
 - Aggregate data suggests **thieves rationally trade between ability to penetrate and ability to fence**
 - High-value heists have predominantly taken place in areas with high amounts of daily activity (urban areas and airports)

WEAPONS EMPLOYED

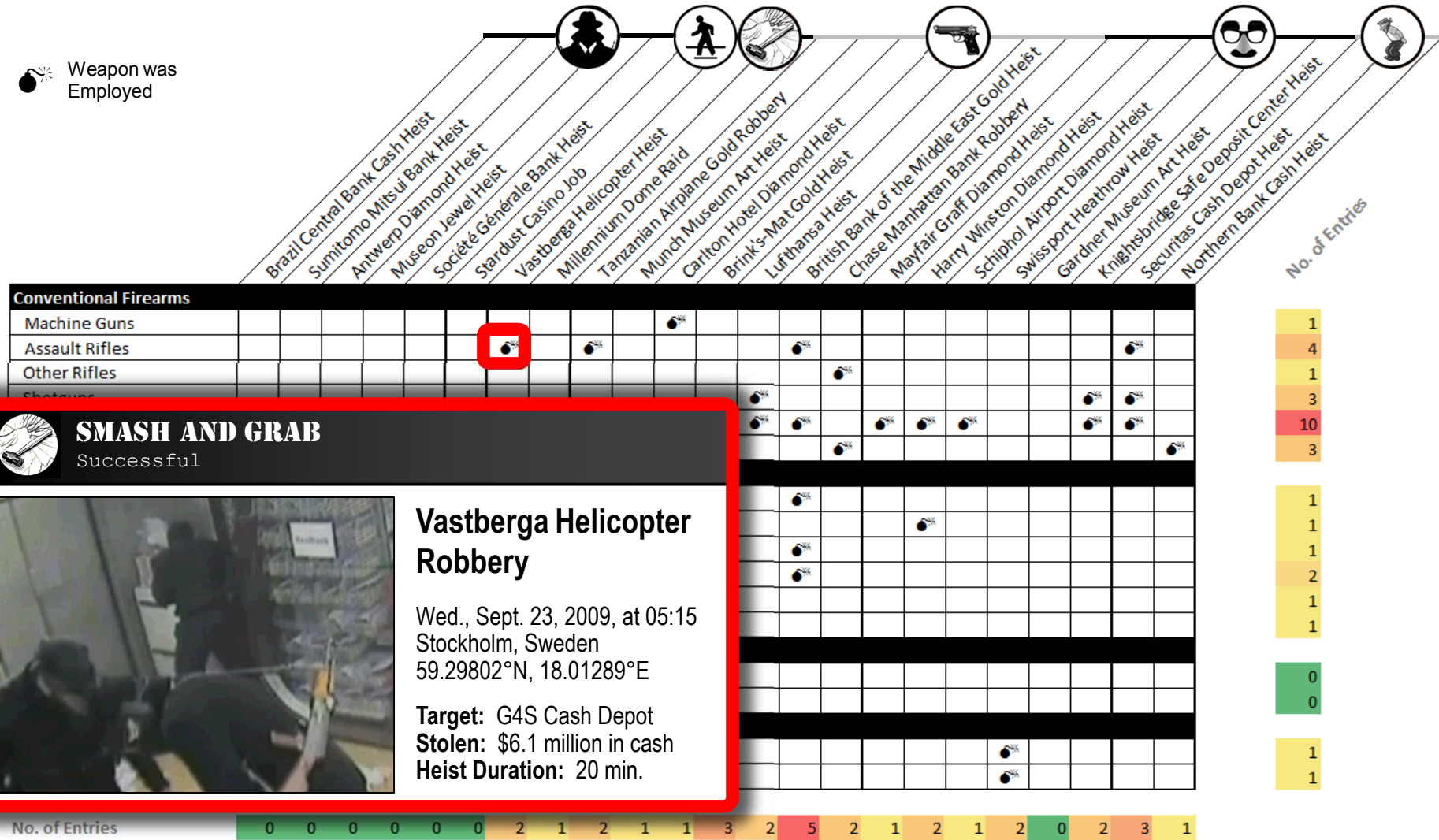


When they threaten the guards with a gun there is not much to be done.

