Strike Force Piccadilly: a public-private partnership to stop ATM ram raids

Strike Force Piccadilly: A Public-Private Partnership to Stop ATM Ram Raids
In press, *Policing: An International Journal of Police Strategies and Management*, 2009, 32(2).

Tim Prenzler
Australian Research Council Centre of Excellence in Policing and Security, Griffith University, Mt Gravatt Campus, Brisbane, Australia, t.prenzler@griffith.edu.au

Abstract
Purpose – To assess the impact of Strike Force Piccadilly, a New South Wales Police initiative to address an upsurge in ram raids targeting automatic teller machines (ATMs). Also to understand the apparent success of the project in terms of a public-private partnership, involving primarily police and the retail and banking sectors.

Design/methodology/approach – The New South Wales Police provided data showing the numbers of attempted and successful ATM ram raids on a monthly basis from August 2005 to April 2008. The preventive interventions were set against these data in a time series format. The study was limited to within-group data, with consideration of displacement effects by reference to recorded crime data and police intelligence. Interviews about the project process were also conducted with three key participants: The police manager leading the project (public sector), the security manager of a major retail shopping centre chain (private sector) and the commercial security operations manager of a major bank (private sector).

Findings – The increase in ATM ram raids was halted, and the number was reduced from 69 in the 12 months before the intervention to 19 in the final 12 months of the post-intervention period – a 72% reduction. For the same periods, successful raids were reduced from 30 down to two – a 93% reduction. The research indicated that the main influences on the decrease were (1) the creation of a police priority alarm response system, and (2) the installation of situational prevention measures, including special bollards. The larger context for success was the partnership formed between police and industry. The interventions were developed through consultation, co-operative research and commitment from all parties.

Originality/value – The study demonstrates the potential significant crime prevention benefits of public-private partnerships, especially when they are well organised and include research and information sharing. Additionally, the findings challenge the often pessimistic literature about police response times by demonstrating how rapid response can be highly effective in certain circumstances.

Keywords – ATMs, ATM ram raids, ATM smash and grab, Situational crime prevention, CPTED, Partnership policing, Rapid response, Emergency response

Paper type – Research paper

Background

The following study concerns an Australian police intervention to reduce ATM ram raids in the greater Sydney area – including Sydney, Wollongong, the Central Coast and Newcastle. From 2005 there were increasing concerns and media reports about an

escalation in ATM ram raids. The New South Wales Police initiated Strike Force Piccadilly to counter the problem. By 2006 the media were reporting significant reductions in raids, continuing in 2007. The project was recognised as a major successful crime prevention initiative, and is featured at the global ATM Industry Association website (ATMIA, n.d.). Because the project involved police working closely with private sector stakeholders, it was also featured in a plenary presentation at the national *Security 2007 Conference* hosted by the Australian Security Industry Association Limited, the peak private security industry association (Chapman, Wilkey & Julian, 2007). The Strike Force Piccadilly methodology exemplifies many of the best aspects of problem-oriented policing, situational crime prevention, crime prevention through environmental design (CPTED) and partnership policing (Goldstein, 1990; Clarke, 1997).

ATMs – automatic teller machines – are also referred to as "automated teller machines", "cash machines", "bank machines" or "cash points". The devices are usually operated by customers inserting a plastic card, with a magnetic strip or other form of encoded information, that allows them to withdraw cash. The electronic networking of ATMs was developed in the late-1960s and led to their uptake around the world from the 1970s (Schreiber, 1994). ATMs can be placed in a great variety of locations. Early versions were built into the walls of banks ("through-the-wall" machines) and serviced from inside the building. However, both customers and retailers sought wider access. Consequently, free-standing machines that are easily transported are now placed in almost every conceivable place where people gather, such as transit hubs, clubs, grocery stores and petrol stations. Some banks have drive through lanes where customers can access machines without leaving their vehicles, and some provide mobile ATMs in vans. June 2007 saw the 40th anniversary of the installation of the first ATM (in London). At the time of the anniversary it was estimated there were 1.6 million machines worldwide (Milligan, 2007).

Security was always an obvious concern with ATMs, and the initial embedding of Personal Identification Numbers (PINs) in cards was a major factor in reassuring customers. However, ATMs have been, and remain, extremely attractive targets for thieves (Guerette & Clarke, 2003; Schreiber, 1994). Muggers will try to take cash from customers immediately after a transaction. Robbers can force victims to remove cash and hand it over. Thieves will attempt to steal cards with the PIN from a home or wallet, or try to work out the PIN of a stolen card using common numbers such as birthdates. More sophisticated thieves have used card-reading devices, which appear to be part of the machine, and copy customers' details. Some have videotaped key strokes from a distance. Others have developed a technique for trapping cards inside machines and then retrieving them after they are abandoned by the customer. Cash deliveries, especially for machines with no interior access, create an opportunity for armed robbery.

The "vault" inside the machine and the whole machine have also become targets. Banks are generally secretive about the amounts of cash stored in ATMs. Obviously they contain very large amounts of money by the standards of ordinary people. Consequently, thieves have tried to cut open machines, or tried to breach casings with explosive devices. Given the time involved in the process and the threat of discovery, a safer alternative is to use a vehicle to remove the whole ATM and take it to a point where the vault can be accessed. This latter type of crime is usually identifiable as an

"ATM ram raid" (sometimes called an "ATM smash and grab"). A "ram raid" refers to any attempt to smash a vehicle through the doors or windows of premises in order to steal valuables. The modus operandi with ATM ram raids is variable but typically involves at least one vehicle (usually stolen), which is used to break into the area where the ATM is located, knock over the machine, and then remove it.

The extent of ATM-related crime, and ram raids in particular, is difficult to determine because they constitute crime sub-categories not covered by official statistics. Incidents are hidden within figures for robbery, theft, vandalism and motor vehicle theft. ATM ram raids are extremely violent in terms of damage to property. They are normally carried out when people are not around, but they can be highly intimidating for witnesses; and they can involve the assault and kidnap of people, especially security guards. Most ATM crimes are committed within a few minutes or less, and the location of ATMs usually facilitates ease of offender access and escape (Scott, 2001).

