THE EXPERIENCE OF E–CRIME

FINDINGS FROM THE NEW ZEALAND CRIME & SAFETY SURVEY 2006

Pat Mayhew and James Reilly

MINISTRY OF
JUSTICE
Tāhū o te Ture

This research was commissioned by the Research, Evaluation and Modelling Unit of the Ministry of Justice. The report has been prepared by the authors and the views expressed in it are those of the authors and do not necessarily represent the views of the Ministry.

Published in December 2007 by the Ministry of Justice, PO Box 180, Wellington, New Zealand

ISBN 978-0-478-29042-X

Contents

Tables

Figures

Boxes

Executive summary

This report presents results from questions in the 2006 New Zealand Crime and Safety Survey (NZCASS 2006) about what can be loosely grouped under a label of 'electronic crime' – e-crime hereafter. The questions were incorporated as a preliminary test of the extent of e-crime in New Zealand. They covered five forms of computer misuse, four forms of mobile phone misuse, and two forms of identity theft – i.e. the use of credit cards for theft, and the use of personal information to commit theft, fraud, or some other crime.

The 5,400 respondents in the 2006 survey answered the e-crime questions. They were a nationally representative random sample of those aged 15 and over in private households in New Zealand. They were interviewed at home by ACNielsen interviewers between February and June 2006. Respondents were asked about e-crime incidents that happened between 1 January 2005 and the date on which they were interviewed – an average reference period of 15.5 months.

The e-crime questions stood apart from the main 'crime counting' questions in NZCASS 2006. These concerned household crimes, such as burglary and theft of and from motor vehicles, and personal crimes, such as assault and theft of personal property. The information on e-crime is not incorporated into the main body of results on the victimisation experience of New Zealanders.

What the e-crime questions covered

E-crime is wide-ranging, and the incidents measured in the survey were by no means exhaustive. It is debatable whether all incidents merit the label of 'crime'. For one, there will be a degree of subjectivity involved. For instance, a phone owner might have reported in the survey that someone used their phone for a purpose that offended them, whereas the user may not have intended to cause offence. Likewise, a picture received on a mobile phone that one phone owner found offensive may not be judged so by another owner. We retain the label of 'e-crime' nonetheless.

The e-crime questions were also modest in scope. For instance, they do not:

- count how many times the incidents occurred
- give details of the incidents, such as degree of upset or extent of monetary loss
- cover whether any of the incidents had been reported to the Police or other authorities
- establish how far risks are associated with the frequency and nature of use of computers, mobile phones, and credit cards. More frequent use of these will increase exposure to risk, as could the manner in which they are used. For instance, those who do not buy goods over the Internet or via email will not leave themselves open to fraudulent transactions.

Nonetheless, the e-crime results from NZCASS 2006 provide up-to-date information about eleven e-crime problems in New Zealand. Other local surveys have been more limited in scope, although the Household Use of Information and Communications Technologies (ICT) Survey (Statistics NZ, 2007) included three questions similar to ones in NZCASS 2006. Both the US National Crime Victimization Survey and the British Crime Survey have also looked at householders as victims of e-crime, although there is by no means exact comparability with NZCASS 2006.

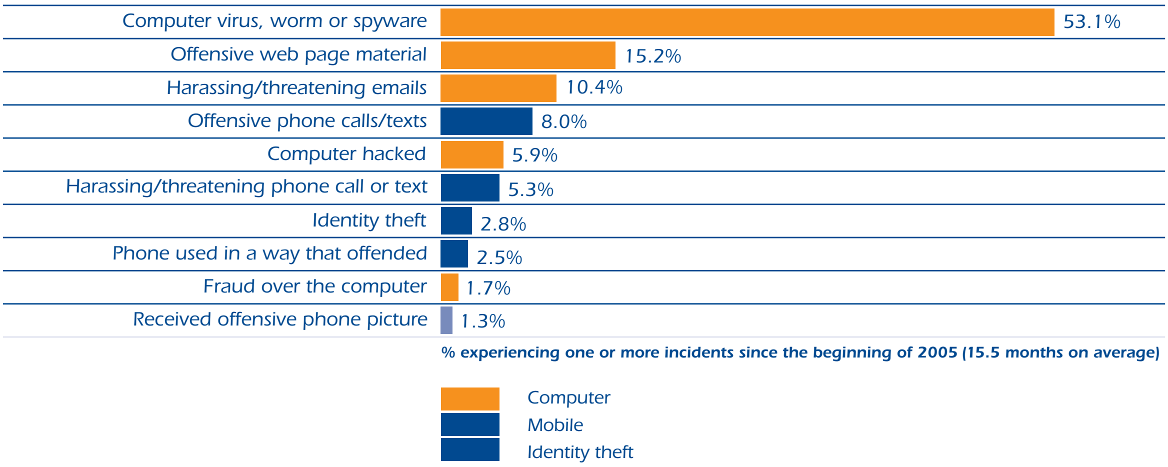
Who answered the e-crime questions?

Exposure to e-crime involving computers depends on people using a computer. About seven in ten New Zealanders said they used a computer at least monthly for personal use to access emails or the Internet. This group was asked the questions on computer misuse. Similarly, e-crime involving mobile phones depends on phone ownership. Eight in ten owned a mobile phone and therefore answered the relevant questions. The question on whether someone, without permission, had used a bank, credit or debit card to steal from the respondent was answered by 94% of the sample. Everyone answered the question on whether someone had used personal information about them without their permission to obtain new credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime. These last two questions are a measure of identity theft.

Experience of e-crime

- **Computer viruses etc.** The most common experience, affecting just over half of computer users, was a computer virus, a worm or spyware (Figure A). It is difficult to assess the significance of this. On the one hand, we do not know how well these terms were understood. On the other hand, respondents may not have known if they had been affected. Estimates from other surveys were generally lower (see below).
- **Offensive web page material.** Fifteen percent of computer users reported having unintentionally encountered material on a web page that they found highly offensive.
- **Harassing email messages.** One in ten computer users had received email messages that said things they found harassing or threatening. We do not know the nature of these messages – in particular whether they were of a personal nature, or more in the way of chain mail, including some items of spam.
- **Offensive use of mobile phones.** Eight percent of mobile phone users had received a call or text that said things they found highly offensive. A smaller proportion (2.5%) had had their phone used in a way that offended them; 1.3% had received a picture they considered offensive.
- **Hacking.** Six percent of computer users said their computer had been hacked – though possibly some users were not aware of this having happened.
- **Harassing mobile phone use.** In NZCASS 2006, 5.3% of phone users reported receiving a call or text that they considered harassing or threatening.
- **Identity theft.** In NZCASS 2006, 2.8% reported one or the other of two forms of identify theft they were asked about. This equates to about 93,000 New Zealanders in private households aged 15 or more.
- **Internet fraud.** Among computer users, 1.7% said they had bought something over the Internet or by email where they believed they were a victim of fraud. This figure is based on all computer users. The proportion among those who had actually used the Internet or email for a purchase would be higher.

Figure A The most common forms of e-crime 2005/06



Other estimates

For some of the forms of e-crime that NZCASS 2006 explored, there are estimates from other surveys. Exact comparisons are difficult because of differences in question wording, different recall periods, etc. This said, the main features are discussed below. There is some debate as to whether in a 'global age', there should be many inter-jurisdictional differences that cannot simply be explained by different survey methodology.

- **Computer viruses etc.** The NZCASS 2006 estimate is three times higher than that from the Household Use of ICT Survey: 2006, which showed that 17% of those with Internet access had experienced *loss or damage* caused by 'a virus or similar' over the last year. It may well be that the NZCASS 2006 question elicited incidents where no *loss* or damage was involved. The NZCASS 2006 figure is also twice as high as that in the 2003/04 British Crime Survey (Wilson et al., 2006).

- **Offensive web page material.** Fewer of those in NZCASS 2006 reported encountering offensive web page material than was the case in the United States in 2004 (Baum, 2006). The slightly different focuses of the questions may explain the difference, or possibly different national sensibilities.

- **Harassing email messages.** The figure of one in ten computer users having received email messages that said things they found harassing or threatening is similar to that in the 2003/04 British Crime Survey.

- **Hacking.** The NZCASS 2006 figure (6%) is higher than that from the 2003/04 British Crime Survey (2%). Survey differences and sampling error may explain the difference.

- **Internet fraud.** The NZCASS 2006 figure is similar to that from a reasonably equivalent question in the Household Use of ICT Survey: 2006, given that the latter specifies that some 'loss' should have occurred.

- **Identity fraud.** The NZCASS 2006 estimate is similar to the estimate from the 2004 US National Crime Victimisation Survey.

- **Misuse of cards.** The NZCASS 2006 figure (one component of identity theft) is rather lower than that from the 2005/06 British Crime Survey (Hoare & Wood, 2007).

Who was most at risk of computer misuse?

The types of people most at risk was not consistent across the five types of computer misuse – computer viruses, hacking, offensive web page material, harassing email messages, and internet fraud. Moreover, because of a low overall prevalence level for those who had been hacked, or who had bought something where they believed they were a victim of internet fraud, it is not possible to detect reliable differences in risk for these. The risk differences for the other three types of computer misuse are below.