Jorunn Christofferson
Munch Museum Press Officer

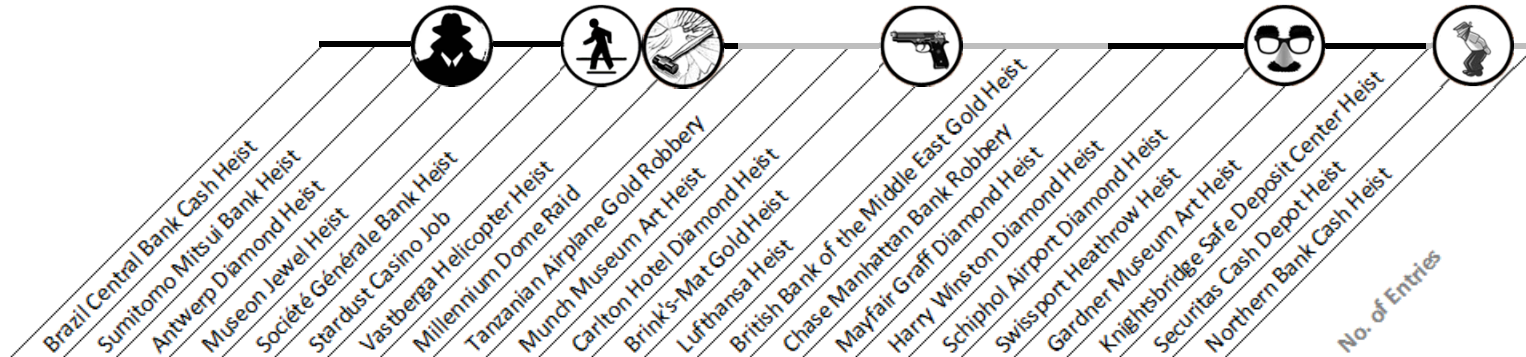
Weapons Employed

Weapon was Employed

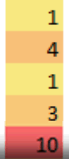


Weapons Employed

Weapon was Employed



Conventional Firearms	Brazil Central Bank Cash Heist	Sumitomo Mitsui Bank Heist	Antwerp Diamond Heist	Museon Jewel Heist	Société Générale Bank Heist	Stardust Casino Job	Vastberga Helicopter Heist	Millennium Dome Raid	Tanzanian Airplane Gold Robbery	Munch Museum Art Heist	Carlton Hotel Diamond Heist	Brink's-Mat Gold Heist	Lufthansa Heist	British Heist	Chase Bank of the Middle East Gold Heist	Mayfair Graff Bank Robbery	Harry Winston Diamond Heist	Schiphol Airport Diamond Heist	Swissport Airport Diamond Heist	Gardner Museum Art Heist	Knightsbridge Safe Deposit Center Heist	Securitas Cash Depot Heist	Northern Bank Cash Heist	
Machine Guns																								
Assault Rifles																								
Other Rifles																								
Shotguns																								



SMASH AND GRAB

Successful



Vastberga Helicopter Robbery

Wed., Sept. 23, 2009, at 05:10
Stockholm, Sweden
59.29802°N, 18.01289°E

Target: G4S Cash Depot
Stolen: \$6.1 million in cash
Heist Duration: 20 min.



TIGER KIDNAPPING

Successful



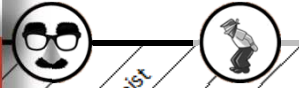
Securitas Cash Depot Heist

Tues., Feb. 21, 2006, at 18:30
Tonbridge, United Kingdom
51.191098°N, 0.277652°E

Target: Securitas Depot
Stolen: \$104 million in cash
Heist Duration: 7.8 hours

Weapons Employed

An unarmed adversary is not an unimportant adversary.



Weapon	Brazil Central Bank Heist	Sumitomo Mitsui Banking Corp. Heist	Antwerp Diamond Heist	Museum Jewel Heist	Société Générale Heist	Stardust Casino Job	Vastberga Heist	Millennium Dome Raid	Tanzanian Airplane Gold Robbery	Munch Museum Art Heist	Carlton Hotel Diamond Heist	Brink's-Mat Heist	Lufthansa Heist									
Conventional Firearms																						
Machine Guns																						
Assault Rifles																						
Other Rifles																						
Shotguns																						
Handguns																						
Unspecified																						
Explosives																						
Grenades																						
Hand Grenades																						
Mortars																						
Plastic Explosives																						
Smoke Bombs																						
Gas and Matches																						
Bladed Weapons																						
Swords																						
Knives																						
Blunt Weapons																						
Hockey Sticks																						
Clubs																						
No. of Entries	0	0	0	0	0	0	2	1	2	1	1	3	2	5	2	1	2	1	0	2	3	1

Weaponless heists account for 3 of the top 4 valued heists in the database.



Heist Name	No. of Entries
Deposit Center Heist	1
Cash Depot Heist	4
Western Bank Cash Heist	1
	3
	10
	3
	1
	1
	1
	2
	1
	1
	0
	0
	1
	1

Weapons Employed

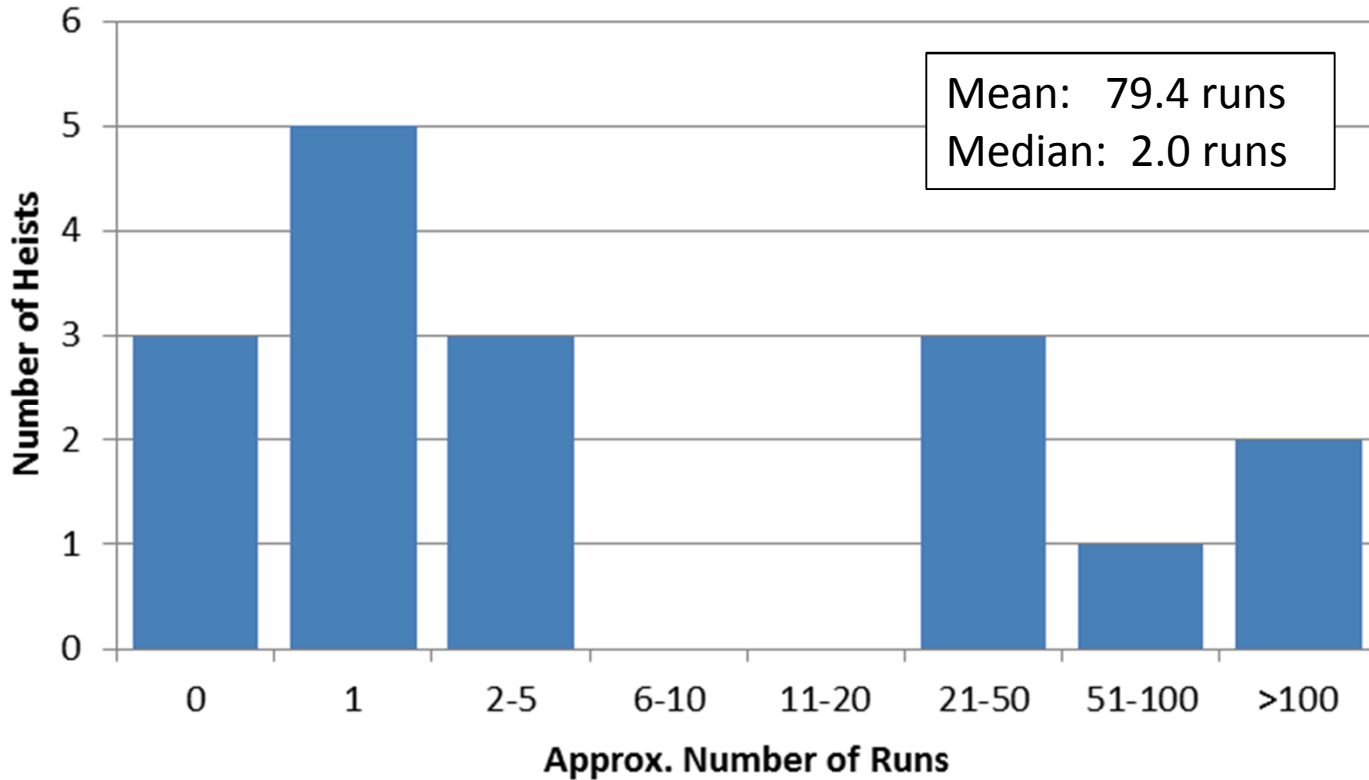
Lessons Learned

- Conventional firearms, rather than explosive, bladed, or blunt weapons, are typical weapons of choice
- **Many high-value heists involve no use of weapons at all**
- **An unarmed adversary is not an unimportant adversary**