ATM crime is one example of the many types of offences where police, responding to a report, usually cannot arrive in time to stop the offence or catch the offenders. This situation has given rise to the recurring discrediting of police rapid response as an effective crime prevention strategy. Research in the United States in the 1970s led to the conclusion that,

> The speed of police response to calls for assistance (1) does not affect arrest rates (the ratio of arrests to crimes reported), (2) is not crucial in satisfying the public, and (3) rarely prevents further injury or damage (Bayley, 1998, p. 52).

Subsequent research has led to some modifications of this view. Studies have shown that citizen satisfaction can increase with the speed of the police response (Percy, 1998). It has also been recognised that reducing response times can prevent the continuation of a crime event and reduce the amount of harm. This is supported, for example, by research on reducing breaches of domestic violence protection orders, where police have provided the holders of protection orders with alarm pendants and then prioritised emergency responses to alarm activations (Lloyd, Farrell & Pease, 1994). An important variable in the equation is the delay between the onset of a crime event and the call to police. Increasing the rapidity at which police are notified of a crime event can theoretically contribute to a more effective interdiction (Gaylord & Galliher, 1991; Percy, 1998). Bayley (1998, p. 53) has also emphasised how police responses can be rendered more effective through a 'graded response' system, in which dispatchers and police are trained to prioritise serious calls or calls where a rapid response might lead to the capture of offenders or prevention of further offences.

ATM security providers and criminals have engaged in a process of "one-upmanship" also common to many crime problems. Techniques by which thieves obtain PINs have been countered in part by instructions about PIN security (such as keeping PINs separate from cards), non-acceptance of PINs using obvious numbers like birth dates, and the encryption of numbers on the ATM screen (to prevent "shoulder surfing" where thieves read the PIN from behind the customer). Various situational prevention and CPTED (crime prevention through environmental design) measures have also

been introduced over time, including the following (Gill, Duffin & Keats, 2005; Guerette & Clarke, 2003; Schreiber, 1994; Scott, 2001):

- Machines placed within protective vestibules accessed via the swipe card.
- Privacy zones marked out on the ground and queuing rails to separate users from potential offenders.
- Telephone hotlines to allow customers whose cards are stolen to cancel transactions.
- Fingerprint, iris and facial recognition technologies.
- Improved "natural surveillance", by locating machines in public places, with good lighting, and transparent walls on vestibules.
- Surveillance cameras.
- Locating machines in police or security stations.
- Static guards on foot duty next to ATMs.
- Limiting amounts that can be withdrawn at any one time.
- The machine "eating" the card following repeat attempts with the wrong PIN.
- Automatic shutters when the machine is not being used.
- Bollards that prevent or deter vehicle access.
- Alarms and tracking devices.
- Dye bombs or smoke bombs that mark or ruin the money and "deny benefits".

All of these measures have limitations. Cash ceilings and hotlines can be partly circumvented when a delay in the discovery of a card theft means that thieves can make multiple withdrawals before authorisation is withdrawn. Bollards and wall fittings can be defeated with powerful vehicles; and some ram raids have been perpetrated with earth moving machinery or forklifts ripping the ATM out of a wall. "Lassoing" is another technique for removing ATMs with a chain attached to a vehicle. Security devices can also be inconvenient and face lack of acceptance by users. Every layer of security usually entails an additional step by a customer and some kind of access restriction or time delay.

There is very little published research on ATM crime prevention. Research based on interviews with convicted ram raiders in the United Kingdom showed they are typically males in their 20s, with long histories of diverse and serious offences, who form teams with clear specialisations (Wilson & Donald, 1999). Another UK study using interviews found ATM offenders were highly prolific but could be deterred by factors such as improved visibility and barriers (Gill, et al., 2005). Research in Greater Manchester in 2001-3 revealed one quarter of "street crimes", such as robbery and bag snatching, were related to ATMs. The study included an intervention in which a small "personal space zone" was painted on the ground around selected machines. In a six month period, robbery around the experimental sites declined from an average of 27 down to 9.2 per site (Holt & Spencer, 2005).

The most relevant study on prevention, by Guerette and Clarke (2003), analysed the impact of special security legislation on ATM-related robberies. Following escalating robberies against customers, Los Angeles and New York city councils legislated security standards in 1991 and 1992 respectively. According to Guerette and Clarke, the following were mandated in both cities: improved lighting, "safety reminders" to customers, and warnings to potential offenders about security measures. New York

required ATMs be located in vestibules with access control and transparent windows, and required security guards where customers were allowed to access ATMs inside banks outside business hours. Los Angeles required reduced vegetation, and risk assessments before installation. Many Los Angeles' banks also adopted cameras, mirrors for users to see behind them, and reduced operating hours at peak crime times. In New York, between 1991 and 1999, ATM robberies declined by 78% from 380, in the peak year, to 82. In Los Angeles, from 1992 to 2000, ATM robberies declined by 88%, from 152 per year to 18.

In the cases outlined in Guerette and Clarke (2003), the initiative came from local government, rather than other potential stakeholders. In one of the earliest socio-legal assessments of ATM crime, Schreiber (1994) was highly critical of banks for failing to acknowledge the vulnerability of ATMs until victims of violent ATM crimes began to litigate. Legislated standards were sometimes opposed by banks on grounds of costs and alleged inconvenience to customers. Schreiber was also critical of the failure of police and banks to work together to address the problem. Lack of cooperation between police and the burgeoning private security sector – including in-house corporate security – has been a point of frequent criticism in relation to the need for better crime prevention (Sarre & Prenzler, 2000). One of the obvious obstacles to cooperation is that the two operate on contrary principles – one provides a free service to all citizens on the basis of need, the other provides a service specific to clients on a commercial basis. Nonetheless, there are areas where the two can work together ethically, with a wider public benefit, and there is a small but growing literature on case studies of successful cooperation in areas such as information sharing and priority call arrangements (Chamard, 2006; CoESS, 2002; Gimenez-Salinas, 2004). Schreiber (1994) concluded that:

> ATM security does not depend on high-tech or expensive security devices but on a quantifiable assessment of risk, coupled with the development of intelligent ATM security policies and the deployment of needed security equipment. Also important are the documentation of security activities at the individual ATM level, the safety education of cardholders, and cooperation between law enforcement and private security officers. These combined efforts can make expanding ATM use … convenient, accurate, and safe (p. 21A).

