Predicting and Preventing The Theft Of Electronic Products*

Dr. Rachel Armitage and Professor Ken Pease

Correspondence should be addressed to: Dr. Rachel Armitage, Senior Research Fellow, Applied Criminology Centre, University of Huddersfield, Floor 14, Central Services Building, Queensgate, Huddersfield, HD1 3DH. Tel: 01484 473854. E-mail: r.a.armitage@hud.ac.uk.

ABSTRACT

The research presented within this paper was conducted as part of a two-year project (Project MARC) to develop and render operational a mechanism to assess the risk of theft of electronic products. Clarke and Newman (2002) proposed the use of two checklists – one to measure vulnerability the other to measure security, as a means of categorising products according to their vulnerability to theft. Consultation with key stakeholders yielded the common view that such a mechanism was worth pursuing, but that it must reflect the language of those who would use it. An extensive consultation with stakeholders from ten European member states ensued. Participants were asked to rate a range of electronic products in terms of vulnerability and security and to explain their ratings. Their responses were used to develop two checklists which incorporate a variety of factors, weighted according to the frequency with which they were expressed. The crime vulnerability checklist developed within this paper is judged fit for purpose as a provisional measurement but urge caution in relation to the security checklist.

CRIME, DESIGN, ELECTRONIC PRODUCTS, RISK-ASSESSMENT MECHANISM, SECURITY, THEFT, VULNERABILITY.

* Dr. Rachel Armitage is a Senior Research Fellow at the Applied Criminology Centre, University of Huddersfield; Professor Ken Pease is Visiting Professor at the University of Loughborough.

INTRODUCTION

This paper presents the findings from research conducted between 2004 and 2006 funded by the European Commission (Project MARC). The aims of the project were to develop a mechanism to assess the risk of theft of electronic products and to take steps to operationalise that mechanism. The views of the authors reflected throughout this paper are that the task of developing such a tool is vital yet daunting. It is vital to build upon the gains made within other sectors, to seize the opportunity presented by the shift in perceptions of responsibility for the reduction of crime, and to draw attention to the existing discrepancy between risk and protection in many consumer electronic products. It is daunting because in spite of extensive evidence for the efficacy of well-designed and implemented opportunity reduction measures, the problem comes when the crime to be prevented (theft of electronic products) is widespread but not generally devastating to its victims and when opportunity reduction finds itself in tension with commercial interests.

Consideration for crime in design

A proposal to develop a mechanism to measure the risk of theft of electronic products and to explore the feasibility of implementing this mechanism suggests two things. First, it implies that the theft of electronic products is problematic. Second, that there exists a need to educate designers, manufacturers, retailers and consumers about the link between design and crime and the possibilities of minimising future theft.

As is highlighted by Clarke and Newman (2005), a wide variety of manufactured products (those which are CRAVED – concealable, removable, available, valuable, enjoyable, disposable) promote diverse crimes: from theft and fraud to robbery, violence and vandalism. In general, products can serve as *tools* for crime or as *targets* for crime. Guns and spray-paint cans are typically tools (for violence and vandalism, respectively) while cash, cars and jewellery are popular targets of theft. The advent of new products, such as laptop computers, mobile phones and MP3 players, by changing the opportunity landscape, can produce mini crime waves, or crime harvests.

Historically, those who design and manufacture products have largely ignored the crime and disorder implications of what they are producing. As Pease (1997) suggests, innovations go through three phases – First, design without consideration for the crime consequences; second, reaping the crime harvest, whereby criminals recognise and exploit vulnerabilities, and finally retro-fitting a solution (which is usually only partial). Modern examples of this include mobile phones (which were initially designed with little consideration for misuse such as cloning and reprogramming), the Apple iPod (what thought was given to the risks of distinguishing a high-spec product by the colour of the headphones worn by the user/potential victim?) and the internet (how much consideration was given to its use as a facilitator of crime when it was originally conceived?). This weakness, however, is not exclusive to modern technology. As Pease (1997) highlights, the Penny Black postage stamp was introduced in 1840, but withdrawn a year later because people were exploiting the fact that the water-soluble red ink with which it was franked could simply be washed off, allowing the stamp to be re-used. The Penny Black had to be replaced with a Penny Red which was franked with a black ink which could not be removed.

A more desirable sequence of events would be that the crime consequences are considered at the design stage, with a regular flow of information between those concerned with crime reduction and those involved with the product's design and manufacture. Ekblom (1997) highlights how designers need to be encouraged to shift their perspective from solely user to user and misuser and highlights how, for this to occur, crime reduction information must become more accessible for designers.

> "Much remains to be properly evaluated, and the working knowledge of prevention that exists is couched in a tangle of inconsistent and loosely defined terms and concepts which render it difficult for designers to access, to think about and to apply" (Ekblom, 1997 p.249).

The historical lack of communication between those whose task it is to reduce crime and those whose task it is to design products has led to the

development of products, buildings and systems which are conducive to the commission of crime and disorder. In these instances, the prime objective has to be reactive i.e. minimising the impact of the crime harvest rather than to take a more proactive approach. Unfortunately, these bolt-on solutions are often significantly more expensive and as the crime event has already occurred, the victim is left both traumatised by their experience and more vulnerable to future crime and disorder. Recent media reports in both the UK and USA have begun to recognise the link between rising rates of street robbery and the increased use of clearly valuable products such as the Apple iPod. Many of these reports have also highlighted the concern that these thefts do not occur in isolation. A victim whose product is stolen not only experiences the loss of their goods (and any associated inconvenience); they may also experience physical injury, emotional trauma or even death.

Pre-empting reservations

Although these concerns will be discussed in more detail in the concluding sections of this paper, the authors feel it necessary to began the paper by highlighting some of the most common misconceptions about the research upon which this paper is based. The first relates to the belief that as stolen goods are often replaced with new (often superior) upgrades, why would consumers want their products to be secure? Whilst recognising that perverse incentives will encourage some consumers to take less security precautions (because they know any product which is stolen will be replaced with a new one), this argument ignores several key issues. First, not all portable electronic products are insured; second, the theft of an electronic product such as a laptop, mobile phone or Portable Digital Assistant (PDA) can be extremely inconvenient (e.g. by the loss of data). Finally, as was highlighted above, the theft of consumer electronic products will generally involve a victim – that victim has not only lost their product, they may have also experienced physical injury and/or emotional trauma.

The second reservation, highlighted throughout the research, is the concern that offenders do not always differentiate between secure and non-secure products at the point of theft. Are offenders generally aware of the security

status of products before they are stolen, or do they simply take the risk and discard products which cannot be reused? This is a valid concern which is backed by some evidence. In their study of the theft of mobile phones, Harrington and Mayhew (2001) found that in only 14% of mobile phone thefts was the mobile phone the specific target. Whilst recognising the validity of this concern (as well as the need for further research into offender decision making at the point of theft), the authors propose that one of the most effective means of reducing the theft of electronic products would be to maximise the number of secure products on the market, thus reducing the odds that a bag (or other receptacle used to carry consumer electronic goods) will contain usable products.