Viruses etc

- More men (58%) than women (48%) reported having been affected by a virus, a worm or spyware.
- Students were also more at risk, as were those towards the top end of the socio-economic scale as measured by the New Zealand Socio-Economic Index (NZSEI).
- In terms of *lower* risk, fewer of the elderly, those living alone, and the retired said they had been affected by a virus. This was also true of those living in the most deprived areas of the country, as measured by the NZ Index of Deprivation.

Differences in computer usage may play a part in these results, with more frequent computer users perhaps being more aware of receiving viruses etc. There may also be different understandings as to what counts as a virus, a worm or spyware.

Offensive web material

- Those aged 15-24 less often encountered offensive material than other age groups. The same applied to those who were single.
- Patterns in terms of socio-economic status tended to indicate that higher status groups said they encountered offensive material more often than lower status groups.
- Māori more often said they encountered offensive material.

It may be that different groups have different thresholds as to what they consider to be offensive material.

Harassing emails

- More women (12%) than men (9%) had received email messages that they found harassing or threatening.
- Those aged 40-49 more often reported harassing or threatening emails too.
- Those in the least deprived areas of New Zealand and those in Auckland reported more harassing or threatening emails.

Again, it is difficult to say whether these results reflect different thresholds as to what is seen as harassing emails.

Who was most at risk of mobile phone misuse?

Differences between groups were similar across the four types of mobile phone misuse. There are four key results from a measure of *any* mobile phone misuse.

- Women reported more misuse than men, especially for offensive calls/texts and phone harassment. Women were also more vulnerable in the 2003/04 British Crime Survey.
- Those aged 15-24 experienced more phone misuse, which tended to decrease with age. Single people also reported more phone misuse, although there will be an overlap with age here.
- Māori reported higher levels of phone misuse than others did.
- A number of other indicators also suggested that those in more stretched social circumstances experienced more phone misuse – for instance, those who were unemployed and/or on benefits; those who rented property; those in the lower NZSEI bands; and those in the most deprived fifth of the country.

Some of the risk characteristics above overlap. The unemployed and those on benefits, for instance, are more often social renters, and Māori are overrepresented in both groups.

Who was most at risk of identity theft?

Even taking the two forms of identity theft together, it is difficult to be statistically confident about which groups were more likely to be at risk because of the low numbers of people affected. However, the indications are that vulnerability to identity theft, which may involve more serious financial consequences than the other forms of e-crime asked about, also tended to be greatest for those in more economically deprived situations – for instance, the smaller ethnic groups, social renters, and those who were unemployed and/or on benefits.

Concern about card misuse

It is clear that e-crime causes concern to New Zealanders.

- Of respondents in NZCASS 2006, 53% said they were very or fairly worried about having a credit card misused – much on a par with worry about having a car stolen, and not far behind worry about being a victim of a traffic accident caused by a drunken driver, burglary, and car vandalism.
- In a recent Unisys survey of a representative sample of New Zealanders (Unisys 2007), 32% of people were extremely or very concerned about viruses and unsolicited email; 31% were concerned about security when shopping or banking on line; and 53% were concerned about other people having unauthorised access to or misusing personal information about them.

All these figures are high, but do not signify that people are more worried than they should be. Worry may be a rational response to the consequences of victimisation. Even if the statistical risk is low, people may still justifiably worry because of the potentially distressing upset if an e-crime incident occurs.

Overview

The results from NZCASS 2006 give some indication of the scale of selective forms of e-crime in New Zealand in 2005/06. They also provide some insight into the types of information and communication technology (ICT) users who faced the highest risks, although for the less frequent forms of e-crime firm statistical conclusions are difficult to reach. However, some conclusions are possible.

- **There is little consistency in the risk of experiencing different forms of computer misuse.** Different forms did not affect different groups in a consistent way. It may be that more frequent computer users are more aware of viruses and hacking, for instance. On other counts, some people may be more sensitive than others about what they encounter in web material and emails.
- **Unwelcome emails.** These were reported more often by women, older people and those of higher socio-economic status. It is difficult to say whether different sensibilities explain this.
- **Ethnicity.** Māori tended to report many of the e-crimes more often. The picture for Pacific peoples was often similar, but the small number of Pacific peoples in the NZCASS 2006 sample means we cannot be sure about this.
- **Social deprivation.** A number of indicators suggested that those in more stretched circumstances experienced more phone misuse and identity theft. The results here echo analysis of other victimisation risks that NZCASS 2006 measured (see Mayhew & Reilly, 2007).

Implications of the findings

The policy implications of the results are modest for several reasons.

- It is difficult to relate differences in risk to patterns of ICT usage. Improved measures of usage would help better explain e-crime vulnerability.
- We have no way of knowing whether the various threats posed by ICT are perceived by different users in the same way, or have the same impact on them.
- We know little about whether 'victims' of some of the e-crimes (for instance, of distasteful email messages and phone calls) were entirely 'innocent'. One recent survey found that many young mobile phone users admitted to committing offences themselves (NetSafe, 2005). This makes it difficult to know how to protect victims when they might sometimes prompt their own victimisation.

Future directions

The e-crime component in NZCASS 2006 was an exploratory exercise. In considering whether it should be repeated, there are four main considerations.

- Additional questions on patterns of ICT usage and on the nature of what happened would be required to add further value. However, further questions would have implications for the length of the survey questionnaire and this would need to be carefully considered.
- The Statistics NZ Household Use of ICT Survey will run every two years from 2006. If it continues to include the two questions on computer e-crime and the one on mobile phone harassment, this will provide a measure of trends in New Zealand. Further questions may also be added.
- A broader assessment of the scale of e-crime requires measurement across households and businesses (who may well bear bigger financial losses). Even though an accurate count of e-crime against businesses may prove difficult, the case for consistent across-sector measurement stands. This would argue for a more dedicated survey able to measure e-crime as it affects householders and businesses.
- Including e-crime questions in NZCASS raises the question as to whether and how they might be incorporated into the main crime count. The fact that neither the NCVS nor the BCS have merged e-crime counts with their main crime counts suggests there may be difficulties in doing this. Moreover, given the changes made to NZCASS 2006 that affected comparisons with the two previous surveys, further changes that affect the overall victimisation count are not advisable.

1 Introduction

This report presents results from questions in the 2006 New Zealand Crime and Safety Survey (NZCASS 2006) about what can be loosely grouped under a label of 'electronic crime' – e-crime hereafter. The questions were incorporated in the survey as a preliminary test of the extent of e-crime in New Zealand. They covered five forms of computer misuse, four forms of mobile phone misuse, and two forms of identity theft – i.e. the use of credit cards for theft, and the use of personal information to commit theft, fraud, or some other crime.

The e-crime questions were asked of all respondents who took part in NZCASS 2006. This was a nationally representative random sample of 4,229 people aged 15 and over in private households in New Zealand, together with a Māori 'booster' sample of 1,187 to improve reliability of findings for Māori. Those who took part were interviewed at home by ACNielsen interviewers between February and June 2006. One person per household was interviewed.

The main purpose of NZCASS 2006 was to measure the amount of crime in New Zealand in 2005 by asking people directly about crimes they had experienced. However, the e-crime questions stood apart from the main 'crime counting' questions. These concerned household crimes such as burglary and thefts of and from motor vehicles, and personal crimes such as robbery, assault and theft of personal property. Here, the survey aimed to provide an alternative measure of crime to Police statistics, by counting crimes both reported and not reported to the Police. Key findings from NZCASS 2006 in this regard can be found in Mayhew & Reilly (2007).[1]

The NZCASS 2006 also took the opportunity to ask those interviewed about a number of other crime-related issues, such as people's concern about crime. E-crime was one of the areas that it was felt useful to explore, albeit without incorporating the information gained into the main body of results on the victimisation experience of New Zealanders.

1.1 The coverage of e-crime in NZCASS 2006

Incidents of e-crime can be seen as crime facilitated by information and communication technology (ICT). ICT involves a range of electronic equipment (e.g., computers, mobile phones, digital cameras, or gaming devices) and modes of electronic information interchange and financial transactions.

There is no consistent or easy definition of e-crime, which is wide-ranging. The actual offence committed may be one of theft, fraud, harassment, or threat of violence, simply perpetrated through ICT. It may involve unauthorised access to a computer system (hacking); distributing software for the commission of a crime; or distributing an electronic virus designed to damage or access a computer system.

The definition of e-crime adopted by New Zealand Police is broader than that in the NZCASS e-crime module. The Police definition covers offences where ICT is:

- the tool used to commit an offence
- the target of an offence (e.g. someone hacks into a computer)

[1] The report can be found at http://www.justice.govt.nz/pubs/reports/2007/crime-safety-survey-2006/key-findings/index.html. Full details of how NZCASS was conducted can be found in Reilly and Sullivan (2007).

- the storage device used in an offence (e.g. images of child sex abuse).

The e-crime incidents measured in NZCASS were by no means exhaustive, but fall into four main groups. (The questions are shown in full in Appendix A.)

- Computer 'threats' – viruses,[2] worms, or spyware,[3] or hacking
- Offensive material – encountered on a web page, in emails, or over a mobile phone
- Fraud – purchases *via* computer believed to have involved fraud
- Identity theft – the use of credit cards for theft, and the use of personal information to commit a crime.

This is shown in more detail in Box 1.1.