Method

Enquiries by the author led to a formal request to the New South Wales Police for access to non-confidential information associated with Strike Force Piccadilly. The Department provided figures on the numbers of attempted and successful ram raids on a monthly basis from August 2005 to April 2008. The main documentary source was a booklet, *ATM Theft Reduction Strategies: Police Resource* (NSWP, 2006), which provides guidelines for ATM security and includes a description of Strike Force Piccadilly. Interviews were also conducted with three key participants:

1. Detective Inspector Murray Chapman, Commander of Strike Force Piccadilly during its main phases of development and implementation;

2. Mr Michael Julian, General Manager, Security, Westfield Limited, one of the largest retail shopping centre chains in Australia; and

3. Ms Melissa Wilkey, Commercial Security Operations Manager, Australian and New Zealand (ANZ) Banking Group.

Two interviews were tape recorded and transcribed and one was conducted by e-mail. Topics included the nature of the crime problem, the nature of the relationships between stakeholders, what strategies were adopted and why, elements of success, and limitations or problems in the project. The above sources were supplemented with a newspaper search on the media search engine *Factiva*, and searches of publicly available New South Wales Police crime data and annual reports.

The main methodological challenge concerned the absence of a control group. Strike Force Piccadilly was a "natural experiment", in the sense that it was a police response to a specific rapidly escalating problem. The initiatives were developed without a full experimental control system, in part because of the emergency nature of the situation. Furthermore, "ATM ram raid" is not an official offence recorded by police. ATM ram raids involve a range of offences, which can include robbery, armed robbery, assault, motor vehicle theft and damage to property. "ATM ram raid" was a composite category created specifically by the Strike Force from reported incidents that in combination matched the characteristics of ATM ram raids. No official numbers on this type of crime were collected prior to that time; and the category was not available for comparative purposes from other major cities, where it appears that ATM ram raids did not constitute a major problem (*Factiva* search). Strike Force Piccadilly did, however, liaise closely with other strike forces, especially those concerned with armed robbery, to compare incident trends and watch for displacement effects. The author also compared the ATM ram raid figures against those for related offences recorded by police in the Sydney Metropolitan Area.

In sum, strictly speaking, the study is confined to an analysis of within-group variation. At the same time, official crime data and the interviews with key insiders (with access to criminal intelligence and business security information) were used to attempt to identify all variables that may have affected ram raids. It should also be noted that the process of developing the Strike Force Piccadilly interventions was also the subject of the research reported here. Consequently, the findings section below includes both process and impact data, and the findings on process are deployed to explain the impact data.

Findings

Process: Defining the problem and developing strategies

The three interviewees confirmed that there was a growing problem with ATM ram raids in the greater Sydney area in 2005. As noted, the exact number cannot be calculated because the raids do not constitute an official crime category for regular recording and reporting purposes. A joint press release in October by the Australian Bankers' Association, the ATM Industry Association and the New South Wales Police, announcing a security review, referred to 25 attacks in three months (ABA, 2005). The upsurge in attacks received press coverage (e.g, *Daily Telegraph*, 2005; Brown & Kennedy, 2005) and drew interest from the parliamentary police oversight committee (Parliament of NSW, 2005). A likely trigger factor for the upsurge was the

enormous growth in free-standing ATMs, with as many as 20,000 machines in New South Wales at the time (Kennedy, 2005). The introduction of the smaller and lighter machines greatly enlarged criminal opportunities in terms of access routes, escape routes and portability.

The New South Wales Police established Strike Force Piccadilly in August 2005. The term "Piccadilly" was a computer generated name. Intelligence gathered by the Strike Force revealed that offenders left very little evidence behind. They wore gloves to protect against leaving fingerprints, and took sufficient time and care to avoid leaving DNA traces. Interviewees reported that information about successful methods was spreading amongst criminals. New groups were entering the field, including offenders released from prison. The Strike Force immediately began using crime reports to generate two categories of incidents: "unsuccessful raid" and "successful raid". With unsuccessful raids, the criminals fail to obtain the cash, but in the process numerous crimes are completed, including motor vehicle theft and major damage to property. From four attempted raids per month in August and September 2005, the number increased to 12 in May 2006. The success rate also rose, from 30% in the first half of the period to 50% in the second half.

The incidence data also showed that large shopping centres were increasingly becoming targets for raids, despite the fact that ATMs were often deep within the buildings in atriums. Many of the raids were extremely daring. A typical scenario involved between two and four stolen vehicles and a team of 4-5 desperadoes. A large four-wheel drive would be used to smash through bollards and front doors, drive through a store-lined passageway and knock over the ATM. The four-wheel drive would be followed by a transit van. The men would load the ATM into the van and, abandoning the first vehicle, make their escape in the van. The ATM would be cut open at a nearby location. Finally, the van would be abandoned (sometimes set on fire to destroy evidence) and the men would scatter in other vehicles – also usually stolen. In some cases, guards who showed up on the scene of the theft were taken hostage until the thieves escaped.