Resources and Risk Acceptance

Testing and Qualification

Practice and Reconnaissance Runs



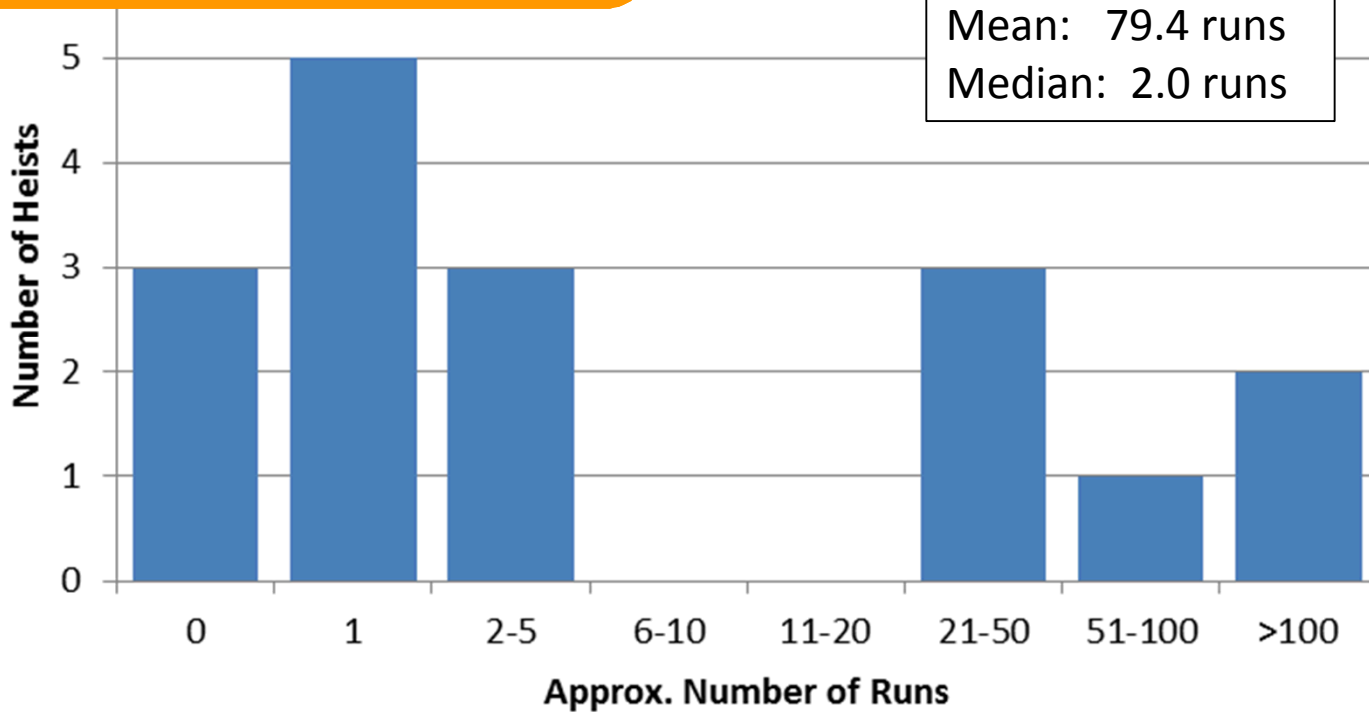
Resources and Risk Acceptance

Testing and Qualification




Test, test, test: Rarely do thieves engage in a heist without a reconnaissance or practice run.

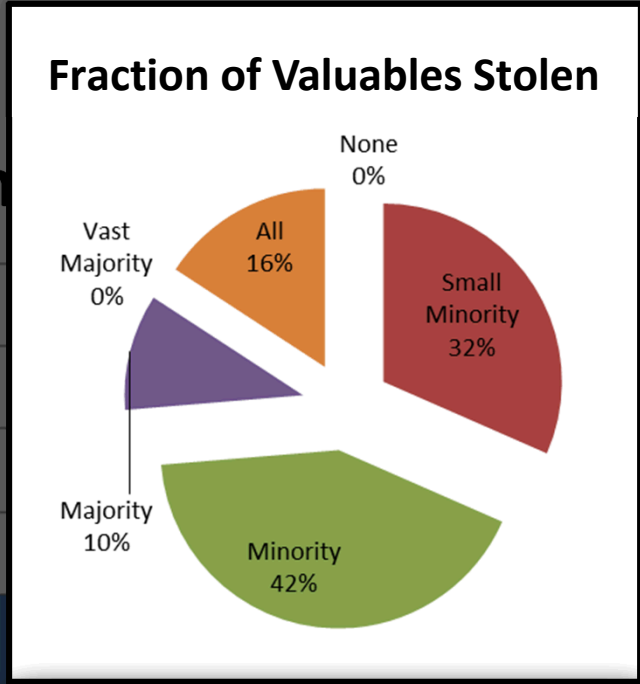
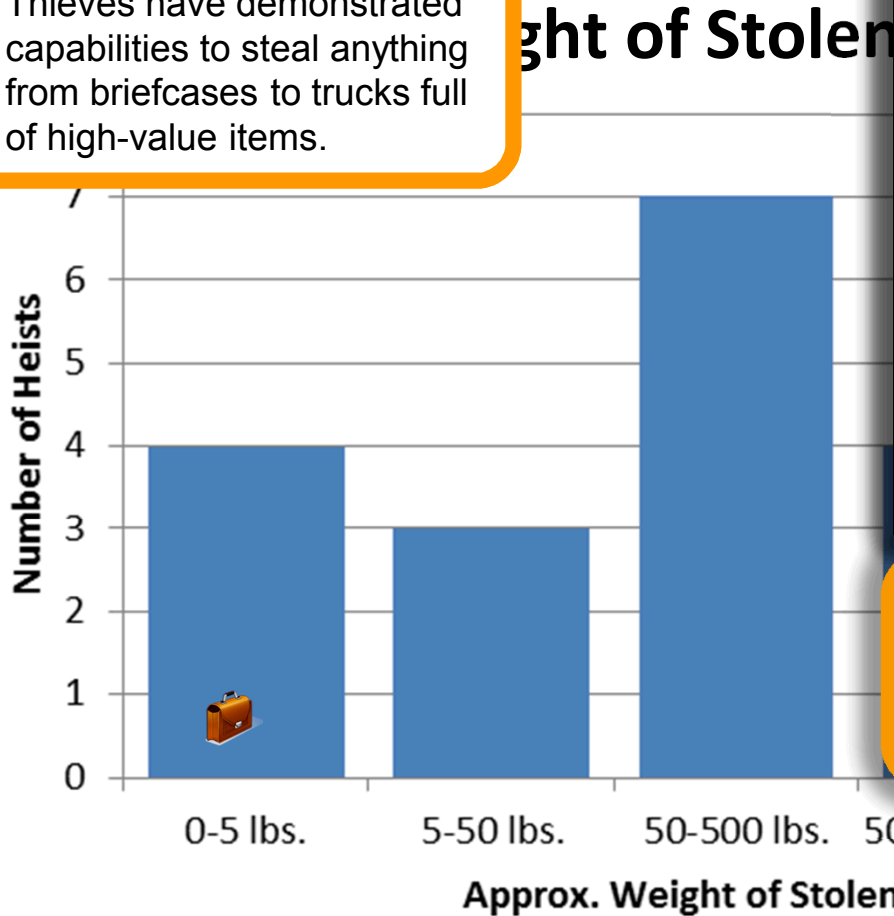
Reconnaissance Runs




