

This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Definition of final crime risk assessment mechanism to measure the risk of theft of electronic products and proof them against theft

PLEASE CITE THE PUBLISHED VERSION

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Armitage, Rachel, Ron Clarke, Ken Pease, Ernesto Savona, Martina Montauti, and Andrea Di Nicola. 2019. "Definition of Final Crime Risk Assessment Mechanism to Measure the Risk of Theft of Electronic Products and Proof Them Against Theft". figshare. <https://hdl.handle.net/2134/2994>.

DEFINITION OF FINAL CRIME RISK ASSESSMENT MECHANISM TO MEASURE THE RISK OF THEFT OF ELECTRONIC PRODUCTS AND PROOF THEM AGAINST THEFT

- Dr. Rachel Armitage, Jill Dando Institute, University College London.
- Professor Ron Clarke, Jill Dando Institute, University College London.
- Professor Ken Pease, Jill Dando Institute, University College London.
- Professor Ernesto Savona, Università Cattolica Del Sacro Cuore.
- Dr. Martina Montauti, Università Cattolica Del Sacro Cuore
- Dr. Andrea Di Nicola, Transcrime

DRAFT DELIVERABLE FOR WP 1 4 OF:

Project MARC – Developing Mechanisms for Assessing the Risk of Crime due to legislation and products in order to proof them against crime at an EU level

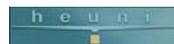


A PROJECT FINANCED BY THE EUROPEAN COMMISSION – DG RESEARCH UNDER THE SIXTH FRAMEWORK PROGRAMME

and coordinated by:



in partnership with:



And in co-operation with:



APRIL 2006

TABLE OF CONTENTS

ABSTRACT	8
1. INTRODUCTION	10
1.1 Risk and Responsibility	10
1.2 Justification for Measuring Risk?	11
1.3 Crime: Risk not Moral Aberration	12
1.4 Opportunity Theories	14
1.5 Risk Assessment and Crime Reduction	17
1.6 The Design of Products and Services and Crime	20
1.7 Crime Reduction Success Achieved through Opportunity Reduction	21
1.8 Progress in other Sectors	23
1.9 The Measurement of Crime Risk: Electronic Products	25
1.10 Developing a Draft Crime Risk Assessment Mechanism	26
1.11 If we keep the Checklists	30
1.12 Do we want to keep the two Checklists?	34
2. METHODOLOGY – DEVELOPING, REFINING AND TESTING THE CRIME RISK ASSESSMENT MECHANISM	39
2.1 Methodological Steps	39
2.2 Step 1: Design the Questionnaire	40
2.3 Step 2: Selection of and Production of Descriptive Reports for a Set of Electronic Products	41
2.4 Step 3: Selection of a Panel of Key Stakeholders	42
2.5 Step 4: Dissemination of the Questionnaire	44
2.6 Step 5: Collection and Analysis of Data	45
3. RESULTS	50
3.1 Participants	50
3.2 Vulnerability versus Security – 15 Individual Products	52
3.3 MP3 Players	52
3.4 Personal Digital Assistants	53
3.5 Digital Cameras	53
3.6 Mobile Phones	54
3.7 Laptop Computers	54
3.8 Correlation between Vulnerability and Security	56

3.9 Aggregate scores – Vulnerability versus Security	56
3.10 Product Type	60
3.11 Sector Type and Perceptions of Vulnerability and Security	60
3.12 Defining Vulnerability – Stakeholders’ Views	62
3.13 FujiFilm Finepix S7000 – Aggregate Vulnerability Score	63
3.14 Apple iPod 20GB – Aggregate Vulnerability Score	59
3.15 Nokia 6230i Mobile – Aggregate Vulnerability Score	64
3.16 Sony Ericsson K700i – Aggregate Vulnerability Score	65
3.17 Sony Vaio VGN B1XP – Aggregate Vulnerability Score	58
3.18 Motorola V600 – Aggregate Vulnerability Score	56
3.19 HP iPAQ rx3715 – Aggregate Vulnerability Score	55
3.20 iAudio M3 – Aggregate Vulnerability Score	55
3.21 Defining security – Stakeholders’ Views	55
3.22 Toshiba Satellite M30X 159 – Aggregate Security Score	47
3.23 Motorola V600 – Aggregate Security Score	42
3.24 Sony Vaio VGN B1XP – Aggregate Security Score	39
3.25 Nokia 6230i – Aggregate Security Score	31
3.26 Sony Ericsson K700i – Aggregate Security Score	31
4. DEFINITION OF THE FINAL CRIME RISK ASSESSMENT MECHANISM	75
4.1 Assessment of Risk – Progress so far	75
4.2 Differences in Market Penetration and Early Warnings about Crime Risk	77
4.3 Improving the Vulnerability Checklist	78
4.4 The Weakness of the Security Checklist	79
4.5 Do Findings Suggest that all Portable Products are Vulnerable to Theft and Should be Treated as Equal in Terms of Security?	81
4.6 What Might the Final Crime Risk Assessment Mechanism Look Like?	83
5. IMPLEMENTING THE FINAL CRIME RISK ASSESSMENT	85

MECHANISM	
5.1 Progress so Far	85
5.2 Proposing a Model for Implementation	85
5.3 Engaging Manufacturers	94
5.4 Balancing Pre-Emptive Assessments with the Risk of Miscalculation	95
5.5. Is This an Exercise in Self-Delusion?	97
6. CRIME PROOFING SERVICES	99
7. RECOMMENDATIONS	108
Appendix 1. Interview Schedule for Key Stakeholders	113
Appendix 2. Stakeholders Questionnaire for Assessing the Vulnerability/Security Levels of a Selection of Electronic Products	119
References	136

LIST OF TABLES

Table 1: Checklist for Risk of Theft	27
Table 2: Checklist for Product Security	28
Table 3: Respondents	30
Table 4: Specific Comments on Checklist One – Assessing Vulnerability	31
Table 5: Specific Comments on Checklist Two – Assessing Security	33
Table 6: Participants’ Scores for Apple iPod	37
Table 7: Participants’ Score for FujiFilm Digital Camera	38
Table 8: Geographical Spread of Participants	51
Table 9: Sector which Participants Represented	52
Table 10: Apple iPod 20GB	53
Table 11: Apple iPod Mini	53
Table 12: iAudio M3	53
Table 13: Palm One Zire 72	54
Table 14: Palm One Tungsten T5	54
Table 15: HP iPAQ rx3715	54
Table 16: Olympus Camedia C-770 Ultra	55
Table 17: Olympus Camedia C-5060	55
Table 18: FujiFilm Finepix S7000	55
Table 19: Motorola V600	56
Table 20: Nokia 6230i	56
Table 21: Sony Ericsson K700i	56
Table 22: Toshiba Satellite M30X159	56
Table 23: Apple Powerbook 15 inch	57
Table 24: Sony Vaio VGN B1XP	57
Table 25: Aggregate Vulnerability Scores and Security Scores for Each Product	58
Table 26: Products Ranked by Vulnerability	59
Table 27: Products Ranked by Security	60
Table 28: Product Type and Perceptions of Vulnerability and Security	61
Table 29: Sector Type and Perceptions of Vulnerability	62
Table 30: Sector Type and Perceptions of Security	62

Table 31: FujiFilm Finepix S7000 – Defining Vulnerability	63
Table 32: Apple iPod 20GB – Defining Vulnerability	64
Table 33: Nokia 6230i – Defining Vulnerability	65
Table 34: Sony Ericsson K700i – Defining Vulnerability	66
Table 35: Sony Vaio VGN B1XP – Defining Vulnerability	67
Table 36: Motorola V600 – Defining Vulnerability	68
Table 37: HP iPAQ rx 3715 – Defining Vulnerability	68
Table 38: iAudio M3 – Defining Vulnerability	69
Table 39: Producing a Scoring System for Vulnerability Factors	70
Table 40: Toshiba Satellite M30X159 – Defining Security	72
Table 41: Motorola V600 – Defining Security	72
Table 42: Sony Vaio VGN B1XP – Defining Security	73
Table 43: Nokia 6230i – Defining Security	74
Table 44: Sony Ericsson K700i – Defining Security	74
Table 45: Producing a Scoring System for Security Factors	75
Table 46: 25 Techniques of Situational Crime Prevention	81
Table 47: Types of Mobile Phone Fraud	84

LIST OF FIGURES

Figure 1: Example of Incentives to Design out Crime in 94 Residential Housing

ABSTRACT

This report presents research conducted as part of a two-year European project (Project Marc) which aims to develop a mechanism to assess the risk of theft of electronic products and to take steps to make that mechanism operational. The view of the authors, reflected throughout this report, is that the task of developing such a tool is vital yet daunting. It is vital because of the need to build upon the gains made within other sectors and the need to seize the opportunity presented by the realisation that crime trends can be explained in terms of the supply of opportunities, that reducing the supply of opportunities will reduce crime and that these tasks are not the sole responsibility of the police. 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.

The report sets out the process of developing a crime risk assessment mechanism and the justification for pursuing the options taken. Initial consultation with a variety of stakeholders yielded the common view that the crime risk assessment mechanism presented must a) measure both risk and protection (ensuring that the two are commensurate), b) reflect the perspectives of those who would be tasked with implementing it and c) reflect the language of stakeholders from a variety of European states. Taking these views on board, the authors conducted an extensive consultation with stakeholders from four sectors (insurance, consumers' organisations, law enforcement and manufacturers of electronic products) from ten European member states. Participants were asked to rate a variety of electronic products in terms of both vulnerability and security and to explain the ratings they gave. 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 authors suggest that the crime vulnerability checklist developed within this report is judged fit for purpose as a provisional

measurement. The security measurement by checklist was concluded to be inappropriate, since it would lead to limited and unimaginative security, and a case-by-case assessment by domain experts is advocated, in the light of measured vulnerability. A two-pronged approach to rating of electronic products (and possibly services) is outlined based upon approaches already deployed in relation to food standards

1. INTRODUCTION

1.1 Risk and Responsibility

This report presents research conducted between 2004 and 2006 seeking to develop a mechanism to measure the risk of theft of electronic products and to take steps towards operationalising that mechanism. The last two decades have seen a major change in the perception of how crime reduction is to be achieved. Following the advance of situational crime prevention and the demonstration that crime trends are more readily explained by the supply of opportunities than the distribution of criminal propensity across the population (Mayhew *et al*, 1976; Felson, 1998; Felson and Clarke, 1998), crime (in particular theft) is widely accepted as a “risk to be calculated...rather than a moral aberration which needs to be explained” (Garland, 1996 p. 450–451).

The second facet of this change in perception is the recognition, first expressed in the Morgan Report of 1991 (Home Office, 1991) and culminating in England and Wales in the Crime and Disorder Act (1998), that the supply of opportunities is under the control of agencies other than the police and that the historic reliance upon police as the primary crime reduction functionaries was both misguided and unfair. Although these advances have resulted in dramatic changes in both perception and policy, the picture remains incomplete. An example is taken from the experience of England and Wales, where there has arguably been more work demonstrating the crime-reductive effects of limiting opportunity than elsewhere in Europe, and therefore the countries where the evidence base is best placed to influence crime control policy.

The Crime and Disorder Act (1998), described by Laycock (2001) as “one of the most significant pieces of legislation in support of crime reduction” (p.21), brought about the widespread introduction of multi-agency partnerships tasked with the reduction and prevention of crime and disorder and the recognition in Section 17 of that Act that relevant

authorities¹ must consider the crime and disorder implications of every decision that they make. Yet, despite a recommendation by the Government's own Foresight committee on crime, there remains a failure to extend the provisions of Section 17 of the Crime and Disorder Act to central government and the private sector (the latter being crucial to this project). In reality this means that whilst legal action² can be used as an incentive to convince local authority planning departments that (for example) housing in the area should be built to Secured by Design standards, which render them less vulnerable to victimisation (Armitage, 2005)³, those who design, manufacture and retail desirable and expensive electronic goods have no legal responsibility for the crime and disorder implications of their products. Considerations of corporate social responsibility are not generally brought to bear on the problem. Whilst legislation alone may not always be the answer, the omission of central government and the private sector from the provisions of the Crime and Disorder Act portrays the message that currently these sectors are not charged as major suppliers of criminal opportunities.

To restate, the emphasis here is on England and Wales, both because much of the research base for situational crime prevention is British, and because the writers know of no legislation equivalent to S17 of the Crime and Disorder Act, which at least demonstrates the emergent mode of thought from which Project MARC sprang.

1.2 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

¹ Local Authorities, Joint Authorities, National Park Authority, Broads Authority and the Police were defined as relevant authorities in the 1998 Crime and Disorder Act. The Police Reform Act (2002) stated that relevant authorities would extend to Primary Care Trusts (April 2004), Fire Authorities (April 2003) and Police Authorities (April 2003).

² In the form of liability in private law for breach of a statutory duty, or liability to judicial review under the doctrine of *ultra vires*.

³ As well as countless other examples involving agencies deemed 'relevant' to the reduction of crime.

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 (discussed in more detail below) 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, as Garland suggests, is 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. As is highlighted below, 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, vehicles) sufficiently justifies the objectives of this task. As pre-eminently desirable and stealable, small electronic products provide an obvious starting point for risk assessment.

1.3 Crime: Risk versus Moral Aberration

While notions of crime have a moral position at their core, being those behaviours which the state has a direct interest in controlling, prudence dictates that crime control proceeds by means other than moral condemnation, to complement actions of the criminal justice apparatus. There is an abundance of theories as to why individuals offend. There are correspondingly many intervention points for the reduction of offending – some of which focus upon the offender (programmes to reduce drug use), some the victim (crime prevention publicity) and others the location in which crimes take place (street lighting, CCTV). Early exponents of the suggestion that criminality can be explained (at least in part) through biological or developmental factors include Cesare Lombroso and his *scuola positiva* in the late nineteenth century whose focus lay upon distinguishing the characteristics of the born criminal. More recently, biological and developmental criminologists have identified factors associated with increased risk of criminality. Although these do not focus exclusively

upon the biological, factors such as hyperactivity and impulsivity (Satterfield and Schell, 1997; Klinteberg *et al.*, 1993), low birth weight (McGee *et al.*, 1984; Kolvin *et al.*, 1990) and brain damage (Brennan *et al.*, 1991; Michaud *et al.*, 1993) have been identified as risk factors associated with criminal and anti-social behaviour.

Authors such as Caspi and Moffit (1995) also emphasise both biological and social processes in crime causality, suggesting that transient, delinquent behaviour can be linked to social factors such as a desire for autonomy and peer delinquency and that the factors distinguishing these short-term offenders from long-term, persistent offenders lay within neurodevelopmental processes. Moffit's (2003) review of the causes of anti-social behaviour distinguishes between two prototypes - life-course-persistent and adolescence-limited. According to Moffit (2003), the former has its origins in neurodevelopmental processes, begins in childhood, and continues into adulthood, the latter has its origins in social processes, begins in adolescence and desists in young adulthood. The focus upon genetic factors in criminality, and in particular the recent work of Moffit (2003), does not focus exclusively upon the biological at the expense of situational factors. In fact, the suggestion that life-course-persistent anti-social behaviour has its origins in early life, but is exacerbated by a high-risk social environment (Moffit, 2003), is entirely consistent with the need to limit criminogenic opportunities, thus minimising the likelihood that those with a propensity to offend will be provided with that opportunity. The development of the sub-discipline of evolutionary psychology is persuasively showing how many of the patterns of crime are explicable by the evolutionary advantage which errant behaviour conferred on our forebears (see for example Walsh and Ellis, 2003).

The view that crime and criminality is abnormal or unusual has declined in popularity over the last half of the twentieth and early part of the twenty-first century with much evidence-based criminological theory focusing upon criminal events as opposed to the offender. Although these theories differ in their focus, many share the theme that opportunity generates crime and begin from the premise that

crime is normal as opposed to something unusual which has to be explained. The crucial point is that whatever the origins of crime, whatever the distribution of criminal propensity across individuals, manipulating the threshold for the translation of inclination into action makes sense. Erecting safety barriers around tall structures from which suicidal people throw themselves makes sense whatever presumptions are made about the causes of suicidal feelings and actions. Such barriers simply raise the threshold (both physically and metaphorically) which the inclination must exceed for a suicide to occur. Classic demonstrations of this come with the reduction of suicide when a 'popular' method of killing oneself ceases to be available (Clarke and Lester 1989).

1.4 Opportunity Theories

Although individuals' propensity to offend varies (and the risk factors affecting this are open to debate, see Pease 2005) there is no questioning the fact that opportunities influence crime levels and that certain people, products and places are more vulnerable than others. Several criminological theories (often referred to as the New Opportunity Theories) highlight how opportunity generates crime, be that opportunity afforded by the physical and social arrangements of society or the design (and subsequent demand) of particular targets. In Section 1.6 below, a brief overview of crime reduction successes achieved on the basis of this perspective will be provided.

Routine Activity Theory (Cohen and Felson, 1979) considers how the structure of modern society and the routine activities of everyday life have created more opportunities for criminal activities. Two factors acting together were shown to explain the rise in burglary in the United States in the 1960s and 1970s. The first was a substantial movement of women into the labour force, which meant that homes were left without "capable guardians" for much of the day. The second, crucial for understanding the origins of Project Marc, was the large increase in the ownership of small, expensive consumer products, which provided many "suitable targets" for burglary. Cohen and Felson (1979) used the acronym VIVA (Value, Inertia, Volume and Access) to

describe these suitable targets. Clarke (1999) expands upon this using the acronym CRAVED (Concealable, Removable, Available, Valuable, Enjoyable and Disposable) to identify hot products. For example, a laptop computer would be concealable and removable, it would be widely available, valuable, enjoyable for personal use and disposable should the offender choose to sell the product. On the other hand, a freezer would be available (with most households containing one), reasonably valuable, but would be very difficult to remove, conceal or dispose of without drawing too much attention to yourself. According to these theories, a laptop would make a much more suitable target than a freezer, thus the increase in the use and availability of small, valuable products such as mobile phones, iPods, game boys, camcorders and hand-held computers have fuelled the opportunities for crimes to be committed.

Rational Choice Theory (Cornish and Clarke, 1986) is influenced by economic thinking and assumes that offenders seek to maximise the benefits of offending and in doing so make rational or quasi-rational choices or decisions based upon the information or cues available to them at the time of offending. Decision processes are likely to vary according to the different stages of criminal involvement, between offenders (based upon age, experience etc.) and between different offence categories. Preventive suggestions seek to influence an offender's decision or choice to commit a crime through 1) increasing what they perceive to be the risks involved in committing that offence (installing a burglar alarm, designing housing estates to maximise natural surveillance), as well as 2) reducing the rewards should that crime occur (property marking). The aim is to ensure that for the offender the perceived costs outweigh the perceived benefits of offending.

Pattern Theory adds spatial and temporal elements to opportunity theories. It suggests that crimes "do not occur randomly in time or space or society" (Brantingham and Brantingham, 1993 p.264). For example, as Brantingham and Brantingham (1993) suggest, bar fights are more likely to occur in Friday nights than Tuesday afternoons, income tax evasions are likely to cluster around the dates in which

payments are due and pilfering of office supplies is likely to cluster geographically around areas with a high density of offices. Pattern Theory suggests that crimes will cluster around nodes (the places where people travel to and from), along pathways (the paths along which people travel to get to different nodes) and at the boundaries to both nodes and pathways (edges). If offenders are viewed as being the same as 'normal' citizens (other than their readiness to commit crime), the way in which they select a target against which to commit a crime is much the same as the method we use to select a service station in which to fill our car with petrol. We a) pass the petrol station just as we realise we need some petrol or b) have passed the petrol station on a previous occasion and know that it offers good value for money, therefore making a particular journey back to that area as and when we need petrol. If the same applies to offending patterns, offenders will select their target because a) they pass it on their way to school/work, to visit a friend or attend a leisure facility (it is in their activity/awareness space) and realise it has poor security, looks unoccupied or has valuable goods on show (or all of the above), therefore selecting to offend against the target there and then or b) they have passed/noticed the target on a previous occasion and decided to offend against the target at a later date. One of the key principles of this theory is that offenders, like everybody else, spend much of their time travelling between the places where they live and the places they attend as part of their leisure/school/work activities and they choose their targets from within their activity and awareness space.