The final reservation raised by in the process of conducting this research is that manufacturers cannot be expected to design undesirable products. Whilst the objective of the research was to reduce the risk of theft of electronic products such as the iPod, mobile phones and PDAs, the aim was not to encourage designers/manufacturers to stop producing these desirable, attractive and distinctive products, rather to ensure that goods which are likely to be targets for theft are as secure as they are attractive.

Justification for Measuring Risk

The case for crime reduction is self-evident. But what justification is there for addressing the management of crime by developing a risk assessment mechanism to measure the risk of theft of electronic goods to complement the more traditional approach of offender detection and conviction? Why should electronic goods be singled out for special attention, and what effect is this likely to have on crime rates across Europe? The major premise of the advance in situational crime prevention and the new opportunity theories is that many individuals, when faced with the chance to make a gain (through criminal behaviour), give in to temptation and select the option which provides the greatest reward for the lowest risk. If crime is viewed as a risk to be avoided, the primary task facing crime reduction practitioners should be identifying those risks and putting interventions in place to reduce them. The demonstration that modifying criminogenic products can be highly effective,

as well as the success of risk assessment tools in other areas of criminology (built environment, young people, vehicle crime) sufficiently justifies the objectives of this task. As pre-eminently desirable and stealable, small electronic products provide an obvious starting point for risk assessment.

As Clarke and Newman (2005) highlight, more than one hundred case studies have been published showing that significant declines in specific kinds of crimes have been achieved through the introduction of situational crime reduction measures (Clarke, 1997; Sherman *et al.,* 1997; Smith *et al.,* 2002). These include the reduction of car crime through the introduction of steering column locks (Webb, 1997) and the reduction of burglary through increasing physical security (Brown and Altman, 1983; Cromwell *et al,* 1991), minimising access (Brantingham and Brantingham, 1975, 1993, 2000; Brantingham *et al,* 1977; Brown and Altman, 1983; Newlands, 1983; Greenberg and Rohe, 1984; Cromwell *et al,* 1991; Bevis and Nutter, 1997; Mirlees-Black *et al,* 1998) and increasing surveillance (Reppetto, 1974; Brown and Altman, 1983; Cromwell *et al.,* 1991; Brown and Bentley, 1993) and a combination of the above (Brown, 1999; Pascoe, 1999; Armitage, 2000). Other situational measures include the reduction of mobile phone fraud (cloning and tumbling) through the introduction of user and account verification technologies (Clarke *et al.,* 2001) and the reduction of violent crime through the introduction of toughened glasses in British pubs (Design Council, 2002). As well as its effectiveness in reducing crime, the appeal of this type of intervention over long term, resource intensive offender based interventions, lays in the practical solutions it offers to those who are tasked with the reduction of crime. For practitioners who are asked to meet crime reduction targets within short timescales (with very little additional resources) many crime reduction theories and interventions, as highlighted by Smith (2000), may appear unfeasible.

> "It is easy to see that happy families tend not to produce criminals. It is hard to see how public policy can decree that family relationships be constructive and positive" (Smith, 2000 p.149).

In short, the evidence for the efficacy of well-designed and implemented opportunity reduction measures is overwhelming, and constantly growing. The acknowledgement of this is evident in measures against terrorism, for example enhanced airport security. The central problem comes when the crime to be prevented is widespread and not generally devastating, and when opportunity reduction finds itself in tension with commercial interests.

Although the task of convincing manufacturers of electronic products to think about the crime implications of their designs may appear daunting, particularly considering the troublesome trade-offs such as aesthetics, convenience and costs (discussed in more detail in Ekblom, 2005), there are several examples of sectors where steps have been taken (either spontaneously or in response to government pressure) to design out crime opportunities from their products and systems. These include the UK Vehicle Licensing System (see Laycock and Webb, 2005), the banking industry (see Levi and Handley, 1998) and the mobile phone industry (see Whitehead *et al*. this issue).

The Measurement of Crime Risk: Developing a Risk Assessment Mechanism

Previous paragraphs have demonstrated the good chance of success which intervening to measure and reduce the risk of theft of electronic products should have. Based upon the widely accepted theoretical proposition that crime responds to opportunity and can therefore be reduced by blocking opportunities, a mechanism to measure the factors which make certain products vulnerable to crime is a relevant tool to enable the prediction of risk and therefore the targeting of resources. The case has been made for measuring risk and intervening to reduce that risk, the remainder of this paper will focus upon what format that measurement might take in respect of electronic products. There are two possible audiences: first crime control agencies who might alert consumers to risks and the precautions that could be taken to minimise them. These are not concerned with design modifications. This audience will not require precision, and risk measurement

directed to this audience is unlikely to attract the hostility of manufacturers, particularly if low risk products gain recognition as such, rather than high risk products attract opprobrium. The second audience comprises manufacturers and retailers and here the landscape is different. Manufacturers will very reasonably object to making costly design modifications on the basis of imperfect risk measurement. To anticipate a conclusion of the present paper, the risk measurement device which was developed as part of this research is less fit for purpose in relation to this second audience.

The process of developing the crime risk assessment mechanism took as its starting point the Secured Goods by Design model (Clarke and Newman, 2002). The mechanism was based upon two quantitative checklists, one which assesses a product's vulnerability to theft in terms of how concealable, available, valuable, enjoyable and disposable it is. The second assesses the product's security features – for example, does it contain technology to negate its financial value if stolen, can it be tracked and has it been field-tested for theft? Vulnerability to theft is indexed by the relationship between scores on the two indices. Products which have high vulnerability/low security will be particularly prone to theft; products which have low vulnerability/high security will be less likely to be targeted. Provided that a product scores highly enough on the security checklist for its predicted level of risk, it can be designated and marketed as a Secured Good by Design (or awarded a similar label depending on choice of accreditation scheme). The two checklists are presented as tables 1 and 2 below.

Table 1 about here.

Table 2 about here.