Box 1.1 Types of incidents covered by the e-crime questions in NZCASS 2006

Computer misuse (asked of respondents with computers)

Computer threats

Affected by a virus, worm or spyware

Been hacked into without permission

Offensive material

Unintentionally encountered material on a web page that was highly offensive

Received email messages that said things that were harassing or threatening

Fraud

Bought something over the Internet or by email where there was a belief of fraud

Offensive material on mobile phones (asked of respondents with mobile phones)

Received a phone call or text message that said things that were highly offensive

Received a phone call or text message that was harassing or threatening

Phone used by someone else for a purpose that offended

Received a picture that was highly offensive

Identity theft (asked of all respondents)

Use of cards or card numbers without permission, for the purpose of theft (asked of those with credit cards, bank cards, Eftpos cards, etc.)

Use of personal information, without permission, to obtain new credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime (asked of all respondents)

[2] A computer virus (or worm) is a computer program that infects or modifies other programs, adding to or overwriting the code of files with a code that can infect other programs.

[3] Spyware is software that covertly gathers user information through the user's Internet connection without the user's knowledge. This is usually for advertising purposes.

For convenience, we use the term 'e-crime' to cover the full tally of incidents asked about in the survey. We acknowledge that the inclusion of identity theft as a form of 'e-crime' is somewhat debatable, since electronic transactions are not necessarily involved. It is also debatable whether all the incidents respondents were asked about merit the label of 'crime', especially as there is a degree of subjectivity involved in some incidents. For instance, a phone owner might have reported in the survey that someone used their phone for a purpose that offended them, whereas the user may not have intended to cause offence. Likewise, a picture received on a mobile phone that one phone owner found offensive may not be judged so by another owner. Buying goods over the Internet or by email where the buyer believed fraud had been involved could also perhaps cover the receipt of goods which did not quite match up to expectations. We retain the 'crime' label nonetheless.

Respondents were asked about e-crime incidents that happened between 1 January 2005 and the date on which they were interviewed. Given the duration of fieldwork – which ran from February 2006 until June 2006 – this means an average 'reference period' of 15.5 months. Table B1 shows the sample sizes, by different group, of those who answered the various e-crime questions.

What the questions do not cover

The e-crime questions were modest in scope. For instance, they do not:

- count how many times the incidents occurred. The e-crime questions only give a measure of how many people had experienced one or more incidents of the types asked about[4]
- give details of the incidents, such as the degree of upset they caused or the extent of monetary loss
- cover whether any of the incidents had been reported to the Police or other authorities
- collect information on what types of computer software users had installed that would help prevent infection by viruses, worms, spyware, or hacking
- establish how far risks are associated with the frequency and nature of use of computers, mobile phones and credit cards. More frequent use of these will increase exposure to risk, as might the manner in which they are used. For instance, those who do not buy goods over the Internet or via email will not leave themselves open to fraudulent transactions.

1.2 Police figures on e-crime

E-crime is particularly unlikely to come to Police attention. The victim may not be aware that an offence has taken place, or that what happened constitutes a crime. Incidents such as viruses seem very unlikely to be brought to Police attention. In the 2003/04 British Crime Survey (BCS) for instance, only 1% of those who had experienced a virus reported it to the Police (Wilson et al., 2006).

[4] For the items asked about which involved computers, it might be reasonable to think of the misuse as affecting the household as a whole, if the computer was for household use. However, it is possible that some forms of computer misuse were directed at the respondent, rather than the household. For this reason, we have treated all incidents asked about in the e-crime module as 'personal' incidents, including those involving computers. This means the raw data has been weighted to better represent New Zealand as a whole by the *personal weight* rather than the household weight. (Mayhew & Reilly (2007) explains weighting procedures.)

Added to this is that it is extremely difficult to establish the number of e-crime incidents recorded by the Police in New Zealand. There are no specific 'electronic' offences of fraud, theft, harassment, threats, or receipt of offensive material – although many such offences are covered by a number of general sections in the Crimes Act 1961.[5] Some seemingly specific e-crime offence codes exist ('computer crime,' for instance, under 'dishonesty – miscellaneous'). However, many other incidents fall within broad offences categories which do not specify modus operandi. Moreover, even for incidents which might fall within the scope of e-crime, it is often difficult to know whether businesses or householders were the target, except where the scene of the offence is recorded as a 'dwelling'.[6]

1.3 Other studies of e-crime

New Zealand

Notwithstanding the limitations mentioned above, the e-crime results from NZCASS 2006 are important in New Zealand as they provide up-to-date information about a number of e-crime problems. However, some other surveys are worth mentioning, and results are taken up from them below. There is more detail in Appendix C, but in brief, the other New Zealand surveys are:

- **Household Use of ICT Survey: 2006** (Statistics NZ, 2007). This asked about (i) computer viruses; (ii) fraudulent activity over the Internet; and (iii) mobile phone harassment. Experience was measured over the past 12 months. There are some subtle differences in coverage and question wording from NZCASS 2006, which limit exact comparisons.
- **A NetSafe survey of young mobile phone users** (NetSafe, 2005).
- **A NetSafe survey of young Internet users** (NetSafe, 2002).
- **An Auckland University survey** in mid-2004 (Curtis et al., 2004). This mainly looked at how people had accessed government information over the preceding 12 months, but it also explored New Zealanders' use of the Internet in general and took up experience of viruses, spam, and theft of bank details.

The surveys above all looked at personal users of ICT. There is one survey that looked at information on commercial experience (Quinn, 2005). It surveyed 218 computer security practitioners in New Zealand. They reported that a quarter of the organisations they covered had experienced unauthorised computer use, and that the number of incidents involving computer viruses had grown in particular.

Other countries

In other countries, there has been a fair degree of research on the extent and impact of e-crime among business users of ICT. In the UK, for instance, the Home Office's Commercial Victimisation Survey of retailers and manufactures covered computer hacking and Internet credit card fraud (see Shury et al., 2005). In the US, a new national survey has been mounted by the Bureau of Justice Statistics and the Department of Homeland Security to estimate the number of cyber

[5] The inclusion of ss248 to ss252 in the Crimes Act 1961 makes it clear that use of a computer is specifically covered. In ss253 and ss254, the Police and other relevant agencies are given qualified exemption to continue activities that would otherwise be illegitimate.

[6] In 2005, there were 362 incidents of 'computer crime' recorded by New Zealand Police. These largely refer to hacking incidents. Just over half (56%) of the incidents had 'dwelling' noted as the scene of the crime.

attacks, frauds, and thefts of information, and resulting losses against businesses. In Australia, an annual computer crime and security survey is carried out by Australian Computer Emergency Response Team (AusCERT), the Australian High Tech Crime Centre, and various state, territory and federal police agencies (AusCERT, 2005).

Householders as victims

Both the US National Crime Victimisation Survey (NCVS) and the British Crime Survey have looked at householders as victims of e-crime. Some results are referred to later. There is more detail about these two surveys in Appendix C. Neither of them gives precise comparative figures to NZCASS 2006 on all fronts, but they provide some pointers.

Box 1.2 Weighted data

Tables in this report are weighted to restore imbalances in the profile of those who responded to the survey relative to the survey population. The weighting takes into account gender, age, ethnicity and urbanisation. A further non-response adjustment accounts for different response rates by region and urbanisation. The weighting also adjusts for a household's probability of selection, and the under-representation of people living in larger households. The profile of the New Zealand population used for weighting comes from Statistics New Zealand's population estimates and projections, which are based on the 2001 Census.

While this weighting corrects for imbalances in the sample of people actually interviewed, it cannot account for all response bias. This is because the people who responded may differ in various respects from those who did not. For instance, they may differ as regards lifestyle or marital status – factors which were not corrected for during weighting.

Box 1.3 Statistical significance

Because NZCASS 2006 estimates are subject to sampling error, differences between population subgroups may occur by chance. Tests of statistical significance are used to identify which differences are reliable ones.[7] Only differences that are statistically significant at the 90% confidence level are reported. This is the level at which, if there was truly no difference, we would expect to see smaller differences than we have observed at least 9 times out of 10. However, most differences reported are statistically significant at the 95% confidence level – where there would be at least a 19 out of 20 chance of differences being smaller than the observed difference, if they were simply due to random sampling variation. The less stringent 90% test is used because the sample size is small for some groups (for example, young people). Reporting at this level increases the number of groups that can be compared.

While statistically significant differences could reflect real differences across surveys or across groups, they could also be caused by other methodological factors, including response bias and design changes.

Although a difference may not be statistically significant (e.g. it might just be due to random sampling variation), it may nevertheless be worth commenting on because the difference, if real, would have relevant policy implications.

[7] The significance tests used in this report allow for the complex multi-stage sample design used for the NZCASS. Tests that assume a simple random sample are not appropriate, as they would overstate the reliability of the results.

2 Computer misuse

2.1 The use of computers

Of those questioned, 68% said they used a computer at least monthly for personal use to access emails or the Internet. (Respondents were not asked whether this was the use of a computer at home, at work, or both.) This is reasonably close to the figure from the slightly later Household Use of ICT Survey: 2006 (Statistics NZ, 2007) (65%) measuring households with access to the Internet at home.