“Since burglars are, in a time–budget sense, primarily non–burglars, their activity spaces, or places they usually spend time, are most likely similar to the activity spaces of non–burglars from similar backgrounds and living in similar areas” (Brantingham and Brantingham, 1984 p.80).

Several research studies support the theory that crimes are likely to cluster around offenders' activity and awareness spaces. These include Greenberg and Rohe (1984), Taylor and Gottfredson (1987), Rengert and Wasilchick (2000) and Wiles and Costello (2000).

All theories outlined above converge in contending that addressing the circumstances of crime rather than the psyche of the offender will gain crime reduction advantage. The only fundamental opposition to this perspective comes from the view that there is a constant amount of criminal inclination in the population which, if thwarted by the removal of opportunities, seeks out new opportunities to replace them. This phenomenon is known as displacement. An extensive literature review makes it clear that displacement does occur, but seldom if ever to an extent which makes opportunity reduction unproductive. Indeed, sometimes the removal of opportunities in one area has a wider crime reductive effect. This is known as 'diffusion of benefits' (see for example Clarke and Weisburd 1994).

Restriction of crime opportunities is, in the writers' view, a moral imperative. It saves from criminal labelling those on the margins of crime, arguably especially those whose potential criminal involvement is transient and limited to the adolescent years. One element in such restriction involves the design of goods and services. It is the most difficult to implement, since crime reduction is not a powerful component of market forces. Indeed, insofar as stolen goods are replaced, and insofar as those who steal things (and those to whom they sell them) would not buy them legitimately, there is a perverse incentive to produce crime-prone goods.

1.5 Risk Assessment and Crime Reduction:

Risk assessment in criminology is not new. As Wiles *et al* (2003) highlight: "There are at least four criminal justice contexts in which understanding and communicating risk is important" (p.1). These four areas in which risk-assessment within criminology has traditionally focused are: the chance of someone embarking on a criminal career; the probability of crime victimisation by location and person; the risk of re-offending and finally, the likelihood of a particular offender being responsible for a particular unsolved crime (offender profiling). To this, the authors would add the risk of victimisation by product – the risk of victimisation by vehicle make and model being relatively

well established whilst the vulnerability of alternative products is still in its infancy (hence the commission of the project reported on here).

The first of these contexts has been the focus of developmental or risk-focused criminology for at least three decades (West and Farrington, 1973; West, 1982; Farrington, 1978, 1986a, 1986b, 1991, 1992, 1995) but has risen in prominence (particularly in the United Kingdom) since the requirement upon Local Authorities to produce a local preventive strategy for children and young people by April 2003. Publications such as Homel *et al*/ (1999), Youth Justice Board (2001) and Wong (2003) highlight the risk and protective factors which increase or reduce the likelihood that young people will become involved in crime and anti-social behaviour – these are generally summarised into the categories: family, school, community/cultural, life events and personal/individual.

The risk of victimisation by location is another field in which crime risk assessment mechanisms have been successfully applied to reduce the vulnerability of the built environment. Coleman (1986) developed a Design Disadvantage Score of 0–15 which identifies the threshold point at which certain environmental factors (i.e. access points, number of dwellings in a block, number of play areas) become associated with crime and disorder. Winchester and Jackson (1982) also produced an index of risk based upon 14 different variables of access and surveillance which were found to be particularly effective in discriminating between houses which had been victimised and those which had not. The more factors a dwelling possesses, the higher the chance of burglary victimisation. Groff and La Vigne (2001) also developed a predictive tool to help identify which properties are more vulnerable to burglary. The ‘Opportunity Score’ is based upon the presence or absence of 10 variables such as street lighting, proximity of property to residence of offenders, proximity to major thoroughfare and housing tenure. Finally, Armitage (2005) has recently developed a risk assessment mechanism – the Burgess Checklist, which is designed for practitioners as a means of identifying which properties will become vulnerable to crime if built (therefore allowing them to challenge planning applications) or, in the case of properties already

developed, allowing resources to be directed towards properties at most risk. The checklist is based upon the Burgess points system described in Simon (1971) who refers to it as “one of the simplest prediction methods” (p.31), with an application in a criminological context described in Nuttall *et al* (1977) who commend it as robust and simple. Essentially, a score is derived from the difference between the mean rate of crime suffered generally, and the rate of crime suffered by properties with a particular characteristic (i.e. being located next to a footpath, being located on a through road, being located next to open land). The method of producing the checklist involved collecting evidence regarding 33 environmental factors for each of 1058 properties. Each of the 33 factors were then cross tabulated against prior victimisation to reveal which factors were most associated with crime prone homes. Environmental factors which were not associated with risk of burglary (or total crime) at a statistically significant level were excluded from the analysis. For those factors which were associated with crime risk, the Burgess method was applied to calculate a score for presence of that factor. For example, if the rate of victimisation of properties in the sample was 10%, the rate for properties next to open land was 15% and for properties not located next to open land was 5%, then the ‘open land’ factor would be scored as +5 for those located next to open land and –5 for those not located next to open land. Properties with the highest scores would be most vulnerable to victimisation. These are just a small sample of examples of the risk assessment tools which have already been developed for assessing risk of victimisation within the built environment.

The automotive industry (particularly the UK Motor Insurance Repair Research Centre) has also developed a comprehensive risk assessment mechanism (New Vehicle Security Rating) which is used by the insurance industry (who founded the Research Centre) to inform the accurate calculation of insurance premiums. Ratings can also be accessed by consumers to predict the risk of theft from and theft of any vehicle (see <http://www.thatcham.org/nvsr/cars/index.html>). The 5 star rating is calculated following attack tests on the vehicle as well as laboratory tests on the security system’s components.

1.6 The Design of Products and Services and Crime

As was highlighted above, a wide variety of manufactured products (those which are CRAVED) promote many different kinds of crime 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 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 can produce mini crime waves, or crime harvests. Increasingly, crime is not solely focused upon the electronic products themselves but also the systems or services associated with those products. For example, a criminal who clones a mobile phone/mobile phone SIM card is stealing the service, i.e. the provision of phone calls as opposed to the product itself. Similarly, electronic products such as MP3 players are not only targets of theft, but the services associated with these products, such as the ability to download music through the internet, have also become targets for criminal activity.

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, the internet or the design of certain types of housing. 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, systems and even urban spaces 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 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.

1.7 Crime Reduction Success Achieved through Opportunity Reduction

If, as these theories suggest, criminals commit crimes where opportunities exist (with low levels of risk and high levels of rewards), it follows that crime can be reduced through altering the target (be that a product, service, place or person) to increase the risk and effort and reduce the potential rewards. This is the central premise of crime reduction techniques such as situational crime prevention (SCP) and crime prevention through environmental design (CPTED) which aim to alter the environment in as systematic and permanent way as possible, so as to increase the effort and risks of committing a crime and reduce the rewards and excuses. These interventions work on the premise that offenders make calculated decisions (of limited rationality in formal decision theory terms) about the most suitable targets to

select. Therefore, altering the target (installing a burglar alarm or CCTV), or portraying the message that you may have altered the target (installing a dummy burglar alarm or installing CCTV in some shops but not others) should render that target less suitable, as perceived by the potential offender.

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 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 (Repetto, 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.

1.8 Progress in other Sectors

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 who have taken steps (either spontaneously or in response to government pressure) to design out crime from within their products and systems. These include the UK Vehicle Licensing System, the banking industry and the mobile phone industry.

Recognising the weaknesses within the UK vehicle registration and licensing system, the then Department of the Environment (DETR), which is now the Department for Transport (DfT), commissioned the Jill Dando Institute to review the existing system and make recommendations for its improvement. Problems within the existing system included database inaccuracy, insecurity within vehicle identification systems, inadequate enforcement, lack of a strategic overview and crime prevention not being awarded sufficient priority. Laycock and Webb (2005) describe the process of developing eleven recommendations for modernising the UK vehicle licensing and registration system and highlight what steps have been taken to implement these recommendations. The eleven recommendations made by the JDI report were accepted in principle by the UK Government, and an Implementation Group, plus several Sub-Groups, were established to take forward the recommendations. Lessons which can be learned from this project, and hopefully replicated within the

electronics industry, include the value of the continual presentation of evidence (delivered in this context through the commissioning of a series of follow-up research papers) and the need to present imaginative proposals within a realistic policy context (Laycock and Webb, 2005).

The banking industry has also gone some way towards recognising and addressing some of the weaknesses within its systems. In 1991, the Home Office commissioned a study, led by Professor Michael Levi, to identify a range of preventive strategies to reduce the level of plastic fraud – which in that year stood at £165.6 million. As Levi and Handley (1998) highlight, most of these recommendations – which included tighter controls over requests to redirect mail; card awareness campaigns and allowing customers to select their own Personal Identification Numbers, were subsequently implemented by the banking industry and relevant partners. A follow-up review (Levi and Handley, 1998) assesses the extent to which subsequent falls in fraud can be attributed to those interventions, concluding that the successful reduction in plastic fraud, which had fallen to £97.1 million by 1996, can be largely attributed to the preventive measures which were implemented following the 1991 report.

To some extent the mobile phone industry has begun to consider the crime implications of its products. For example, as highlighted by Clarke *et al* (2001), U.S. cell phone companies virtually eliminated “cloning,” which had cost them more than \$800 million in 1995, by extensive modifications made to their software systems. There was little evidence of displacement as a result of these modifications because other forms of cell phone fraud showed only modest rises when the cloning epidemic was eliminated. However, despite moves such as development of the Central Equipment Identity Register (CEIR) which allows all five UK networks to bar a phone which is reported lost or stolen (through its unique IMEI number) from use within the UK, crime reduction considerations have been highly reactive and limited in their effects. For example, the failure to require the compulsory registration of pay-as-you-go mobile phones allows criminals to communicate with total anonymity and facilitates the activities of

organised criminals due to the difficulties faced by law enforcement agencies when attempting to track the users of specific phones (Briscoe, 2001; NCIS, 2003; Myhill, 2004). In addition, research suggests that even with the steps taken by the mobile phone industry to develop the CEIR, offenders are stealing mobile phones to export outside the UK, where their IMEI is not barred (Harrington and Mayhew, 2001; BBC News, 2003; Britain Attacks Mobile Phone Theft, 2003; Metropolitan Police, 2003; Tackling Worldwide Trade in Stolen Mobiles, 2003; Ananova, 2004). In addition, offenders are continuing to steal and re-programme (change the IMEI) of mobile phones for re-sale within the UK.

1.9 The Measurement of Crime Risk: Electronic Products

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 report will focus upon what format that measurement might take in respect of electronic products. There are two possible audiences: 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 report, the risk measurement device which was developed under MARC is less fit for purpose in relation to this second audience.

Work package 12 of Project Marc introduced the draft Crime Risk Assessment Mechanism and described the methodology utilised to refine it. To avoid repetition, but still ensure that the reader is clear how the authors came to this position, below is a brief review of progress to date.

1. 10 Developing a Draft Crime Risk Assessment Mechanism

The process of developing a draft Crime Risk Assessment Mechanism took as its basis the Secured Goods by Design model presented by Clarke and Newman in 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 a product 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 Secured Goods 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: Checklist for Risk of Theft

	Items	Item Score
CONCEALABLE	<i>Check one</i> On person (score 2) In bag (score 1)	
REMOVABLE	<i>Check one</i> Can be carried in one hand (scores 2) Can be carried with two hands (score 1)	
AVAILABLE	<i>Score 1 for each</i> Used outside the home Commonly left in parked cars	

	Marketed to young males Minimal search time for thief to locate product
VALUABLE	<i>Score 1 for each</i> Costs at least one day's wages Provides access to phone services Provides access to the internet Provides access to credit
ENJOYABLE	<i>Score 1 for each</i> Entertaining Addictive Fashionable Luxury item Status item Aggressive advertising emphasising these themes
DISPOSABLE	<i>Score 1 for each</i> Widely in demand Value easily assessed Street price less than 50% of one day's wages
TOTAL SCORE	

Table 2: Checklist for Product Security

Security Feature	Score
<ul style="list-style-type: none"> Customer education designed into marketing (e.g. security instructions included in package) (score 1) 	
<i>Replacement guarantee to consumer if product stolen. Check one:</i> <ul style="list-style-type: none"> Within 90 days (score 1) Within 1 year (score 2) Life of product (score 3) 	
<ul style="list-style-type: none"> Customer education to minimize risk of theft of product included in retailer training (score 1) 	
<ul style="list-style-type: none"> Valid means of unique identification of product (e.g. source tagging) (score 3) 	
<ul style="list-style-type: none"> Valid means of tracking ownership of product through life cycle (e.g. chipping) (score 3) 	
<ul style="list-style-type: none"> Technology designed to delay or defeat attempted theft of item (e.g. packaging) (score 3) 	
<ul style="list-style-type: none"> Technology to negate the financial value of the item if stolen (e.g. PIN) (score 3) 	
Cost of inclusion of security features has been: <ul style="list-style-type: none"> 10% or more of production cost (score 2) 	

<ul style="list-style-type: none"> • Up to 10% of the production cost (score 1) • Zero cost (score 0)
<p>Cost of security feature included in product has been:</p> <ul style="list-style-type: none"> • Absorbed by manufacturer (score 2) • Shared with retailer (score 1) • Shared with customer (score 0) • Passed on to customer (subtract 1)
<p>Product has been field-tested for theft*</p> <ul style="list-style-type: none"> • Yes (score 1) • No (score 0)
<p>TOTAL SCORE</p>

*Field-testing consist of market research into the product's perceived attractiveness to thieves.

Although the authors considered the proposed mechanism to be an excellent basis for developing a crime risk assessment tool, the choice between three ways of progressing needed to be made before proceeding.

- 1) Should we accept the original mechanism as it was proposed in 2002 with little or no revision?
- 2) Should we accept its principles of risk versus protection, but reject the proposed means of assessing these?
- 3) Should we reject both the proposed model and its principles and adopt a different approach to crime proofing products?

The first stage towards making this decision involved a consultation exercise with key stakeholders regarding the principles of the model as well as the specific content of each checklist. Using existing fora such as the Home Office Designing Out Crime Working Group as well as the CEN Crime Proofing Expert Group as a starting point, stakeholders were selected using a snowball process. 30 individuals were invited to take part in the consultation exercise, of whom 12 agreed to participate. The 12 individuals who took part were either interviewed face-to-face (see interview schedule at appendix 1), or if they preferred, the interview schedule was used as a formal template for them to complete as an electronic questionnaire.

Table 3 below displays the name, organisation and rationale for selection for the 12 respondents who took part in the consultation process.

Table 3: Respondents

Name	Organisation	Rationale for selection
Dr. Lorraine Gamman	Design Against Crime Initiative, Central Saint Martins College of Art and Design	Expert in Design Against Crime
Caroline Davey and Andrew Wootton	Salford University	Work on Design Council Design Against Crime projects such as “Think Thief – A Designer’s Guide to Designing out Crime” and “Evidence – Design Against Crime Case Studies”
Jane Milne	Association of British Insurers	Member of Home Office Designing out Crime Working Group
Nina Shuttlewood	Home Office	Member of Home Office Designing out Crime Working Group
Offer Stern–Weiner	Home Office – Street Crime Action Team	Snowball (through Nina Shuttlewood)
James Winter	BT Redcare	Member of CEN Crime Proofing Expert Group
Paul Ekblom	Home Office	Expert in Design Against Crime
James Brown	Selectamark	Member of CEN Crime Proofing Expert Group
Tim Pascoe	PRCI	Chair of DOCA and Chair of CEN Standard on designing out crime in residential housing (CEN TC325 ENV: 14383–3).
Anon	DTI	Member of CEN Crime Proofing Expert Group
Anon	Anon	Member of CEN Crime Proofing Expert Group
Anon	Anon	Member of Home Office Designing out Crime

Working Group		
Ebrima I Chongan	Home Office	Snowball (through Nina Shuttlewood)

In general, respondents felt that a crime risk assessment mechanism for measuring the vulnerability of electronic products to theft was an idea worth developing. However, concerns were expressed regarding the lack of flexibility of a quantitative mechanism (in a rapidly changing field such as consumer electronics), the need to ensure that the mechanism could be completed using a prototype (re-designing a product post development would be prohibitively expensive for manufacturers), the subjectivity of certain questions and the issues of increased bureaucracy and workload.

1.11 If we keep the Checklists:

Respondents made key suggestions regarding the content and design of the mechanism, should we decide to pursue this option. The specific comments made by respondents are presented in red font in the final column of tables 4 and 5 below. Proposed changes to the vulnerability checklist relate largely to issues of clarity and subjectivity. Proposed changes to the security checklist are more specific, with many respondents suggesting that this checklist would be very difficult to complete without detailed product information.