Although the authors considered the proposed mechanism to be an excellent basis for developing a crime risk assessment tool, concerns remained. These related to both the content and design of the checklists as well as a more general concern about their implementation. Some of these concerns are highlighted below:

- **Lack of flexibility –** Are rigid checklists appropriate for use within the rapidly changing field of consumer electronics? Would this mechanism be able to reflect the life cycle of electronic products from innovation through to saturation or need to grow and evolve as offenders' *modus operandi* changed?
- **Implementation –** Could such a mechanism be completed at the prototype stage? How likely is it that manufacturers would be able to rate a product's desirability, popularity and status before it was developed and advertised? Re-designing a product (to rectify poor scores) could be prohibitively expensive for manufacturers.
- **Subjectivity –** Certain elements of the vulnerability checklist are subjective and open to misinterpretation. For example, what is fashionable to one person may not be to another; the price of one day's wages will also differ greatly between those completing the checklist.
- **Inter-Rater Reliability –** An informal pilot on two electronic products revealed a large variance between scores. For example, of the eight participants who completed the checklists,[i] the Apple iPod scored between 11 and 18 out of a possible 21 for the vulnerability checklist (both the mean and median scores were 16) and between 0 and 3 for the security checklist (the mean score was 1 and the median 0). If this variation occurred whilst piloting the checklists on an audience being guided through the procedure, what variations would occur when the checklists were being completed unaided?
- **Whose Role are we assuming? –** When completing the checklist it is unclear whose role you are assuming. Are you assuming the role of the offender, the user or misuser? One example of this included the category 'Concealable'. This could be interpreted as concealable by the thief once the product had been stolen, or to a legitimate user's ability to conceal the product.
- **Products as Part of a System –** The category 'Removable' does not adequately reflect the nature of many consumer electronic products – which are part of a system. For example, the iPod itself may be used

outside the home, but the charger, CD-Rom and software allowing the product to be used are typically not.

To restate, the initial review of the extant crime risk assessment mechanism revealed several concerns. However, a decision was made that the essential principle of the original mechanism – that risk should be commensurate with protection - should be retained; but that the existing mechanism should be revised to ensure that it: a) Reflects the language of those whose task it would be to apply it, rather than imposing the language of criminologists; b) reflects the language of stakeholders from a variety of European states; c) must be based upon a user-derived approach, rather than imposing a mechanism upon key stakeholders.

METHODOLOGY - REFINING AND TESTING THE CRIME RISK ASSESSMENT MECHANISM

The process of revising the existing mechanism involved conducting an extensive consultation with key stakeholders from a variety of sectors representing both original and accession European states. The methodological steps taken are outlined below.

Design of the Questionnaire

A decision was made at the outset of this section of the project, that due to the need to consult with stakeholders from a mix of European states. Given the language limitations of the researchers involved, the most appropriate method for collecting information would be through questionnaires, distributed electronically and translated into any language chosen by participants. Face-to face interviews would have been prohibitively expensive. Telephone interviews would have imposed a strain upon participants of varying fluency in the language used.

The questionnaire was designed to collect information on both a) participants' views of the theft risk presented by a variety of electronic products and b) participants' views (in their own words) of what makes a product vulnerable or secure. These data were collected by providing detailed information on a

product's price, dimensions, weight, specifications and in-built security features, and asking them to rate each product as low, medium of high in terms of its vulnerability and existing levels of security. Of just as much importance as the rating was the participant's explanation for that selection. For this reason, participants were asked to give three reasons why they had made each selection. A copy of the questionnaire can be requested from the authors. It is worth highlighting at this stage that the assessments made by participants regarding product vulnerability/security, although hopefully informed by their role within one of the chosen sectors, were simply based upon their views of the product in question. Weaknesses with this methodology include the risks of differential interpretation. Whilst one participant may be considering the vulnerability of a product whilst being carried on the street, others may be imagining its vulnerability whilst based within the home/office. Assessments may also be influenced by age (as well as gender). What is considered desirable (and therefore vulnerable) by one person, may not be assessed as such by another.

Selection of and Production of Descriptive Reports for a Set of Electronic Products

The five electronic products – MP3 players, digital cameras, personal digital assistants (PDAs), mobile telephones and laptop computers were selected due to their putative varied vulnerability to theft at the time of the research. To allow a sufficient level of data without placing high demands upon participants' time, three models of each product type were included in the questionnaire i.e. three models of mobile phone, three models of PDA, and so on.

The three models of each of the five product types were selected to ensure a balance of popularity, price, specifications and dimensions. To ensure a standard and repeatable methodology, products (and the information included on each product) were selected (and gathered) using the following process:

a) Selecting the three makes/models awarded the highest score on the Which Best Buy guide (www.which.net). If the review of a product were split into categories, for example, the digital camera review included

best buys for cameras with less than 4Mp, 4Mp to 5Mp and 5.1Mp or more, the best buy model was selected from each range.

b) Fixing a specific date on which to identify each product's price and specifications;
c) Searching three online stores to find the price of each make/model;
d) Selecting the cheapest price from the three stores.

For example, for MP3 players, the Apple iPod 20Gb was selected as the best buy Hard Disk MP3 player from Which online. On the 26th May 2005, the three websites: Dixons, PCWorld and Currys were searched to establish the price for which they sold this product. All three sold the product for £189.99; therefore, this price was included on the stakeholder questionnaire.

Selection of a Panel of Key Stakeholders

To ensure that responses were gathered from stakeholders representing an equal mix of original and accession European member states, the two research teams (Jill Dando Institute, UK and Università Cattolica Del Sacro Cuore, Italy) were given a list of countries from which to select their participants. Each research team were asked to select three original European states and two accession states. This gave a total of six original and four accession states.

Once countries had been selected, one representative (from each country) from the following four sectors was identified and invited to take part in the research:

1. Law enforcement
2. Consumers
3. Manufacturers of electronic products
4. Insurance

The selection of countries from each of these lists, and stakeholders from each of the above sectors involved a snowball process generally starting with the countries in which the research team was based, i.e. Italy and the UK. Countries were selected based upon the number of stakeholders from that

country who were willing to take part. An example of the steps taken to select stakeholders is outlined below[ii]:

1. Using the UK as a starting point, a number of contacts from within each of the four sectors (as well as academics) were asked to provide details of individuals working within these sectors from the UK;
2. Individuals were contacted and asked if they would be willing to complete the questionnaire;
3. Individuals were also asked if they would be willing to provide names/contact details of their counterparts in the additional eleven countries.
4. These contacts from the additional countries were then asked if they would be willing to take part, and also asked for details of those working within their field from alternative countries;
5. This process continued until the five countries with the most participants willing to take part were selected;

At the end of this process 31 (out of a possible 40) contacts agreed to complete, and were sent the questionnaire. Twenty-two participants returned completed questionnaires within the required deadline.

Dissemination of the Questionnaire

Once participants had been selected, they were contacted by e-mail, which explained the background of the project, the role of the questionnaire as part of the wider project, the task they were being asked to complete and the likely deadlines involved. The introductory e-mails did not include the questionnaire.

Once the stakeholder had agreed in principle, the e-mail was followed by a phone-call (where possible and appropriate) explaining the project in more detail and clarifying any uncertainties that they may have. This stage of the process was also used to discuss issues such as anonymity and the preferred language into which participants would require the questionnaire to be translated.