Following limited success in reducing the number of raids, in June 2006 the Commander of Strike Force Piccadilly organised a conference of stakeholders to address the problem. The meeting was facilitated by Westpac Bank, and was well attended by members of the Australian Bankers' Association (ABA), the cash-in-transit industry, the Shopping Centre Council of Australia and the ATM Industry Association (ATMIA). The purpose of the meeting was to obtain as much information as possible about current security strategies, their strengths and weakness, and the key factors facilitating ram raids; as well as to engage stakeholders in the development of a coordinated prevention strategy. The approach represented a shift from a traditional "investigate and charge" methodology, with a police monopoly, to a wider cooperative situational prevention approach. The meeting, which adopted an open forum format, identified the following points.

- A number of organisations were attempting to address the problem in isolation from the others.

- Existing security devices were fairly basic, including back-to-base alarms, CCTV, bollards, and wall and floor fixings.

- Organisations were scoping alternative strategies in different areas. These included target hardening strategies (such as chain guards), techniques to reduce rewards (including money degradation and dye packs), and devices that aid the location and recovery of stolen property (such as smoke bombs and tracking devices).

- Most organisations used a combination of alarms, including seismic alarms (triggered by vibrations), reed switches (triggered when doors on the machines or premises are breached), panic buttons for guards, power failure alarms, and heat/smoke alarms (that detect attacks with oxy acetylene or cutting tools).

- In isolation, most of the strategies could be defeated. For example, thieves defeated camera identification by wearing balaclavas and using stolen vehicles. Standard bollards and fixtures were easily defeated with large vehicles or cutting equipment. GPS tracking only led to an empty vandalised ATM.

- Some strategies, such as dye explosives, were considered to pose a safety risk to security guards.

- Alarm response times by security firms were usually well above the time taken by the gangs, who were coordinated, efficient and well equipped.

- A large number of false alarms was generated, as many as 40 per night across Sydney, which made security firms reluctant to call police. Police also held a power to fine firms for nuisance alarm calls. Alarms could be set off by cleaning equipment, or even by passing trucks and nearby construction.

- Alarm response firms tended to call police only after machines had been stolen. This could be up to half an hour after the raid occurred.

Out of this relatively bleak picture the Strike Force Commander developed a more refined set of questions about the features of successful and unsuccessful raids. Subsequently, stakeholders fed back data that showed promise for more systematic exploitation:

- There were no ram raids against ATMs located in areas that could not be accessed by a vehicle, such as upper floors of shopping centres with restricted access or at the end of narrow passageways.

- There were also no raids against ATMs with a combination of (1) alarmed premises and (2) internal bollards or barriers directly adjacent to the machine (see Figure 1).

- A strong indication of a genuine ram raid in progress was when multiple alarm systems activated, and this usually occurred on average only once a night in Sydney.

- Multiple alarm activations occurred mainly between 10.30pm and 5.30am, but mainly around 1-2am.

Figure one about here

While this consultative process was underway, police analysts were engaged in data assessments. Evidence from crime scenes and interviews with arrested offenders revealed two crucial facts:

- The ram raiders were extremely concerned about capture and gave themselves a very short operating window of approximately two minutes. If they encountered a delay they would abandon the raid.

- The raiders used scanners to listen in on the police radio system. If police were called, they would usually abandon the raid.

The first point shed some light on the earlier finding about internal bollards. In the words of the Strike Force Commander:

> During debriefs a number of offenders reported they we're happy to stay in a carpark, in high performance cars, and cut bollards outside the entrance of shopping centres because they didn't want to activate intruder alarms. They would cut the bollards, and if the police turned up they would make good their escape out the carpark exits. Once they drove the four-wheel drive and the van through the front of the shopping centre they'd breached an intruder alarm and the clock started ticking. Plus they would be stuck in the mall and they would then have to get out of the truck and defeat the bollards around the machine before they could ram the machine. Basically they were all worried that once the security guard or the police turned up they would just put their car across the entrance and they'd be stuck in the shopping centre.

The combination of these factors led to reconsideration of the utility of police rapid response, subject to a number of determining factors. If false alarms could be reliably screened out, and police could prioritise genuine calls, it might be possible to reach the scene inside the thieves' window of opportunity, especially in the quiet period after midnight. The Commander took these ideas to meetings with the Australian Shopping Centre Council, ABA and ATMIA, who were strongly supportive. The Head of Security for Westfield shopping centres proposed that the priority response should be complemented with a system for sharing information about security. Theoretically, the police rapid response would be enhanced by reducing the window of opportunity through the widest possible application of best practice security measures: restricting vehicle access, and the inner bollard/alarm combination; as well as advancing and trialling some of the more promising strategies under review, such as more resistant bollards. An immediate likely benefit of this combination of strategies was the capture, and incapacitation in prison, of the main gang members. An additional long-term benefit was the likely deterrent effect on other criminals, as word spread that the risks in ATM attacks outweighed the potential rewards.

A detailed plan and rationale were developed that received approval from the Police Deputy Commissioner Operations. A dedicated 1800 toll-free number was given out

to all relevant alarm monitoring companies. This number bypassed the public emergency call system. The companies agreed to use the 1800 number when a "multiple alarm" activation occurred and provide police dispatchers with the location of the ATM. Multiple activations that triggered 1800 calls usually involved two alarms (e.g., seismic alarm followed by power failure) or often three. The monitors were given discretion about what combination of alarms they thought constituted a probable ram raid. (Single or questionable alarm activations were investigated by security firms and/or referred to the general police call number.) Police agreed to broadcast the 1800 calls over the radio dispatch system as "ram raid in progress" and to proceed "on urgent duty with lights and sirens". Dispatchers and patrol officers were informed about the system and instructed about the need to prioritise a response. The 1800 system came into operation in Sydney in July 2006. In December it was extended to the greater Sydney area at the request of industry partners following a round of meetings with stakeholders in regional centres.

The second idea regarding information sharing resulted in five main practical outcomes:

1. The development and distribution of a 14 page easy-to-read illustrated booklet outlining all key aspects of ATM security (NSWP, 2006). The guidelines describe how situational factors – such as vehicle access, alarms, bollards and barriers, and lighting – can be modified to reduce the risk of attack. The guidelines allowed site managers and organisations to carry out a simple assessment themselves and make improvements based on best practice.