Table 4: Specific Comments on Checklist One – Assessing Vulnerability

Items	Item Score	Proposed Changes
CONCEALABLE <i>Check one</i> On person (score 2) In bag (score 1)		1. Visibility to offenders.
REMOVABLE <i>Check one</i> Can be carried in one hand (scores 2) Can be carried with two hands (score 1)		1. Add something which identifies whether product is wireless/not fixed to floor/wall.
AVAILABLE <i>Score 1 for each</i> – Used outside the home		1. “Minimal search time for thief to

	<ul style="list-style-type: none"> - Commonly left in parked cars - Marketed to young males - Minimal search time for thief to locate product 	<p>locate” needs to be more specific.</p> <p>2. Change “marketed to young males” to “product has a games/camera function”.</p>
VALUABLE	<p><i>Score 1 for each</i></p> <ul style="list-style-type: none"> - Costs at least one day’s wages - Provides access to phone services - Provides access to the internet - Provides access to credit 	<ol style="list-style-type: none"> 1. “Costs at least one day’s wages” is too low. 2. “Costs at least one day’s wages” needs to be more specific i.e. >£200 or >average daily income in 2005. 3. Add “provides access to user’s identity”. 4. Add “product has a distinctive design or colour” or “product can easily be identified from a distance”. 5. Clarify “access to credit”.
ENJOYABLE	<p><i>Score 1 for each</i></p> <ul style="list-style-type: none"> - Entertaining - Addictive - Fashionable - Luxury item - Status item - Aggressive advertising emphasising these themes 	<ol style="list-style-type: none"> 1. What is the difference between fashion and status?
DISPOSABLE	<p><i>Score 1 for each</i></p> <ul style="list-style-type: none"> - Widely in demand - Value easily assessed - Street price less than 50% of one day’s wages 	<ol style="list-style-type: none"> 1. Add something which allows you to identify whether the product is usable once in the

	<p>hands of a misuser.</p> <p>2. Add “product is not easily attributed to owner i.e. mass produced/ no batch number”.</p> <p>3. Need to identify demand for second hand products – people don’t want some products second hand.</p>
TOTAL SCORE	

Table 5: Specific Comments on Checklist Two – Assessing Security

Security Feature	Score	Proposed Changes
<ul style="list-style-type: none"> Customer education designed into marketing (e.g. security instructions included in package) (score 1) 		
<p><i>Replacement guarantee to consumer if product stolen. Check one:</i></p> <ul style="list-style-type: none"> Within 90 days (score 1) Within 1 year (score 2) Life of product (score 3) 		<p>1. This should be removed as it could be counter-productive – a) people may be complacent if they have a replacement guarantee, b) this may encourage false claims of theft.</p>
<ul style="list-style-type: none"> Tracking technology such as RFIDs to make recovery of item easier if stolen, particularly during journey from manufacturer to consumer (score 3) 		
<ul style="list-style-type: none"> Customer education to minimize risk of theft of product included in retailer training (score 1) 		<p>1. Add something on “ease of use of security features.”</p>

	2. Do the security features rely upon user to activate?
<ul style="list-style-type: none"> Valid means of unique identification of product (e.g. source tagging) (score 3) 	<ol style="list-style-type: none"> Add "product listed on 3rd party register". "You do this with/without embedding in a registration system".
<ul style="list-style-type: none"> Valid means of tracking ownership of product through life cycle (e.g. chipping) (score 3) 	<ol style="list-style-type: none"> Add "tracking location". Tagging and chipping have virtually the same outcome so manufacturers would be unlikely to do both.
<ul style="list-style-type: none"> Technology designed to delay or defeat attempted theft of item (e.g. packaging) (score 3) 	
<ul style="list-style-type: none"> Technology to negate the financial value of the item if stolen (e.g. PIN) (score 3) 	1. Add something on difficulty of over-riding security
<p>Cost of inclusion of security features has been:</p> <ul style="list-style-type: none"> 10% or more of production cost (score 2) Up to 10% of the production cost (score 1) Zero cost (score 0) 	<ol style="list-style-type: none"> Suggested that this information would not be easily available Does higher costs on security always equate to a more secure product?
<p>Cost of security feature included in product has been:</p> <ul style="list-style-type: none"> Absorbed by manufacturer (score 2) 	1. Does it matter who absorbs the cost? Surely a

<ul style="list-style-type: none"> • Shared with retailer (score 1) • Shared with customer (score 0) • Passed on to customer (subtract 1) 	<p>cost passed onto the customer would only affect sales as opposed to security.</p>
<p>Product has been field-tested for theft*</p> <ul style="list-style-type: none"> • Yes (score 1) • No (score 0) 	<ol style="list-style-type: none"> 1. Field-testing is pointless as this has to be pre-development. 2. If this is designed for post-product use, should products be attack-tested rather than just perceived attractiveness?
<p>TOTAL SCORE</p>	

*Field-testing consist of market research into the product's perceived attractiveness to thieves.

1. 12 Do we Want to Keep the Two Checklists?

In addition to content, participants also commented upon the design of the mechanism and whether the existing tool was appropriate for the task of measuring the risk of theft of electronic products. In general, participants took the view that the concept of risk versus protection should be pursued, but that the design of the existing mechanism was inappropriate for the electronics industry. Concern was raised regarding the lack of flexibility of a quantitative mechanism and whether it would adequately reflect the life cycle of electronic products from innovation through to saturation or grow and evolve as offenders' *modus operandi* changed. Alternative options suggested by participants included:

1. One checklist which includes a set of security standards which all electronic products must comply with;

2. Similarly, adopting a proven crime reduction intervention (such as Chipping of Goods) and requiring that all electronic products above a certain value adopt this approach;
3. Qualitative guidance (similar to that issued to developers and police for crime reduction within the built environment) which manufacturers can use in developing products;
4. An Advisory Panel of experts who adopt an iterative process of not only designing out crime within products and systems, but also ensuring that the product/system is user-friendly. This process bears similarities to the problem-oriented approach (discussed below) and would involve research, conception, development and evaluation (iteration one), followed by a proposed intervention, followed by iteration 2, followed by a proposed intervention, followed by iteration three (and so on). This process has been tested at Central Saint Martins College of Art and Design on two projects – Stop Thief and Karrysafe;
5. A problem oriented approach based on Ekblom’s 5Is model which, rather than awarding a quantitative score, guides key agencies through the process of identifying and targeting a crime problem. Ekblom (2005) applied the 5Is model to the design process and highlights the steps which would need to be taken:
 - Intelligence – The collection and analysis of information on the crime problem and its perpetrators, causes and consequences. Applying this to the objectives of Marc would involve collecting data on which exact products (including model and make) are stolen, and the details of offenders’ *modus operandi*. Although the collection of intelligence is crucial to the success of crime reduction interventions, the difficulty of building this into the Marc model is that the product/system would have to be on the market (leaving interventions to alter the design extremely expensive).

- Intervention – Applying generic principles through practical methods. In relation to Marc, this includes the measures included on the Security checklist.
- Implementation – Making the intervention happen on the ground.
- Involvement – Mobilising agencies to act as responsible crime preventers and implement the intervention.
- Impact – Evaluating the success of the intervention as a crime reduction measure. This stage of the process would be crucial to the Marc model and would ensure that the interventions remained effective in light of changing *MOs* and product demand.

The final stage of developing the draft mechanism involved presenting the proposed model as well as the consultation findings to the Marc Crime Proofing Steering Group (which included both internal Marc partners as well as external partners) who were asked to comment on the original model and to make a decision regarding the options for progressing. Before making any decisions, Steering Group members were asked to apply the draft mechanism to two electronic products – the Apple iPod (20GB) and a FujiFilm Finepix A607 digital camera. Participants were given the product and their accompanying instructions booklets as well as additional information on the cost, weight and retailer from which the product was purchased. Participants were asked to complete the draft mechanism on their own and record their scores (presented below). The exercise was designed to test ease of use as well as inter-rater reliability.

Table 6: Participants' Scores for Apple iPod

Vulnerability (min 0, max 21)	Security (min 0, max 25)
14	0
16	0
18	0
16	3
17	0
11	0

16	0
17	3

Table 7: Participants' Scores for FujiFilm Digital Camera

Vulnerability (min 0, max 21)	Security (min 0, max 25)
14	1
8	0
18	0
14	0
19	0
8	0
7	0
14	2

Partners were asked to present the scores which they had awarded to each product and to discuss how they arrived at that score. The issues raised by partners are summarised below.

- **Inter-Rater Reliability** – The scores awarded to each product differed greatly, with some statement/questions revealing contrasting answers amongst participants. For example, 'Commonly left in car parks' produced several different answers with participants unable to agree what constituted common and to whom.
- **Whose Role are we assuming?** – Participants were assuming different roles whilst answering the questions (these included user, misuser and manufacturer), and depending upon the role assumed, questions were resulting in very different answers. One example of this included the category 'Concealable'. Some participants interpreted this as concealable by the thief once the product had been stolen, others interpreted it as relating to how concealed the product was by the legitimate user
- **Lack of Clarity** – Participants felt that certain statements/questions remained unclear. Two examples of this

include: 'Minimal search time for thief to locate product' and 'costs at least one day's wages'.

- **Subjectivity** – Participants felt that the certain categories, in particular 'enjoyable' were subjective and open to misinterpretation.
- **Products as Part of a System** – Participants expressed concerns regarding the category 'Removable' and highlighted that many electronic products 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.
- **Lack of Information** – Participants expressed concern regarding manufacturers' willingness to share information on the cost of security. There was also concern regarding questions relating to the street price of products which participants felt unable to answer accurately without further information.
- **Irrelevant Measures** – It was felt that the cost of the security features built into the product was largely irrelevant and although it may affect the product's sales figures, it would not affect the security levels themselves. Similarly, it was felt that the cost of security should not be used as an indicator for the level or effectiveness of that security.
- **Unintended Consequences** – Participants suggested that the category 'Replacement Guarantee' should be removed due to the likelihood that it may encourage complacency as well as fraudulent insurance claims.

In general, participants concluded that the exercise was useful for revealing a) the variation between participants' scores b) the juxtaposition of high risk and low security scores, particularly for the iPod and c) the need to capture both information relating to a product's vulnerability and inherent security. In light of this, a decision was made to retain the principles contained within the draft mechanism – that risk should be commensurate with protection, but to develop a different framework for measurement. The remainder of this report focuses upon the production of an alternative method for measuring the principles of risk and protection, before presenting recommendations for implementation of the mechanism.

2. METHODOLOGY – DEVELOPING, REFINING AND TESTING THE CRIME RISK ASSESSMENT MECHANISM

To recapitulate, consultations with key stakeholders (based within the UK) as well as members of the Marc Crime Proofing Steering Group revealed that, in general, participants felt that the final Crime Risk Assessment Mechanism must:

1. Reflect the need for risk/vulnerability and protection/security to be commensurate;
2. Reflect the language of those whose task it would be to apply the mechanism, rather than imposing the language of criminologists;
3. Reflect the language of stakeholders from a variety of European states;
4. Be developed using a bottom-up approach, rather than imposing a mechanism upon key stakeholders.

2.1 Methodological Steps

As a means of achieving the objectives of this work package and the task set by members of the Marc Crime Proofing Steering Group, the following methodological steps were implemented:

Step 1: Design Questionnaire

The questionnaire had to reflect the need to collect stakeholders' opinions – in their words, regarding the vulnerability and security of a selection of electronic products. As a means of maximising the likelihood that participants would take part, the questionnaire included a minimal number of open-ended questions, with the main bulk of the questionnaire asking closed-ended questions which offered tick-box options for responses.

Step 2: Selection of and Production of Descriptive Reports for a Set of Electronic Products

The second step involved the collection of data relating to the price, dimensions (width, height and depth), weight, colour, specifications, links to services and any additional built-in security features for three models of the five following portable electronic products: MP3 players, Personal Digital Assistants (PDAs), Digital Cameras, Mobile Telephones and Laptop computers.

Step 3: Selection of a Panel of Key Stakeholders

The next step involved the selection of a panel of key stakeholders willing to take part in the project who represented a mix of representatives of manufacturers, representatives of consumers, representatives from the insurance industry and representatives of law enforcement. The selection of stakeholders also had to include a balance of original and accession European member states.

Step 4: Dissemination of the Questionnaire

The fourth step involved disseminating the questionnaire (in electronic format) to the stakeholders who agreed to take part. Language barriers also had to be addressed.

Step 5: Collection and Analysis of Data

The final step involved the collection of completed questionnaires and the analysis of findings.

Each of the above steps are explained in more detail in the ensuing paragraphs.

2.2 Step 1: Design the Questionnaire

A decision was made at the onset of this section of the project, that due to the need to consult with stakeholders from a mix of European states, and the language constraints of the researchers involved, the most appropriate method for collecting information would be through questionnaires, distributed electronically and translated into the chosen language of participants. Face-to-face interviews would have

been prohibitively expensive and researchers would have faced language difficulties. Alternatively, telephone interviews would have been difficult given the language constraints of the researchers and respondents involved.

The questionnaire was designed to collect information on both a) participants' views of the risk level of 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 additional in-built security features, and asking them to rate each product as low, medium or 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 found at appendix 2.

2.3 Step 2: 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 by the Marc Crime Proofing Steering Group as the portable electronic products most vulnerable to theft. 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.

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:

1. 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 to be 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.

2. Fixing a specific date on which to identify each product's price and specifications;
3. Searching three online stores to find the price of each make/model;
4. 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.

2.4 Step 3: 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 (JDI and UCSC) were given a list of countries from which to select their participants. JDI was asked to select three countries from the following list of original European member states:

1. UK
2. Ireland
3. Sweden
4. Belgium
5. Portugal
6. Denmark
7. Greece

And two countries from the following list of accession European member states:

1. Cyprus
2. Czech Republic
3. Hungary
4. Latvia
5. Malta

Similarly, UCSC was asked to select three countries from the following list of original European member states:

1. Austria
2. Finland
3. France
4. Germany
5. Italy
6. Luxembourg
7. Netherlands
8. Spain

And two countries from the following list of accession states:

1. Lithuania
2. Poland
3. Slovenia
4. Slovakia
5. Estonia

This gave a total number of six original European member states 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 project:

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 within that country who were willing to take part. An example of the steps taken to select stakeholders is outlined below⁴:

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. 22 participants returned completed questionnaires within the required deadline.

2.5 Step 4: 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

⁴ This example is based upon the JDI research team's experience and was replicated for the UCSC team starting with Italy.

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.

2.6 Step 5: Collection and Analysis of Data

Once the final questionnaires had been collated, responses were inputted into SPSS for analysis. The analysis detailed in the results section below involves the following 20 steps:

- Analysis of the proportion of respondents who awarded a rating of low, medium or high for perceived vulnerability of each of the 15 products;
- Analysis of the proportion of respondents who awarded a rating of low, medium or high for perceived security of each of the 15 products;

- Analysis of the correlation between vulnerability and security – do products which are perceived to be the most vulnerable have the highest levels of security?
- The vulnerability scores awarded to each product by all respondents were aggregated to give a total vulnerability score for each of the 15 products. A rating of low was awarded 1 point, medium 2 points and high 3. The points awarded to each product by all 22 respondents were totalled to give a score of between 22 (22 x 1) and 66 (22 x 3);
- The security scores awarded to each product by all respondents were aggregated to give a total security score for each of the 15 products. A rating of low was awarded 1 point, medium 2 points and high 3. The points awarded to each product by all 22 respondents were totalled to give a score of between 22 (22 x 1) and 66 (22 x 3);
- The mean vulnerability score was calculated by totalling the vulnerability scores for the 15 products and dividing that total by 15;
- The mean security score was calculated by totalling the security scores for each of the 15 products and dividing that total by 15;
- Products were ranked by vulnerability and security scores to identify the most and least vulnerable and the most and least secure;
- The mean vulnerability and security scores were calculated for each of the five product types i.e. MP3 player, digital camera, laptop, mobile phone and personal digital assistant to assess which product types were considered to be the most vulnerable and which were perceived to be the most secure;
- Perceptions of vulnerability and security were analysed by sector group i.e. law enforcement, insurance, manufacturers, ESO and

consumer associations, to establish whether there was any variation of assessments;

- In the original questionnaire respondents were asked to rate each product's vulnerability to theft and to give three reasons for that rating. For each of the products which scored above the mean value in terms of vulnerability scores, a detailed assessment of the qualitative responses was conducted. This involved analysing the responses for each product and creating common factors from those responses. For example, 'costly', 'pricey', 'expensive' and 'costs a lot' would be clustered under the heading 'expensive';
- To ensure that the procedure of allocating responses to vulnerability factors was valid and repeatable, the authors conducted the categorisation process separately before agreeing on acceptable vulnerability factors;
- Once categories were agreed, frequencies were allocated to each vulnerability factor/category. This process was again conducted separately by two of the authors to maximise inter-rater reliability;
- Because respondents were asked to give a maximum of three reasons for their rating, where respondents gave more than three responses, the first three answers only were utilised for this section of the analysis. Where participants gave responses which did not address the question i.e. it is vulnerable because: "The UK has a high rate of mobile phone theft", these responses were again excluded from this section of the analysis;
- This process was repeated for each of the 15 electronic products to produce 15 vulnerability tables which included a vulnerability factor and the frequency with which that factor was mentioned;
- In the original questionnaire respondents were asked to rate each product's security level and to give three reasons for that

rating. For each of the products which scored above the mean value in terms of security scores, a detailed assessment of the qualitative responses was conducted. This involved analysing the responses for each product and creating common factors from those responses. For example, 'cable lock', 'space for a cable lock', 'ability to lock computer to surface', would be clustered under the heading 'cable lock';

- To ensure that the procedure of allocating responses to security factors was valid and repeatable, two of the authors conducted the categorisation process separately before agreeing upon acceptable security factors;
- Once categories were agreed, frequencies were allocated to each security factor/category. This process was again conducted separately by two of the authors to maximise inter-rater reliability;
- As with the vulnerability factors, responses which were considered irrelevant were excluded, as were respondents' fourth, fifth etc. reasons for their rating (they were asked to provide a maximum of three reasons);
- This process was repeated for each of the 15 products to produce 15 security tables;
- The 15 vulnerability tables were aggregated to give one final table containing all vulnerability measures and the frequencies which those measures had been mentioned for all 15 products. A weighting score was then produced by dividing the frequency score by the maximum potential frequency with which that factor could have been mentioned. For example, if 'expensive' was mentioned 22 times, this figure was divided by 330 (22 multiplied by 15) and multiplied by 100;
- The 15 security tables were aggregated to give one final table containing all security measures and the frequencies which

those measures had been given for all 15 products. A weighting score was then produced by dividing the frequency score by the maximum potential frequency with which that factor could have been mentioned. For example, if 'password' was mentioned 17 times, this figure was divided by 330 (22 multiplied by 15) and multiplied by 100.

3. RESULTS

3.1 Participants

As was discussed within the methodology, 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 8 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 8: Geographical Spread of Interview Participants

Country	Frequency	Percentage
UK	4	18%
Italy	4	18%
Czech Republic	3	14%
Hungary	2	9%
Poland	2	9%
Lithuania	2	9%
Sweden	2	9%
Spain	1	5%

Netherlands	1	5%
Total	21	100%

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 9 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 9: Sector which Participants Represented

Sector	Frequency	Percentage
Insurance	7	32%
Law Enforcement	6	27%
Consumers Associations	6	27%
Manufacturers of Electronic Products	2	9%
ESOs	1	5%
Total	22	100%

The questionnaire which participants were asked to complete focused upon the two principles, vulnerability and security. For 15 electronic products (three models of five products), participants were asked to rate the product in terms of its vulnerability and security and then to give three qualitative reasons for that rating. The following section looks at the ratings awarded to each of the 15 products.

3.2 Vulnerability versus Security – 15 Individual Products:

Of the three Mp3 players – the Apple iPod 20 GB, the Apple iPod Mini and the iAudio M3, the Apple iPod 20GB was considered the most vulnerable to theft. As tables 10, 11 and 12 highlight, 68% of respondents considered the Apple iPod 20GB to be highly vulnerable to theft, this is compared to 59% of respondents who felt that the iAudio M3 was highly vulnerable to theft and 55% respondents who felt that the iPod Mini was highly vulnerable to theft. Of the three products, the iAudio M3 was considered the least secure, with 86% of respondents perceiving it to have low security compared to 68% of respondents who felt that the Apple iPod 20 GB and the Apple iPod Mini had low security.

3.3 Mp3 Players

Table 10: Apple iPod 20GB

	Vulnerability	Security
Low	0	68% (15)
Medium	32% (7)	32% (7)
High	68% (15)	0

Table 11: Apple iPod Mini

	Vulnerability	Security
Low	14% (3)	68% (15)
Medium	32% (7)	32% (7)
High	55% (12)	0

Table 12: iAudio M3

	Vulnerability	Security
Low	9% (2)	86% (19)
Medium	32% (7)	5% (1)
High	59% (13)	9% (2)

3.4 Personal Digital Assistants

Of the three Personal Digital Assistants, the Palm One Tungsten T5 was considered to be the most vulnerable with 64% of respondents rating its vulnerability to theft as high. This is compared to 59% of respondents rating the HP iPAQ rx3715 as having high vulnerability to theft and only 27% of respondents rating the Palm One Zire 72 as being highly vulnerable to theft.

In terms of security, all three products were considered to have low levels of security but the HP iPAQ rx3715 was considered the least secure with 91% of respondents rating its security as low.

Table 13: Palm One Zire 72

	Vulnerability	Security
Low	41% (9)	86% (19)
Medium	32% (7)	14% (3)
High	27% (6)	0

Table 14: Palm One Tungsten T5

	Vulnerability	Security
Low	9% (2)	86% (19)
Medium	23% (5)	9% (2)
High	64% (14)	0

Table 15: HP iPAQ rx3715

	Vulnerability	Security
Low	9% (2)	91% (20)
Medium	32% (7)	9% (2)
High	59% (13)	0

3.5 Digital Cameras

The tables below reveal how the FujiFilm Finepix S7000 was considered by respondents to be the most vulnerable of the three

digital cameras to theft. 86% of respondents rated its vulnerability as high compared to 59% for the Olympus Camedia C-5060 and 41% for the Olympus Camedia C-770. All three cameras were considered to have low security levels, but the Olympus Camedia C-770 was rated as having the lowest levels of security. 91% of respondents rated its security as low.