Once a stakeholder had agreed to take part, the questionnaire was sent electronically. Approximately one week before the first deadline, participants were sent an e-mail (or received a phone call) reminding them about the questionnaire and asking them to let the research teams know if they were facing any difficulties. If participants asked for an extension to the deadline, this was offered. Those participants who did not ask for an extension and did not return the questionnaire were sent several reminders until the stage where time would not allow their inclusion. To this end, it is suggested that every step was taken to accommodate as many participants as possible. The number of those from whom information was obtained is frankly disappointing in the light of the efforts taken to recruit respondents, and is attributed primarily to the perception that crime risk is a matter of criminal inclination rather than criminal opportunity.

Collection and Analysis of Data

The analysis detailed in the results section below focused upon the association between vulnerability and security for each of the 15 products; the association between vulnerability and security for product type (i.e. mobile phone, PDA etc.); variations in perceptions between respondents from each sector and finally qualitative analysis of respondents' definitions of vulnerability and security

RESULTS

Participants

As noted above, the original aim was to interview four participants (one from each of the four sectors – law enforcement, insurance, consumers' associations and manufacturers of electronic products) from ten European countries. Although the research teams contacted many stakeholders from each of these sectors from a variety of European countries, the final responses analysed below reflect the views of 21 participants from nine European countries. Five of these countries are original and four are accession European member states. The extreme difficulty of recruiting respondents may itself be indicative of the fact that the notion of crime-reductive design of electronic products is not yet something which engages

the interest and attention of many of those whose involvement would be necessary to successful implementation of a risk-based assessment of electronic products.

Table 3 below displays the number of participants who took part from each country. The results reveal that only the UK and Italy achieved the maximum four respondents. Three respondents took part from the Czech Republic, two from Hungary, Poland, Lithuania and Sweden and one from Spain and the Netherlands.

Table 3 about here

In addition to the four participants from ten countries, the research team invited the views of those working for the European Standardisation Organisations (ESOs) ETSI, CEN and CENELEC. One response was returned from ETSI making the total number of respondents 22.

Table 4 below shows that of a possible 10 (one from each of ten countries), seven respondents represented the insurance sector, six represented the law enforcement sector, six represented consumers' associations, two respondents represented manufacturers of electronic products and one respondent represented ESOs.

Table 4 about here.

Vulnerability versus Security

Although the main aim of the research was to utilise responses to the questions 'what makes a product vulnerable/secure' to design a revised crime risk assessment mechanism, the research also aimed to assess variations in perceptions of vulnerability and security between individual products i.e. Apple iPod 20GB, by product type i.e. MP3 player and by the sector of each respondent i.e. manufacturers. As was highlighted within the methodology section, respondents were asked to review the details of 15 electronic products (photo, dimensions, price, weight, specifications) and make

judgements regarding that product's vulnerability and security. A product perceived to have low vulnerability/security would be awarded 1 point, a product awarded medium vulnerability/security would be awarded 2 points and a product considered to have high levels of vulnerability/security would be awarded 3 points. As there were a total of 22 respondents, the minimum score awarded to a product i.e. the lowest level of vulnerability/security would be 22 (22 x 1) and the highest would be 66 (22 x 3).

Figure 1 displays the aggregate vulnerability and security scores for each of the 15 electronic products. The products to the left of the graph are those with very little variation between the perceived levels of vulnerability and security. For example, the Toshiba Satellite M30X 159 has a vulnerability score of 49 and a security score of 47. In contrast, the products to the right of the graph show the greatest variation between perceived levels of vulnerability and security. For example, the FujiFilm Finepix S7000 has a vulnerability score of 63 (66 being the highest possible score) and a security score of 27 (22 being the lowest score).

Figure 1 about here

The product considered by this sample of respondents to be the most vulnerable to theft was the FujiFilm Finepix S7000 digital camera, followed by the Apple iPod 20GB MP3 player and the Nokia 6230i mobile phone. The products considered to be the least vulnerable to theft included the Palm One Zire 72 PDA, the Toshiba Satellite M30X 150 laptop and the Olympus Camedia C-5060 and C-770 digital cameras. Products considered to be the most secure included the Toshiba Satellite M30X 159 laptop computer, the Motorola V600 mobile phone and the Sony Vaio VGN B1XP laptop computer. Products considered to be the least secure included the Palm One Tungsten T5 PDA, the Olympus Camedia C770 and the HP iPAQ rx3715 PDA.

Products which scored higher than the mean in terms of perceived vulnerability and lower than the mean in terms of perceived security –

suggesting that thy would be the most vulnerable, were the FujiFilm Finepix S7000 digital camera, the Apple iPod 20GB MP3 player, the HP iPAQ rx3715 PDA and the iAudio M3 MP3 player. The only product which scored lower than the mean in terms of perceived vulnerability and higher than the mean in terms of perceived security was the Toshiba Satellite M30X 159.

As well as highlighting the variations between products, the results also revealed that vulnerability scores are consistently higher (irrespective of product) than security scores (i.e. the blue line never rises above the red line in figure 1). This suggests that for the sample of respondents included in this research, the 15 products were all perceived to have a higher level of vulnerability to theft than security. The mean vulnerability score for the 15 products was 54.5, whilst the mean security score was 30.3.

Product Type

Aggregating the responses by product type i.e. MP3 player, PDA, mobile phone, digital camera and laptop computer, revealed that mobile phones were considered to be the most vulnerable to theft, with PDAs considered to be the least vulnerable. Laptops were considered to be the most secure, whilst PDAs were considered to be the least secure. The analysis also revealed that whilst there is little variation between the vulnerability scores awarded to each product type – the most vulnerable product type had a mean score of 58 and the least had a mean score of 50 (a difference of 8), the security scores showed greater variation. The most secure product had a mean security score of 38, whilst the least secure had a mean score of 24 – a difference of 14.

Table 5 about here

Sector Type and Perceptions of Vulnerability and Security

Table 6 displays the difference between responses awarded to the sample of 15 products by sector of respondent. The results revealed that respondents from law enforcement were the most likely to rate the sample of products as having high vulnerability to theft whilst manufacturers of electronic products

were less likely to perceive the sample of products to be highly vulnerable to theft.

Table 6 about here

Table 7 reveals that participants from the insurance sector were most likely to consider the sample of electronic products as having low levels of security. Participants from European Standardisation Organisations and Consumer organisations were the most likely to consider the sample of products as having high levels of existing security.

Table 7 about here

Defining Vulnerability – Stakeholders' Views

As well as ranking the 15 products in terms of their perceived vulnerability to theft and their perceived levels of existing security, respondents were asked to give three reasons for each of these ratings. The rationale behind this methodology was that the final crime risk assessment mechanism should be developed using the language of the stakeholders whose task it will be to implement it, rather than being imposed by criminologists. The three reasons given by the respondents were therefore to be used as the basis for the revised risk assessment mechanism.

