LIBER QUARTERLY 18 (2), September 2008 – ISSN: 1435-5205. P101-106
http://liber.library.uu.nl/
Igitur, Utrecht Publishing & Archiving Services

Security in Libraries: Matching Responses to Risks

Martin Gill

Director, Perpetuity Research & Consultancy International (PRCI) Ltd.,
148 Upper New Walk, Leicester LE1 7QA, UK,
m.gill@perpetuitygroup.com

Abstract

Security in libraries is a major issue. The need to permit public access and at the same time protect what are often valuable resources can sometimes conflict. In this paper it is argued that it is vital to develop a holistic strategy, and one of the best ways of developing effective responses is to understand how offenders behave and target security resources to counteracting specific threats.

Key Words: Security; crime prevention; offenders' perspectives

One of the most striking findings from work with offenders is that when asked why they chose the target they did, they too often say, 'because it was easy'. This is not because security was absent, rather because they had the skills and resources to manage the risks that different security measures posed. We have tested out the approaches used by offenders in a variety of settings including the finance sector, retailing and libraries and galleries. In this paper I would like to briefly discuss the approach that has been taken and suggest why offenders provide a valuable source of information that can greatly inform the security response.

Along with colleagues I have been involved in understanding the motivations and techniques used by offenders who have committed quite varied offences from shop theft and fraud, to burglary and robbery, to drug offences and arson. They have at various points either been interviewed one-to-one, or we have held focussed group discussions in prison or in the community. We have returned some offenders to crime scenes (typically retail stores) to better understand how they choose targets and spot what they consider to be vulnerabilities and then exploit them.[1]

What must be stressed is that developing a good security response is based on a number of very important principles and/or practices. These include the senior management team showing strong support for the security operation; the organisation developing a full understanding of the threats via good risk assessments (and this includes understanding process vulnerabilities); collecting data about security breaches which can inform the choice of appropriate mitigation; creating an organisational culture that is conducive to good business as well as good security; properly managing a response plan and ensuring that it its implemented effectively. All of these, and more must be done well if security is to work; and too often it does not.[2]

A key way of understanding specific weaknesses is to learn from offenders, that is using offenders to conduct penetration tests (sometimes called mystery shopping).[3] Another way is to understand from more general research how they get around security measures and build this knowledge into the response.

What we do know is that offenders make decisions at a number of key stages and by understanding the sorts of issues that are important at each of these stages we can begin to build responses that may make people less likely to commit a crime, in other words we can try and dissuade them. There are six key points at which offenders make decisions.[4]

The first of these is 'choosing the target'. Sometimes we know that what guides this choice is the type of good they need to steal. This might be anything that can easily be sold. Some thieves, though, 'steal to order'. They might be asked to steal a book or magazine and knowing they have a ready buyer makes theft more attractive. It is often the case that people steal because they want to use the goods themselves. There may be several places that they can steal the book or magazine from. They may choose the nearest, or they may choose a place that they know or believe is easy to steal from. What we do know from thieves is that they learn quickly, the criminal grapevine spreads fast, so it is important for security managers to be on the ball all the time; it is a very unwise course of action to be known as an easy target.

The second key decision stage is 'entering the target'. At this stage thieves are on enemy territory and so one of the most important considerations for them is not to attract attention to themselves, or to be noticed. So meeters and greeters can be unwelcome if they show too much attention, and guards and others who make eye contact with thieves are a potential threat to manage especially if they then follow the thieves or appear to take a special interest in them. Staff who are alert and give the appearance they will spot something, and guards who appear engaged are a major problem to a thief and these are too often not given the prominence they merit in organisational strategies.

The third key stage is locating the product to steal. Sometimes the thief will know exactly what he/she wants and so will head for the area where the products are located. Thieves have to be careful that they don't look suspicious (e.g. look around too much because they are scared they are being followed) which can attract the attention of alert staff and engaged guards. In finding the product they hope that the security will not be too difficult to compromise. A tag can be ripped off/torn out; a property marking stamp (if it is considered a problem and often it will not be) can be dealt with in the same way; blind spots (created by high shelves for example) can negate the fact that CCTV is present. For a thief the existence of security is only an issue if it cannot easily be overcome, and most of the time it can.