Table 16: Olympus Camedia C-770 Ultra

	Vulnerability	Security
Low	5% (1)	91% (20)
Medium	55% (12)	9% (2)
High	41% (9)	0

Table 17: Olympus Camedia C-5060

	Vulnerability	Security
Low	14% (3)	82% (18)
Medium	23% (5)	14% (3)
High	59% (13)	5% (1)

Table 18: FujiFilm Finepix S7000

	Vulnerability	Security
Low	0	82% (18)
Medium	14% (3)	14% (3)
High	86% (19)	5% (1)

3.6 Mobile Phones

Of the three mobile phones included in the study, the Nokia 6230i was considered the most vulnerable with 73% of respondents rating its vulnerability to theft as high. Both the Nokia 6230i and the Sony Ericsson K700i were rated by 64% of the respondents as having low levels of security.

Table 19: Motorola V600

	Vulnerability	Security
Low	9% (2)	32% (7)
Medium	27% (6)	46% (10)
High	64% (14)	23% (5)

Table 20: Nokia 6230i

	Vulnerability	Security
Low	5% (1)	64% (14)
Medium	23% (5)	32% (7)
High	73% (16)	5% (1)

Table 21: Sony Ericsson K700i

	Vulnerability	Security
Low	0	64% (14)
Medium	36% (8)	32% (7)
High	64% (14)	5% (1)

3.7 Laptop Computers

Of the three laptop computers included in the study, the Sony Vaio VGN B1XP was considered to be the most vulnerable with 64% of respondents rating its vulnerability to theft as high. The Apple Powerbook 15 inch was considered to be the least secure of the three products with 77% of respondents rating its security levels of low.

Table 22: Toshiba Satellite M30X 159

	Vulnerability	Security
Low	18% (4)	14% (3)
Medium	41% (9)	46% (10)
High	41% (9)	36% (8)

Table 23: Apple Powerbook 15 inch

	Vulnerability	Security
Low	14% (3)	77% (17)
Medium	32% (7)	14% (3)
High	55% (12)	9% (2)

Table 24: Sony Vaio VGN B1XP

	Vulnerability	Security
Low	0	36% (8)
Medium	36% (8)	50% (11)
High	64% (14)	14% (3)

3.8 Correlation between Vulnerability and Security

When these individual judgements regarding each product's vulnerability and security are correlated, the results suggest that there is a significant negative association between security and vulnerability ($p = 0.016$). This suggests that in general, the majority of responses suggested that products with high vulnerability also had low security. This may reflect a flaw in the approach taken. In principle the two scores are meant to be independent. However, if people when considering vulnerability have in mind the level of security, a negative association would inevitably appear. There is nothing in the content of the questions to invite contamination of this kind, but the possibility should be borne in mind.

3.9 Aggregate Scores – Vulnerability versus Security

The table below displays the relationship between vulnerability and security when all responses are aggregated. For example, for each product the score for vulnerability (1 for low, 2 for medium, 3 for high) is totalled for all 22 responses. The maximum level of vulnerability would therefore be 66 (3×22) and the maximum level of security would be 66 (3×22). When scores are aggregated, unlike the analysis of individual responses, the correlation between vulnerability and security

is not statistically significant ($p = 0.855$) suggesting that there is little consensus across individuals' responses.

Table 25: Aggregate Vulnerability and Security Scores for Each Product

Product	Aggregate Vulnerability Score	Aggregate Security Score
Apple iPod 20GB	59	29
Apple iPod Mini	53	29
iAudio M3	55	27
Palm One Zire 72	41	25
Palm One Tungsten T5	54	23
HP iPAQ rx3715	55	24
Olympus Camedia C-770 Ultra	52	24
Olympus Camedia C-5060	52	27
FujiFilm Finepix S7000	63	27
Motorola V600	56	42
Nokia 6230i	59	31
Sony Ericsson K700i	58	31
Toshiba Satellite M30X 159	49	47
Apple Powerbook 15 inch	53	29
Sony Vaio VGN B1XP	58	39
<i>Mean</i>	<i>54.5</i>	<i>30.3</i>

Table 25 displays each of the 15 products' aggregate vulnerability and security scores. The results reveal that the vulnerability scores (high being the most vulnerable) awarded to the 15 products are much higher than the security scores. The mean vulnerability score for the 15 products is 54.5. Dividing this score by 22 (the number of respondents) suggests that the average vulnerability score awarded to electronic products is 2.5, the maximum vulnerability score being 3 (high). The mean security score for the 15 products is 30.3. Dividing this score by 22 (the number of respondents) suggests that the

average security score awarded to this sample of products was 1.4 (3 being the highest security).

Table 26 reveals that the product considered the most vulnerable to theft is 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 computer and the Olympus Camedia C-5060 and C-770 digital cameras.

Table 26: Products Ranked by Vulnerability (high scores being products perceived to be most vulnerable)

Product	Aggregate Vulnerability Score	Aggregate Security Score
FujiFilm Finepix S7000	63	27
Apple iPod 20GB	59	29
Nokia 6230i	59	31
Sony Ericsson K700i	58	31
Sony Vaio VGN B1XP	58	39
Motorola V600	56	42
HP iPAQ rx3715	55	24
iAudio M3	55	27
Palm One Tungsten T5	54	23
Apple iPod Mini	53	29
Apple Powerbook 15 inch	53	29
Olympus Camedia C-770 Ultra	52	24
Olympus Camedia C-5060	52	27
Toshiba Satellite M30X 159	49	47
Palm One Zire 72	41	25

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.

Table 27: Products Ranked by Security (with the highest score representing products perceived to be the most secure).

Product	Aggregate Vulnerability Score	Aggregate Security Score
Toshiba Satellite M30X 159	49	47
Motorola V600	56	42
Sony Vaio VGN B1XP	58	39
Nokia 6230i	59	31
Sony Ericsson K700i	58	31
Apple iPod 20GB	59	29
Apple Powerbook 15 inch	53	29
Apple iPod Mini	53	29
FujiFilm Finepix S7000	63	27
iAudio M3	55	27
Olympus Camedia C-5060	52	27
Palm One Zire 72	41	25
HP iPAQ rx3715	55	24
Olympus Camedia C-770 Ultra	52	24
Palm One Tungsten T5	54	23

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

3.10 Product Type

When the 15 products are aggregated by product type i.e. MP3 player, PDA, mobile phone, digital camera and laptop computer, the results reveal that there is very little difference between the scores awarded for perceived vulnerability. The highest score is 57.7 for mobile phones and the lowest score is 50 for PDAs. However, the scores for security show greater variability with the most secure product type being the laptop computer with a score of 38.3 and the least secure product type being the PDA with a perceived security score of 24. This supports some of the earlier comments made by stakeholders that all mobile consumer electronic products are vulnerable, irrespective of variations in specification, price or dimensions and that any accreditation scheme should simply require a set of security standards for each of these products.

Table 28: Product Type and Perceptions of Vulnerability and Security

Product Type (N=3)	Aggregate Vulnerability Score (mean)	Aggregate Security Score (mean)
MP3 Player	55.7	28.3
PDA	50	24
Digital Camera	55.7	26
Mobile Phone	57.7	34.7
Laptop	54.5	38.3

3.11 Sector Type and Perceptions of Vulnerability and Security

Table 29 below displays the difference between responses awarded to the sample of 15 products by sector of respondent. The results reveal that respondents from law enforcement were the most likely sector 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 29: Sector Type and Perceptions of Vulnerability

Sector	Low (% who awarded this rating)	Medium (% who awarded this rating)	High (% who awarded this rating)
Law Enforcement	11	20	69
Insurance	7	32	61
Consumers’ Associations	12	36	52
Manufacturers of Electronic Products	14	50	36
European Standardisation Organisations	0	33	67

Table 30 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 30: Sector Type and Perceptions of Security

Sector	Low (% who awarded this rating)	Medium (% who awarded this rating)	High (% who awarded this rating)
Law Enforcement	62	34	3
Insurance	80	15	5
Consumers’ Associations	62	25	13
Manufacturers of Electronic Products	71	29	0
European Standardisation	67	7	27

Organisations			
---------------	--	--	--

3.12 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 following section of the report attempts to define vulnerability using the language of the respondents who were surveyed. Each of the products scoring above average in terms of aggregate vulnerability (and later security) scores is looked at individually before an attempt is made to summarise what makes a product vulnerable to theft.

3.13 FujiFilm Finepix S7000 – Aggregate Vulnerability Score 63 (out of a possible 66).

This product was considered by the sample of respondents to be the most vulnerable to theft. The reasons give for the rating of high vulnerability are listed in the table below.

Table 31: FujiFilm Finepix S7000 – Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	5
Carried openly	1
Commonly used	2
Desirable	1
Distinctive – can be identified from a distance	1
Expensive	11
Fashionable	0

Good brand name	3
High quality specifications	4
Looks expensive	2
Marketable/Easy to re-sell	3
No association to a specific person	1
Popular	4
Popular amongst young people	0
Small/Light	4

3.14 Apple iPod 20GB – Aggregate Vulnerability Score 59 (out of a possible 66)

The Apple iPod 20GB was considered by the sample of 22 respondents to be the second most vulnerable product scoring 59 out of a possible 66. The table below outlines the reasons given by respondents for the high rating for vulnerability.

Table 32: Apple iPod 20GB – Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	4
Carried openly	1
Commonly used	0
Desirable	1
Distinctive – can be identified from a distance	3
Expensive	8
Fashionable	2
Good brand name	1
High quality specifications	3
Looks expensive	0
Marketable/Easy to re-sell	4
No association to a specific	0

person	
Popular	6
Popular amongst young people	4
Small/Light	13

3. 15 Nokia 6230i Mobile – Aggregate Vulnerability Score 59 (out of a possible 66)

The Nokia 6230i mobile phone was considered by respondents to be the second (joint) most vulnerable product to theft. The reasons given for this high rating are identified in the table below.

Table 33: Nokia 6230i – Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	2
Carried openly	0
Commonly used	3
Desirable	2
Distinctive – can be identified from a distance	0
Expensive	7
Fashionable	2
Good brand name	2
High quality specifications	3
Looks expensive	0
Marketable/Easy to re-sell	2
No association to a specific person	0
Popular	4
Popular amongst young people	2
Small/Light	9

3. 16 Sony Ericsson K700i – Aggregate Vulnerability Score 58 (out of a possible 66)

The Sony Ericsson K700i mobile phone was considered to be the fourth most vulnerable product by the sample of 22 stakeholders scoring 58 out of a possible 66. The reasons given for this high rating are outlined in the table below.

Table 34: Sony Ericsson K700i – Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	3
Carried openly	0
Commonly used	1
Desirable	1
Distinctive – can be identified from a distance	0
Expensive	7
Fashionable	2
Good brand name	0
High quality specifications	6
Looks expensive	0
Marketable/Easy to re-sell	2
No association to a specific person	0
Popular	7
Popular amongst young people	2
Small/Light	9

3.17 Sony Vaio VGN B1XP – Aggregate Vulnerability Score 58 (out of a possible 66)

The Sony Vaio VGN B1XP laptop computer was considered to be the fourth (joint) most vulnerable product from the sample, scoring 58 out

of a possible 66. The reasons given for its high rating are listed in the table below.

Table 35: Sony Vaio VGN B1XP – Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	7
Carried openly	0
Commonly used	1
Desirable	2
Distinctive – can be identified from a distance	0
Expensive	9
Fashionable	0
Good brand name	4
High quality specifications	2
Looks expensive	0
Marketable/Easy to re-sell	2
No association to a specific person	0
Popular	6
Popular amongst young people	0
Small/Light	7

3.18 Motorola V600 – Aggregate Vulnerability Score 56 (out of a possible 66).

The Motorola V600 mobile phone was considered by the sample of 22 respondents to be the sixth most vulnerable electronic product, scoring 56 out of a possible 66. The reasons given for its high rating are detailed in the table below.

Table 36: Motorola V600 – Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	7
Carried openly	0
Commonly used	2
Desirable	1
Distinctive – can be identified from a distance	0
Expensive	5
Fashionable	4
Good brand name	0
High quality specifications	2
Looks expensive	0
Marketable/Easy to re-sell	0
No association to a specific person	0
Popular	3
Popular amongst young people	2
Small/Light	10

3.19 HP iPAQ rx3715 – Aggregate Vulnerability Score 55 (out of 66).

The HP iPAQ rx3715 personal digital assistant was considered by the sample of 22 respondents to be the seventh most vulnerable product, scoring 55 out of a possible 66. The reasons given for this high rating are detailed in the table below.

Table 37: HP iPAQ rx3715 – Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	3
Carried openly	0
Commonly used	1
Desirable	2

Distinctive - can be identified from a distance	1
Expensive	7
Fashionable	0
Good brand name	2
High quality specifications	6
Looks expensive	1
Marketable/Easy to re-sell	1
No association to a specific person	0
Popular	5
Popular amongst young people	0
Small/Light	11

3.20 iAudio M3 - Aggregate Vulnerability Score 55 (out of 66)

The iAudio M3 Mp3 player was judged by the sample of 22 respondents to be the seventh (joint) most vulnerable product, scoring 55 out of a maximum 66. The reasons given for the high rating are detailed in the table below.

Table 38: iAudio M3 - Defining Vulnerability

Explanation for Rating	Frequency
Attractive Design	2
Carried openly	0
Commonly used	0
Desirable	0
Distinctive - can be identified from a distance	0
Expensive	7
Fashionable	1
Good brand name	0
High quality specifications	1

Looks expensive	0
Marketable/Easy to re-sell	2
No association to a specific person	0
Popular	3
Popular amongst young people	1
Small/Light	13

If all responses are aggregated to create a list of ‘vulnerability measures’ against a total frequency, this can be used to create a weighting system for measuring the likely risk of theft. Table 38 below displays each measure against the frequency of responses, followed by the score, which represents the frequency as a proportion of the maximum potential score if all participants had given that answer for all 15 products. The maximum potential number of responses is 330 – 22 respondents multiplied by 15 products.

Table 39: Producing a Scoring System for Vulnerability Factors

Explanation for Rating	Frequency (maximum potential score is 330)⁵	Score (frequency/330 x 100)
Attractive Design	33	10
Carried openly	2	1
Commonly used	10	3
Desirable	10	3
Distinctive – can be identified from a distance	5	2
Expensive	61	19
Fashionable	11	3
Good brand name	12	4
High quality specifications	27	8

⁵ 22 (participants) x 15 (products)

Looks expensive	3	1
Marketable/Easy to re-sell	16	5
No association to a specific person	1	1 ⁶
Popular	38	12
Popular amongst young people	11	3
Small/Light	76	23

Although this will be explored in the final section, a potential option for the final vulnerability scoring system could include providing the option of awarding minus scores for inverse measures. For example a product which is considered distinctive and can be identified from a distance would score 1; a product which is not identifiable from a distance would score -1.

3.21 Defining Security – Stakeholders’ Views

As has been discussed throughout this report, a mechanism to measure the risk of theft of electronic products must take into account both the vulnerability of that product and existing levels of security, ensuring that the two are commensurate. As well as being asked to rank the 15 products in terms of their levels of security, the 22 participants were asked to give three reasons why they had awarded that score. The following section of this report looks at the measures considered by stakeholders to define security. Responses for the five products which scored higher than the mean in terms of their aggregate security scores are analysed in attempt to create a ‘security’ measure.

3.22 Toshiba Satellite M30X 159 – Aggregate Security Score 47 (out of a possible 66)

The Toshiba Satellite M30X 159 was considered by the 22 respondents to be the most secure of the 15 products (even though it only scored

⁶ 0.3 has been rounded up to give a figure of 1.

47 out of 66). The table below outlined the reasons given for this relatively high score.

Table 40: Toshiba Satellite M30X 159 – Defining Security

Explanation for Rating	Frequency
BIOS password	1
Cable-lock	6
Password protection	9
Phone/card locking	0
PIN code	0
Requires installation	1
Serial number	1

Compared to the extensive reasons given by respondents to describe why a product is vulnerable to theft, the definitions of security are limited. One reason for this could be that although this product (and the four others discussed below), scored highly relative to the rest of the sample, the score of 47 out of a possible 66 suggests that it was still not considered to be a secure product.

3.23 Motorola V600 – Aggregate Security Score 42 (out of 66)

The Motorola V600 mobile phone was considered by the sample of 22 stakeholders to be the second most secure product, even though the aggregate score for this product was just 42 out of a possible 66.

Table 41: Motorola V600 – Defining Security

Explanation for Rating	Frequency
BIOS password	0
Cable-lock	0
Password protection	4
Phone/card locking	4
PIN code	1
Requires installation	0

Serial number	0
---------------	---

Again, it should be highlighted that respondents do not appear able to define security in relation to these products, suggesting that the ‘Security’ element of the proposed mechanism may have to be developed following additional research.

3.24 Sony Vaio VGN B1XP – Aggregate Security Score 39 (out of 66)

The Sony Vaio VGN B1XP was considered by the sample of 22 stakeholders to be the third most secure product even though its aggregate security score was only 39 out of a possible 66.

Table 42: Sony Vaio VGN B1XP – Defining Security

Explanation for Rating	Frequency
BIOS password	1
Cable-lock	0
Password protection	9
Phone/card locking	0
PIN code	0
Requires installation	1
Serial number	0

3.25 Nokia 6230i – Aggregate Security Score 31 (out of 66)

The Nokia 6230i mobile phone was considered by the sample of 22 respondents to be the fourth most secure of the 15 products. Even though this product was considered to be the fourth most secure, and scoring above the mean in terms of its security, it still only scored 31 out of a possible 66. Reasons given by the stakeholders for the relatively high score are detailed in the table below.

Table 43: Nokia 6230i – Defining Security

Explanation for Rating	Frequency
BIOS password	0
Cable-lock	0
Password protection	1
Phone/card locking	2
PIN code	0
Requires installation	0
Serial number	0

3.26 Sony Ericsson K700i – Aggregate Security Score 31 (out of 66)

The Sony Ericsson K700i mobile phone was considered to be the (joint) fourth most secure product by the sample of 22 respondents. Even though this product was considered to be relatively secure, it still only scored 31 out of a possible 66. The reasons given by the respondents for its relatively high security score are outlined in the table below.

Table 44: Sony Ericsson K700i – Defining Security

Explanation for Rating	Frequency
BIOS password	0
Cable-lock	0
Password protection	1
Phone/card locking	2
PIN code	1
Requires installation	0
Serial number	0

Although the original intention was create a final crime risk assessment mechanism based upon the responses given by stakeholders (meaning that the risk factors would be defined by those likely to use the tool and written in their language), very few responses were given by stakeholders when they were asked to define security.

The following table makes some attempt to score the security factors given.

Table 45: Producing a Scoring System for Security Factors

Explanation for Rating	Frequency (maximum potential score is 330) ⁷	Score (frequency/330 x 100)
BIOS password	2	1
Cable lock	6	2
Password protection	24	7
Serial number	1	3
Requires installation	2	1
PIN code	2	1
Phone/card locking	8	2

⁷ 22 (participants) x 15 (products)

4. DEFINITION OF THE FINAL CRIME RISK ASSESSMENT MECHANISM

4.1. ASSESSMENT OF RISK – PROGRESS SO FAR

As has been detailed throughout this report, the task of developing a crime risk assessment mechanism to measure the risk of theft of electronic products took as its starting point a model developed by Clarke and Newman (2002) entitled Secured Goods by Design. Consultation with twelve UK stakeholders as well as the Marc Crime Proofing Steering Group addressed the options of whether we should:

- a) Retain the Secured Goods by Design model with little or no revisions,
- b) Accept the principles of that model – that risk should be commensurate with protection, but reject the proposed means of assessing these, or
- c) Reject both the proposed model and its principles and adopt an entirely different approach to crime proofing products.