There was little difference between men and women in computer use, although those under 60 made appreciably more use of computers than those aged 60 or more. Asians were the most active computer users (83% used a computer at least monthly), followed by NZ Europeans (70%). Those in employment and students were more frequent users than others, as were those of higher socio-economic status as measured by the New Zealand Socio-Economic Index (NZSEI).[8] As might be expected, those in the most deprived quintile (fifth) of the country as measured by the NZ Index of Deprivation (NZDep) were less frequent users.[9] Māori and Pacific peoples were relatively infrequent users. So too were social renters,[10] and those in less densely populated areas of New Zealand.[11] These patterns of computer use are in line with the Auckland University survey (Curtis et al., 2004) for instance, insofar as results can be compared.

Table 2.1 shows the proportion of computer users who reported experiencing the various forms of computer misuse they were asked about once or more since the beginning of 2005.

[8] NZSEI is a scale that reflects the socio-economic status of people based on the occupation of the main income earner in their household. Each participant in NZCASS 2006 was given a score between 10 and 90 based on this occupation. These scores were then grouped into six ranges for presentation of the data in tables. The higher the score, the higher the socio-economic status.

[9] NZDep was developed by the Health Services Research Centre at the Ministry of Health. It is made up of a weighted average of nine census measures of socio-economic status and has become a standard measure of relative deprivation in New Zealand. The index divides New Zealand into equal tenths. A score of 10 indicates that a geographic area is in the most deprived 10% of all areas in New Zealand. For this report, the deciles have been reduced to quintiles (five parts) to make better use of sample numbers.

[10] Social renters is the term we use for people who rent from a local authority or the Housing New Zealand Corporation. Those who rented but refused to say who they rented from, who gave an 'other' response, or who did not know their landlord, are included among social renters.

[11] Less densely populated areas (with populations of 30,000 or less) are made up of secondary urban areas (with populations from 10,000 to 29,999) and minor urban and rural areas (the remaining areas). 'Other major urban areas' comprises metropolitan cities other than Auckland (i.e. Wellington, Christchurch) and other main urban areas (with populations of over 30,000).

Table 2.1 Prevalence of different forms of computer misuse 2005/06

Experienced once or more since beginning of 2005[1]	% of computer users
Computer threats	
Computer has been affected by a virus, a worm or spyware	53.1
Computer has been hacked into without your permission	5.9
Offensive material	
Unintentionally encountered material on a web page that you found highly offensive	15.2
Received email messages that said things you found harassing or threatening	10.4
Fraud	
Bought something over the Internet or by email where you believed you were a victim of fraud	1.7

Notes:

[1] Respondents were asked about incidents that happened between 1 January 2005 and the date on which they were interviewed – an average reference period of 15.5 months.

2.2 Computer threats

Viruses etc.

Just over half (53%) of computer users said they had been affected by a virus, a worm or spyware. It is difficult to have much confidence in this measure.

- On the one hand, respondents might have been affected without realising it.
- On the other hand, it is difficult to know how well the terms 'virus', 'worm' and 'spyware' were understood. Some respondents may have been thinking about email messages that came from an unreliable source, or 'phishing' scams when an email that looks like it comes from a bank, airline, etc. asks for personal details on the pretext that it can update its security measures.
- Estimates from other surveys also differ (see Appendix C). The NZCASS 2006 figure is rather lower than that reported in the Auckland University survey (Curtis et al., 2004) for receiving a virus (62%). However, it is about twice as high as that registered in the 2003/04 BCS (Wilson et al., 2006) – albeit the BCS question was restricted to viruses alone. The NZCASS 2006 figure is also three times higher than in the Household Use of ICT Survey: 2006 (Statistics NZ, 2007), which showed that 17% of those with Internet access had experienced loss or damage caused by 'a virus or similar' over the last year. The restriction to incidents that caused loss or damage may explain the lower figure than in NZCASS 2006. The NZCASS 2006 question gives no indication of whether incidents involved loss or damage and in the BCS about two-thirds of incidents did not do so.

Hacking

A much smaller proportion (6%) of computer users said their computer had been hacked, although it is possible that some users were not aware of this having happened. Again, this is a higher figure than in the 2003/04 BCS (2%) (Wilson et al., 2006).

Fraud

Among all computer users, 1.7% said they had bought something over the Internet or by email where they believed they were a victim of fraud. The proportion among those who had actually used the Internet or email for a purchase would be higher. (In the mid-2004 Auckland University survey [Curtis et al., 2004], just over half of respondents had not bought goods over the Internet in the last year.)

The question in the Household Use of ICT Survey: 2006 (Statistics NZ, 2007) survey is reasonably similar, although it specifies loss from Internet fraud. Nonetheless, the 1.1% of Internet fraud victims from the Statistics NZ survey is very similar to the NZCASS 2006 result.

2.3 Offensive material

Offensive web page material

Fifteen percent of computer users reported having unintentionally encountered material on a web page that they found highly offensive. This is lower than the 25% of those in the 2004/04 BCS (Wilson et al., 2006) who reported having accessed or received offensive or upsetting material via the Internet in the last year. The fact that the BCS question covered receipt of offensive material as well as an 'unintentional encounter' may be a factor here.

Harassing or threatening emails

One in ten computer users said they had received email messages that said things they found harassing or threatening. This is in line with the figure from the 2003/04 BCS (12%) which asked a similar question (Wilson et al., 2006). We do not know the nature of the emails received – in particular whether they were of a personal nature, or more widely directed, including some instances of spam.[12] The term 'harassing' might also have been quite widely interpreted – to denote a wide range of inbox messages that the user would have preferred not to have been sent.

2.4 Who was most at risk of computer misuse?

The types of people most at risk was not consistent across the five types of computer misuse asked about. Men, for instance, more often reported viruses, whereas women more often reported receiving harassing or threatening emails. The picture according to socio-economic status, as measured by NZSEI, was also erratic. Such differences in the patterns of misuse would be concealed in an overall measure of computer misuse. In addition, the overall measure would be dominated by the pattern for viruses. Therefore, it is not helpful to look at risk difference with an overall measure of computer misuse.

[12] Spam can be seen as the electronic equivalent of junk mail regularly received in the post and in newspapers and magazines (cf. McCusker, 2005). In the 2004 Auckland Survey (Curtis et al., 2004), 53% said they had received 'spam'. The figure seems rather low by current standards.

Rates for different groups of three of the five types of computer misuse are shown Table B2. Risk differences for those who had been hacked or bought something where they believed they were a victim of internet fraud are not shown in Table B2. For these measures, prevalence levels were low, which means that any differences between groups were difficult to detect as relative standard errors (RSEs) are above the level at which any confidence can be placed in the results.[13]

Some features of risk differences for the other three types of computer misuse are below.

- **Viruses.** More men (58%) than women (48%) reported having been affected by a virus, a worm or spyware. (Males were also more at risk in the Auckland University survey (Curtis et al., 2004). Students were also more likely to report viruses, worms or spyware, as were those in the second highest of the NZSEI bands. In terms of lower risk, fewer of the elderly, those living alone, and the retired said they had been affected by a virus, as did those in the most deprived areas in the country. Pacific peoples also fell into the low-risk group, although caution is needed here on statistical grounds. Differences in computer usage may play a part in these results, with more frequent computer users perhaps being more aware of the effect of viruses, etc. There may also be different understandings as to what counts as a virus, a worm or spyware.

- **Offensive web material.** Those aged 15-24 less often encountered offensive web material than other age groups, as did flatmates, and Pacific peoples. Māori were rather more likely to encounter offensive material. Patterns in terms of socio-economic status were not very robust, but tended to indicate that higher status groups encountered offensive material more often than lower status groups. All these results may reflect differences in thresholds for what is considered offensive.

- **Harassing emails.** More women (12%) than men (9%) had received email messages that they found harassing or threatening. (The BCS found no gender difference.) Those aged 40-49 more often reported receiving harassing or threatening emails. In the BCS, those of higher socio-economic status were more often victimised, and there was also some evidence of this in NZCASS 2006 insofar as those in the second and third highest NZSEI bands (though not the highest) more often reported harassing or threatening emails, as did those in the least deprived areas of New Zealand, and in Auckland. Again, it is difficult to say whether different sensibilities regarding the nature of emails play a part in these results.

[13] Most RSEs exceed 15%. The RSE is obtained by dividing the standard error of the estimate by the estimate itself; it is then expressed as a percentage of the estimate.

3 Mobile phone misuse

3.1 The use of mobile phones

Of those questioned, 79% said they used a mobile phone at least monthly for personal use. Given the rapidly expanding use of mobile phones, comparisons with other sources of data are not helpful. In the Household Use of ICT Survey: 2006 (Statistics NZ, 2007) though, 80% said they had personal use of a mobile phone over the past year.

The picture of who are the most frequent users of mobile phones is not unexpected: those aged 15-39, Asians, those in employment, students, those of higher socio-economic status, those in the less deprived areas of New Zealand, and those in Auckland.