2. The New South Wales Police made Crime Prevention Officers (CPOs) available to carry out on-site risk assessments and provide reports with recommendations for improved security. (Consideration had been given to legislating standards. However, it was agreed that adequate provision, at least in the interim, was available under the New South Wales *Environmental Planning and Assessment Act*, which gives police input into the development approval process, frequently via CPOs.)

3. Strike Force Piccadilly analysts generated confidential intelligence reports that were distributed by e-mail to stakeholders shortly after each attempted ram raid. The de-identified reports gave details of attempted ram raids and reinforced the factors set out in the guidelines, by focusing on security devices absent in successful raids and present in unsuccessful raids. Westfield security took a lead in designing the form used to produce the intelligence reports:

> None of us got hit more than three or four times, but aggregated it's an awful lot. So we created a form that the owners of properties would fill out whenever they had a ram raid. There was a set of questions: "Was it open entry? Were there bollards? Did they run over the bollards? Did they cut the bollards? What did they use to cut the bollards?" … The initial response was, "We don't want to share that information. It's confidential." So we said, "We don't want to know how much money was taken, we don't want to know the victim's name or the name of the company, just the suburb it happened in and the MO" [*modus operandi*].

4. Industry members agreed to share information about the benefits and problems associated with trial technologies.

5. Police undertook to continue to consult with the stakeholders, to obtain feedback on the project and provide advice and assistance on any relevant matters.

The intelligence reporting system began in September 2006. The guidelines were published and distributed in December 2006. The communication and assistance strategies were maintained from the initial conference.

Impact

Figure 2 shows all attempted ram raids, both successful and unsuccessful, from August 2005 to April 2008. The data indicate an immediate and dramatic drop in the number of raids from a peak of 14 in July 2006, following the implementation of the 1800 hot line in Sydney on July 20th. There was then something of a bumpy plateau effect from September 2006 to March 2007 – around 4.5 per month. This was followed by a spike up to seven in April, followed by a drop to one in May. A fluctuating pattern then followed around 1.6 per month. The figure also marks the introduction of additional preventive measures, including the risk assessment guidelines, the extension of the hotline to the Greater Sydney area, and the intelligence reports.

Figure 2 about here

The data do not allow for the effects of the different prevention strategies to be disentangled. In fact, given the number of ATMs and the variety of organisations managing machines, it was impossible to quantify all the changes made, such as relocation of machines or installation of bollards and barriers. However, it is clear that the introduction of the 1800 number coincided with a steep drop in offences – although it was not until March 2007 that all initiatives were fully implemented. The available pre-intervention data cover 12 months from the start of data collection in August 2005 to the introduction of the hotline near the end of July 2006. An appropriate post-intervention period for comparative purposes is the 12 months from May 2007 to April 2008, after all initiatives should be have been bedded down (apart from ongoing security upgrades). In the pre-intervention period there were 69 raids (both "successful" and "unsuccessful"), an average of 5.7 per month. In the post-intervention period there were 19, an average of 1.6 per month, making for a 72% decline ($t = 3.26$, 11 d.f., $p = 0.008$).

Figure 3 disaggregates the data in Figure 2 in terms of successful and unsuccessful raids. Pre-intervention, there were 30 successful raids, with an average of 2.5 per month. Post-intervention there were two successful raids, making an average of 0.1 per month – a 93% reduction ($t = 4.69$, 11 d.f., $p = 0.001$). An additional relevant aspect is that the number of raids was increasing in the pre-intervention period, so not only was the overall incidence significantly reduced but the increasing incidence was stopped and turned around. Furthermore, the post-intervention phase saw a tailing off in both unsuccessful and successful raids.

Figure 3 about here

Explaining the impact

Police intelligence was able to explain the effect of the 1800 hotline by assessing crime scene data and debriefing arrestees. In the words of the Strike Force Commander:

> Once the 1800 number was operating, when the first real ram raid occurred a multiple alarm was detected. It was broadcast immediately. The offenders heard it over the radio and had to abandon the offence and start to flee. The police arrived on the scene and were able to pursue the offenders and it resulted in a number of arrests after a high-speed car chase.
>
> The offenders started doing things they normally wouldn't have done. They left exhibits that they'd normally take with them: peeled off balaclavas, gloves were being lost. Offenders started getting clumsy and were dropping things when they heard police were on their way.

This pattern continued, with a number of significant arrests and collection of DNA and other evidence. The proportion of unsuccessful raids increased from 50% in the second half of the pre-intervention period to 64% in the first four months after the intervention. Between August 2005 and June 2007, 97 persons were arrested for 491 offences related to ATM ram raids; and 21 separate gangs "were identified, dismantled or disrupted" (Interview 1). The arrests resulted from the snowball effect of apprehensions at or near the scene, information from arrestees, increasing amounts of evidence that allowed for forensic data matching, and some undercover work:

> Forensic Armed Robbery Unit people would come out and examine the crime scenes. So a lot of people were identified through analysis of physical exhibits, and through police investigations of suspects (Interview 1).

The very large majority of arrests resulted in convictions and jail terms, with the remainder still in progress through the courts. The "mopping up" of suspects is ongoing.

Police intelligence indicated there was a partial displacement effect, with some ram raider gangs moving into armed robberies of cash-in-transit (Interview 1). However, the New South Wales Police Armed Robbery Squad was able to arrest these offenders. (See NSWP 2007, p. 24ff on task force formation and targets in 2006-7.) During this period the rates of major offences recorded by police in the Sydney Metropolitan Area were either stable or in decline, with the exception of "steal from motor vehicle" (Goh & Moffatt, 2008, p. 18). Specifically, there were no statistically significant differences between 2006 and 2007 for "robbery with a firearm", "robbery with a weapon not a firearm", "break and enter – dwelling" and "malicious damage to property". There were statistically significant reductions in "robbery without a weapon", "break and enter – non-dwelling" and "motor vehicle theft".