Alternative options raised by participants included:

- a) Having just one checklist which contained a set of security standards and requiring all electronic products to comply with these standards;
- b) Adopting a proven crime reduction intervention, such as Chipping of Goods, and again requiring all electronic products to implement these measures
- c) Producing qualitative guidance similar to that used within the field of designing out crime within the built environment and developing processes (including the Iterative or 5Is processes detailed in section 1.12) to implement this guidance.

The results of the consultation exercise revealed that, in general participants felt that the principles of the original mechanism should

be retained, but a different framework for measurement should be developed. Participants felt that the final mechanism must:

- a) Reflect the need for risk and protection to be proportionate;
- b) Reflect the language of those whose task it would be to apply the mechanism i.e., manufacturers and designers of electronic goods as opposed to criminologists;
- c) Reflect the language and the views of stakeholders from a variety of European states and d) be developed using a bottom-up approach which is transparent to those implementing it at a future date.

Section three 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 within section three remains fit for purpose in relation to the first audience, but does not achieve the precision necessary for the second. Issues which remain unclear and which need to be addressed before the final crime risk assessment mechanism can be considered for application include:

- a) Whether two checklists can be justified based upon the lack of variability in vulnerability scores awarded by respondents;
- b) Whether the different responses from original and accession states warrant a phased mechanism which differs between countries;
- c) How the clarity of the vulnerability checklist may be enhanced, addressing the weaknesses within the security checklist;
- d) How to engage manufacturers of electronic products (who represented just 9% of the sample);

e) How to overcome the perverse incentives which allow consumers to benefit from the theft of electronic products through an upgraded replacement;

f) How to produce a mechanism which is flexible enough to accommodate the changes in risk and protection, and

g) 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 report will focus upon refining the weaknesses in the presentation and implementation of the mechanism before presenting a series of recommendations, and reconsidering some of the assumptions on which the approach taken was based.

4.2 NATIONAL DIFFERENCES IN MARKET PENETRATION AND EARLY WARNINGS ABOUT CRIME RISK.

Although the theoretical propositions discussed throughout this report should make it clear how certain products and services (as well as places and people) are more vulnerable to crime, and that these vulnerabilities can be predicted and prevented based upon calculations of risk, it should be borne in mind that both risk and protection do not remain static. A product's vulnerability to crime varies according to its position within the product life cycle, as well as offenders' ability to adapt to its inherent security features (Ekblom, 1999; Pease, 2001). Clarke and Felson (1998) suggest that thefts of mass produced consumer goods are affected by their position with the life cycle from innovation - where thefts would remain low due to the small number of homes containing (or people owning) these products, through to growth and mass market stages - where thefts would increase due to the increased demand and availability. Finally, when a product reaches the saturation stage, thefts will decline due to the reduction in legitimate purchase price as well as the falling levels of demand. This theory is supported by Wellsmith and Burrell (2005) who found that the property stolen in domestic burglaries changes according to its

price and ownership levels. As well as varying over time, a product's vulnerability also varies between countries, a point which was highlighted in the analysis of responses from the nine countries included in the consultation exercise. This was highlighted, in particular, by the two products the Apple iPod MP3 player and the Apple Powerbook laptop computer. These two products were rated as highly vulnerable by the majority of respondents however, those from the accession member states, in particular Lithuania and the Czech Republic, rated these products as lower in terms of their vulnerability, stating that the products are not popular and that they would be difficult to re-sell with low marketability. The final mechanism and the system of applying it, must take these differences into account.

At a minimum, the application of the checklist approach as currently envisaged is a consciousness-raising exercise. One way of using this approach is via the communication of crime risks (both absolute for a product type and differentially amongst models within a product type) from countries with high penetration of a stealable (CRAVED) product, to those countries with low penetration. This would at least forewarn of upcoming dangers, and perhaps confer some slight competitive advantage on those models shown to be less vulnerable in early-uptake countries.

4.3 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 39 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.

4.4. THE WEAKNESS OF THE SECURITY CHECKLIST

The recommendation to be reached at the end of this report 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 45 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 developed by Ron Clarke (see below) reflects such a richness of alternative methods that the checklist approach seems formulaic by contrast.

Table 46: Twenty Five Techniques of Situational Crime Prevention

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
<p>1. <i>Target harden</i></p> <ul style="list-style-type: none"> ▪ Steering column locks and ignition immobilisers ▪ Anti-robbery screens ▪ Tamper-proof packaging 	<p>6. <i>Extend guardianship</i></p> <ul style="list-style-type: none"> ▪ Go out in group at night ▪ Leave signs of occupancy ▪ Carry cell phone 	<p>11. <i>Conceal targets</i></p> <ul style="list-style-type: none"> ▪ Off-street parking ▪ Gender-neutral phone directories ▪ Unmarked armoured trucks 	<p>16. <i>Reduce frustrations and stress</i></p> <ul style="list-style-type: none"> ▪ Efficient lines ▪ Polite service ▪ Expanded seating ▪ Soothing music/muted lights 	<p>21. <i>Set rules</i></p> <ul style="list-style-type: none"> ▪ Rental agreements ▪ Harassment codes ▪ Hotel registration
<p>2. <i>Control access to facilities</i></p> <ul style="list-style-type: none"> ▪ Entry phones ▪ Electronic card access 	<p>7. <i>Assist natural surveillance</i></p> <ul style="list-style-type: none"> ▪ Improved street lighting ▪ Defensible 	<p>12. <i>Remove targets</i></p> <ul style="list-style-type: none"> ▪ Removable car radio ▪ Women's 	<p>17. <i>Avoid disputes</i></p> <ul style="list-style-type: none"> ▪ Separate seating for rival soccer fans ▪ Reduce 	<p>22. <i>Post instructions</i></p> <ul style="list-style-type: none"> ▪ "No Parking" ▪ "Private Property"
<p>3. <i>Screen exits</i></p> <ul style="list-style-type: none"> • Ticket needed for exit ▪ Export documents ▪ Electronic merchandise tags 	<p>8. <i>Reduce anonymity</i></p> <ul style="list-style-type: none"> ▪ Taxi driver IDs ▪ "How's my driving?" decals ▪ School uniforms 	<p>13. <i>Identify property</i></p> <ul style="list-style-type: none"> ▪ Property marking ▪ Vehicle licensing and parts marking ▪ Cattle branding 	<p>18. <i>Reduce temptation and arousal</i></p> <ul style="list-style-type: none"> ▪ Controls on violent pornography ▪ Enforce good behaviour on soccer field ▪ Prohibit racial slurs 	<p>23. <i>Alert conscience</i></p> <ul style="list-style-type: none"> ▪ Roadside speed display boards ▪ Signatures for customs declarations ▪ "Shoplifting is stealing"
<p>4. <i>Deflect offenders</i></p> <ul style="list-style-type: none"> ▪ Street closures ▪ Separate 	<p>9. <i>Use place managers</i></p> <ul style="list-style-type: none"> ▪ CCTV for double-deck 	<p>14. <i>Disrupt markets</i></p> <ul style="list-style-type: none"> ▪ Monitor pawn shops 	<p>19. Neutralize peer pressure</p>	<p>24. Assist compliance</p>

bathrooms for women <ul style="list-style-type: none"> Disperse pubs 	buses <ul style="list-style-type: none"> Two clerks for convenience stores Reward vigilance 	<ul style="list-style-type: none"> Controls on classified ads. License street vendors 	<ul style="list-style-type: none"> "Idiots drink and drive" "It's OK to say No" Disperse troublemakers at school 	<ul style="list-style-type: none"> Easy library checkout Public lavatories Litter receptacles
5. <i>Control tools/weapons</i> <ul style="list-style-type: none"> "Smart" guns Restrict spray paint sales to juveniles Toughened beer glasses 	10. <i>Strengthen formal surveillance</i> <ul style="list-style-type: none"> Red light cameras Burglar alarms Security guards 	15. <i>Deny benefits</i> <ul style="list-style-type: none"> Ink merchandise tags Graffiti cleaning Disabling stolen cell phones 	20. <i>Discourage imitation</i> <ul style="list-style-type: none"> Rapid repair of vandalism V-chips in TVs Censor details of modus operandi 	25. Control drugs and alcohol <ul style="list-style-type: none"> Breathalyzers in bars Server intervention programs Alcohol-free events

Sources: Ronald V Clarke and John Eck (2003) *Become a Problem Solving Crime Analyst*. Cullompton, UK: Willan Publishing; Derek B. Cornish and Ronald V. Clarke (2003) "Opportunities, Precipitators and Criminal Decisions. In *Theory for Practice in Situational Crime Prevention, Crime Prevention Studies*, Vol 16. Monsey, NY: Criminal Justice Press. Website: www.popcenter.org

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.

4.5. DO FINDINGS SUGGEST THAT ALL PORTABLE PRODUCTS ARE VULNERABLE TO THEFT AND SHOULD BE TREATED AS EQUAL IN TERMS OF SECURITY?

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 in section three again 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.

In the section below on electronic services, the point is made that the product/service dichotomy is increasingly unhelpful. To illustrate the point, Table 47 illustrates the kind of fraudulent activities which mobile telephony enables. The point is that a crime type which has been traditionally thought of as tangible (mobile phone theft) can be thought of in terms of its facilitation of service-related crime. Mobile phones throughout much of Europe are shifting towards 3G technology. Downloadable viruses and Trojan horses (executable files), malicious code that calls premium numbers or delivers unwanted content, theft and fraudulent subsidy of handsets, denial of service attacks (jamming and flooding), and piracy of ringtones, images, music, games, and videos, might be expected to increase (Lloyd 2003).

Table 47: Types of Mobile Phone Fraud

Subscription fraud and identity theft
International roaming fraud
Agent and reseller fraud
Network and equipment hacking
Internet exchange of fraud information
Insider fraud and collusion
Call selling operations
Premium rate service fraud
Social engineering

Source: Based on Lloyd (2003)

4.6. 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 and services 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. NB because services are weightless, all agreements for electronic services should be rated alongside products.

Alongside the assessment mechanism outlined above, there should be concentrated study of theft characteristics as described in Section 4.4 above, and a process whereby emerging crime problems in countries with high penetration by a new product be communicated to others to anticipate and seek to deflect such trends. The example which springs immediate to mind as topical is the in-car satellite navigation system.

5. IMPLEMENTING THE FINAL CRIME RISK ASSESSMENT MECHANISM

5.1 PROGRESS SO FAR

It is hoped that the preceding text has explained the rationale for developing a crime risk assessment mechanism to assess the risk of theft of electronic products and the methodology for developing this tool. Section 4.1 highlighted the issues which remained unclear and the need to produce a system which would be accepted by both crime prevention practitioners (as a tool for advising about risk) as well as manufacturers, who would require a higher level of precision due to the modifications they would be required to make. Section 4 has discussed the concerns regarding the weaknesses with the two checklists as well as issues relating to the need to consider the changing nature of a product's vulnerability.

The remaining issues are dealt with in Section 5. These include:

1. The presentation and implementation of the mechanism – what will it look like and how will it be used?
2. How to engage manufacturers and pre-empt the understandable concerns.
3. How to change a system which incentivises theft – for manufacturers whose stolen product needs to be replaced with a new purchase and for consumers whose stolen product is often replaced with a new upgrade.
4. How to balance the need to assess the potential vulnerability of a product with the risk of miscalculation.

5.2 PROPOSING A MODEL FOR IMPLEMENTATION

Presentation

It is proposed that the mechanism presented within this report 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. 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.

Food Standards Agency – Healthy Logo

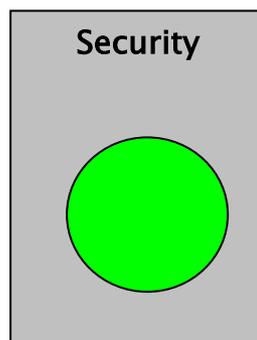
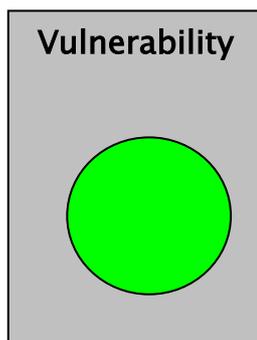


In a similar vein, the UK building industry has an accreditation scheme for buildings which allows them to be labelled as Secured by Design (and therefore marketed using the appropriate logo) where they meet the required standards of security. The Netherlands also have an accreditation scheme – Police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

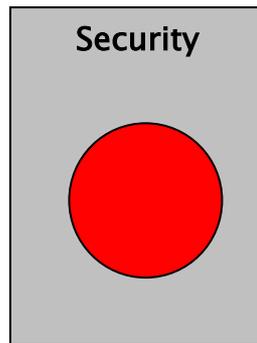
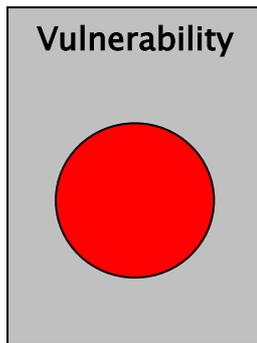
UK ACPO – Secured by Design



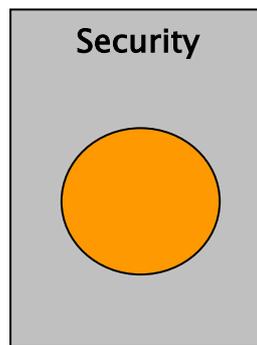
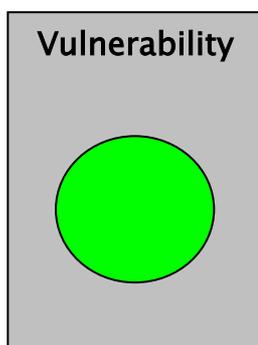
In addition to the proposed voluntary accreditation scheme and associated label, it is recommended that the electronics industry are invited/encouraged to introduce a second labelling system which would enable consumers to easily and immediately identify the levels of vulnerability and security of a 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 EUROPOL 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 (see section 4). Below is an illustration of the proposed system.



This combination of green vulnerability and green security would be an ideal scenario. The product has low vulnerability to theft, but also has high levels of security making it an unlikely target for theft.



This combination of red vulnerability and red security would be a worst case scenario. The product has high vulnerability to theft, but low levels of security making it a likely target for theft.



This combination of green vulnerability and amber security would also be acceptable as the level of security is higher than the estimated level of risk. However, the amber (as opposed to green) security would warn consumers that the product is not as secure as others.

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' label (illustrated above) 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 reason 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'. Equally, 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.

A Word of Caution

The 'traffic light' system discussed above, to some extent, replicates that proposed by the UK Food Standards Agency for foods to contain clear front of pack information on the level of fat, sugar and saturates contained in products. It was proposed that the food traffic lights system be introduced on a voluntary basis and the announcement by five of the UK's biggest food firms in February 2006 that they are to use their own labelling system (which is slightly less transparent) has been portrayed as a failure of the original proposal. Surely this should be seen as a positive. The pressure placed upon the food industry through extensive publicity, consultation and policy changes has

resulted in five major food companies taking a voluntary decision to display clear labels on the front of their products displaying the nutritional content of these foods. That the system is slightly less transparent than that proposed by the UK government is a challenge for the future. If this were replicated within the electronics industry and pressure from the government and consumers resulted in manufacturers adopting a similar system (although not the exact system we are proposing), this would be a huge leap for designing out crime.

Implementation

Although it is proposed that the final mechanism (presented in section four) 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. The first rationale for suggesting multiple incentives lies with the findings from the original consultation exercise with 12 key stakeholders (see section 1.10). Although the majority of respondents felt that the accreditation scheme was worth developing, many highlighted the need for the scheme to be implemented in conjunction with alternative incentives such as educating the public to demand secure products, financial incentives for manufacturers to develop secure products and legislation requiring the crime proofing of products.

The second rationale for recommending that the accreditation scheme should be accompanied by additional incentives 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. The flow chart below highlights the many different incentives which have enabled the Secured by Design scheme to succeed. It is recommended that a similar environment is replicated for electronic products. The details of each incentive are outlined below.

Housing Providers:

The UK Housing Corporation is the Government body which a large proportion of social housing (managed by Registered Social Landlords). Through its Enhanced Quality Assessments and Supplementary Multiplier for Sustainable Housing, the Housing Corporation (and therefore the national Government) is able to offer financial incentives for Registered Social Landlords who choose to build their new housing to the Secured by Design Standard.

In addition to financial incentives, research has been published (Armitage and Everson, 2003) which informs developers of the importance consumers (house buyers) give to security and their willingness to pay for additional security. This research has allowed policy makers to challenge developers who suggest that housing described or marketed as 'secure' would give consumers the impression that the areas had a high crime rate.

Developers also have the potential to use Voluntary European building standards (The European Standard for the Reduction of Crime and Fear of Crime by Urban Planning and Building Design: ENV 1483 parts 1,2 and 3) to differentiate their product (housing) from others. In addition to these building standards, developers who build their properties to the Secured by Design standard are able to market their product as being less likely to experience crime.

In addition to the Secured by Design scheme which allows developers to differentiate their product according to the security it has, developers are encouraged to build secure properties through the availability of enhanced funding, research findings to suggest that

consumers want and will pay for additional security as well and European building standards.