3.2 Mobile phone misuse

Table 3.1 shows the proportion of respondents who reported the various forms of mobile misuse they were asked about. Again, the figures relate to incidents from the beginning of 2005 until the interview in 2006. As with computer misuse, exposure to unwelcome forms of mobile phone use is likely to depend on the extent and patterns of phone usage. As said, there were no NZCASS 2006 measures of levels of phone usage. Those who have phones with cameras will also be more likely to receive offensive pictures.[14]

Eight percent of users had received a call or text that said things they found highly offensive. A smaller proportion (5.3%) had received a call or text that was considered harassing or threatening – fairly close to the 3.7% from a slightly more restricted question in the Household Use of ICT Survey: 2006 (Statistics NZ, 2007). Even fewer (2.5%) had had their phone used in a way that offended them, and 1.3% had received a picture they considered highly offensive.

Table 3.1 Prevalence of different forms of mobile phone misuse 2005/06

Experienced once or more since beginning of 2005[1]	% of phone users
Received a phone call or text message that said things that were highly offensive	8.0
Received a phone call or text message that was found harassing or threatening	5.3
Phone used by someone else for a purpose that offended	2.5
Received a picture that was highly offensive	1.3
Any of the above	12.1

Notes:

1 Respondents were asked about incidents that happened between 1 January 2005 and the date on which they were interviewed – an average reference period of 15.5 months.

[14] Pretesting on this question demonstrated that text and numbers can be formed into pictures – some of which were considered offensive.

The 2002/03 BCS also had a question that subsumes the first and second item in Table 3.1, showing a rate of 9% among phone users – similar to the NZCASS 2006 results. In the NetSafe (2005) survey of young mobile phone users, 23% of phone users said that they had received an offensive, pornographic, abusive or threatening text or picture on their phone.

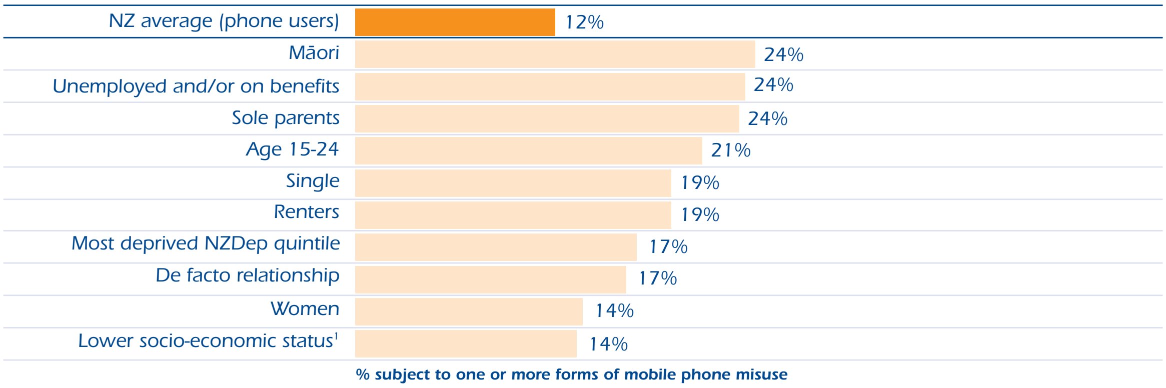
3.3 Who was most at risk of mobile phone misuse?

Differences between groups were generally consistent across the four types of mobile phone misuse. However, since few people had a phone used in a way that offended or received an offensive picture, reliable differences between different groups are difficult to detect because of large RSEs. The greater similarity of risk patterns for mobile phone misuse may be because the items were more similar in type than was the case for the computer misuse items.

Rates for offensive calls or texts, phone harassment or threats, and any mobile phone misuse experienced by different groups are in Table B3. The main higher-risk groups are below (see also Figure 3.1).

- Māori reported higher levels of phone misuse than others did. Pacific peoples did so too, although the small number in the sample prevents the results from reaching statistical significance. Asians reported the lowest rates, but again numbers are too small to be confident about this.
- Those who were unemployed and/or on benefits experienced more phone misuse than others, as did sole parents.
- Those aged 15-24 experienced more phone misuse, which tended to decrease with age. The overall average was 12%, but 21% of those aged 15-24 reported one or more types of misuse, whereas only 4% of those aged 60 or over did so. In the 2002/03 BCS, young users also reported more phone misuse.
- Single people reported more misuse, although there will be an overlap with age here.
- People who rented their homes also reported more misuse than homeowners.
- Those living in the most deprived quintile of the country also experienced more phone misuse than those in other quintiles.
- Those in the lower NZSEI bands reported more phone misuse than those in higher status groups.
- Women reported more phone misuse than men did, especially for calls and texts that were offensive, and for harassing calls or texts. Women were also more vulnerable in the BCS on these measures.

Figure 3.1 Those at higher risk of mobile phone misuse 2005/06



Notes:

1 Those in groups NZSEI 10-39.

The percentages at the end of the bars are based on unrounded numbers, which is why the length of the bars can differ somewhat.

Respondents were asked about incidents that happened between 1 January 2005 and the date on which they were interviewed – an average reference period of 15.5 months.

4 Identity theft

This section looks at the two remaining e-crime questions – whether from the beginning of 2005 until the time of the interview, someone had:

(i) used a card or card number, without permission, to steal from the respondent

(ii) used personal information about the respondent without their permission to obtain new credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime.

Taken together, these two items can be seen as equating with identify theft, although there will be other forms of this. First, we deal briefly with each of the items in turn.

4.1 Card use and misuse

Card use

Of those questioned, 94% said they used a credit card, bank card or debit card. (The question related to the three types of cards taken together.) Other estimates of use of this range of cards are difficult to come by, but the NZCASS 2006 figure seems plausible given current financial payment patterns. As one would expect, card use was lowest among those aged 15-24, students, single people (who will be younger), social renters, those of lower socio-economic status, and those living in the most deprived quintile of the country. Card use was also rather lower among non-NZ Europeans.

The extent of card misuse

Of card users, 2.3% said that since 1 January 2005 somebody had used a credit, bank or debit card or card number, without permission, to steal from them. There was no information collected on how this happened, but it could have involved the card being stolen; the card being lost; 'card-not-present fraud' (including fraud conducted over the Internet or by telephone, fax or mail order); or a card being stolen in the course of mail delivery. In the 2003/04 BCS, one-fifth of card fraud was the result of cards being stolen or lost.

The BCS question is reasonably similar to that in NZCASS 2006. Four percent of card users reported in the 2005/06 BCS that over the last year someone had used their credit or bank cards, or their card details, to buy things or withdraw cash (Hoare & Wood, 2007). The BCS figure is statistically significantly higher than the NZCASS 2006 result.

Risk differences in card misuse

Table B4 shows risks of card misuse for different groups. It is important to note, however, that the low prevalence level for card misuse (2.3% overall), combined with small sample numbers in some groups, make it unwise to take apparent differences at face value.

4.2 Misuse of personal information

Among the NZCASS 2006 sample, 1.1% reported that someone had used personal information about them – without their permission – to obtain new credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime.

Risk differences in misuse of personal information

The small numbers affected overall again mean that differences in risks for sub-groups are statistically fragile. Therefore, it is difficult to be certain about the extent of any real distinction between these groups. (See Table B4.)

4.3 Any identity theft

Overall, 2.8% reported that one or the other of the two forms of identify theft they were asked about had occurred once or more since the beginning of 2005. This equates to about 93,000 New Zealanders aged 15 or more in private households. The estimate from the American NCVS was very similar (3%), albeit based on a slightly broader range of 'screener' questions, but referring to a shorter period of six months.

In NZCASS 2006, 0.4% of respondents reported *both* forms of identity theft – too small a group on which to comment.

While NZCASS 2006 did not ask about problems that arose as a result of identity theft, the NCVS showed that a third of victimised households experienced one or more problems as a result (Baum, 2006). The most common problems included being contacted by a debt collector or creditor, banking problems, or problems with credit card accounts. About two-thirds of households experiencing identity theft reported some type of monetary loss as a result.

4.4 Who was most at risk of identify theft?

The pattern for both forms of identity theft was fairly similar. Taking the two forms together gives a slightly more reliable base for looking at differences between groups. Even so, risk differences are statistically weak. The figures are in Table B4.

The results indicate a number of risk differences.

- Those aged 60 or more were less likely to experience identity theft (1.9% did so against 3.1% for other age groups). Lower risks for the elderly were also found in the 2003/04 BCS.
- Māori reported a higher level of identity theft (4.2%). Non-NZ Europeans as a whole were more at risk, but the figures for Pacific peoples and Asians on their own are unsound. (The 2003/04 BCS also found that non-whites in England and Wales were more often victimised.)
- Social renters were at greater risk (5.6%).
- So too were those who were unemployed and/or on a benefit (4.3%).
- Those who were divorced or separated seemed to experience more identity theft (4.5%).
- So too did those living in Auckland (3.7%).

Some of these risk characteristics overlap. The unemployed and those on benefits, for instance, are more often social renters, and Māori are overrepresented in both groups (Mayhew & Reilly, 2007). It cannot be known whether receipt of benefits provides opportunities for others to take advantage.

In NZCASS 2006, there was no evident pattern of risk in relation to socio-economic status, although in the NCVS in the United States (Baum 2006) and the 2003/04 BCS in England and Wales (Wilson et al., 2006) those in higher income brackets emerged as most likely to experience identity theft. Rural households in the United States were less likely than urban or suburban households to have a member experience identity theft, but in NZCASS 2006 there was no similar pattern evident. The larger sample sizes in the US and England and Wales surveys may provide sounder results.