The information sharing and situational prevention aspects of the project also appeared to produce positive outcomes. The results of experimentation with security

devices were shared amongst stakeholders, disseminated via the police. Bolted down and/or hollow bollards were found to be completely ineffective. Thieves could cut through them in seconds with high powered cutting tools, or simply knock them over. Attempts to fill bollards with a special concrete mix or "steel cruciform" also proved fruitless, as did rubber materials designed to melt onto the cutting blade. Chain guards similarly had limited effect, unless they were combined with other measures. Two types of target hardening/access control devices, however, were shown to be effective in either preventing or significantly delaying removal of bollards (and ATMs). One was the invention of a "rotating core". Steel ribbing on the free spinning core would catch the blade and grind it down or make the blade spin uselessly. Initially it was found that a drill bit could be used to stop the core spinning. However, a process for toughening the metal was then developed, making the core resistant to drilling. Soon after this breakthrough, two other groups invented more effective fill: "You cut right into the steel, but as soon as you hit the core the blade dies" (Interview 2). Another successful intervention from this period was the "Raminator". This is a device that utilises either a bracket or base plate, attaching the ATM to the floor, which bends to absorb impact but does not break and is difficult to cut.

It was not possible to comprehensively map the installation of security devices. In many cases police were informed of installations, and provided advice. But, in general, the private sector stakeholders were unwilling to release figures for reasons of confidentiality and security. The Task Force Commander estimated there were a large number of installations, and that "banks aggressively installed internal bollards at their most vulnerable locations and made this a priority security measure". The bank Security Manager emphasised the value of the intelligence system in deciding where to prioritise security upgrades (Interview 3). Some stakeholders indicated that moving machines to safer locations would compromise customer access. Nonetheless, there were relocations of machines as well as installations of cut-resistant bollards outside premises (Figure 4). There were only a few requests for risk assessments by police as organisations developed their own capacity. However, the Crime Prevention Officers reported they found the guidelines particularly useful when advising on ATM security in relation to development applications under the *Environmental Planning and Assessment Act* (Interview 1).

Figure 4 about here

Discussion

Strike Force Piccadilly appears to have been an extraordinary success in reducing ATM ram raids in the greater Sydney area. From alarming peaks of 12 raids in May and 14 in July 2006, the number was reduced to an average of 1.6 per month in the last 12 months of data. Furthermore, the number of successful raids was reduced from peaks of five and six per month down to an average of 0.1 for the last 12 months. As always, with these types of interventions, it is important to test for alternative explanations and check for displacement effects. In the case of Strike Force Piccadilly, there is ample evidence for the effectiveness of the interventions, by way of ram raids abandoned before completion and the testimony of arrested felons. Police intelligence indicated there was a small displacement effect, primarily to armed robbery. However, a focused response by police appears to have quickly extinguished the displacement-related robberies. Furthermore, in a period of generally static crime

rates, there was no evidence of a more general displacement effect in crimes reported to police.

The results highlight how a traditional but often discredited policing strategy – rapid response – can be put to good effect to (1) detect crimes in progress and prevent their continuation, (2) contribute to the arrest and incapacitation of offenders, and (3) generate a preventive deterrent effect. The Strike Force Piccadilly example supports Bayley's (1998) contention that the effect of rapid response can be enhanced by minimising the time between the onset of a crime and the call to police, and by ensuring dispatchers and patrol officers prioritise target crimes. The overall crime reduction effect of Strike Force Piccadilly was also facilitated by the more focused deployment of criminal intelligence and traditional follow up investigations.

The results also indicate that a strategy based on police interdiction is likely to work best with strong support from parallel agencies, such as private security. That support can be direct – as in formal alarm response protocols – or more indirect – in the form of CPTED applications on private property at the physical location of high-risk crime targets (Guerette & Clarke, 2003; Schreiber, 1994). To get through the project stages of development, implementation and maintenance, a systematic process of engagement of all stakeholders was required, involving formal and informal meetings, one-to-one discussions, and good relations between parties. Of particular note was the use of information sharing (including by e-mail), experimental research, and commitment to implement recommendations supported by evidence. Interviewees agreed that businesses had saved millions of dollars by not installing ineffective security, such as hollow and bolted bollards, thanks to the willingness of companies doing research to share their findings.

Crime problems like ATM ram raids that occur on private property raise the question of who is responsible for crime (Chamard, 2006; Sarre & Prenzler, 2000). In the Sydney case, separate private sector organisations were struggling to contain the problem. The raids were also seen as a policing challenge, given the threat to public safety entailed in a violent crime, and the large sums of money involved with potential flow-ons to the public. Consequently, both sides took a share of responsibility and agreed to work together. In the words of the Westfield Security Manager, "There should be no competition with public safety". And what is notable about the project is that an effective division of labour was adopted on a rough *quid pro quo* basis. Police prioritised ram raid alarm calls (subject to a continuing triage system), while the private sector conducted research and implemented situational prevention measures (cf., Gaylord & Galliher, 1991, on police rapid response interacting with environmental design principles).

The Police Commander concluded:

> Without the help of the industry supplying data we would never have been able to identify some of the solutions which were put in place – without consulting with the industry and without giving them the information back. The R&D about anti-ramming devices was important. But getting the industry to use what appeared to be working was also important.

In similar terms, the Westfield Security Manager stated:

> With the 1800 number the cops got to the scene faster and they got 'em, they caught these guys, great job. But it was up to us to design prevention, which we did. We could have done a lot on our own but we would not have done as a good a job without the information coming from the police.

The ANZ Banking Group Security Manager emphasised how "trust between the partners fostered collaboration". This was particularly important in the area of confidentiality of data: "Trust encouraged each party to be more transparent and forthcoming with research, development and improvement initiatives". Consequently:

> The quality of the industry-wide trend analysis provided a strong business case for the allocation of resources:
>
> - For banking security representatives to obtain approval for capital expenditure funding to improve and upgrade security protection measures across their ATM networks
> - For NSW Police to allocate and maintain resource levels to Strike Force Piccadilly
> - For shopping centre owners to allocate funding to upgrade/strengthen their "at-risk" premises.