Resources and Risk Acceptance

Mass Properties

 Thieves have demonstrated capabilities to steal anything from briefcases to trucks full of high-value items.



 Thieves have demonstrated the ability to execute highly targeted heists.

Resources and Risk Acceptance

Lessons Learned

- **Thieves of high-value items are often a lot like us:**
 - Ambitious and disciplined
 - Good systems engineers and project managers
- **Schedule:** Thieves often take **months or years to plan** a high-value heist
- **Testing and Qualification:** **Rarely do thieves execute a heist without a recon or practice run**
- **Human Resources:**
 - Thieves need the ability to work well in small teams
 - Thief operations are **almost always supported by a larger team effort**
- **Mass Properties:**
 - Thieves have demonstrated capabilities to **steal anything from briefcases to trucks full of high-value items**
 - Thieves have demonstrated the ability to execute **highly targeted** heists
- **Budget:** Thieves are **willing to invest large amounts of money** in planning and preparation, justified in part by the probable financial returns.
- **Recruiting:** The typical high-value item thief is:
 - A 36-year-old man
 - Career criminal
 - Native to the country that is home to the asset he plans to steal

Insider Information and Actions

Lessons Learned

- **Insider involvement is exceedingly common** in the planning and execution of high-value heists.
- Insiders come in a variety of flavors:
 - Origin: Unwitting, Recruited, Planted, Opportunistic, or **Coerced**
 - Role: Passive, **Active Nonviolent**, Active Violent
- **Coerced, active nonviolent insiders** tend to be the most frequently observed type in high-value heists.

FAILURES AND MISTAKES

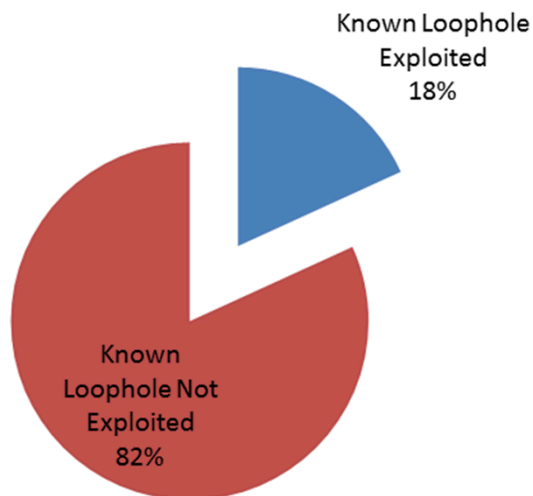
I mean, there is no security system that can't be bypassed, because there always is a human mind and a human hand activating them.

Valerio Viccei, Criminal
Knightsbridge Safe Deposit Center Heist

Failures and Mistakes

Blue Force Issues

Exploitation of Known Security Vulnerabilities

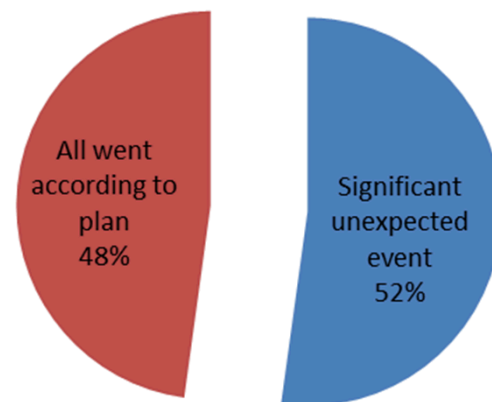


Examples:

- Antwerp Diamond Center would not consent to insurance investigator evaluation
- Gardner Museum underfunded security and did not implement recommendations from security consultant two years prior to heist

Red Force Issues

Occurrence of Unexpected or Plan-Altering Events during Heist



Examples:

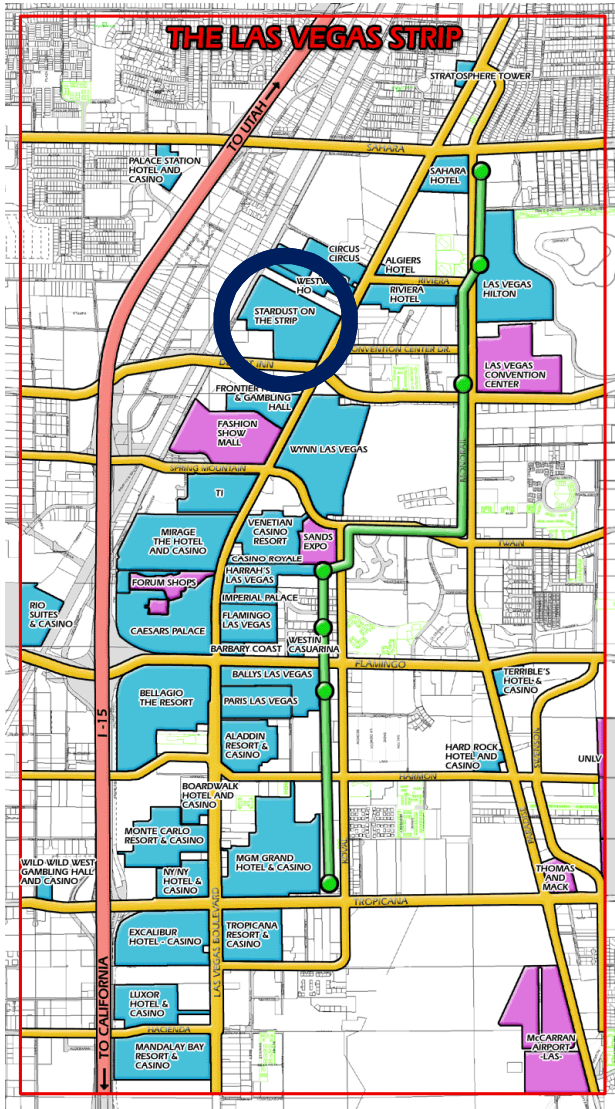
- Stressed Brink's-Mat employee inability to remember vault combination
- Chase Manhattan bank manager's disguised communications
- Knightsbridge thieves on wrong radio channel
- Société Générale late-night cash drop and storm

Failures and Mistakes

Lessons Learned

- In a small but significant number of cases, decisions to not invest in appropriate security led to substantial losses
- **Thieves' plans are not always perfect**, and it is common for unplanned events to require them to alter their plans

Las Vegas: September 1992



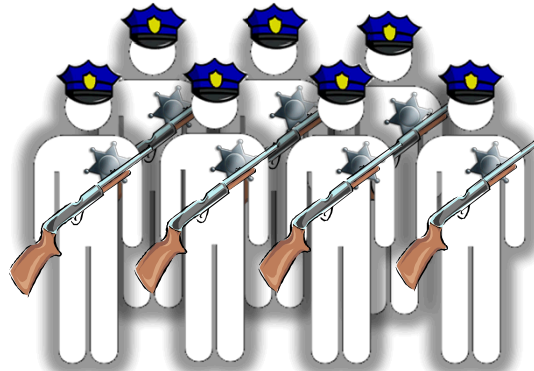
😊 \$800,000
in Cash and Chips

Defeated Security Measures

Security Guards



Incapacitated
Guard Force



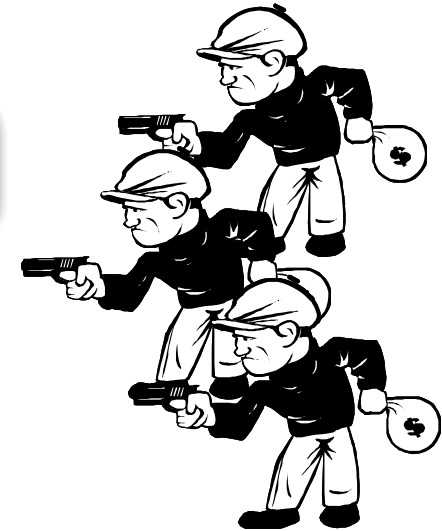
Large Generatable Guard Force



Relying on a small on-duty guard force to detect incursions is highly susceptible to attacks designed to prevent guards from acting as effective sensors or responders.



Sensor / First
Responder
Guard Force



Deception Methods

Deception Method was Employed



DECEIVE, SUBDUE, AND SEIZE

Successful



Gardner Museum Art Heist

Sun., March 18, 1990, at 01:24
 Boston, United States of America
 42.338768°N, 71.098859°W

Target: Gardner Museum
Stolen: \$440 million in artwork
Heist Duration: 1.4 hours

Physical Disguises

- Disguise of Thief-Possessed Building
- Disguise of Theft in Progress
- Vehicles that Blend with Surrounding
- Disguised/Concealed Surveillance Equipment
- Disguised/Concealed Operations Equipment
- Physical Disguise or Concealment of Loot
- Disguised
- Disguised

Deception Methods



DECEIVE, SUBDUE, AND SEIZE

Successful

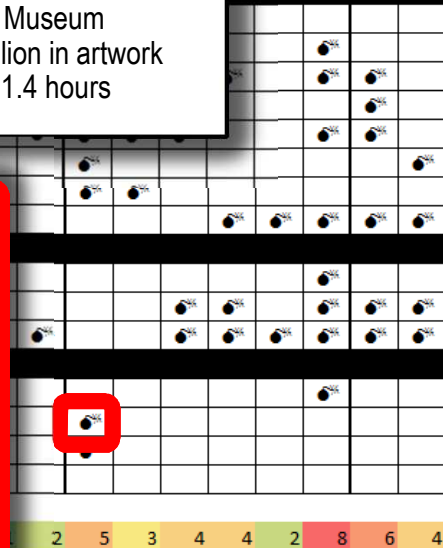
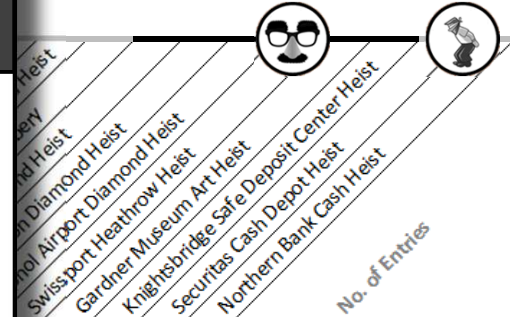


Mayfair Graff Diamond Heist

Sun., Aug. 6, 2009, at 16:40
 London, United Kingdom
 51.509821°N, 0.141851°W

Target: Graff Diamonds Store
Stolen: \$68.9 million in jewelry
Heist Duration: 2 minutes

No. of Entries



Defeated Security Measures

Security Measure was Encountered and Defeated/Circumvented



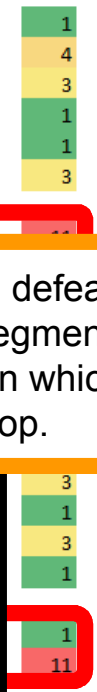
Keys, cameras, and guards, are among the most frequently defeated security measures in the heist database.