Looking first at the definition of vulnerability, Table 8 displays the responses given to the question 'what makes a product vulnerable?' alongside the frequency with which that response was given. To minimise the number of factors in any future risk assessment mechanism, the responses provided by respondents were clustered into common themes. For example, 'costly', 'pricy', 'expensive', and 'costs a lot' were clustered under the heading 'expensive'. To ensure that the procedure of allocating responses was valid and repeatable, the authors conducted the categorisation process separately before agreeing on common vulnerability/security factors. The results reveal that of a maximum potential score of 330 (22 participants multiplied by 15 products), the most frequent response to the questions – 'what makes a

product vulnerable?' was small/light with a score of 76. Expensive was the second most common response (with a score of 61), followed by popular (38), attractive design (33) and high quality specifications (27).

Table 8 about here

Defining Security – Stakeholders' Views

The responses given by stakeholders when asked to define 'what makes a product secure?' are outlined in the table below. Although very few responses were given by respondents, Table 9 makes some attempt to score the security factors given.

Table 9 about here

DISCUSSION

The results section of this paper presents the findings of the extensive consultation with European stakeholders and presents a draft version of the crime risk assessment mechanism. It is the authors' view that the crime risk assessment mechanism developed as part of this project will need to be sold to two audiences: crime control agencies that might alert consumers to risk and provide cautionary advice, and manufacturers who would be asked to develop their products based upon the findings. The risk mechanism presented remains fit for purpose in relation to the first audience, but does not achieve the precision necessary for the second. Issues which remain uncertain include:

a) How the clarity of the vulnerability checklist may be enhanced, addressing the weaknesses within the security checklist;
b) Whether two checklists can be justified based upon the lack of variability in vulnerability scores awarded by respondents;
c) How to engage manufacturers of electronic products (who represented just 9% of the sample);

d) How to overcome the perverse incentives which allow consumers to benefit from the theft of electronic products through an upgraded replacement;
e) How to produce a mechanism which is flexible enough to accommodate the changes in risk and protection, and
f) How to strike a balance between the risk of miscalculating vulnerability and the costs of re-designing products (post manufacture) which may prove prohibitively expensive.

The remaining sections of this paper will focus upon refining the weaknesses in the presentation and implementation of the mechanism before reconsidering some of the assumptions on which the approach taken was based.

Improving the Vulnerability Checklist

The task which participants undertook made no reference to the CRAVED framework. This was deliberate, because to frame the task in terms which assumed the validity of the CRAVED framework would be to assume what we set out to test. The downside of this is that the data do not allow a direct test of CRAVED. Insofar as Table 8 can be interpreted in CRAVED terms, it endorses the relevance of CRAVED factors. Many of the comments clearly refer to CRAVED factors. Expensive means valuable, small/light reflects concealable, popular and desirable (and perhaps fashionable) mean enjoyable, and marketable means disposable. However, the meaning of other factors cited as contributing to vulnerability have to be interpreted. Does 'high quality specifications' stand proxy for expensive? Is 'good brand name' a marker for expensive, enjoyable, disposable, or none of these? The impression which we have is that CRAVED remains a good analytic framework. Notwithstanding this, the search for a simpler measure of vulnerability should be undertaken simply because simplicity in use is valuable. Lacking details of the actual relative vulnerability of the products included (which would require an enormous research project in its own right) the aggregate judgement of vulnerability made by our expert respondents was used as the benchmark for a possible simpler measure.

Exploratory analysis was undertaken with the variables of price, weight, price per unit weight and aggregate vulnerability score. Surprisingly, there was no relationship between price and rated vulnerability, and only a modest and statistically unreliable association between price per unit weight and vulnerability score. This pattern reproduced itself within each product type as well as across products. Excluding the most expensive products (laptops) increases the relationship between price and vulnerability, but does not render it statistically reliable. We must thus conclude that rated vulnerability is not reducible to the simpler variables of weight and price. Whether rated vulnerability approximates more closely to theft rates than price and weight, as noted above, can only be determined by a very substantial additional research programme. Assuming the domain experts involved as respondents bring knowledge and experience to the table, the conclusion is reached that their judgements of vulnerability cannot be reduced to simpler measures of weight and cost. This has to be a provisional judgement. The small range of vulnerability scores noted earlier remains troubling. CRAVED, in the writers' view, remains the best available organising framework for vulnerability to theft.

The Weakness of the Security Checklist

The recommendation to be reached at the end of this paper is that the security checklist is not a sound basis for evaluating product security. The central reason is that the progress of the research, and consultations with respondents and others, demonstrated that this approach would impose an artificial ceiling upon the exercise of ingenuity and skill in crime-reductive engineering and design. It also understates the degree to which security is specific to product type. For example, most of the security measures set out as Table 9 are specific to individual product types or pairs of product types. Since no general or common security features emerge, the justification for standardisation disappears. With hindsight, the classic matrix (see Table 10) developed by Ron Clarke (see Cornish and Clarke, 2003) reflects such a richness of alternative methods that the checklist approach seems formulaic by contrast.

Table 10 about here

What can be retrieved from the security checklist idea is the notion that when invited to make global estimates of security and vulnerability, vulnerability was virtually across the board judged greater than security. In other words, security is generally perceived to fall short of commensurability with vulnerability.

Should all Portable Electronic Products be treated as Equally Vulnerable?

Although the consultation process revealed that participants felt that the final mechanism must measure risk and protection separately and ensure that they are commensurate, the results presented above throw some doubt on this decision. The aggregate security scores, which presented the score awarded for the perceived security (1 being low, 2 being medium and 3 being high) of each of the 15 products by the 22 respondents, revealed a large mean difference in the scores awarded to different products. For example, PDAs were considered to be the least secure, with a mean (aggregate score divided by 3) security score of 24. Laptop computers were awarded a mean security score of 38. In direct contrast to this, the variation between product types for perceived vulnerability varies very little. The mean aggregate vulnerability score for PDAs (considered the least vulnerable) was 50; however, for mobile phones (the product considered to be the most vulnerable) this score was only 57.

To précis, vulnerability within products of the same type varied little. Rated security varied much more. Do these findings suggest that all portable consumer electronic products of the same type are similarly vulnerable to theft irrespective of the level of security incorporated (within the range of security levels currently incorporated)? To address this point, we need to consider details of criminal method which are not routinely gathered. Put informally, there are two questions to be addressed:

1. Are the relevant products ‘naked’ at the point of theft?
2. Are a non-trivial number of the products discarded, or is a theft aborted when a thief knows the particular model carried by the intended victim?

These questions are linked in that, to the extent that the nature of products are not evident at the point of theft, upon being recognised for what they are, are they thrown away? For example a wallet stolen by an 18-year-old containing photo ID of a woman of 80 is of little direct value to the thief and may be discarded. It is believed that all the products are typically ‘clothed’ (in handbags, pockets or carrying cases) at the point of theft. The possible exception may be MP3 players, but this is unclear until we know whether they are stolen while in use. Mayhew and Harrington (2001) suggest that in only some 14% of mobile phone theft was the mobile phone the exclusive target. Anecdotal evidence and observation suggests that even the least valued portable electronic product is not without value, and is seldom or ever discarded. Taken together, a tenable conclusion is that perceived value may be the primary driver of mobile phone theft, with the other elements of craved taking a secondary role.