Conclusion

This paper has described a successful public-private partnership to halt the increase in a serious violent crime, and then reduce and almost eliminate the incidence of attempted and successful attacks. It appears that the key strategy was a mix of strategies: a hotline from private security firms to police; and the installation of a range of target hardening and access control strategies. The key point is that behind these applied techniques was a larger problem-oriented strategy of consultation, research and information sharing amongst all stakeholders

Acknowledgements

Thanks to Murray Chapman, Michael Julian, Melissa Wilkey for interviews and assistance; to Detective Superintendent Bingham of the New South Wales Police for permission to access to data; and to the journal reviewers for helpful advice. This research was funded by an Australian Research Council Linkage Grant.

References

ABA (2005), "Review of ATM Security", *Joint Media Release*, Australian Bankers' Association. www.bankers.asn.au/default.aspx?ArticleID=944, accessed 29 April 2008.

ATMIA (n.d.) Ram raid information sharing webpage. ATM Industry Association. http://www.atmia.com/mig/atmsecurityramraids/, accessed 29 April 2008.

Bayley, D. (1998), Ed., *What Works in Policing*, Oxford University Press, New York.

Brown, M. & Kennedy, L. (2005), "Raids force new look at ATM safety", *Sydney Morning Herald*, 27 August, p. 5.
Chamard, S. (2006), *Partnering with Businesses to Address Public Safety Problems*, US Department of Justice, Office of Community Oriented Policing Services, Washington, DC.
Clarke, R. (1997), Ed., *Situational Crime Prevention: Successful Case Studies*, Harrow and Heston, Guilderland, NY.
Daily Telegraph (2005), "Smash and grab: ATMs replace banks as raid of choice", 30 April, p. 10.
Goh, D. & Moffatt, S. (2008), *NSW Recorded Crime Statistics 2007*, New South Wales Bureau of Crime Statistics and Research, Sydney.
Chapman, M., Wilkey, M. & Julian, M. (2007) "Strike Force Piccadilly, ATM Ram Raids – An intervention and prevention model", *Security 2007 Conference*, Australian Security Industry Association Limited, Sydney, 10-12 July.
CoESS (2002), *Report of the Seminar Public-Private Partnerships*, Confederation of European Security Services, Wemmel (Belgium).
Gaylord, M. & Galliher, J. (1991), "Riding the underground dragon: Crime control and public order on Hong Kong's Mass Transit Railway", *British Journal of Criminology*, Vol. 31, pp. 15-26.
Gill, M., Duffin, M. & Keats, G. (2005), *ATM Crime: Offenders' Perspectives*, Perpetuity Research and Consultancy International, Leicester.
Gimenez-Salinas, A., (2004), "New approaches regarding private/public security", *Policing and Society*, Vol. 14, pp. 158-174.
Goldstein, H. (1990), *Problem-oriented Policing*. New York: McGraw-Hill.
Guerette, R. & Clarke, R. (2003), "Product life cycles and crime: Automated teller machines and robbery", *Security Journal*, Vol 16, pp. 7-18.
Holt, T. & Spencer, J. (2005), "Little yellow box: The targeting of automatic teller machines as a strategy in reducing street robbery", *Crime Prevention and Community Safety: An International Journal* , Vol. 7, pp. 15-28
Kennedy, L. (2005), "Three arrested over ATM raids", *Sydney Morning Herald*, 3 November, p. 3.
Lloyd, S., Farrell, G. & Pease, K. (1994), *Preventing Repeated Domestic Violence: A Demonstration Project on Merseyside*. London: Home Office, Police Research Group.
Milligan, B. (2007), "The man who invented the cash machine", *BBC News*, 25 June. http://newsvote.bbc.co.uk, accessed 29 April 2008.
NSWP (2006), *ATM Theft Reduction Strategies: Police Resource*, New South Wales Police, Sydney.
NSWP (2007), *Annual Report 2006-7*, New South Wales Police, Sydney.
Parliament of NSW (2005), Minutes of the General Purpose Standing Committee No. 3, Examination of Proposed Expenditure for the Portfolio Areas Police, and Utilities, Wednesday 21 September, http://143.119.255.90/isysquery/f42b86dd-614a-4225-b002-2cbf7d958c47/27/doc/, accessed 30 April 2008.
Percy, S. (1998), "Response time and citizen evaluation of police", in Bayley, D. (Ed.), *What Works in Policing*, Oxford University Press, New York.
Sarre, R. & Prenzler, T. (2000) "The relationship between police and private security: Models and future directions", *International Journal of Comparative and Applied Criminal Justice*, Vol. 24, pp. 92-113.
Scott, M. (2001), *Robbery at Automated Teller Machines*, US Department of Justice, Washington DC.

Schreiber, B. (1994), “The future of ATM security”, *Security Management*, March, pp. 18A-21A.

Wilson, A. & Donald, I. (1999), “Ram raiding: Criminals working in groups”, in Cantor, D. & Alison, L. (Eds.), *Offender Profiling Series: III – The Social Psychology of Crime: Groups, Teams and Networks*, Ashgate Publishing, Aldershot.