A review of research evidence on identity theft found that victims were most likely to be victimised by people who have access to their identifying information, such as family members and those sharing living quarters (Newman and McNally, 2005). The review also found that most of the ways in which offenders use other people's identities are relatively unsophisticated, and that offline theft is much more common than online identity theft.

5 Concern about e-crime

It is clear that e-crime causes concern to New Zealanders. NZCASS 2006 only asked people whether they were worried about having credit cards misused, but a recent Unisys survey of public perceptions towards security covers this and other e-crime areas (Unisys, 2007).

In NZCASS 2006, 23% of respondents said they were very worried about having a credit card misused, and 30% said they were fairly worried. These figures were on a par with worry about having a car stolen, and not far behind worry about being the victim of a traffic accident caused by a drunken driver, being burgled, and having a car vandalised. Those who were most worried about credit card misuse were women, young men aged 16-24, those in minority ethnic groups, students, and beneficiaries.[15] With the exception of women, those in the 'most worried' groups had some justification for their concern, given that their risks were higher than average – even though small. Levels of worry about credit card misuse in New Zealand according to NZCASS 2006 were a little a little lower than those in England and Wales according to the 2005/06 BCS (Hoare & Wood, 2007).[16]

In the Unisys (2007) survey of a representative sample of New Zealanders aged 18 or more in April 2007, 56% were 'very' or 'extremely concerned' about other people obtaining or using their credit card – a little higher than the NZCASS 2006 figures (53%). The Unisys survey showed that 53% were concerned about other people having unauthorised access to, or misusing personal information about them, while just under a third were concerned about viruses and unsolicited email, and about security when shopping or banking on line.

While the figures for 'worry' or 'concerned' are high, contrasting these with much lower levels of actual risk to conclude that people are 'more worried or concerned than they should be' is not necessarily sensible. Worry may be a rational response to the *consequences* of victimisation, rather than the risk. Even if the statistical risk is low, people may still justifiably worry because of the potentially distressing upset *if* an e-crime incident occurs.

[15] In the NZCASS question about worry about credit card misuse, 14% said it was not applicable to them – presumably because they had no credit card. This is a higher figure than the 6% in the e-crime questions who said they did not have a credit, bank or debit card. The fact that the e-crime question referred to all three types of cards, not just credit cards, is likely to explain this.

[16] In NZCASS, 53% were very or fairly worried, whereas the figure in the BCS was 57%. The BCS question, however, asked about both credit cards and bank cards.

6 Overview

ICT involves a range of electronic equipment and modes of electronic information and financial interchange. It is now well recognised by providers and users that ICT has spawned a variety of types of crime and abuse, and ways of committing crimes and abuse that were not necessarily foreseen (see, for example, Choo et al., 2007). The research literature in the field has grown apace, and it is not the intention to review it here. Apart from anything else, it covers areas of ICT crime and misuse that stretch far beyond the interests of the e-crime module in NZCASS 2006.

6.1 Implications of the findings

A reasonable question is whether the present results have implications for policies to deal with e-crime. In limited respects, they do.

First, they give an indication of the scale of some forms of e-crime in New Zealand.

- Being affected by viruses, worms and spyware is the most common experience among computer users, with just over half of them affected at least once in a period of about 15-16 months on average. It is seems likely from other studies, though, that the majority of these incidents caused no loss of data or computer damage.
- Fifteen percent of computer users had encountered offensive material on web pages.
- One in ten computer users had received harassing or threatening email messages, although we do not know how personal in nature these were.
- Just under one in ten mobile phone users had received offensive calls and texts on their mobile phone – these being more likely to be personally directed.
- One in twenty mobile phone users had received harassing or threatening calls or texts on their mobile phones.
- Other forms of e-crime were relatively uncommon, but the more serious threat of identity theft affected just under 3% of those in NZCASS 2006.

Secondly, the results give some indication of the types of ICT users who faced the highest risks. Four points are of note.

- **Different forms of computer misuse.** The various forms of computer misuse did not affect different groups in a consistent way. It may be that differences in computer usage play a part in that more frequent computer users are more aware of viruses and hacking, for instance. And some people may be more sensitive than others about unwanted offensive web material or the nature of emails. But there was no very clear pattern.
- **Unwelcome emails.** These were reported more often by women, older people and those of higher socio-economic status. It is difficult to say whether different sensibilities explain this.
- **Ethnicity.** Māori tended to report more e-crime. The picture for Pacific peoples was often in the same direction, but the small number of Pacific peoples in the NZCASS 2006 sample means we cannot be sure about this.

- **Social deprivation.** A number of indicators suggested that those in more stretched circumstances experienced more phone misuse and identity theft, which may carry more serious financial consequences. The results here echo analysis of other victimisation risks that NZCASS 2006 measured (Mayhew & Reilly, 2007).

It should be recognised, though, that the policy implications of the present results are modest in other respects. The main reasons follow from what has already been said.

- It is difficult to relate differences in risk to patterns of ICT usage. Better measures of usage would help explain e-crime vulnerability better.
- We have no way of knowing whether the various threats posed by ICT are perceived by different users in the same way – or have the same impact on them. There was no information collected to shed light on this.
- We know little about whether 'victims' of some of the e-crimes (for instance, of distasteful email messages and phone calls) were entirely 'innocent'. They could have themselves engaged in similar behaviour to offenders. The NetSafe survey of young mobile phone users, for instance, showed that about half of 'victims' who received offensive, abusive or threatening material on their phones admitted to sending the same (NetSafe, 2005). This makes it difficult to know how to protect victims when they might sometimes prompt their own victimisation.

6.2 Implications for NZCASS

The e-crime component of NZCASS 2006 was intended as a preliminary measure of the extent of e-crime in New Zealand. No decision has been made as to whether the module will be repeated, either in its present or in a revised form. Four considerations will influence future directions.

- To get better value from e-crime questions in understanding relative risks, the survey requires additional questions on different patterns of ICT usage and on the nature of incidents. This is problematic given that space in the questionnaire is already at a premium.
- The Statistics NZ Household Use of ICT Survey will run every two years from 2006. This includes two questions on computer e-crime and one on mobile phone harassment. If these are retained or added to, they will provide a measure of trends in New Zealand.
- While it has been useful to get a picture of the extent of some sorts of e-crime against householders, a broader assessment of the scale of the problem requires measurement among businesses (which may well bear bigger financial losses). This would argue for a more dedicated survey that was able to measure e-crime as it affects householders and businesses.
- Including e-crime questions in NZCASS raises the question as to whether and how they might be incorporated into the main crime count. The fact that neither the NCVS nor the BCS have merged e-crime counts with those for other crimes points to difficulties. One difficulty is that it is not known how far some of the e-crime incidents in the e-crime module were also picked up in the main victimisation screening components, relating to threats for instance. Even more important is that changes made to NZCASS for 2006 affected comparisons with the two previous surveys, and further changes that may affect the overall victimisation count are not advisable.

References

Allen, J., Forrest, S., Levi, M., Roy, H. & Sutton, M. (2005). *Fraud and technology crimes: Findings from the 2002/03 British Crime Survey and the 2003 Offending, Crime and Justice Survey.* Home Office Online Report No. 34/05. London: Home Office.

Australian Computer Emergency Response Team (AusCERT). (2005). *Australian computer crime and security survey.* Brisbane: Author.

Baum, K. (2006). *Identity theft, 2004: First estimates from the National Crime Victimization Survey.* Bureau of Justice Statistics Bulletin. NCJ 212213. Washington, DC: Bureau of Justice Statistics, U.S. Department of Justice.

Cantor, D., & Lynch, J. P. (2000). Self-report surveys as measures of crime and criminal victimization. In *Criminal Justice 2000: Measurement and analysis of crime and justice: Vol. 4.* Washington, DC: United States Department of Justice.

Choo, R., Smith, R. & McCusker, R. (2007). *The future of technology-enabled crime in Australia.* Trends and Issues No. 341. Canberra: Australian Institute of Criminology.

Curtis, C., Vowles, J. & Curtis, B. (2004). *Channel-surfing: How New Zealanders access government.* Prepared for the State Services Commission. Auckland: Auckland University Survey Research Unit.

Hoare, J. & Wood, C. (2007). Plastic card and identity fraud. In J. Flatley (Ed.), *Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey.* Home Office Statistical Bulletin 10/07. London: Home Office.

Mayhew, P. & Reilly, J. (2007). *The New Zealand Crime and Safety Survey 2006: Key Findings.* Wellington: Ministry of Justice.

McCusker, R. (2005). *Spam: Nuisance or menace, prevention or cure?* Trends and Issues No. 294. Canberra: Australian Institute of Criminology.

NetSafe (Internet Safety Group). (2005). *The text generation: Mobile phone and New Zealand youth.* Auckland: Author.

NetSafe (Internet Safety Group). (2002). *Internet safety issues for young New Zealanders.* Auckland: Author.

Newman, G. & McNally, M. (2005). *Identity theft literature review.* Final report to the National Institute of Justice. NCJ 210459. Washington, DC: National Institute of Justice.

Quinn, K. J. S. (2005). *New Zealand computer crime and security survey.* Dunedin: Alpha-Omega Group.