What Might the Final Crime Assessment Mechanism Look Like?

The CRAVED framework remains tenable as a framework for measuring product vulnerability. What is required is some measure of vulnerability provisionally based on CRAVED, i.e. with CRAVED prompts preceding a general assessment of vulnerability not constrained by answers to the CRAVED prompts. A group should be convened with representatives of manufacturers and consumer organisations. If CRAVED proves contentious, a threshold of value/weight for electronic products should be established above which the process below is followed. Assessed security should be referred on to a EUROPOL hosted technical group which can deem security features as good, adequate or insufficient with rated vulnerability, yielding a three level rating.

Proposing a Model for Implementation

In terms of suggestions for future implementation, the authors propose that the mechanism should be used as a tool to inform the labelling of consumer electronic products. It is recommended that two systems should be introduced which will help consumers make informed decisions when purchasing electronic products and also allow manufacturers to market their products as 'Secure'. The first system would be an accreditation scheme and associated logo which would allow products meeting the required standards to be marketed as a 'Secure Product' (or whatever label is chosen). The exact specifications would be refined following further consultation, but the authors suggest that to be awarded this label, products must have a security rating which is equal to (or higher than) the vulnerability score. If a product has a high vulnerability score it must have 'good' security features (rated by a EURPOL technical group). If the product has an 'insufficient' level of security, it can still be labelled as a 'Secure Product' as long as the vulnerability score is equally low.

Similar systems are utilised in the food and building industry which enable products to be labelled as 'Secure' or 'Healthy' if they meet certain criteria. The 'Healthy' logo was proposed by the UK Food Standards Agency in their consultation regarding the labelling of food (see Figure 2). This system would allow food which met the relevant criteria, in terms of salt, sugar and fat content, to be labelled as 'Healthy' and therefore carry the logo.

Figure 2 about here

In a similar vein, the UK building industry has an accreditation scheme for buildings which allows them to be labelled as Secured by Design (and therefore marketed using the appropriate logo) where they meet the required standards of security (see Figure 3). The Netherlands also have an accreditation scheme – Police Label Secured Housing - which allows consumers to identify whether buildings meet certain security standards.

Figure 3 about here

In addition to the proposed voluntary accreditation scheme and associated label, it is recommended that the electronics industry are invited/encouraged to introduce a second labelling system which would enable consumers to easily and immediately identify the levels of vulnerability and security of a product. It is proposed that this system should be based upon the 'signposting system' (currently being suggested by the UK Food Standards Agency) and should include two signposts (one for vulnerability and one for security) which would be coloured according to the product's ratings (awarded using the vulnerability checklist and the EURPOL three level rating). If a product scores highly in terms of vulnerability to theft, the vulnerability traffic light would be red (i.e. stop). If the product had a medium score in terms of its vulnerability to theft the traffic light would be amber (i.e. proceed with caution). If the product had a low vulnerability to theft, the traffic light will be green (go ahead). The security traffic light would be coloured using the same red, amber and green, but the ratings would be awarded by the EUROPOL technical group as opposed to a formulaic security checklist. Below (Figure 4) is an illustration of the proposed system.

Figure 4 about here (needs to be in colour)

What are the authors' reasons for proposing the two systems of presentation as opposed to the traffic lights alone or the accreditation scheme alone? Firstly, with the accreditation system alone, where products fail to achieve the 'Secure' or manufacturers decide not to apply for it, the product would contain no information on risk of theft. With the two systems in place, a product which has failed to meet the relevant standards or has not applied for the accreditation scheme would still contain the basic information to inform consumers about its risk of theft. Where a label is absent, consumers may not associate this with a negative message. They may never have seen the 'Secure' label and would therefore not make a choice based upon its absence. However, where the 'Secure' label was absent because the product had failed to meet the relevant criteria, the consumer would still be able to interpret from the traffic light system that the product had high levels of vulnerability and low levels of security.

The second rationale for suggesting the two systems is impact. Although further research would be required to test this assertion, it is suggested that the traffic light system would allow consumers to interpret with greater ease the information being portrayed i.e. the product is vulnerable to theft, but it is OK because it has high levels of security. With the accreditation scheme label alone, it may not be clear to consumers what the label means and why the product has it (or does not have it). This assertion is supported by research conducted into the Secured by Design label in the UK (Armitage, 2000) which found that although the logo would have been present on the marketing of properties, only 5% of residents were aware that they lived in housing considered to be 'Secure'. In this case it is suggested that residents who did not live in Secured by Design housing (either because their properties had failed to comply with the standards or because the developers had decided not to apply for the award) would be unlikely to be aware of this deficiency in the security of their property.

Bearing this in mind, why not recommend the use of the traffic light system without the accreditation scheme? The authors recommend that the two systems each serve a purpose and should therefore be implemented together. The 'Secure' label allows manufacturers to gain a commercial advantage over products without the label. It would be a simple, recognisable label which could be used for marketing purposes. The traffic light system allows consumers to immediately recognise a product's vulnerability to theft as well as its existing level of security even if they have no knowledge of the particular accreditation scheme.

Although it is proposed that the final mechanism and associated traffic light and accreditation schemes should be introduced on a voluntary basis, the authors recommend that these schemes should not be introduced in isolation and would need to be supported by publicity, further research, financial incentives and even legislation. This suggestion is informed by the experiences of crime reduction accreditation schemes implemented within other sectors. The Secured by Design voluntary accreditation scheme which

was developed in 1989 is awarded to developers who design and build housing to an agreed set of standards (these include physical security, access, surveillance, territoriality and management and maintenance). Although Secured by Design has become increasingly popular over the last decade, this has not been achieved in isolation and a number of incentives are offered alongside the scheme. These incentives have been aimed at developers, consumers and policy makers (locally, regionally and nationally) and take the form of legislation, publicity and enhanced funding.

CONLCUSIONS

Engaging Manufacturers

The prediction of crime risk, although interesting, will remain without impact unless those designing and manufacturing products have some incentive to consider the crime and disorder implications of their actions. As the results section of this paper showed, of the four sectors consulted, manufacturers of electronic products were the most difficult to engage and only represented 9% of the sample.

As was highlighted in the discussion, although it is recommended that the crime risk assessment mechanism should be utilised on a voluntary basis, it is essential that its introduction is accompanied by publicity, research, policy and legislative change. For manufacturers to accept the benefits of considering the crime implications of their design, they must be convinced: a) That consumers want secure products and are willing to pay an additional premium for security; b) That national, regional and local governments are taking crime seriously and will introduce policy and legislation that creates an environment in which criminogenic design will not be tolerated; c) That they (manufacturers) will receive a financial incentive to design secure products, and d) that they (manufacturers) will be able to gain commercial advantage by differentiating their product based upon its levels of security. For this scheme to achieve maximum impact, it is essential that its introduction is accompanied by measures to address these issues. Examples taken from the field of designing out crime within the built environment include: 1) The commissioning of research to establish whether consumers want secure

products and whether they are willing to pay an additional premium for these goods; 2) Legislation to extend the powers of Section 17 of the Crime and Disorder Act to the private sector (and to whole of Europe); 3) Financial incentives for manufacturers who design secure products (these can be justified through costs saved i.e. criminal justice system, insurance claims etc.); 4) Commissioning research to establish whether manufacturers would gain a commercial advantage through producing secure products.