Figure 1: Examples of Internal Bollards and Barriers

(NSWPS, 2006, p. 12; used with permission)

Figure 2: All ATM Ram Raids, Combined Successful and Unsuccessful, August 2005 to April 2008

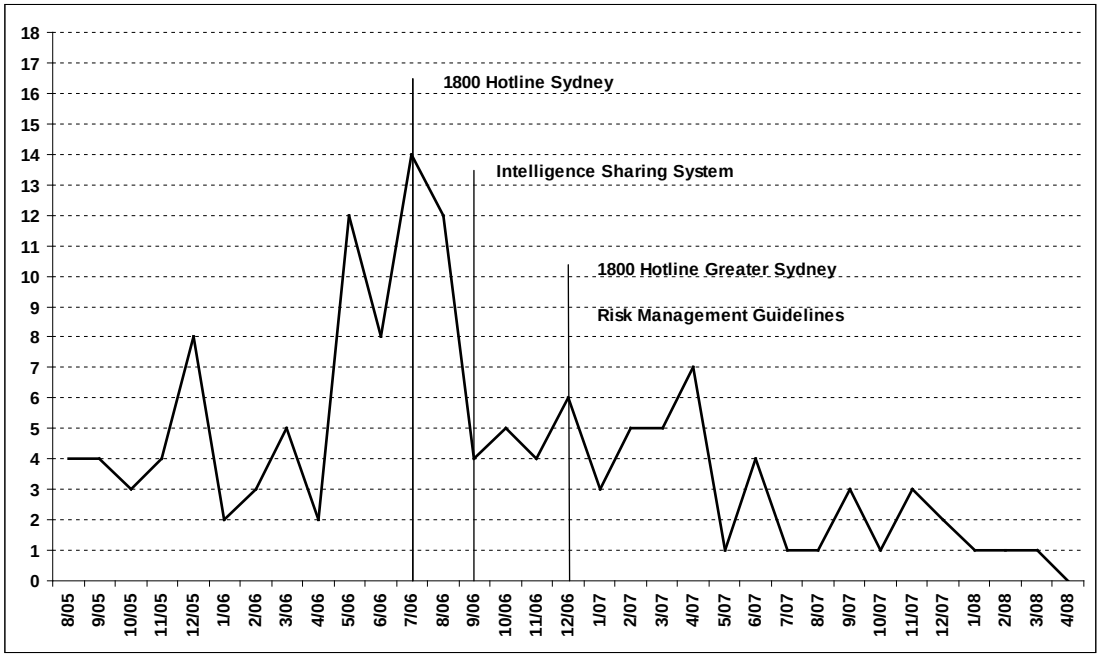


Figure 3: Successful and Unsuccessful ATM Ram Raids, August 2005 to April 2008

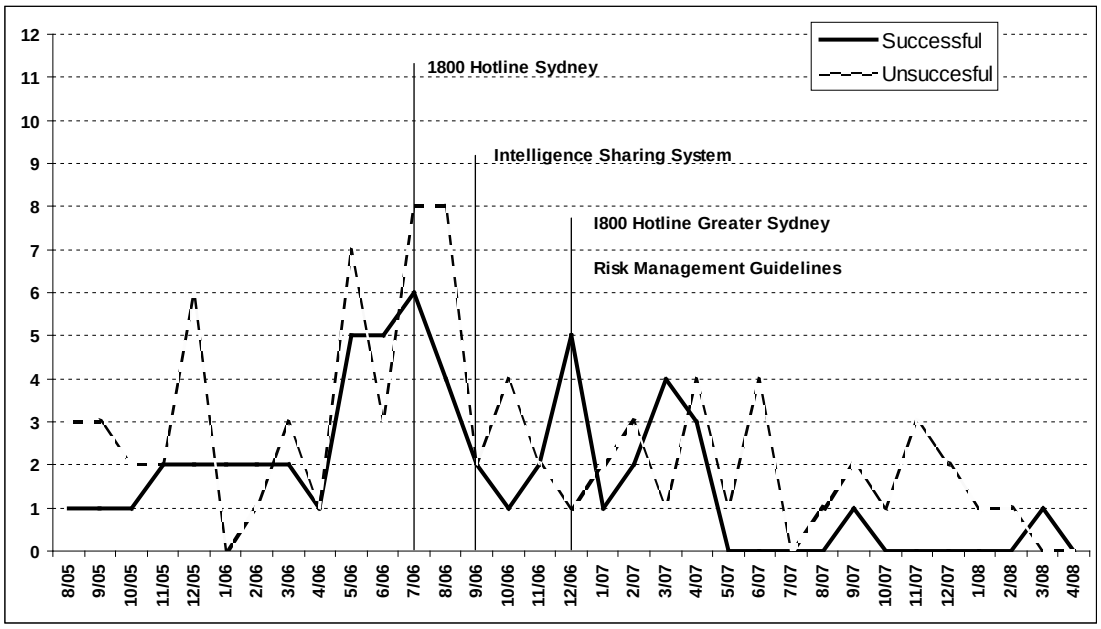
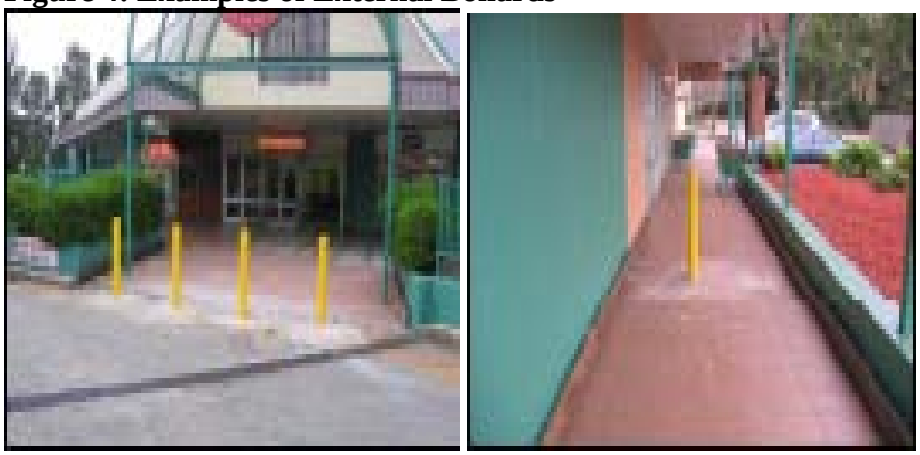


Figure 4: Examples of External Bollards



(NSWPS, 2006, p. 12; used with permission)