Reilly, J. and Sullivan C. (2007). *The 2006 New Zealand Crime and Safety Survey: Technical Report.* http://www.justice.govt.nz/pubs/reports/2006/crime-safety-survey-2006/technical-report/index.html

Shury, J., Speed, M., Vivian, D., Kuechel, A. & Nicholas, S. (2005). *Crime against retail and manufacturing premises: Findings from the 2002 Commercial Victimisation Survey.* Home Office Online Report No. 37/05. London: Home Office.

Statistics New Zealand. (2007). *Household use of information and communication technology, 2006.* Wellington: Author.

Unisys (2007). *Unisys Security Index New Zealand.* A Consumer Link Survey April 2007. Wellington: Author.

Wilson, D., Patterson, A., Powell, G. & Hembury, R. (2006). Fraud and technology crimes: *Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources.* Home Office Online Report 09/06. London: Home Office.

Appendix A
The NZCASS 2006 questions on e-crime

The e-crime questions in NZCASS 2006 were located in the questionnaire as shown in Box A1. The e-crime questions, asked of all respondents, were in a self-contained module. Further details of the content and structure of the NZCASS 2006 questionnaire are in Mayhew & Reilly (2007).

Box A1 Main topics covered in NZCASS 2006

1 Main questionnaire ▪ Attitudes to local crime and incivilities ▪ Concern about crime ▪ Confidence in the criminal justice system ▪ Neighbourhood Support ▪ Victimisation 'screener' questions-to ascertain experience of household and some personal crimes	**4 Demographic questionnaire** Age, household type, ethnicity, tenure, employment status, marital status, etc.
2 Victim Form (details of victimisation incidents)	**5 Self-completion I – Offences by partners**
3 Experience of e-crime	**6 Self-completion II – Offences by people well-known**
	7 Self-completion III – Sexual victimisation

The precise wording of the e-crime questions is in Box A2. Respondents could answer yes or no, and they were allowed the option of refusing to answer (although very few refused).

Box A2 The e-crime questions NZCASS 2006

Q1 The following questions are about any misuse of computers, mobile phones and credit cards. Do you use a computer for emails or accessing the Internet at least monthly for your personal use?

Q2 *(If yes at Q1).* Using [this] showcard, as far as you know, have any of the following affected your personal use of a computer since 1 January 2005?

- The computer has been affected by a virus, worm or spyware.
- The computer has been hacked into without your permission.
- You bought something over the Internet or by email where you believe you were a victim of fraud.
- On a web page, you unintentionally encountered material that you found highly offensive.
- You received email messages that said things that you found harassing or threatening.

Q3 Do you use a mobile phone at least monthly for your personal use?

Q4 *(If yes at Q3).* Using [this] showcard, have any of the following affected your personal use of a mobile phone since 1st January 2005?

- The mobile phone has been used by someone else for a purpose that offended you.
- You have received a phone call or text message that said things that you found highly offensive.
- You have received a picture that you found highly offensive.
- You have received a phone call or text message that you found harassing or threatening.

Q5 Do you use a credit card, bank card or debit card, for example Eftpos?

Q6 *(If yes at Q5).* Since 1 January 2005 has somebody used any of your cards or numbers, without permission, to steal from you?

Q7 Since 1 January 2005, has somebody used personal information about you without permission to obtain new credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime?

Notes:

1 For questions 2 and 4, a showcard was handed to the respondent for them to see the questions that were being asked.

Appendix B Supplementary tables

Table B1 Sample numbers

	Computer users	Mobile phone users	Card users	All respondents
Gender				
Male	1334	1639	2012	2199
Female	1908	2415	3050	3217
Age				
15-24	461	625	598	695
25-39	1007	1297	1390	1441
40-59	1264	1507	1797	1850
60 or older	508	619	1270	1423
Ethnicity[1]				
European	2476	2909	3675	3897
Māori	832	1319	1568	1698
Pacific peoples	93	167	196	220
Asian	219	238	258	276
Marital status				
Legally married	1628	1830	2262	2363
De facto relationship	478	656	740	765
Single/never married	685	978	1045	1174
Widowed	123	147	423	492
Divorced/separated	317	426	568	595
Household composition				
One person living alone	351	453	850	945
Sole parent	281	439	482	517
Couple/no children	876	1018	1344	1412
Couple/children	1154	1330	1423	1505
Extended family/whānau	175	283	358	397
Flatmates	160	199	218	226
Family – other combination	192	268	318	337

	Computer users	Mobile phone users	Card users	All respondents
Employment status				
Employment or self-empl'd	2192	2591	2890	2979
Home duties	200	270	312	331
Retired	291	368	922	1045
Unemployed and/or on benefits	245	453	595	643
Student	280	319	280	350
Tenure				
Owned	2246	2559	3278	3482
Private renters	736	1041	1172	1243
Social renters[2]	168	332	455	523
NZSEI				
NZSEI 70-90 (high status)	411	404	455	471
NZSEI 60-69	455	475	577	597
NZSEI 50-59	762	827	958	993
NZSEI 40-49	558	775	959	1029
NZSEI 30-39	461	695	878	961
NZSEI 10-29	376	589	849	941
NZ Index of Deprivation				
Quintile 1 (least deprived)	645	690	815	845
Quintile 2	608	695	853	881
Quintile 3	651	762	972	1045
Quintile 4	688	863	1101	1188
Quintile 5 (most deprived)	650	1044	1321	1457
Urbanisation				
Auckland	816	982	1149	1215
Other major urban areas	1392	1705	2135	2287
Less densely populated areas	1034	1367	1778	1914
All respondents	**3242**	**4054**	**5062**	**5416**

Notes:

1 Ethnicity is multiple response, so sample numbers add to more than the total sample. Europeans comprise those who said they were New Zealand European and a much smaller proportion who said they belonged to another European ethnic group or gave 'New Zealander' as their response.

2 Social renters predominantly rent from a local authority or the Housing New Zealand Corporation. Those who rented but refused to say who they rented from, who gave an 'other' response, or who did not know their landlord, are included among social renters.

These are the unweighted sample sizes for different groups in NZCASS 2006. Some categorisations are chosen to ensure that the sample size in any one group is not too small for reliable analysis.

Table B2 NZCASS 2006 estimates of computer misuse for different groups

% experienced once or more since the beginning of 2005 (prevalence rate)

	Virus, worm or spyware	Offensive web material	Harassing/ threatening emails
Gender			
Male	58	16	9
Female	48	14	12
Age			
15-24	55	10*	8*
25-39	56	17	11
40-59	55	18	12
60 or older	38	13	9
Ethnicity			
European	54	16	11
Māori	56	19	10
Pacific peoples	35*	7*	2*
Asian	51	12	10
Marital status			
Legally married	53	16	11
De facto relationship	50	17	12
Single/never married	56	13	8
Widowed	29*	13	8
Divorced/separated	55	14	9
Household composition			
One person living alone	43	16	9
Sole parent	52	19*	11
Couple/no children	44	15	11
Couple/children	60	16	11
Extended family/whānau	51	16	11
Flatmates	51	9*	5*
Family – other combination	53	16	8*

	Virus, worm or spyware	Offensive web material	Harassing/ threatening emails
Employment status			
Employment or self-empl'd	54	16	11
Home duties	47	16	14*
Retired	33	11*	9
Unemployed and/or on benefits	55	19*	6*
Student	60	12*	9
Tenure			
Owned	53	15	11
Private renters	53	16	7
Social renters	48	14	10
NZSEI			
NZSEI 70-90 (high status)	52	19	10
NZSEI 60-69	58	16	14*
NZSEI 50-59	53	18	13
NZSEI 40-49	54	11*	9
NZSEI 30-39	51	16	7
NZSEI 10-29	49	11*	10
NZ Index of Deprivation			
Quintile 1 (least deprived)	52	16	13
Quintile 2	55	15	11
Quintile 3	53	15	10
Quintile 4	56	14	8
Quintile 5 (most deprived)	47	16	10
Urbanisation			
Auckland	53	14	13
Other major urban areas	54	17	9
Less densely populated areas	51	14	10
All respondents	**53**	**15**	**10**

Notes:

* Denotes a RSE of 15% or more. These are shown for differences in risk which appear larger or smaller than the average. This means the risk figure should be viewed with caution.