Consumers:

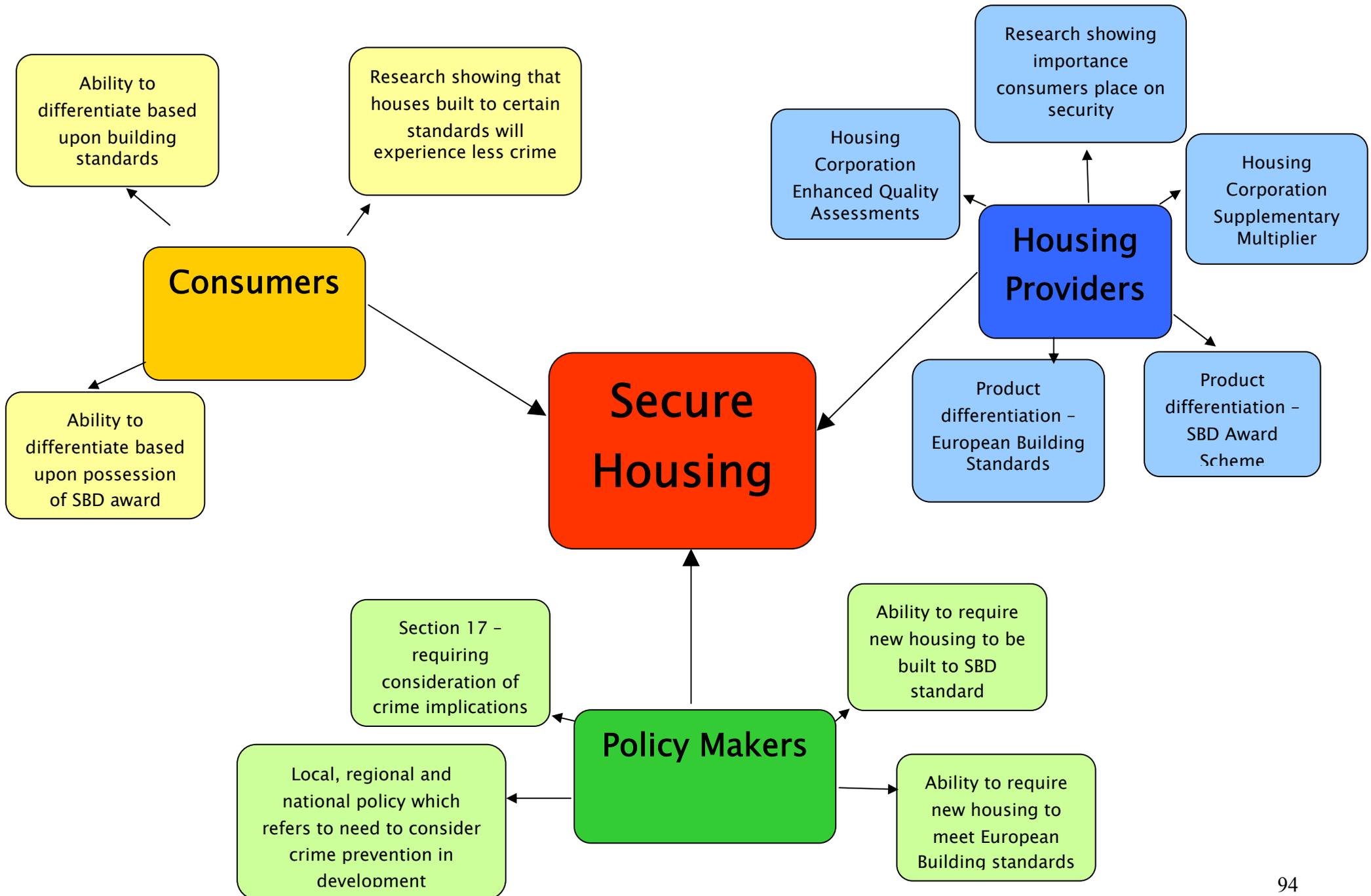
Due to the funding and publication of research into the effectiveness of the Secured by Design scheme (Armitage, 2000), consumers are able to make an informed choice about the importance of this award.

Consumers are also able to differentiate between products (houses) based upon whether they are built to the standard required by the Secured by Design scheme as well as the relevant European Building standards.

Policy Makers:

Local authorities, who make decisions regarding the development of housing within their area are bound by both national legislation (in the form of Section 17 of the Crime and Disorder Act 1998) as well as local, regional and national policy guidance (i.e. Safer Places) which requires them to consider the crime and disorder implications of their development decisions. These legislative requirements increase the pressure placed upon local decision makers to ensure that new housing is built to Secured by Design standards.

Figure One: Example of Incentives to Design out Crime in Residential Housing



5.3 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 displayed in section three of this report showed, of the four sectors consulted, manufacturers of electronic products were the most difficult to engage and only represented 9% of the sample.

As the previous section highlights, 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 were highlighted in section 5.2, these 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.

To avoid losing the momentum built throughout Project Marc, it is recommended that a Working Group is established to facilitate further

consultation on the implementation of the proposed system and to take forward the recommended proposals. It is essential that manufacturers, consumers and policy makers are represented on the group and that, where possible, those who took part in the research are invited to continue their involvement.

5.4 BALANCING PRE-EMPTIVE ASSESSMENTS WITH THE RISK OF MISCALCULATION

One of the key messages to come from the initial consultation process was that the final mechanism must be able to be applied 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.

Overestimating Vulnerability

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 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.

Underestimating Vulnerability

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 the 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.

5.5 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 section of the report concludes with an attempt to pre-empt the main criticisms the Marc proposals may receive. These can be summarised as follows: 1) Consumers do not want their products to be safe as a theft typically results in an upgraded replacement; 2) Offenders who steal a bag or burgle a home will not try to differentiate between secure and unsecure products, they will simply take the bag and keep what is usable and throw away what is not; 3) You cannot ask manufacturers/designers to produce undesirable products.

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 invariably 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. The authors suggest that the EU should commission further research into this issue to establish to what extent these claims are warranted. In addition, further consultation with the insurance sector should take place to attempt to increase the incentives for manufacturers to produce and consumers to buy secure products.

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 US TO DESIGN 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.

6. CRIME PROOFING ELECTRONIC SERVICES

This section draws heavily on the innovative work of Graham Farrell and Jennifer Mailley of Loughborough University, in particular on their work with mobile phone crime. This debt is gratefully acknowledged. Funded by the Engineering and Physical Science Research Council in the UK, the work is still in progress. Further information about publication plans are available from g.farrell@lboro.ac.uk

In 2000, Richard Davis and Ken Pease wrote:

“More and more electronic entertainment equipment is delivered as a service – usually in the form of a signal. Televisions, mobile phone and computers are all means of delivering the service – and the electronic equipment itself is increasingly becoming nothing more than the access point to the service. As such there is every likelihood that the hardware will increasingly be sold cheaply or given away free as a way of attracting customers to the service.

This will not be limited to current signal-based entertainment. Already music downloaded from the Internet and ‘video on demand’ are showing there is little which cannot be provided as a service rather than in ‘hard’ form. If this happens, then the hardware so popular with thieves at present will become unattractive, because the real value will reside in the service.”
(Davis and Pease 2000; 62)

This points up the enormously important point about electronic and some other services, namely that they exist in different states at different points in the process. There is a plausible simile in electricity (and to some degree other utilities) which exists as potential (literally, as voltage) until realised for purposes of heating and lighting. With convergent technologies, many treasured distinctions will cease to be helpful, and that between electronic products and services is probably one of them. The conclusion to this section is that ideally strategies of measuring and protecting electronic entities should not be segregated into services and objects. Whether the CRAVED approach will be helpful in the light of this will be discussed. A thought-out and detailed application of CRAVED thinking to information theft is

presented in Newman and Clarke (2003). This forms a comprehensive background to the conception of product and service theft as intimately linked. Speaking about information, they write:

“[Information] may be at one time be intellectual property, at others a list of names and addresses... at others a series of instructions.... Thus, the idea of information as a product is far more complex than one particular criminogenic consumer product, such as a handgun. ... Unfortunately the complexity and variety of information... makes it especially difficult to suggest specific design changes” (p73)

The difficulty which this creates for the security checklist in the dual checklist approach will be discussed both at the end of this section and at the end of the report. First, a brief account of what is generally understood by crime against electronic services will be offered.

Criminal misuse of electronic services is taken to include the following:

- Theft of electronic services billed as services e.g. mobile phone airtime, cable, satellite and other services.
- Illicit use of electronic services as a facilitator of other crime e.g. Phishing leading to identity theft, banking fraud, use of the internet to commit copyright theft and other Internet and e-commerce related fraud.
- The disruption of electronic service through malice or recklessness.

This restricted scope is necessary in writing this section, but certainly partial. In the early days of computer crime, when legislation did not reflect digital reality, some hacking offences were prosecuted as unlawful abstraction of electricity. In the same way, theft of cable service changes the focus from the entertainment acquired to the means of acquiring it. It may be that the appropriate focus is (as in the above example) the best available ‘pinch point’ for preventive intervention, whatever that may be. It is instructive that prosecutions in relation to Internet child pornography focuses primarily (but far from exclusively) upon the possession of images on the alleged perpetrator’s computer. This may be a problem because of cross-jurisdiction issues, but that simply illustrates that the pinch-point (or

points) for intervention should not be separated according to whether the crime entity is considered as service or product.

Hacking is frequently involved in the commission of theft of electronic services. Moitra and Konda define the terms *attack* and *incident* in this context, where an *attack* is

“a series of intentional steps taken by an attacker to achieve an unauthorised result”

and an incident is:

“a group of related attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites and timing.” (Moitra and Konda 2004; 44).

Attacks include root break-ins, account break-ins, denials of service, corruption of information, access attempts, and disclosure of information, finding distinct patterns of repeat victimisation of the same targets. Over one quarter (27%) of the 6684 computer sites studied by Moitra and Konda experienced at least three attacks, and they suffered an average of twelve attacks. The ten most victimized sites experienced an average of 369 attacks. As for volume crime, events are concentrated on a small proportion of eligible victims, making the prevention task more manageable (Farrell 2005). Repeat victimisation has long been known to exist for many types of crime, and its possibilities for policing and prevention are now more consistently recognised (see Farrell and Pease 1993, Pease 1998, and Farrell 2005 for reviews). Some service providers suffer disproportionately in terms of the number of attacks and the financial value of the resulting theft of services. Such thefts will cluster in time and space.

Subscription fraud occurs when a fraudster uses a false or fake identity to gain access to an electronic service, for example to obtain a subscription to a mobile phone in the U.K. (Bolton and Hand 2002) *Superimposed fraud* occurs where a service is used and charged to the account of an unsuspecting payee who has an account. In this scenario the person does exist and so they receive the bill for the services used by the fraudster. An example of superimposed fraud is where mobile

phone cloning occurs, and where sufficient payment authorisation details are obtained. *International roaming fraud* involves subscription fraud to obtain mobile phones in one country, and using them elsewhere, running up high rate and premium rate roaming call charges in the process. The theft of these services is estimated to run into billions of Euros.

The use of electronic services directly facilitates intellectual property theft. Illegal MP3 and film exchanges are facilitated immensely by the internet even though theft of electronic services itself is not the central issue (see above for a discussion of the service/product nexus).

Identity theft occurs where the details of an individual are stolen or copied for the purpose of using goods and services in their name. Identity theft itself leads to other crimes such as the emptying of bank accounts and obtaining credit cards or other credit in the name of the victim. E-commerce crime has been tackled most comprehensively to date by Newman and Clarke (2003).

Electronic services are frequently misused, as a parallel to criminal damage within 'meat-space'. Bombardment with spam emails is an infamous form, as are spam SMS texts to mobile phones, and short-duration 'dropped calls' to mobile phones (where a recipient who returns the call to a revenue-share number is charged at a high rate). In the UK, the telecommunications regulator Ofcom notes that electronic services can be formally 'misused' and that this can warrant legal action under sections 128-130 of the Communications Act 2003. Currently, "A person misuses a network or service if the effect or likely effect of their behaviour is to cause unnecessary annoyance, - inconvenience or anxiety to another person". (Ofcom 2005; 2). However, the growth of the misuse of 'silent' telephone calls (resulting from telemarketers over-using predictive dialling) means that Ofcom is currently considering revising the legal definition of misuse to cover these types of calls (Ofcom 2005).

According to AEPOC (European Association for the Protection of Encrypted Works and Services), theft or piracy of Pay-TV in Europe takes two common forms:

- Coded Pay-TV signals for digital transmission are stolen by private viewers.
- Local TV stations and cable networks illegally transmit content that does not belong to them.

In both cases, programming is illegally accessed by forging the smart-cards and digital decoders necessary to receive the signals. AEPOC estimates that every year some 1 billion € is spent in the European Union for smart-cards and decoding equipment used to hack into Pay-TV. Datamonitor forecasts 2.3 million digital pay-TV pirate households in Eastern Europe by the end of 2010, with a consequent loss to operators of 700 million euros between 2004 and 2010. The European Commission (COM 2003) asserts that the knowledge-based economies of the 21st century will rely increasingly on pervasive electronic pay services and that piracy will have the same detrimental effects in the knowledge society as white-collar crime and counterfeiting of goods in the 20th century. The report recommends that “legal protection against piracy of electronic pay services will make a central contribution to achieving the Union’s ambitious target of becoming the most dynamic and competitive economy by 2010.” (COM 2003; pg 2)

“Piracy occurs in a number of different ways ranging from pyramid structures, sometimes linked to organised crime, to smaller local phenomena. Thousands are at work across Europe and beyond on the technical means for cracking encrypted conditional-access signals and reaping a profit on their illicit endeavours.

Commercially, piracy is organised along simple lines. It takes very little capital to build a profitable business. Sometimes, devices for unauthorised CA decoding are manufactured and offered simply to help sales of satellite dish (parabolic antennae) rather than for direct profits. The hacker's smart-card is handed out in this case as a purchasing incentive.

Certain retailers and installation companies have been known to advise subscribers not to renew their regular subscriptions, giving them hacker smart-cards at a reduced price instead.

Illegal smart-cards also circumvent decoders that have been loaned or rented to subscribers. Conditional-access systems come with special software interfaces to make decoders inoperable once they have not been returned at the end of the rental period. The device can be made operational again only if the decoder is used with an authorised smart-card. Illegal cards can totally circumvent this process. Often, stolen decoders and illegal cards are offered bundled together, adding theft of material goods to the violation of conditional access systems.”

(source: AEPOC (undated))

Many components necessary for the reprogramming of the cards, for changing parameters of the decoders and the blank cards themselves are legally available and have legitimate uses, thus control of their distribution is difficult. In the USA, DIRECTV utilises an access card to decode a signal. There is a page on E-bay explaining why auctions of such cards will not be allowed.

A robust and scalable conditional access (CA) system can prevent piracy (Datamonitor 2005). Farrell (2005) contends that the solution may lie in using incentives to bring industry and/ or public action to implement security. In early 1991, DirecTV and Spain’s Canal Satellite Digital inserted computer code into the hacked smartcards being used by some TV pirates. The code added up over time to form an executable programme which ended the functionality of the cards. Legally used cards had previously been ‘vaccinated’ during normal updating, which illegal card users avoided as part of their method of avoiding detection.

Smart wallets are essentially mobile phones which incorporate chips allowing diverse financial activities and transactions. They typically use near-field communication (NFC). NFC is currently used for non-contact travel cards in London (the Oyster card) and other cities. NFC is expanding rapidly in coverage and, when incorporated into mobile phones “could turn your mobile phone into a travel pass, wallet, cinema ticket or your door key” (Economist 2005). Historically NFC is aligned with Radio Frequency Identifiers (RFIDs) which serve as smart electronic tags on consumer products (see Whitehead 2005). NFC–

mediated development of mobile phones into smart wallets (see below), will generate a range of new and enticing criminal opportunities. London's Oyster Card is a non-contact swipe card, exchangeable between persons and transport systems which "allows you to store up to three Travel cards or Bus Pass season tickets, and cash to pay as you go." (Transport for London 2005). The credit that it stores can be swiped in exchange for transportation, but is capable of use for other types of transaction. These smart cards can be topped-up via a variety of means - online, at free-standing machines, or by phone. As the average monetary value stored on a card increases, so will its attractiveness as a target of theft, robbery or fraud. The geography of such crimes will expand with the use of the cards in other cities across the EC. The next step is the integration of this NFC technology into mobile phones to produce 'smart wallets' which can be swiped and topped-up in a similar fashion. When personal and financial information comes to be integrated with (or accessed by) smart wallets, and so the potential for fraud, and large-scale fraud, will be very much greater. Once personal information is obtained it can be used or sold on. Without adequate security, it seems reasonable to expect that software hacks will quickly be developed to attack smart wallets, and that this will drive a crime wave of theft and robbery. The higher rewards and the sophisticated know-how involved may mean that organised crime is quick to move into and expand this market. This anticipated crime harvest needs urgent research and preclusive action.

Security measures have already been developed to prevent theft of electronic services. Statistical models that detect patterns of ostensibly fraudulent use, including of electronic services, are becoming increasingly sophisticated (Fawcett and Provost 1997). Such software typically looks for exceptional patterns, and are most familiar in relation to credit card usage where card owners are contacted directly if an unusual pattern of use occurs. The detection systems are now becoming increasingly sophisticated in response to adaptations by offenders (Bolton and Hand 2002).

There are already instances where theft of electronic services could be prevented but preventive action is not taken due to a lack of

incentives. Theft of mobile phone airtime via SIM-cards has been substantially prevented, but theft of handsets continues. Network providers quickly realised that they would have to foot the bill for stolen phones where the same SIM card was used. The result is a smoothly-running system whereby stolen SIM cards are automatically disconnected when a phone is reported stolen. Yet mobile phone handsets are still frequently stolen despite the fact that the technology has long existed whereby they could also be remotely disconnected by networks (via their IMEI numbers). This is because, in contrast to SIMS, service providers benefit from continued use of handsets if the SIM is replaced. Two phones are now on the network if the stolen phone plus a replacement are being used. In the first instance (SIMS), networks had a financial incentive for crime prevention and rapidly produced a flawless smooth-running crime prevention system. In the second, networks had no financial incentive (and if anything a financial incentive towards inaction), and although the crime prevention effort is making some headway (via remote disconnection of IMEIs, the unique identified of each handset), it is slow and faltering.⁸ This is discussed here as an illustration of the need for the analysis of incentives for crime prevention as these are critical to implementation, and hence to crime prevention. At the root of the problem lies recognition of the fact that market forces are not sufficient to control theft of electronic services, which is why independent research is required.

Newman and Clarke (2003) make the case for the relevance of the CRAVED framework to electronic service (information) crime. Products or services as transmitted information is eminently concealable, removable, valuable and disposable (four of the six elements of craved), and (contingently) available and disposable (the remaining two elements). Yet, as they stress, the design or other solutions are not as straightforward as with many products. To anticipate, this is a point that we came to recognise for electronic products, namely that CRAVED is an adequate means of assessing vulnerability, but measures of security are crude, since they are based upon simple and obvious security features which are already recognised. In a serious search for crime reduction effect, one would release the ingenuity of

⁸ The situation is more complex than this due to IMEI re-programming, the development of IMEI databases (local EIRs and the international CEIR), but our in-depth study shows the principle holds true (Farrell et al. 2005).

designers and engineers to devise novel security solutions, such as was evident in the covert building of code to disable pirated TV service access cards. This cannot be readily captured in checklist form. There are echoes here of long-running debates among security practitioners about the value of security standards, namely that they encourage building down to just meet a standard, rather than building up to achieve effective performance. This theme will be taken up in the recommendations section of the report. Finally here, it should be stressed that nothing in the foregoing should be taken to suggest different principles in estimating vulnerability and protection as between electronic products and services. That separation bespeaks a worldview inappropriate to the digital age.

7. RECOMMENDATIONS

Recommendation 1: To extend the provisions of Section 17 of the UK Crime and Disorder Act to central government as well as the private sector and to introduce similar legislation throughout Europe.

Justification 1: Despite recommendations by the UK government's own Foresight Committee on crime, there remains a failure to extend the provisions of Section 17 of the act to central government and the private sector. There are three reasons why the provisions should be extended: 1) Extending the provisions of Section 17 would allow private sector companies, including designers and manufacturers of electronic products, to be help legally responsible for the crime implications of their actions. 2) Extending the provisions of Section 17 would avoid the current situation whereby local authorities are required to consider the implications of their decisions upon crime and disorder, for example requiring all new build housing to meet the Secured by Design standard. Yet, a developer who appeals against a refusal of planning permission (which was based upon their inability to meet the required security levels) can appeal to the government's Planning Inspectorate who are not bound by Sec 17 and therefore overturn the appeal. 3) An extension of Sec 17 provisions would convey the message that crime reduction is not the sole responsibility of the public sector and that the private sector must take responsibility for their decisions. In a similar vein to the impact which Health and Safety legislation had on working practices, this extension may change the way that designers and manufacturers work, not because of the real threat of legal action, but because it is accepted that they hold some responsibility for the reduction of crime.

Recommendation 2: It is recommended that the mechanism presented in this report is used as a tool to inform the labelling of consumer electronic products and that two labelling systems are introduced. The first an accreditation scheme plus associated logo, the second a signposting scheme which allows consumers to immediately identify risk of theft without a requirement for further knowledge or investigation. It is recommended that the accreditation scheme should be introduced on a voluntary basis and that the signposting scheme is introduced, initially on a voluntary basis, with a provision that a failure

of manufacturers to adopt the system would result in an introduction of compulsory labelling.