Three most common defeat methods all attack segments of the security system in which humans are in the loop.

Three most common security measure defeat methods:

- (1) Threats on guards or on key- or combination-holding employees
- (2) Using recognized employees to enter and/or vouch for entry
- (3) Gaining control of CCTV monitoring stations

Security Measure	Bank Cash Heist	Bank Heist	Home Heist	Home Bank Heist	No Job	Helicopter Heist	Home Raid	Airplane Gold Robbery	Art Heist	Diamond Heist	Hat Gold Heist	British Heist	British Bank of the Middle East Gold Heist	Chase Manhattan Bank Robbery	Mayfair Graff Diamond Heist	Harry Winston Diamond Heist	Schiphol Airport Diamond Heist	Swissport Heathrow Heist	Gardner Museum Art Heist	Knightsbridge Safe Deposit Center Heist	Securitas Cash Depot Heist	Northern Bank Cash Heist	
Threats on guards																							
Threats on key- or combination-holding employees																							
Using recognized employees																							
Gaining control of CCTV																							



Resources and Risk Acceptance

Recruiting



The typical high-value item thief is a 36-year-old man who is a career criminal and native to the country that is home to the asset he intends to steal.

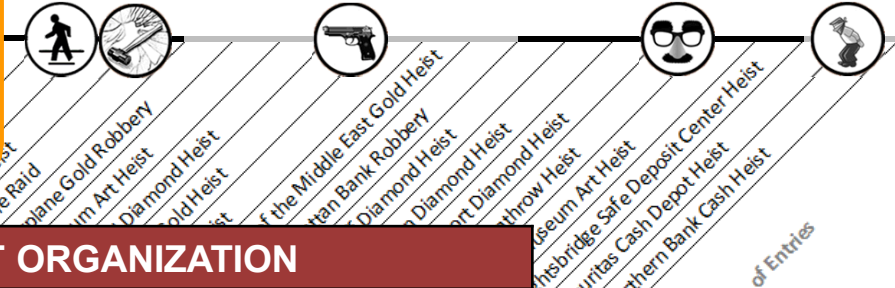
List of Occupations for High-Value Heist Accomplices

Employees	Managers	Business Owners	Illicit	Other
Appraiser	Airline Cargo Supervisor	Adult Store Owner	Career Criminal	Cage Fighter
Cashier	Security Chief	Bar Owner	Drug Dealer	Soldier
Construction Worker	TV Producer	Camera Store Owner	Gang Leader	Unemployed
Delivery Driver	Youth Club Leader	Coffee Shop Owner	Hacker	
Doorman		Garage Owner	Petty Thief	
Electrician		Jewelry Designer		
Electronics & Alarms Expert		Minicab Agency Owner		
Engineer		Safe Deposit Center Owner		
Gardener				
Journalist				
Musician				
Pizzeria Worker				
Postal Worker				
Roofer				
Security Guard				
Used Car Salesman				

Deception Methods



Thieves or coerced accomplices that **blend in by occupation** exist more frequently inside than outside the targeted organization.



RELATION TO TARGET ORGANIZATION

Inside



There is no clear limitation to what level of occupational role thieves or their coerced accomplices will take; there are virtually equal numbers of examples of inside managers, employees, and customers

Deception Methods

ROLE

Owner

- Knightsbridge
- Sumitomo Mitsui

Manager

- Lufthansa
- Securitas
- Northern Bank

Employee

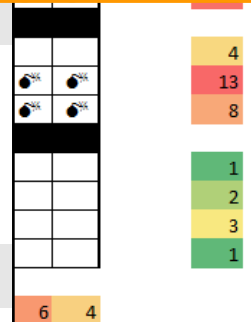
- Stardust Casino
- Brink's-Mat
- Securitas
- Schiphol Airport*
- Société Générale*
- Swissport Heathrow*
- British Bank of the Middle East