Balancing Pre-Emptive Assessments with the Risk of Miscalculation

One of the key concerns regarding the likely success of a risk assessment mechanism for electronic products was that the final mechanism must be applicable at the prototype stage as any security changes required post-production would be prohibitively expensive. The ideal scenario, like that found in designing out crime in the built environment, would be for assessments of vulnerability and security to be made before a product is developed to enable changes to be made to the design without requiring it to be rebuilt. Although this scenario is (eventually) working well within the built environment, with most Architectural Liaison Officers/Crime Prevention Design Advisors consulted at the concept stage, in an industry which moves as quickly as consumer electronics, there is a risk that vulnerability will be miscalculated. One example where vulnerability was miscalculated was set-top boxes which enable viewers to receive digital stations. As Ekblom (2005) highlights, these were ideal candidates for theft in that they weighed very little, were very small in size and were likely to cost in excess of £100. As is often the case with electronics products, the level of risk of this product was altered almost instantly by the industry's decision to give the boxes away whilst recouping costs on service subscription payments. Ekblom (2005) questions whether "the forecast can be estimated and particularised to a type of product, in its anticipated environment of use, with sufficient confidence for design decision-makers to say 'we accept this product is at exceptional risk of theft (and it is in our interest to reduce that risk)" (Ekblom, 2005 p.25). Whilst the authors accept this reservation, they do not accept that the risk of miscalculation outweighs the risk of inaction. The dangers of miscalculation in assessing vulnerability involve a) overestimating vulnerability (and risking

disapproval from manufacturers), or b) underestimating vulnerability which would risk the safety of consumers.

The potential negative consequences of overestimating the vulnerability of a product are 1) the disapproval of manufacturers due to consumers avoiding a product which has been mistakenly labelled as vulnerable, and 2) consumers taking additional security precautions to counteract a product's vulnerability.

In response to the first point, how likely is it that a miscalculation would result in a challenge from manufacturers? The authors propose that there are two reasons why this would be unlikely. Firstly, a miscalculation is more likely to involve a product i.e. set-top box rather than a make/model of a product. In this instance all manufacturers of that product would have been equally affected by the negative assessment rather than an individual company. The second reason that a challenge would be unlikely is that, like the case of set-top boxes, the miscalculation would not be immediately apparent and may take months/years to come to light. Manufacturers, who would be focusing upon the next product, are unlikely to spend time and energy challenging an assessment which took place several years before. The second point, that consumers take additional precautions in response to an inaccurate warning would surely be a risk worth taking.

The risk of underestimating vulnerability would be a more serious concern. The risk of making a false assessment is possible and is likely to be increased where assessments are made too early i.e. a product appears less vulnerable but changes in advertising/endorsements could alter its popularity. To avoid this, the system developed must ensure that assessments take place early enough to avoid expensive changes to the design of the product, but late enough to be able to capture all relevant information relating to the product. The assessment system must also be flexible enough to move with changes in the market.

These risks highlight the need to consult extensively with manufacturers, retailers, designers and consumers before any system for implementation is

finalised. Although the risks would need to be considered carefully and consumers made aware of the speculative nature of the assessments, concerns regarding possible risks should not override the potential benefits of implementing this system.

Is This an Exercise in Self-Delusion?

Although interesting in its own right, the development of an assessment to measure the risk of theft is worthless unless manufacturers implement it and consumers accept it. This paper is concluded by revisiting the reservations highlighted in the introduction and, where feasible, proposing solutions.

Addressing Perverse Incentives

Although this should not be used as an excuse by the electronics industry to avoid the issue of securing their products, there are obvious weaknesses in the process of claiming for stolen electronic products which act as a disincentive for consumers to demand more secure goods. Although this is a valid concern which needs to be addressed, the argument that consumers are largely pleased to have an electronic product stolen because the insurance company will replace it with a newer model ignores three points: 1) That many small consumer electronic products are uninsured; 2) That the loss of a product such as a laptop, MP3 player or PDA invariable means the loss of data and an inconvenience to the consumer; 3) That a theft of a product rarely takes place in isolation. The victim whose product is stolen may experience physical injury, emotional trauma or even death. Recent media reports have highlighted these issues. Both the Sunday Times (UK) and the Daily Telegraph reported in late 2005 and early 2006 that street robbery was soaring as muggers target iPod users (Street Robbery Soars as iPod Users Targeted, 2005; Street Robberies Soar as Muggers Target iPod Users, 2006). This problem has also been widely reported in the USA with coverage of Steve Jobs (Apple computers) personally contacting the family of a teenager killed for his iPod (Jobs Calls Family of Stabbing Victim, 2006). Opposing the proposed system of securing electronic products on the premise that consumers will not want to avoid theft and would prefer to become a victim of crime if they receive a new phone is both unconvincing and uninformed.

Will Offenders Differentiate?

A valid point highlighted throughout the consultation process is that offenders who steal a bag or burgle a property will not take the time to differentiate between secure and unsecure products. They will simply take the bag/burgle the property in the hope that the contents will be re-usable. One of the most effective methods of avoiding this would be to maximise the number of products which achieve the 'Secure Product' label, thus reducing the odds that the bag taken by an offender will contain any usable products. Reducing the likely benefits of stealing a bag (or burgling a property) would in turn reduce the appeal of such a target.

You Cannot Ask Manufacturers and Designers to Develop Undesirable Products

The final criticism is a misconception which must be addressed. The aim of the proposed system is not to encourage manufacturers and designers to develop products which will not be attractive to consumers, the aim is to ensure that the products which are highly desirable (due to their popularity and value) are equally secure. Manufacturers obviously want their products to be attractive to consumers, and there is no suggestion that products should be made less popular, fashionable or desirable. Rather that the factors which make the product attractive to consumers are accompanied by commensurate security factors which make them unattractive to offenders.

ACKNOWLEDGEMENTS

This research was conducted as part of Project MARC – funded by the European Commission under the Sixth Framework Programme. We acknowledge the contributions made by Professor Ernesto Savona and Martina Montauti (Università Cattolica Del Sacro Cuore).

REFERENCES

Armitage, R. (2000) *An Evaluation of Secured by Design Housing within West Yorkshire – Briefing Note 7/00.* London: Home Office.