Justification 2: The accreditation scheme and associated logo would allow manufacturers to market their goods as 'secure'. The signposting system would allow consumers to immediately identify the level of risk of theft of that product and to take the necessary action. For example, if the product was highly vulnerable but had low levels of security, the consumer could a) decide to avoid purchasing this product or b) purchase the product but take additional security precautions. The accreditation scheme serves a marketing purpose; the signpost scheme serves an educational purpose. Introducing the accreditation scheme without the signposting scheme would risk consumers presented with a product without a 'secure' label (because the product failed to meet the required standards to achieve the Secure award) being unaware of any security deficiency with that product.

Recommendation 3: It is recommended that the European Commission introduce the two schemes in conjunction with continued publicity (relating to the need to design out crime), further research (see recommendations 7.4, 7.5 and 7.6), the introduction of financial incentives and legislative requirements to consider crime in the design of electronic products.

Justification 3: The example of designing out crime within the built environment highlights how success has only been achieved following the introduction of a variety of incentives to encourage developers to build secure properties. These include: 1) Research highlighting that consumers want secure properties and are willing to pay a premium for security; 2) Research to show that properties built to the Secured by Design standard are less likely to experience crime; 3) Financial incentives for developers whose buildings meet the Secured by Design standard; 4) Legislative requirements for local authorities to consider the crime and disorder implications of their decisions (planning and development policy).

Recommendation 4: The European Commission should fund further research to identify which makes and models of products are most

vulnerable to theft, and circumstances of theft and recovery when stolen.

Justification 4: At present, police recorded crime data would not allow researchers to identify the make and model of stolen products. An in-depth study of actual levels of crime would serve two purposes: 1) To validate the findings of this report i.e. do products which score highly on the Marc vulnerability checklist actually experience higher levels of crime? 2) To confront manufacturers with the reality of the crime risks of their products. 3) To clarify the choice between similar security requirements across all products of the same type, or to think in product-specific terms.

Recommendation 5: The European Commission should ensure that (post-implementation) research is undertaken to establish whether products which meet the accreditation scheme criteria actually experience less theft than those which do not.

Justification 5: It is essential that any success is publicised and used to further sell the scheme. Research into the effectiveness of the scheme should also have an improvement orientation, allowing any weaknesses with the scheme to be addressed.

Recommendation 6: The European Commission should stimulate further research to identify: 1) What priority consumers place on security and 2) Whether they are prepared to pay a premium for additional security.

Justification 6: Similar research within the built environment revealed that consumers purchasing a new home placed security as their number one priority (over and above features such as downstairs WC, garage, fitted carpets etc.) and that consumers did not expect additional security to be included in the price. This research enables developers to be confronted with the evidence that additional security would give them a market advantage and that they would be able to charge an additional premium for secure homes without the risk of putting consumers off.

Recommendation 7: It is recommended that, where possible, measurements of risk should take place at the prototype stage. This will avoid the need for expensive changes.

Justification 7: Although measuring risk too early can risk miscalculation, it is essential that the assessment takes place early enough to allow changes to the design.

Recommendation 8: It is recommended that discussions take place with the insurance sector to establish whether the perverse incentives which disincentivise security precautions (due to old products being upgraded) can be revised.

Justification 8: Any risk that consumers will avoid secure products should be minimised and perverse incentives removed.

Recommendation 9: The European Commission should encourage further research to establish a) what proportion of consumer electronic goods are insured; b) the level of inconvenience caused to consumers when electronic goods are stolen and c) the proportion of thefts of consumer electronic goods which involve violence (and the effect this has upon the victim).

Justification 9: The authors of this report do not agree with the suggestion that consumers will not want their products to be secure because products which are stolen are replaced with new upgraded models. This argument does not address the fact that a large proportion of consumer electronic goods are uninsured, that the loss of data on a laptop or PDA can cause a huge inconvenience and, most importantly, that the theft of a consumer electronic product does not take place in isolation and for many victims the experience can be extremely frightening. Further research would provide data to challenge the assumption that consumers want their goods to be stolen.

Recommendation 10: The European Commission should consider further research into the decisions made by offenders when selecting consumer electronic goods as targets.

Justification 10: One of the arguments against increasing the security of electronic products is that the majority are not targeted, but are simply in a stolen handbag, car or house. Further research is required to establish what proportion of electronic goods are stolen from handbags and what proportion are specifically targeted.

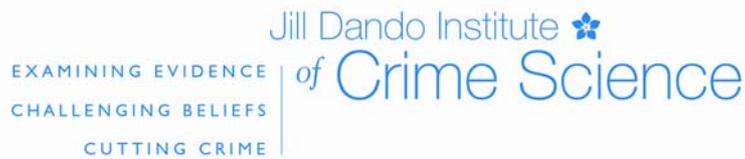
Recommendation 11: The European Commission must address the misconception that designers and manufacturers are being asked to produce undesirable goods.

Justification 11: One of the misconceptions of the proposals contained within this report is that manufacturers are being asked to produce undesirable goods. This is not the case and the proposals simply suggest that a desirable product must have commensurate levels of security. If it is desirable it must be equally secure.

Recommendation 12: That a Working Group be set up to take forward the recommendations and proposals contained within this report.

Justification 12: The work reported here advances understanding of security and vulnerability of electronic products and services, which could be built upon. It is essential that any Working Group be made up of consumers, manufacturers, retailers, policy makers and academics.

Appendix 1 – Interview Schedule for Key Stakeholders



Project Marc - Developing Mechanisms for Assessing the Risk of Crime due to legislation and products in order to proof them against crime at EU level.

In an attempt to reduce the levels of theft of electronic products, a consortium of universities has been funded by the European Commission to consider the most effective means of ‘proofing’ electronic products against theft.

Our response has been to develop and expand upon a method proposed by Ron Clarke and Graeme Newman in 2002 which assesses products in terms of:

1. The product’s vulnerability to theft in terms of its attractiveness, value etc,
2. The product’s security features.

Vulnerability to theft is indexed by the relationship between scores on the two indices. High vulnerability/low security items will be particularly prone to theft. Provided that a product scores highly enough on the security checklist for its predicted level of risk, it can be designated and marketed as *Secured Goods by Design (SGD)*. Clarke and Newman see manufacturers’ involvement as voluntary. Those familiar with the crime reduction landscape will recognise the parallels with the Secured by Design scheme applying to buildings.

In the current project, key stakeholders like yourself are being asked to comment on whether such a crime risk assessment mechanism and associated accreditation scheme are the most effective ways of proofing products against theft (and if not what they see as more promising approaches), whether the existing checklists are clear, uncontentious and likely to be subscribed to by manufacturers and finally, how such a scheme, (or any more promising scheme proposed by the stakeholder) should be managed and implemented.

We ask for your name and the organisation which you represent as a means of ensuring that participants are credited in any reports/publications. If you wish to remain anonymous, your name can be excluded from the questionnaire. If you would like to be credited in the final report, but do not want your comments to be attributed to yourself or your company, we will ensure that this takes place. There is an opportunity to select the appropriate level of anonymity at the end of the questionnaire.

Name.....

Organisation.....

Question 1:

Our response to the request to consider the most effective means of proofing electronic products against theft has been to design a crime risk assessment mechanism which can be used to measure a product's risk of theft as well as its security features. It is envisaged that this mechanism will be used to ascertain whether a product can be awarded *Secured Goods by Design (SGD)* status should a manufacturer decide to apply for this seal of approval.

1a) Based upon your experience, do you think that a crime risk assessment mechanism and associated accreditation scheme is worth developing as a means of reducing the theft of electronic products?

1b) In your view, what are the benefits of this approach?

1c) In your view, what are the weaknesses associated with this approach?

1d) Please outline an alternative strategy which you would favour over the risk-assessment/accreditation scheme outlined above. If your experience suggests that the proposed approach is without value, we would be grateful if you could complete the interview schedule, even where it applies specifically to the proposed approach.

Question 2:

From your experience, what, if anything, is currently being done to ensure that security considerations are incorporated into the design/manufacture of electronic products?

Question 3:

Are you aware of any existing security standards or award schemes which apply to electronics products?

Question 4:

Are you aware of any companies which routinely consider designing out crime in the design and manufacture of their products?

Question 5:

As was mentioned in the introduction, we propose to develop a crime risk assessment mechanism to measure a product's vulnerability to crime alongside its security features. To qualify for a *Secured Goods by Design* (SGD) award, products must have levels of security commensurate with their vulnerability to theft.

The existing checklists are set out below. Based upon your general and specific comments, we will refine these checklists and pilot them on a sample of 60 electronic products before a final mechanism is developed.

1. Checklist for Risk of Theft:

	Items	Item Score
CONCEALABLE	<i>Check one</i> On person (score 2) In bag (score 1)	
REMOVABLE	<i>Check one</i> Can be carried in one hand (scores 2) Can be carried with two hands (score 1)	
AVAILABLE	<i>Score 1 for each</i> Used outside the home Commonly left in parked cars Marketed to young males Minimal search time for thief to locate product	
VALUABLE	<i>Score 1 for each</i> Costs at least one day's wages Provides access to phone services Provides access to the internet Provides access to credit	
ENJOYABLE	<i>Score 1 for each</i> Entertaining Addictive Fashionable Luxury item Status item Aggressive advertising emphasising these themes	
DISPOSABLE	<i>Score 1 for each</i> Widely in demand Value easily assessed Street price less than 50% of one day's wages	
TOTAL SCORE		

5a) Based upon your experience, do you think that this checklist would be applicable to electronic products?

--

5b) Do you have any general comments about this checklist as a means of measuring a product’s vulnerability to theft?

--

5c) Do you have any specific comments about the checklist i.e. wording, scores, clarity, appeal to manufacturers?

--

Question 6:

Below is the second checklist, which is designed to measure a product’s security features.

2. The Checklist for Product Security:

Security Feature	Score
<ul style="list-style-type: none"> Customer education designed into marketing (e.g. security instructions included in package) (score 1) 	
<i>Replacement guarantee to consumer if product stolen. Check one:</i> <ul style="list-style-type: none"> Within 90 days (score 1) Within 1 year (score 2) Life of product (score 3) 	
<ul style="list-style-type: none"> Customer education to minimize risk of theft of product included in retailer training (score 1) 	
<ul style="list-style-type: none"> Valid means of unique identification of product (e.g. source tagging) (score 3) 	
<ul style="list-style-type: none"> Valid means of tracking ownership of product through life cycle (e.g. chipping) (score 3) 	
<ul style="list-style-type: none"> Technology designed to delay or defeat attempted theft of item (e.g. packaging) (score 3) 	
<ul style="list-style-type: none"> Technology to negate the financial value of the item if stolen (e.g. PIN) (score 3) 	
<i>Cost of inclusion of security features has been:</i> <ul style="list-style-type: none"> 10% or more of production cost (score 2) Up to 10% of the production cost (score 1) Zero cost (score 0) 	
<i>Cost of security feature included in product has been:</i> <ul style="list-style-type: none"> Absorbed by manufacturer (score 2) Shared with retailer (score 1) Shared with customer (score 0) Passed on to customer (subtract 1) 	
<i>Product has been field-tested for theft*</i> <ul style="list-style-type: none"> Yes (score 1) No (score 0) 	
TOTAL SCORE	

*Field-testing consist of market research into the product’s perceived attractiveness to thieves.

6a) Based upon your experience, do you think that this checklist would be applicable to electronic products?

6b) Do you have any general comments about this checklist as a means of measuring a product's existing levels of security?

6c) Do you have any specific comments about the checklist i.e. wording, scores, clarity, appeal to manufacturers?

Question 7:

Are you aware of any existing incentives to encourage those working within the electronics industry to consider the crime implications of their products?

Question 8:

Which of the following do you think would be most likely to influence the manufacturers of electronic products to crime proof their products (please rank these in order, 1 being the most likely to influence manufacturers to crime proof their products)?

- Consumer demand
- Financial incentives
- Legislation requiring crime proofing of products
- Financial penalties i.e. fines/taxes
- Naming and shaming
- Rewarding good design i.e. *Secured Goods by Design* scheme
- Legislation making it easier for civil litigation against manufacturer
- Other.....

Question 9:

In terms of implementing the *Secured Goods by Design* award for electronic products, Clarke and Newman proposed the following process for awarding this standard:

- 1) Manufacturer decides to apply for *Secured Goods by Design*;
- 2) Undertakes an analysis of inherent risk of theft with checklist one;
- 3) Completes assessment of security measures using checklist two, and makes any necessary improvements in security;
- 4) Submits plans to those responsible for managing the scheme i.e. trade association;
- 5) Trade association grants *Secured Goods by Design* seal of approval (or not);
- 6) Trade association reviews the theft history of the product on an annual basis to determine any improvements needed in security to retain *Secured Goods by Design* status.

9a) In your view, would manufacturers be interested in applying for *Secured Goods by Design* Status?

9b) In Secured by Design, which is a similar award given to housing developers who design and build their properties to specific standards, the award is owned and managed by the Association of Chief Police Officers and the assessments and support is provided by local police architectural liaison officers. In your view, who might appropriately have responsibility for managing the *Secured Goods by Design* scheme?

Question 10:

In your view, is there a public demand for secure electronic products?

Question 11:

Finally, what do you think that government's role should be in ensuring that products are designed to be crime resistant?

This questionnaire has been sent to key stakeholders within the fields of designing out crime and the electronics industry. We would like the views of as many important stakeholders as possible and we therefore ask you to suggest two more people to take part in this interview whose experience and expertise should be tapped.

- 1.....
- 2.....

Finally, please could you select the level of anonymity which you request:

I would be happy for my answers to be attributed to me by name and organisation

I would be happy for my name and organisation to be credited in the final report, but would like my answers to remain anonymous

I am happy for my answers to be included in the final report, but do not want my name or organisation to be mentioned

Appendix 2 – Stakeholder Questionnaire for Assessing the Vulnerability/Security Levels of a Selection of Electronic Products

Project Marc

Developing Mechanisms for Assessing the Risk of Crime due to Legislation and Products in Order to Proof them against Crime at an EU Level.

Stakeholder Questionnaire



A PROJECT FINANCED BY THE EUROPEAN COMMISSION – DG RESEARCH
UNDER THE SIXTH FRAMEWORK PROGRAMME

and coordinated by:



in partnership with:



And in co-operation with:



In an attempt to reduce the levels of theft of electronic products, a consortium of universities has been funded by the European Commission to consider the most effective means of ‘proofing’ electronic products against theft. We are developing a method proposed by Ron Clarke and Graeme Newman in 2002 which assesses the risk of an electronic product being stolen with reference to two measurable indices:

- Vulnerability to theft in terms of their attractiveness, value etc,
- Existing security features.

A product’s risk of theft is a result of an assessment of these two indices; this means that if an electronic product shows high levels of vulnerability and low levels of security features, it will be particularly prone to theft. The advantage of this measurement is the ability to predict and manage the risk of theft of electronic products and to create a standard that allows certain products to be rated as *Secured Goods by Design (SGD)*.

This interview forms part of phase two of the project. Our initial consultation confirmed that, in general, participants wanted to retain the notion of a mechanism which consists of two checklists measuring both risk and protection respectively, but to re-produce the contents of those checklists to address issues of lack of clarity, subjectivity and poor inter-rater reliability.

As part of this process, we are consulting with representatives from the four sectors – law enforcement, insurance, consumers and manufacturers from 10 European countries (including a mix of original and accession states). We are asking participants to rate a sample of 5 products (3 models of each) in terms of their:

- Vulnerability to theft (high, medium or low), and
- Existing levels of security (high, medium or low)

We are also asking participants to explain their ratings.

We ask that you complete the following questionnaire electronically and return it to Dr. Rachel Armitage (mail@rachelarmitage.co.uk) by the 29th July. Once responses have been analysed, we may conduct a short follow-up telephone interview to clarify any issues. If you have any queries whilst completing the questionnaire, please feel free to contact me at the above e-mail address.

We ask for your name and the organisation which you represent as a means of ensuring that participants are acknowledged for their help in resulting reports and publications. If you would like to be acknowledged in the final report, but do not want your comments to be attributed to yourself or your company, we will ensure that this takes place. There is an opportunity for you to select your desired level of anonymity at the end of the questionnaire.

Name.....

Organisation.....

Please read this brief report on MP3 players before completing questions 1- 12.

The table below contains a summary of the main features of three MP3 players. Please read this information before answering the questions below.			
	Apple iPod 20Gb	Apple iPod Mini	iAudio M3
Price	€276.25 (£189.99)	€202.29 (£139)	€289.43 (£199)
Dimensions (WxDxH) cm	6.1 x 1.4 x 10.4	5.1 x 1.3 x 9.1	6.1 x 1.4 x 10.4
Weight	158g	102g	136g
Colour	Player and headphones are a white	Blue, pink, green or silver. Headphones are white.	Silver or brown
Internal memory	20Gb	4Gb	20Gb
Fingerprint recognition	×	×	×
Link to services	Apple iTunes provides a convenient legitimate method of purchasing music electronically to play on the iPod. However, the iPod will play music which is downloaded illegally.	Apple iTunes provides a convenient legitimate method of purchasing music electronically to play on the iPod. However, the iPod will play music which is downloaded illegally.	No copyright protection system
Additional built-in security features.	Free laser engraving if purchased directly from Apple. Serial number but no reference to registering this with apple.	Free laser engraving if purchased directly from Apple. Serial number but no reference to registering this with apple.	×
			

Qu.1: In your opinion, how vulnerable is the Apple iPod (MP3 player) to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. Please tick one box only.

- Low
- Medium
- High

Qu.2: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.3: In your opinion, how secure is the Apple iPod (MP3 player)? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

Low
Medium
High

Qu.4: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.5: In your opinion, how vulnerable is the Apple iPod Mini (MP3 player) to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

Low
Medium
High

Qu.6: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.7: In your opinion, how secure is the Apple iPod Mini (MP3 player)? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

Low
Medium
High

Qu.8: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.9: In your opinion, how vulnerable is the iAudio M3 (MP3 player) to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
- Medium
- High

Qu.10: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.11: In your opinion, how secure is the iAudio M3 (MP3 player)? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low
- Medium
- High

Qu.12: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Please read this brief report on Personal Digital Assistants (PDAs) before completing questions 13-24.

The table below contains a summary of the main features of three PDAs. Please read this information before answering the questions below.

	Palm One Zire 72	Palm One Tungsten T5	HP iPAQ rx3715
Price	€189.06 (£129.97)	€290.87 (£199.99)	€384.16 (£264.13)
Dimensions (WxDxH) cm	7.5 x 1.7 x 11.6	7.8 x 1.5 x 12.1	7.1 x 1.6 x 11.4
Weight	136g	146g	158g
Internal memory	32mb	256mb	64mb
Digital camera function	✓	×	✓
MP3 Player	✓	✓	✓
Telephone	×	×	×
Bluetooth enabled	✓	✓	✓
Fingerprint recognition	×	×	×
Additional built-in security features.	×	×	×



Qu.13: In your opinion, how vulnerable is the Palm One Zire 72 (PDA) to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
 Medium
 High

Qu.14: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.15: In your opinion, how secure is the Palm One Zire 72 (PDA)? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low
- Medium
- High

Qu.16: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.17: In your opinion, how vulnerable is Palm One Tungsten T5 (PDA) to theft?

A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
- Medium
- High

Qu.18: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.19: In your opinion, how secure is the Palm One Tungsten T5 (PDA)?

A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low
- Medium
- High

Qu.20: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.21: In your opinion, how vulnerable is HP iPAQ rx3715 (PDA) to theft?