The method of taking the product, the fourth decision stage, may require some skill, and there are various techniques thieves use. Getting a document out of a library may mean secreting it somewhere under the outer clothing, or in a bag perhaps containing goods purchased legitimately in a shop/cafe located on the premises. They may hide what they have stolen inside some other document which they own or can legitimately take out. Thieves may use the technique of distraction, by, for example, working with another thief who can draw attention away from the theft act by creating a disturbance of some kind; some thieves make stealing easier by working in collusion with dishonest staff, we do know this is not uncommon in the retail sector; and whatever techniques they use exploiting blind spots is common. The important point here is that understanding what thieves do and alerting staff to this can provide an extra level of security, and a fairly cost-effective one too.

The fifth decision stage involves thieves leaving the scene and getting away without being caught. Amongst the things thieves need to do here are avoid activating alarms (assuming that there is someone competent there to deal with them) and ensure they have not been followed by someone who can intervene or alert others. They may rely on less than complete diligence in the way guards check people leaving the library for example. But the thief can check this first simply by observing and getting to know the weak areas.

The final stage is where the thief has to decide how to dispose of the goods. This is something that an organisation may be able to monitor. Checking second-hand good outlets to see whether there are any stolen items being traded has proved fruitful in the past. Building up intelligence on the latest popular item being traded may also give clues as to what is vulnerable to theft. Sometimes staff can be alerted to provide insights here. Certainly it is wrong to be heavily reliant on measures such as CCTV.[5]

It is possible to look at the role of the thief even further, going beyond trying to influence their decision making to understanding the resources they need to commit the offence.[6] This is based on the premise that for an offence to take place there needs to be a motivated offender that is capable of committing an offence. What makes an offender capable will be the resources he/she has available. It is perhaps helpful to consider what resources a thief in a library may use, adapting information gleaned from shop thieves. This is mentioned only in passing here but merits attention because it offers another way of looking at offending. There are seven resources that have been identified.

1. *Resources for handling emotional state*. Thieves need to be emotionally prepared to break the law. Sometimes drugs or alcohol facilitate this.
2. *Resources derived from personality traits*. Features of a personality, such as confidence, may facilitate thieving. Confidence can sometimes be derived from good preparation.
3. *Knowledge-based resources*. Thieves will have to have knowledge, that is facts most often borne of experience, that provide them with what they need to commit the offence. This would typically include believing that they knew the risks posed by different security measures and a sense that they could be managed by effective thieving.
4. *Skills-based resources*. Whereas knowledge is about the facts that are known to offenders, skills are about the techniques needed to apply that knowledge.

5. *Resources derived from physical traits*. This can involve being able to fight should the thief be confronted, or it may involve being able to run fast to get away.
6. *Tools or 'crime facilitators', including weapons*. Facilitators here might include baggy clothes for concealing goods.
7. *Associates and contacts*. This can be important for placing an order for goods, providing a means of distraction for committing the offence, helping with the getaway, and buying stolen goods.

Thieves are often quite skilled in what they do. Understanding what 'resources' may be needed to commit an offence helps to identify the *modus operandi* used by thieves and may give clues as to what is needed to prevent the offence. It is another aspect of how we can potentially acquire very specific details about offending that we can then use to inform prevention efforts.

Summary

The basis for this article is that security is often not given sufficient priority in organisations, and too often the absence of an effective strategy means that the various parts are not properly co-ordinated to form an effective whole. By understanding what thieves do we have been able to assess some of the ways in which security is compromised, and they all too often don't find it that difficult. There are right ways of ensuring good security and the positive thing is that good strategies are often not the most expensive. But we do need to understand the problems, and we do need to ensure that we develop realistic and workable solutions; thieves tell us that is much more of a challenge than many organisations, and this includes libraries, fully comprehend.

Notes

[1] See also a recent review, P. Cromwell, G. Alexander, P. Dotson: 'Crime and Incivilities in Libraries: Situational Crime Prevention Strategies for Thwarting Biblio-Bandits and Problem Patrons', *Security Journal* 21(2008)3, 147–158.

[2] The police have an accreditation scheme called ‘Secured Environments’ where organisations that manage their security effectively can apply for accreditation and obtain police approval. See, www.securedenvironments.com.

[3] Sometimes rather than using offenders in penetration tests — which can be sensitive — we use our own staff.

[4] Gill, M. (2006) *Shoplifters on Shop Theft: Implications for Retailers*. Leicester: Perpetuity Research and Consultancy International. www.perpetuitygroup.com.

[5] Gill, M. (2006) ‘CCTV: Is it Effective?’, in M. Gill (ed.), *The Handbook of Security*. London: Palgrave, MacMillan.

[6] Gill, M. (2005) ‘Reducing the Capacity to Offend: Restricting Resources for Offending’, in N. Tilley (ed.), *The Handbook of Crime Prevention and Community Safety*. Collumpton: Willan.