Bevis, C. and Nutter, J.B. (1997) *Changing Street Layouts to Reduce Residential Burglary: Paper presented to the American Society of Criminology.* Atlanta.

Brantingham, P.L. and Brantingham, P.J. (1975) Residential Burglary and Urban Form. *Urban Studies,* 12, 273-284.

Brantingham, P.L and Brantingham, P.J (1993) Environmental Routine and Situation: Towards a Pattern Theory of Crime. *Advances in Criminological Theory.* 5, 259-294.

Brantingham, P.L and Brantingham, P.J. (2000) *A Conceptual Model for Anticipating Crime Displacement: Paper presented at the American Society of Criminology Conference.* San Francisco.

Brantingham *et al,* (1977) Perceptions of Crime in a Dreadful Enclosure. *Ohio Journal of Science,* 77, 256-261.

Brown, J. (1999) *An Evaluation of the Secured by Design Initiative in Gwent, South Wales* (unpublished MSc. Dissertation). Scarman Centre for the Study of Public Order: Leicester.

Brown, B. B. and Altman, I. (1983) Territoriality, Defensible Space and Residential Burglary: An Environmental Analysis. *Journal of Environmental Psychology,* 3, 203-220.

Brown, B. and Bentley, D. (1993) Residential Burglars Judge Risk: The Role of Territoriality. *Journal of Environmental Psychology,* 13, 51-61.

Clarke, R.V. (1992) Introduction. *In:* R.V. Clarke (ed.) *Situational Crime Prevention – Successful Case Studies.* New York: Harrow and Heston. p. 3-36.

Clarke, R.V (Ed.) (1997) *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Monsey, NY: Criminal Justice Press.

Clarke, R.V. *et al.* (2001) Controlling Cell Phone Fraud in the US – Lessons for "Foresight". *Security Journal.* 14 (1), 7-22.

Clarke, R. V. and Eck, J. (2003) *Become a Problem Solving Crime Analyst*. Cullompton, UK: Willan Publishing.

Clarke, R.V. and Newman, G.R (2002) *Secured Goods by Design – A Plan for Security Coding of Electronic Products,* London, Department of Trade and Industry.

Clarke, R.V. and Newman, G.R. (2005) Introduction. *In:* R. V. Clarke and G. R. Newman (eds.) *Designing Out Crime from Products and Systems.* Cullompton, UK: Willan Publishing.

Clarke, R. V. and Newman, G.R (2005) Modifying Criminogenic Products: What Role for Government. *In:* R. V. Clarke and G. R. Newman (eds.) *Designing Out Crime from Products and Systems.* Cullompton, UK: Willan Publishing.

Cornish, D.B. and Clarke, R.V. (2003) Opportunities, Precipitators and Criminal Decisions. In *Theory for Practice in Situational Crime Prevention, Crime Prevention Studies*, Vol 16. Monsey, NY: Criminal Justice Press.

Cromwell, P.F. *et al.* (1991) *Breaking and Entering: An Ethnographic Analysis of Burglary.* Newbury Park, California: Sage.

Design Council (2002) *Design Against Crime*. London: Design Council.

Ekblom, P. (1997) Gearing Up Against Crime: A Dynamic Framework to Help Designers Keep Up with the Adaptive Criminal in a Changing World. *International Journal of Risk, Security and Crime Prevention.* 2 (4), 249-265.

Ekblom, P. (2005) Designing Products Against Crime. In N. Tilley (ed.) *Handbook of Crime Prevention and Community Safety*. Cullompton, UK: Willan Publishing.

Greenberg, S. and Rohe, W. (1984) Neighbourhood Design and Crime: A Tale of Two Perspectives. *Journal of American Planning Association,* 50 (1), 48-61.

Harrington, V. and Mayhew, P. (2001) *Mobile Phone Theft – Home Office Research Study 235.* London: Home Office.

Jobs Calls Family of Stabbing Victim (2005, July 06) Available from: <URL: http://money.cnn.com/2005/07/06/news/newsmakers/stevejobs_ipod/>. [Accessed 03 March 2006].

Laycock, G. and Webb, B (2005) Designing Out Crime from the UK Vehicle Licensing System. *In:* R. V. Clarke and G. R. Newman (eds.) *Designing Out Crime from Products and Systems.* Cullompton, UK: Willan Publishing.

Levi, M. and Handley, J. (1998) *The Prevention of Plastic and Cheque Fraud Revisited.* Home Office Research Study 182, London: Home Office.

Mirlees-Black, C. *et al. (*1998) *The 1998 British Crime Survey – England and Wales.* London: Home Office.

Newlands, M. (1983) *Residential Burglary Patterns in a Vancouver Neighbourhood* (unpublished honors thesis). Simon Fraser University.

Pascoe, T. (1999) *Evaluation of Secured by Design in Public Sector Housing – Final Report.* Watford: BRE.

Pease, K. (1997) Crime Reduction. *In:* M. Maguire *et al* (eds.) *The Oxford Handbook of Criminology: Second Edition.* Oxford: Clarendon Press.

Reppetto, T.A. (1974) *Residential Crime.* Cambridge, MA: Ballinger.

Sherman, L.W., Gottfredson, D., MacKenzie, D., Eck, J., Reuter, P., and Bushway, S. (eds.) (1997) *Preventing Crime: What Works, What Doesn't and What's Promising.* Office of Justice Programs Research Report. Washington, DC: US Department of Justice.

Smith, D.J. (2000) Changing Situations and Changing People. *In:* A. von Hirsch (eds.) *Ethical and Social Perspectives on Situational Crime Prevention.* Portland, Oregon: Hart Publishing.

Smith, M.J., Clarke, R.V., and Pease, K. (2002) Anticipatory Benefits in Crime Prevention. *In:* N. Tilley (ed.) *Analysis for Crime Prevention.* Crime Prevention Studies, Vol 13. Monsey, NY: Criminal Justice Press.

Street Robbery Soars as iPod Users Targeted (2005, October 09). Available from: <URL: http://www.timesonline.co.uk/article/0,,2087-1817433,00.html>. [Accessed 03 March 2006].

Street Robberies Soar as Muggers Target iPod Users (2006, January 27) Available from: <URL: http://news.telegraph.co.uk/news/main.jhtml?xml=/news/2006/01/27/nrob27.xml&sSheet=/news/2006/01/27/ixnewstop.html>. [Accessed 03 March 2006].

Webb, B. (1997) Steering Column Locks and Motor Vehicle Theft: Evaluations from Three Countries. *In:* R. V. Clarke (ed.) *Situational Crime Prevention: Successful Case Studies* (2nd ed.) Guilderland, NY: Harrow and Heston.

1

[i] This took place at the MARC Crime Proofing Steering Group. Even though partners were given a detailed explanation of the checklists, and how to apply them, the scores still differed between them.
[ii] This example is based upon the JDI research team's experience and was replicated for the Università Cattolica Del Sacro Cuore team starting with Italy.

1