A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
- Medium
- High

Qu.22: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.23: In your opinion, how secure is the HP iPAQ rx3715 (PDA)? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

Low

Medium

High

Qu.24: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Please read this brief report on digital cameras before completing questions 25-36.

The table below contains a summary of the main features of three digital cameras. Please read this information before answering the questions below.

	Olympus Camedia C-770 Ultra Zoom	Olympus Camedia C-5060	Fuljifilm Finepix S7000
Price	€315.49 (£216.95)	€450.87 (£309.95)	€450.87 (£309.95)
Dimensions (WxDxH) cm	10.5 x 6.9 x 6.0	12 x 7.5 x 9	12.1 x 9.7 x 8.2
Weight	280g	534g	500g
Resolution	4.0	5.0	6.3
Bluetooth	×	×	×
Video capture	✓	✓	✓
Fingerprint recognition	×	×	×
Additional built-in security features.	×	×	×



Qu.25: In your opinion, how vulnerable is the Olympus Camedia C-770 Ultra Zoom (digital camera) to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
 Medium
 High

Qu.26: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.27: In your opinion, how secure is the Olympus Camedia C-770 Ultra Zoom? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low
 Medium

High

Qu.28: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.29: In your opinion, how vulnerable is the Olympus Camedia C-5060 (digital camera) to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

Low

Medium

High

Qu.30: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.31: In your opinion, how secure is the Olympus Camedia C-5060? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

Low

Medium

High

Qu.32: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.33: In your opinion, how vulnerable is the Fujifilm Finepix S7000 (digital camera) to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

Low

Medium

High

Qu.34: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.35: In your opinion, how secure is the FujiFilm Finepix S7000? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

Low

Medium

High

Qu.36: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Please read this brief report on mobile phones before completing questions 37-48.

The table below contains a summary of the main features of three models of mobile-phones. Please read this information before answering the questions below.

	Motorola V600	Nokia 6230i	Sony Ericsson K700i
Price	€ 257.55 (£176.95)	€296.95 (£203.99)	€ 257.59 (£176.95)
Height (cm)	8.8	10.3	9
Weight	116 g	99 g	93 g
Depth (cm)	2.36	2	2
Display Type	65 k TFT Colour	Active TFT Colour Display	Colour Display
Form Factor	Clamshell	×	×
Internal Memory	5 MB	30 MB	41 MB
GPRS	(2u/4d)AMR	Class 10 (4+1, 3+2)	✓
WAP	✓	✓	✓
Bluetooth	✓	✓	✓
Infrared	×	✓	✓
Integrated Digital Camera	✓	✓	✓
Performance Features	Quad-band	Tri-band	Tri-band
SMS	✓	✓	✓
MMS	✓	✓	✓
Talktime	Up to 450 mins	Up to 3-5 hours	8 hours
Stand-by Time	Up to 250 hours	Up to 150-300 hours	300 hours
Link to services	Motorola V600 provides access to web. Bluetooth technology enables to contact other mobiles nearby and provides wireless data connectivity.	Nokia 6230i provides access to web. Bluetooth technology enables to contact other mobiles nearby and provides wireless data connectivity.	Sony Ericsson k700i provides access to web. Bluetooth technology enables to contact other mobiles nearby and provides wireless data connectivity.
Additional built-in security features.	Call restrictions, phone lock, new password capability.	×	×
			

Qu.37: In your opinion, how vulnerable is the Motorola V600 to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
- Medium
- High

Qu.38: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.39: In your opinion, how secure is the Motorola V600? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low
- Medium
- High

Qu.40: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.41: In your opinion, how vulnerable is the Nokia 6230i to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
- Medium
- High

Qu.42: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.43: In your opinion, how secure is the Nokia 6230i? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low
- Medium
- High

Qu.44: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.45: In your opinion, how vulnerable is the Sony Ericsson K700i to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. Please tick one box only.

- Low
- Medium
- High

Qu.46: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.47: In your opinion, how secure is the Sony Ericsson K700i? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. Please tick one box only.

- Low
- Medium
- High

Qu.48: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Please read this brief report on laptops before completing questions 49-60.

The table below contains a summary of the main features of three models of laptop. Please read this information before answering the questions below.

	Toshiba Satellite M30X 159	Apple PBook G4 15 inch	Sony Vaio VGN B1XP
Price	€ 1162.99 (£799.03)	€ 2299.67 (£1579.99)	€ 1413.53 (£971.73)
Height (cm)	2.95 (front)/3.76 (rear)	2.8	2.9 cm
Weight	3.10 kg	2.5 kg	2.3 kg
Depth (cm)	27.43	24.1	25.5
Case Colour	×	Aluminium	Magnesium Alloy
Screen Size	15.4''	15.2 ins	14.1''
CPU Family	Intel Centrino	PowerPC G4	Intel Centrino
CPU Speed	1.60 GHz	1670 MHz	1.70 GHz
Hard Disk Size	60 GB	80 GB	60 GB
Memory Size	512 MB	512 MB	512 MB
Integrated modem	✓	✓	✓
Integrated Network	✓	✓	✓
Wireless System	✓	✓	✓
DVD-ROM/CD-RW	✓	✓	✓
Operating System	Microsoft Windows XP Home Edition	Apple MacOS X Version 10.3 Panther	Microsoft Windows XP Professional
Built-in Bluetooth	×	✓	×
Built-in Network Card	✓	✓	✓
Software Included	✓	✓	✓
Link to services	Toshiba Satellite M30X 159 provides access to web, wherever it runs into a wireless network. It can also be connected to web by using cables.	Apple PBook G4 15 inch provides access to web, wherever it runs into a wireless network. It can also be connected to web by using cables	Sony Vaio GN B1XP provides access to web, wherever it runs into a wireless network. It can also be connected to web by using cables
Additional built-in security features.	Slot for cable-lock; HDD memory (by screw only); user power-on password; supervisor password.	×	Norton Internet Security; Norton Password Manager
Battery-life	Up to 3.5 hours	4.5 hours	4 hours
			

Qu.49: In your opinion, how vulnerable is the Toshiba Satellite M30X 159 to theft?

A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
- Medium
- High

Qu.50: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.51: In your opinion, how secure is the Toshiba Satellite M30X 159? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low
- Medium
- High

Qu.52: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.53: In your opinion, how vulnerable is the Apple PowerBook 15” to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

- Low
- Medium
- High

1.

2.

3.

Qu.55: In your opinion, how secure is the Apple PowerBook 15”? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

- Low

Medium
High

Qu.56: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.57: In your opinion, how vulnerable is the Sony Vaio VGN B1XP to theft? A rating of low would suggest that the product will rarely be stolen; a rating of high would suggest that the risk of theft is high. *Please tick one box only.*

Low
Medium
High

Qu.58: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Qu.59: In your opinion, how secure is the Sony Vaio VGN B1XP? A rating of low would suggest that the product has low levels of in-built security; a rating of high would suggest that the product has substantial levels of in-built security. *Please tick one box only.*

Low
Medium
High

Qu.60: Please provide up to three reasons why you have given this rating.

1.

2.

3.

Finally, please could you select the level of anonymity which you request.

I would be happy for my answers to be attributed to me by name and organisation

I would be happy for my name and organisation to be credited in the final report, but would like my answers to remain anonymous

I am happy for my answers to be included in the final report, but do not want my name or organisation to be mentioned

REFERENCES

AEPOC (undated) Accessed via http://www.aepoc.org/press_service/hi_aeback.html on 18 January 2005.)

ANANOVA (2004) *Police Launch Mobile Phone Unit*. [online]. Available from: http://www.ananova.com/news/story/sm_847785.html?menu=news.technology.mobilephones. [Accessed 12th October 2004].

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

Armitage, R. (2005) *Secured By Design – An Investigation of Its History, Development and Future Role in Crime Reduction*. Unpublished PhD Thesis, The University of Huddersfield, Huddersfield, West Yorkshire.

BBC News (2003, December 17) *Mobile Phone Crime Blitz Launched*. [online]. BBC News UK Edition. Available from: <http://news.bbc.co.uk/1/hi/uk/3326171.stm>. [Accessed 12th October 2004].

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

Bolton, R.J. and D.J. Hand. 2002. 'Statistical fraud detection: A review' *Statistical Sciences*, 17(3), 235–255.

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. (1984) Burglar Mobility and Preventive Planning. In: R.V. Clarke and T. Hope (eds.) *Coping with Burglary: Research Perspectives on Policy*. Boston, Kluwer–Nijhoff. p. 77–96.

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.

Britain Attacks Soaring Mobile Phone Theft (2003, December 17). Available from: http://www.chinadaily.com.cn/en/doc/2003-12/17/content_291210.htm. [Accessed 12th October 2004].

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.

Brennan, P, *et al*. (1991) Congenital Determinants of Violent and Property Offending, *In*: D. Pepler & K. Rubin (eds.) *The Development and Treatment of Aggression*. Hillsdale, New Jersey, Erlbaum.

Briscoe, S. (2001) *The Problem of Mobile Phone Theft*. Crime and Justice Bulletin No. 56. Sydney, New South Wales Bureau of Crime Statistics and Research.

Caspi, A. and Moffit, T.E. (1995) The Continuity of Maladaptive Behaviour. From Description to Explanation in the Study of Antisocial Behaviour. *In*: D. Cicchetti and D. Cohen (eds.) *Developmental Psychopathology – Volume 2*. New York, Wiley. P. 472–511

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. (1999) *Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods*. Police Research Series Paper 112, London, Home Office.

Clarke, R.V. and Lester, D. (1989) *Suicide: Closing the Exits*. New York: Springer-Verlag.

Clarke, R.V. and Weisburd, D. (1994) Diffusion of crime control benefits: Observations on the reverse of displacement. *In R.V. Clarke (ed) Crime Prevention Studies 3*. 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 Newman, G. (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. (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.

Cohen. L.E. and Felson.M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*. 44, 588–608.

Coleman, A. (1986) *Utopia on Trail: Vision and Reality in Planned Housing*. London, Hilary Shipman.

COM (2003) Commission of the European Communities: *On the legal protection of Electronic Pay Services*. Accessed via http://www.eu.int/comm/internal_market/media/docs/elecipay/com-2003-198_en.pdf on 18 January 2005.

Cornish, D. and R.V. Clarke (Eds.) (1986). *The Reasoning Criminal*. New York, Springer-Verlag.

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

Datamonitor (2005) "Digital pay-TV Piracy in Eastern Europe. The need for a secure and flexible conditional access system." Datamonitor, August 2005. Accessed via http://nds.com/pdfs/Datamonitor_EE_Piracy_whitepaper_August2005.pdf on 18 January 2005.

Davis, R. and K. Pease. 2000. 'Crime, Technology and the Future' *Security Journal*, 13, 59-64.

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

Economist, The. 2005. 'In the very near future' 08 December 2005.

Eklom, 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.

Eklom, P. (1999). Can we make crime prevention adaptive by learning from other evolutionary struggles? *Studies on Crime and Crime Prevention*. 6, 27- 51.

Eklom, P. (2005) Designing products against crime. In N. Tilley (ed.) *Handbook of Crime Prevention and Community Safety*. Cullompton, UK, Willan Publishing

Farrell, G. 2005. 'Progress and prospects in the prevention of repeat victimisation' in N. Tilley (Ed.) *Handbook of Crime Prevention and Community Safety*. Cullompton: Willan Publishing.

Farrell, G. and K. Pease. 1993. *Once Bitten, Twice Bitten: Repeat Victimisation and its Implications for Crime Prevention*. Crime Prevention Unit paper 46. London: Home Office. Available at www.homeoffice.gov.uk/prgpubs/fcpu46.pdf

Farrington, D (1978) *The Family Backgrounds of Aggressive Youths* in L. Hersov, M. Berger and D. Shaffer (eds.) *Aggression and Antisocial Behaviour in Childhood and Adolescence*. Oxford, Pergamon.

Farrington, D (1986a) *Age and Crime* in M. Tonry & N. Morris (eds.) *Crime and Justice* Vol. 7. Chicago, Uni. of Chicago Press.

Farrington, D (1986b) *Stepping Stones to Adult Criminal Careers* in D. Olweus, J. Block and M.R. Yarrow (eds.) *Development of Antisocial and Pro-social Behaviour*. New York, Academic Press.

Farrington, D. P (1991) *Childhood Aggression and Adult Violence*, in D. Pepler and K. H Rubin (eds.) *The Development and Treatment of Childhood Aggression*, Hillsdale, New Jersey, Lawrence Erlbaum.

Farrington, D (1992) *Juvenile Delinquency* in J.C. Coleman (ed.) *The School Years* (2nd Ed.) London, Routledge.

Farrington, D.P (1995) *Teenage Antisocial Behaviour* in M. Rutter (ed.) *Psychosocial Disturbances in Young People. Challenges for Prevention*. Cambridge, Cambridge University Press.

Fawcett, T. and F. Provost. 1997. 'Adaptive fraud detection' *Data Mining and Knowledge Discovery*, 1(3), 291–316.

Felson, M. (1998) *Crime and Everyday Life, Second Edition*. California, Pine-Forge Press.

Felson, M. and Clarke, R. V. (1998) *Opportunity Makes the Thief. Practical Theory for Crime Prevention*. Police Research Series Paper 98, London, Home Office.

Garland, D. (1996) Limits of the Sovereign State: Strategies of Crime Control in Contemporary Societies. *British Journal of Criminology*. 36, 445–471.

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.

Groff, E.R. and LaVigne, N.G. (2001) Mapping an Opportunity Surface of Residential Burglary. *Journal of Research in Crime and Delinquency*, 38 (3), 257–278.

Home Office (1991) *Safer Communities: The Local Delivery of Crime Prevention through the Partnership Approach. Standing Conference on Crime Prevention (The Morgan Report)*. London, Home Office.

Homel, R. *et al* (1999) *Pathways to Prevention: Developmental and Early Intervention Approaches to Crime in Australia*. National Crime Prevention, Attorney General's Department, Canberra.

Klinterberg, B. A. *et al.* (1993) Hyperactive Behaviour in Childhood as Related to Subsequent Alcohol Problems and Violent Offending: A Longitudinal Study of Male Subjects. *Personality and Individual Differences*, 15, 381–388.

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].

Kolvin, I. *et al.* (1990) *Continuities of Deprivation?* Aldershot: Avebury.

Laycock, G. (2001) *Scientists or Politicians – Who has the Answer to Crime? Inaugural Lecture, April 26*. University College London.

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.

Lloyd, D. 2003. *International Roaming Fraud: Trends and Prevention Techniques*. 17 December 2003: Fair Isaac Corporation.

Mayhew, P. *et al.* (1976) *Crime as Opportunity*, Home Office Research Study No. 34, London, Home Office.

McGee, R *et al.* (1984) Perinatal, Neurological, Environmental and Developmental Characteristics of Seven year old Children with Stable Behaviour Problems. *Journal of Child Psychology and Psychiatry*, 25, pp. 573–586.

Metropolitan Police (2003). A New Weapon to Combat Phone Theft. [online]. *The Job*, 36 (919). Available from: http://www.met.police.uk/job/job919/live_files/2.htm. [Accessed 1st October 2004].

Michaud, L.J. *et al.* (1993) Traumatic Brain Injury as a Risk Factor for Disorders in Children. *Archives of Physical and medical Rehabilitation*, 74, 368–375.

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

Moffit, T.E. (1993) “Life-Course-Persistent” and “Adolescence-Limited” Antisocial Behaviour: A Developmental Taxonomy. *Psychological Review*, 100, 674–701.

Moitra, S. D. and S.L. Konda. 2004. 'An empirical investigation of network attacks on computer systems' *Computers and Security*, 23, 43-51.

Myhill, P. (2004) *The Application of Situational Crime Prevention to Organised Crime*. Unpublished MSc Thesis, University College London.

NCIS (2003) *UK Threat Assessment - The Threat from Serious and Organised Crime 2003*. [online]. London, NCIS. Available from: <http://www.ncis.co.uk/ukta/2003/ukta2003.pdf>. [Accessed 12th October 2004].

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

Newman, G. and R.V. Clarke. 2003. *Superhighway Robbery: Crime Prevention and E-Commerce*. Cullompton: Willan Publishing.

Nuttall, C. *et al.* (1977) *Parole in England and Wales, Home Office Research Study No. 38*. London, Home Office.

Ofcom. 2005. 'A consultation on persistent misuse' *In The Frame: The Regular TUFF Newsletter*. The Telecommunications United Kingdom Fraud Forum.

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.

Pease, K. (1998) *Repeat Victimisation: Taking Stock*. Crime Detection and Prevention Series Paper number 90. London: Home Office.

Pease, K. (2001). *Cracking Crime through Design*. London, Design Council.

Pease, K. (2005) 'No Through Road: Closing Pathways into Crime.' In K.Moss and M.Stephens (eds) *Crime Reduction and the Law*. London: Routledge.

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

Rengert, G.F. and Wasilchick, J. (2000) *Suburban Burglary: A Tale of Two Suburbs – Second Edition*. Springfield, Illinois, Charles C. Thomas Publishers.

Satterfield, J.H. and Schell, A. (1997) A Prospective Study of Hyperactive Boys with Conduct Problems and Normal Boys: Adolescent and Adult Criminality. *Journal of the American Academy of Child and Adolescent Psychiatry*, 36, 1726–1735.

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.

Simon, F.H. (1971) *Prediction Methods in Criminology – Including a Prediction Study of Young Men on Probation, Home Office Research Study 7*. London, Home Office.

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. p. 147–174.

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].

Tackling Worldwide Trade in Stolen Mobiles (2003, December 12). Available from: http://www.cellular.co.za/news_2003/122003-tackling_worldwide_trade_in_stol.htm. [Accessed 12th October 2004].

Taylor, R. and Gottfredson, S.D. (1987) Environmental Design, Crime and Prevention: An Examination of Community Dynamics. *Crime and Justice: An Annual Review of the Research*. 8, 387–416.

Transport for London. 2005. *Your Guide to Oyster*. London: Transport for London. (At: http://www.tfl.gov.uk/tfl/fares-tickets/2006/downloads/oyster-guides-06/TFL-Oyster_English.pdf , accessed December 2005).

Walsh, A. and Ellis, L. (2003) *Biosocial Criminology: Challenging Environmentalism's Supremacy*. New York: Nova.

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.

Wellsmith, M. and Burrell, A. (2005) The Influence of Purchase Price and Ownership Levels on Theft Targets: The Example of Domestic Burglary. *British Journal of Criminology*. Advance Access published on January 13, 2005, DOI 10.1093/bjc/azi003.

West, D.J and Farrington, D.P (1973) *Who Becomes Delinquent?* London, Heinemann.

West, D.J (1982) *Delinquency: its Roots, Careers and Prospects*. London, Heineman.

Whitehead, S. 2005. *Radio Frequency Identification (RFIDs) as a Potential Solution to Mobile Phone Crime* Unpublished manuscript prepared for EPSRC project. Loughborough University.

Wiles, P. and Costello, A. (2000) *The 'Road to Nowhere': The Evidence for Travelling Criminals*. Home Office Research Study 207, London, Home Office.

Wiles, P; Simmons, J and Pease, K. (2003) Crime Victimization: Its Extent and Communication. *Journal of the Royal Statistical Society: Series A*. 166 (2), 247–252.

Winchester, S. and Jackson, H. (1982) *Residential Burglary: The Limits of Prevention*, Home Office Research Study Number 74. London, Home Office.

Wong, K. (2003) *Rethinking Prevention – A Child-Focused Approach to using Protective and Risk Factors in Youth Crime Prevention*. London, Nacro.

Youth Justice Board (2001) *Risk and Protective Factors Associated with Youth Crime and Effective Interventions to Prevent it, Research Note 5*. London, Youth Justice Board.