Tenant

- Antwerp
- Brazil Central Bank

Customer

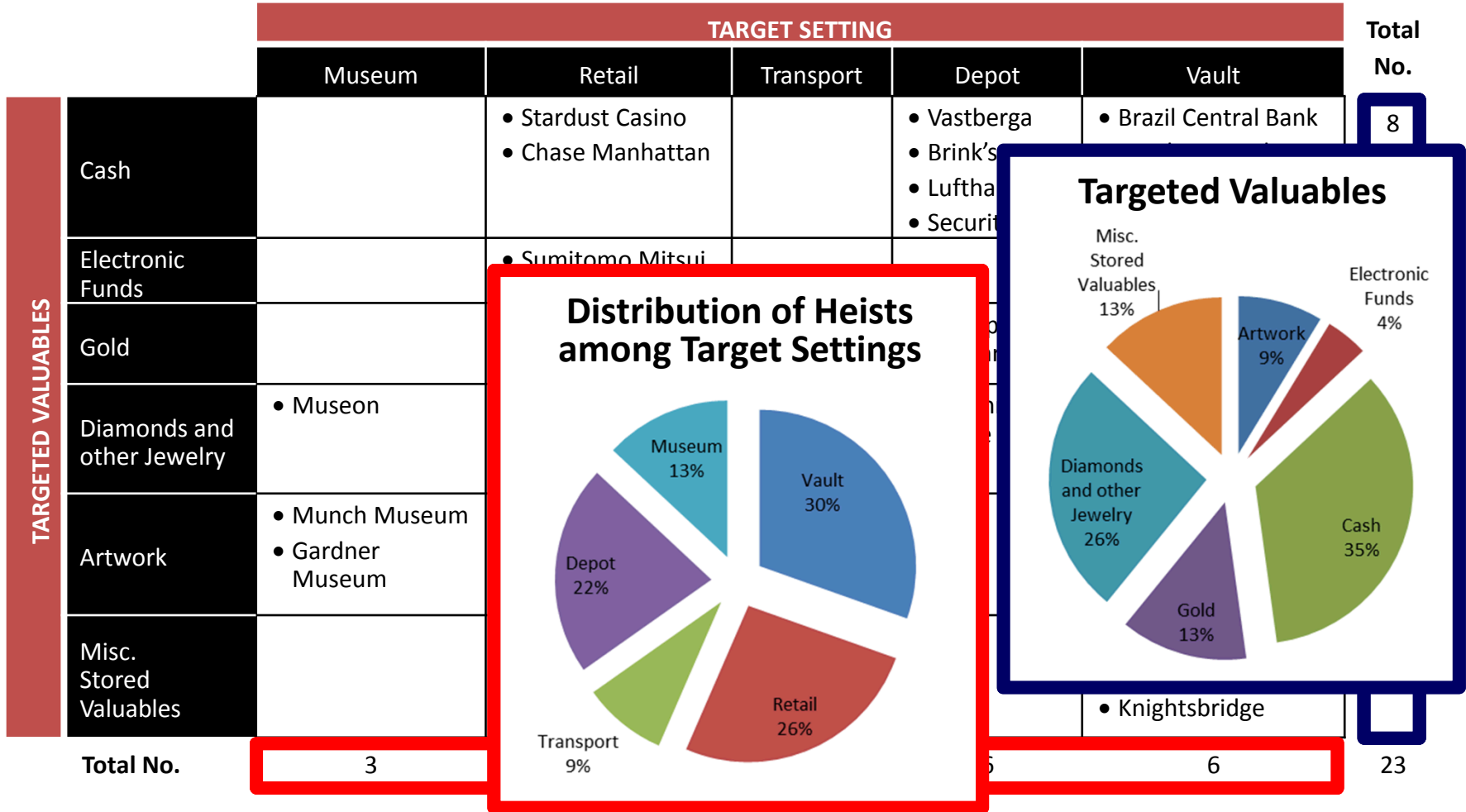
- Sumitomo Mitsui*
- Société Générale
- Knightsbridge



* Heist in which a thief posed in a role he did not legitimately hold.

Timing and Target Selection

Targeted Valuables and Settings

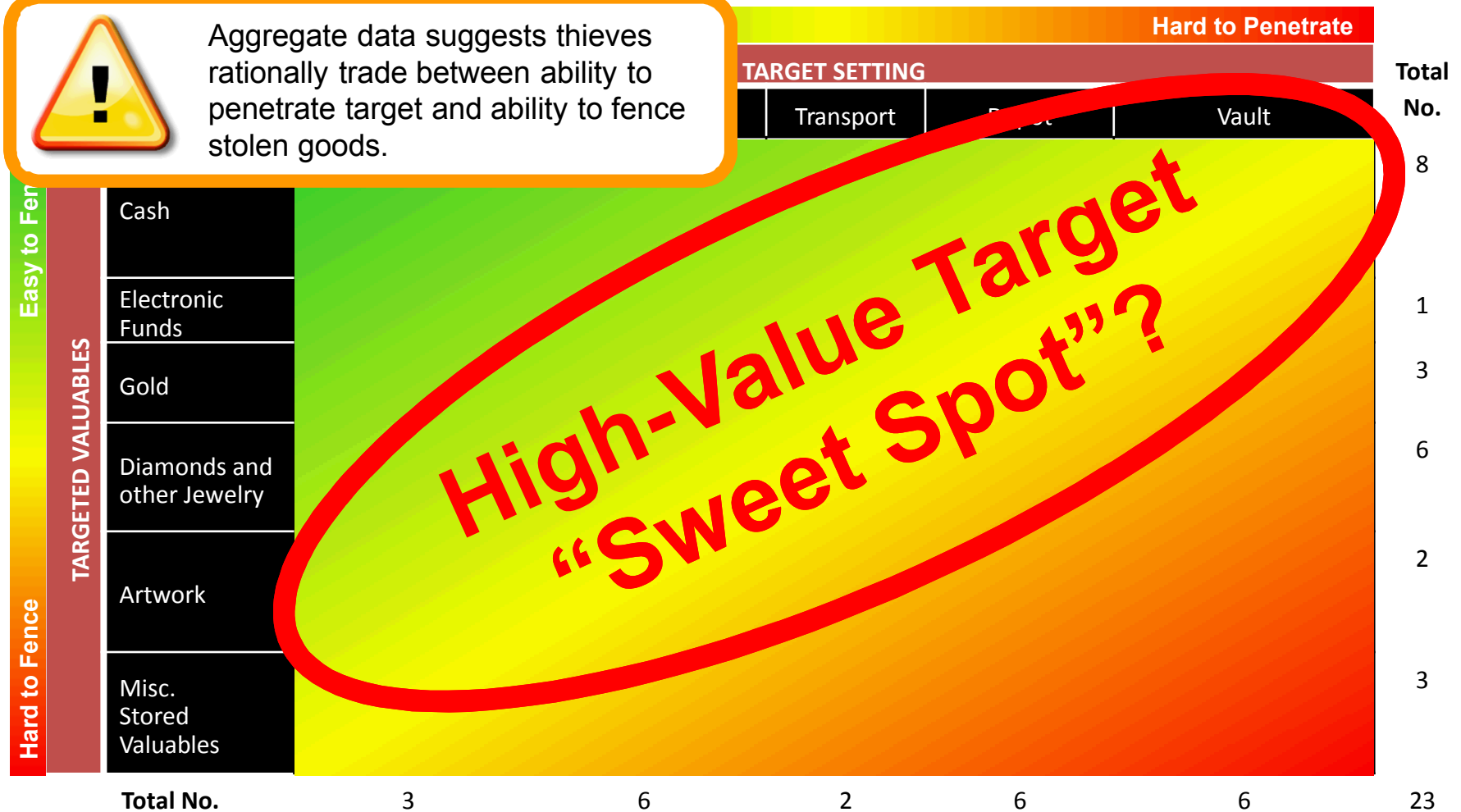


Timing and Target Selection

Targeted Valuables and Settings



Aggregate data suggests thieves rationally trade between ability to penetrate target and ability to fence stolen goods.



