



PULLING THE PLUG ON COMPUTER THEFT

Policing and Reducing Crime Unit - Police Research Series Paper 101
Paula Whitehead and Paul Gray
December 1998

Summary

This study examines some key issues surrounding the theft of computer hardware and component parts from commercial organisations. The report aims to inform future operations against computer theft by providing insight into the methods used by thieves and fences and highlighting examples of effective police practice in dealing with them. It also looks in detail at the experience of six commercial organisations in Salford to reveal the impact of computer theft on staff and business. The report recommends a number of crime prevention measures to reduce victimisation.

Main findings

The cost of commercial computer theft is large. In the area studied, theft of computers made up 18% of all non-residential burglary. The average cost per incident in the area studied was £2,616.

Repeat victimisation appears to be common - 25% of all computer crimes from commercial premises were repeats, with 23% of the sample accounting for 42% of the incidents.

Identification of stolen computers can take a long time and can be resource intensive. It is worth considering the use of alternative strategies to obtain convictions - such as using intelligence gathered from informants to arrest offenders at the scene of the crime.

Computer theft changes to meet the demands of the market. Thieves research the market prior to committing a theft and meet with dealers to establish whether or not there is a demand for specific items.

There are two main categories of offenders specialising in the theft of computers from commercial organisations: 'professional teams' and local 'gangs'. Professional teams are willing to travel to other areas to offend. They are well organised and choose targets very carefully. They may also have a

tendency to repeat a successful modus operandi and to engage in repeat victimisation. Local gangs avoid keeping anything in their homes, which might connect them to computer theft, and tend to dispose of equipment locally through individual dealers or dealer networks.

Fences use trade journals and magazines advertising second-hand computers to sell stolen equipment. Out of 30 telephone numbers taken from LOOT magazine, advertising the sale of computer hardware, ten belonged to convicted handlers.

A quick response to incidents would also increase the chance of apprehending offenders. As an example of good practice, the business estate in the studied police sub-division implemented a scheme between the local authority and some of the companies on the estate. Utilising state of the art communications technology, a dedicated security patrol with a high profile vehicle can respond instantly to any intrusions. None of the participating companies have suffered any further crime and more are now requesting to join the scheme. The scheme was approved by the police and costs shared by business and the local authority. This highlights the possible successes to be had from a well thought out multi-agency approach.

Points for action

The following summarises the key points for police operations and other crime prevention action:

Prevent repeat victimisation

- Once victimised, commercial and public sector organisations are likely to suffer a repeat attack. Organisations need to know this. Any crime prevention measures need installing as soon as possible after an offence because it is then that the risk of a further offence is highest.

Improve record keeping

- Commercial and public sector organisations need to be made aware that they can assist the police considerably in the detection of computer hardware theft by keeping detailed and accurate records of the equipment they have purchased. One of the most important items of information is a record of serial numbers.
- Organisations should back-up any information or data stored on their computers to reduce problems caused by computer theft. Data back-ups should be stored in a separate place to reduce the chance of them being stolen along with computer hardware.

Design against crime

- Glass fronted offices should be avoided because it makes it easier for offenders to break into premises.
- Public access, combined with glass buildings, allows almost unlimited 'casing of the joint'. The incidence of commercial burglaries could be reduced through design solutions drawn up with force Architectural Liaison Officers.
- Public buildings that are traditionally difficult to secure, for example educational establishments and hospitals, can make their vulnerable areas more secure by using a swipe card entry system. Staff can also be issued with identity cards.

Slow the offenders down

- To give police time to respond to burglar alarms and to increase the perception of risk among offenders, measures should be taken to increase the time taken to commit office burglaries. Bolting or wiring down computers and restricting access to areas where they are housed should slow offenders down.

Improve policing operations

- Identifying stolen computers is difficult and it is often a problem proving that recovered property has been stolen. It may be more effective to catch offenders in possession of stolen equipment-particularly when they are in the act of committing a crime. This makes the identification process easier.
- Lack of knowledge of computers and computer terminology has caused problems in the past for operations against computer theft. Therefore, it is important to maintain the right skills mix in operations against computer thieves and fences, using officers with knowledge of computers and computer crime.
- Inexperienced officers can be supported and guided by training manuals (with photographs) which describe computer parts and the language used by the industry - language that is also used by computer thieves, fences and informants.
- Due to the technical nature of computers and their component parts it is important that officers with experience in this area are used to maximum effect. Once arrests have been made it may be beneficial to retain officers with computer crime experience, before they return to normal duties, to help with processing offenders. To this end it may help to build an 'exit strategy' into the operational plan to cover prisoner handling and processing including all matters of bail, charging, file preparation and disclosure - and to choose suitable locations where suspects should be prosecuted.

Other related PRC papers

CPU paper 54: *Crime on Industrial Estates*

CDP paper 58: *Combating Burglary: An evaluation of three strategies*

CDP paper 59: *Biting Back: Tackling repeat burglary and car crime*

CDP paper 69: *Disrupting the Distribution of Stolen Electrical Goods.*

PRS paper 98: *Opportunity Makes the Thief: Practical theory for crime prevention.*