A Few More Examples

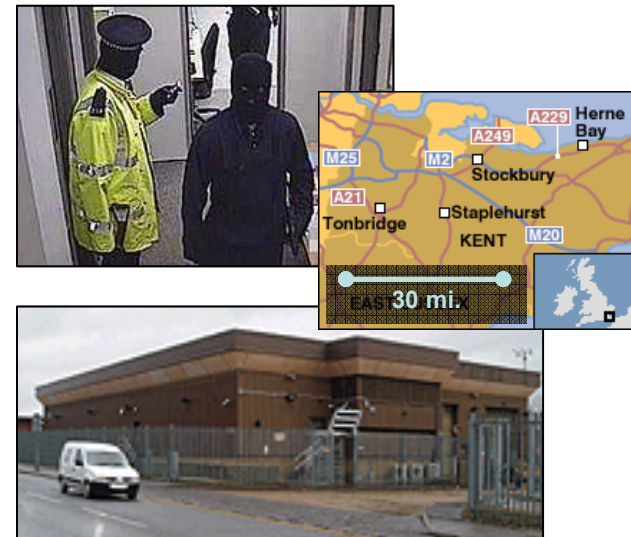
Schiphol Airport: Netherlands, 2005

Two men dressed in KLM uniforms drive a stolen KLM vehicle into the secure freight area at Schiphol Airport. They then intercept a truck carrying **\$115 million** (FY12 equiv.) worth of diamonds bound for a flight to Antwerp.



Securitas Depot: United Kingdom, 2005

Depot manager and his family is kidnapped by thieves posing as policemen. On threat of death to his family, manager is driven to the depot to tell the control room operator to let in seven thieves with a van. The thieves make off with about **\$104 million** (FY12 equiv.) in cash.



A Few More Examples

Brink's-Mat Depot: United Kingdom, 1983

Seven armed, masked men enter the depot 10 minutes after its opening. The six employees present are subdued and bound, and the two employees with the vault keys and combinations are called by name and coerced at gunpoint to open the vault. Seventy-six boxes of gold bullion worth **\$86 million** (FY12 equiv.) are loaded into a van and disappear.





Stardust Casino: United States, 1992

Casino worker on his lunch break walks past security guards, carrying a backpack of cash and chips worth **\$800,000** (FY12 equiv.). Worker is never seen again.




Idea: Heist Baseball Cards


SUBDUE AND SEIZE
Successful




Vastberga Helicopter Robbery


Wed., Sept. 23, 2009, at 05:15
Stockholm, Sweden
59.29802°N, 18.01289°E



Target: G4S Cash Depot
Stolen: \$6.1 million in cash
Heist Duration: 20 min.


Security Force Profile	Thief Profile
Active Guard Station Planning Stage Knowledge Planning Stage Response	Native Citizenship 4 Accomplices on Scene 1 Team in Vicinity
Notable Security Measures: Video surveillance Bullet/Smash-proof glass Reinforced steel doors Padlocked cages	Notable Circumvention: Roof entry via helicopter Cut-to-fit custom explosives Cut-to-fit ladders Circulating saw for padlocks
No Known Insiders	Armament: AK-47 Explosives
Est. Expenditures: \$2,000 Benefit/Cost Ratio: 3,050 Est. Planning Time: 30 days	
Risk of Capture: Medium Risk of Death: Medium	


STEALTH RAID
Successful



Brazil Central Bank Cash Heist

Sat., Aug. 6, 2005, at 04:00
Fortaleza, Brazil
3.734031°S, 38.522256°W



Target: Central Bank Vault
Stolen: \$81.9 million in cash
Heist Duration: Up to 30 hrs.

Security Force Profile	Thief Profile
Inactive Guard Station Aftermath Stage Knowledge Aftermath Stage Response	Mixed Citizenship 14 Accomplices on Scene 1 Team in Vicinity
Notable Security Measures: Video cameras Motion detectors Locked vault door Thick iron and cement floor	Notable Circumvention: Dug tunnel under 1.5 city blocks Created CCTV blind spot Used existing CCTV and motion detector blind spot
Recruited, Passive Insider – Bribed Security Guard	Armament: None Known
Est. Expenditures: \$700,000 Benefit/Cost Ratio: 117 Est. Planning Time: 3 months	
Risk of Capture: Low Risk of Death: Medium	

Heist Traceability

ID	Heist Name	Internet Sources				Book Sources		
		Time	BBC	Discovery	History	Flawless	True Crime	Heists
1	Brazil Central Bank Cash Heist	✓	✓			✓		✓
2	Sumitomo Mitsui Bank Heist							
3	Antwerp Diamond Heist	✓		✓	✓	✓		✓
4	Museon Jewel Heist			✓				
5	Société Générale Bank Heist						✓	✓
6	Stardust Casino Job			✓				
7	Vastberga Helicopter Heist	✓						
8	Millennium Dome Raid							
9	Tanzanian Airplane Gold Robbery							
10	Munch Museum Art Heist			✓				✓
11	Carlton Hotel Diamond Heist				✓	✓		
12	Brink's-Mat Gold Heist		✓			✓	✓	✓
13	Lufthansa Heist	✓			✓			✓
14	British Bank of the Middle East Gold Heist	✓	✓		✓	✓		
15	Chase Manhattan Bank Robbery							
16	Mayfair Graff Diamond Heist		✓			✓		
17	Harry Winston Diamond Heist			✓		✓		
18	Schiphol Airport Diamond Heist					✓		
19	Swissport Heathrow Heist							
20	Gardner Museum Art Heist	✓		✓	✓			
21	Knightsbridge Safe Deposit Center Heist		✓			✓	✓	
22	Securitas Cash Depot Heist		✓			✓		✓
23	Northern Bank Cash Heist		✓			✓		