Table B3 NZCASS 2006 estimates of mobile phone misuse for different groups

% experienced once or more since the beginning of 2005 (prevalence rate)

	Call or text found highly offensive	Call or text found harassing/ threatening	Any mobile phone misuse[1]
Gender			
Male	6	4	10
Female	10	6	14
Age			
15-24	15	10*	21
25-39	9	7	14
40-59	5	3	8
60 or older	2*	1*	4*
Ethnicity			
European	7	5	11
Māori	18	11	24
Pacific peoples	13*	6	19*
Asian	6	3	9
Marital status			
Legally married	4*	2	7
De facto relationship	10	9*	16
Single/never married	14	8	19
Widowed	7	1*	10
Divorced/separated	8	9	13
Household composition			
One person living alone	8	4	11
Sole parents	17	11*	24
Couple/no children	4	3	7
Couple/children	7	5	11
Extended family/whānau	14*	7	21*
Flatmates	14*	7	18*
Family – other combination	7	5	10

	Call or text found highly offensive	Call or text found harassing/ threatening	Any mobile phone misuse[1]
Employment status			
Employment or self-empl'd	6	4	10
Home duties	10	3	12
Retired	2	1*	3*
Unemployed and/or on benefits	18	14*	24
Student	13*	9	19*
Tenure			
Owned	6	4	9
Private renters	14	9	19
Social renters	13*	6	19
NZSEI			
NZSEI 70-90 (high status)	5	2	7*
NZSEI 60-69	6	3	10
NZSEI 50-59	7	5	11
NZSEI 40-49	8	5	13
NZSEI 30-39	11*	6	13
NZSEI 10-29	9	8	14
NZ Index of Deprivation			
Quintile 1 (least deprived)	5*	3	8*
Quintile 2	7	5	10
Quintile 3	9	5	13
Quintile 4	8	6	13
Quintile 5 (most deprived)	12	7	17
Urbanisation			
Auckland	9	5	13
Other major urban areas	8	5	12
Less densely populated areas	7	6	11
All respondents	**8**	**5**	**12**

Notes:

1 Based on all mobile misuse items (see Table 3.1).

* Denotes a RSE of 15% or more. These are shown for differences in risk which appear larger or smaller than the average. This means the risk figure should be viewed with caution.

Table B4 NZCASS 2006 estimates of identity theft for different groups

	Cards used for theft[1]	Personal information used for crime[2]	Any mobile phone misuse[1]
% experienced once or more since the beginning of 2005 (prevalence rate)			
Gender			
Male	2.2	1.0	2.7
Female	2.3	1.3	3.0
Age			
15-24	3.6*	1.2	3.7*
25-39	2.3	1.4*	3.0
40-59	2.1	1.2	2.9
60 or older	1.5	0.8*	1.9*
Ethnicity			
European	2.0	0.9	2.5
Māori	3.0*	2.2*	4.2*
Pacific peoples	2.6*	2.2*	3.4
Asian	3.1	1.0	3.6*
Marital status			
Legally married	2.0	0.9	2.6
De facto relationship	2.6*	1.9*	3.5*
Single/never married	2.6*	1.0	2.6
Widowed	1.5*	1.0	2.1
Divorced/separated	3.0*	2.2*	4.5*
Household composition			
One person living alone	1.4*	0.7	0.7*
Sole parents	2.8*	2.1*	2.1*
Couple/no children	2.2	1.0	1.0*
Couple/children	2.4	1.1	1.1*
Extended family/whānau	2.6*	1.8	1.8*
Flatmates	3.1*	0.5*	0.5*
Family – other combination	1.6*	1.4	1.4*
Employment status			
Employment or self-empl'd	2.3	1.1	2.9
Home duties	2.1	1.4	2.9
Retired	1.6*	0.6	1.9*
Unemployed and/or on benefits	2.8*	3.0*	4.3*
Student	2.8*	0.7	2.9
Tenure			
Owned	2.2	0.8	2.6
Private renters	2.0	1.3	2.7
Social renters	4.2*	3.9*	5.6*
NZSEI			
NZSEI 70-90 (high status)	2.7*	0.8	2.8
NZSEI 60-69	3.0*	0.9	3.6*
NZSEI 50-59	2.3	0.8	2.9
NZSEI 40-49	2.4	1.5*	3.2
NZSEI 30-39	1.7*	1.1	1.9*
NZSEI 10-29	2.0	1.4	2.8
NZ Index of Deprivation			
Quintile 1 (least deprived)	3.4*	1.1	3.8*
Quintile 2	1.9	0.6*	2.1
Quintile 3	1.4*	0.9	2.1
Quintile 4	1.9	1.5	2.8
Quintile 5 (most deprived)	2.7*	1.6*	3.4*
Urbanisation			
Auckland	3.5*	1.1	3.7*
Other major urban areas	1.4	1.2	2.1
Less densely populated areas	2.3	1.2	2.9
All respondents	**2.3**	**1.1**	**2.8**

Notes:

1 Based on the question 'Since 1 January 2005, has somebody used any of your cards or numbers, without permission, to steal from you?'

2 Based on the question 'Since 1 January 2005, has somebody used personal information about you without permission to obtain new credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime?'

3 Either of the previous two items.

* Denotes RSE of 15% or more. These are shown for differences in risk which appear larger or smaller than the average. This means the risk figure should be viewed with caution.

Appendix C Other estimates

Box C1 shows other New Zealand surveys which have covered some of the same e-crime ground as NZCASS 2006.

Box C1 Other New Zealand surveys of personal ICT users

	Source	Sample	Relevant coverage	Referred to as
Household Use of Information and Communications Technologies (2006)	Statistics New Zealand (2007)	c. 15,000 households and 30,000 individuals. (Supplement to the Household Labour Force Survey.)	See text below Virus (causing loss/ damage) Internet fraud (causing financial loss) Harassing/threatening mobile text, pixt or other messages	Household Use of ICT Survey: 2006
NetSafe mobile phone users surveys	NetSafe (2005)	c. 1,500 decile 4 high school pupils aged 12-19	Own and others' crime and harassment	The NetSafe young mobile phone users survey
NetSafe Internet users surveys	NetSafe (2002)	c. 2,600 pupils in primary, intermediate and secondary schools in Auckland	Broad crime and safety issues	The NetSafe young Internet users survey
Auckland University survey of access to government information	Curtis et al. (2004)	Telephone survey of 5,000 respondents aged 18 or older (mid-2004).	Virus; spam; theft of bank details (phone or email)	The Auckland University survey

Statistics New Zealand survey

Probably the most important other New Zealand survey is by Statistics New Zealand, carried out in the last quarter of 2006 (Statistics New Zealand, 2007). With a large sample size, its main purpose was to collect information from New Zealand households and individuals about the access to and use of ICT. It included three questions on e-crime over the previous 12 months.

- Whether *someone* in the household experienced loss of data, time and/or damage to the *household* computer because of a virus or something of a similar nature. This is most equivalent to Question 1 in the NZCASS 2006 e-crime module (see Box 1.1), although the latter does not mention damage or loss of time or data. The Statistics New Zealand survey also refers to anyone in the household, rather than just the respondent (as in NZCASS 2006), and to a *home computer*, rather than any computer the respondent might have used, as in NZCASS 2006. (The question was in the household questionnaire and was completed by one member of the household.)
- Whether an individual home computer user had been victim of a fraudulent activity that resulted in some loss (e.g. money). This is most similar to Question 9 in the NZCASS 2006 module.

- Whether an individual mobile phone user had received text, pixt or other messages that were harassing or threatening.[17] This is most similar to Question 8 in the NZCASS 2006 module, although this specifies a phone call or text message, whereas the Statistics New Zealand question referred to other messages rather than calls.

The US National Crime Victimization Survey

The NCVS also provides comparative measures of some of the forms of e-crime against householders covered by NZCASS 2006. The NCVS carried a special component in 2004 which asked householders about identity theft and its consequences (Baum, 2006).

There were three questions, covering credit card thefts, thefts from existing accounts, and misuse of personal information.[18] However, it is difficult to draw comparisons between NZCASS 2006 and the NCVS results.

- Only those aged 18 years or older were questioned in the NCVS.
- More important, the NCVS questions asked about the experience of the respondent or *anyone else in their household*.
- Also, the NCVS asked about incidents which had occurred over the previous six months. While the longer 'recall period' used in NZCASS 2006 (approximately three times longer than in the NCVS) will mean a higher count, it is unlikely to be commensurately higher. This is because the longer the recall period, the less complete the reporting of incidents will be because of memory loss (see, e.g., Cantor and Lynch, 2000).

[17] There were follow-up questions on whether anyone was told about this, and who it was. Results will be published in the ICT in New Zealand: 2006 report, due by the end of 2007.

[18] The three NCVS questions were:

During the last 6 months, that is since –/20–, have you or anyone in your household discovered that someone:

(a) used or attempted to use any existing credit cards or credit card numbers without permission to place charges on an account

(b) used or attempted to use any existing accounts other than a credit card account – for example, a wireless telephone account, bank account or debit/check cards – without the account holder's permission to run up charges or to take money from accounts

(c) used or attempted to use personal information without permission to obtain NEW credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime?

Question (a) is similar to NZCASS Question 10, although the NCVS question is restricted to credit cards (rather than other bank cards as well). Question (c) is the same wording as Question 11 in NZCASS, although NZCASS might have picked up some incidents that might have been reported in the NCVS in Question (b).

British Crime Survey

The BCS has also used a household sample to look at some of the e-crimes covered by NZCASS 2006.

- There are results reported from the 2005/06 BCS on misuse of credit and bank cards (Hoare and Wood, 2007). The question is similar to NZCASS 2006 Question 6 (see Box A2).
- There are also results from the 2005/06 BCS on forms of identity fraud other than through the misuse of credit and bank cards. The question, however, is rather different in form from the one used in NZCASS 2006, which asked whether someone has used personal information without permission to obtain new credit cards or loans, run up debts, open other accounts, or otherwise commit theft, fraud, or some other crime.
- There are results from the 2003/04 BCS on computer viruses, computer hacking, and receiving harassing or offensive email messages (Wilson et al., 2006).
- Allen et al. (2005) report results from the 2002/03 survey on a question about whether mobile phone users had received any voice or text message that they considered offensive or a form of harassment. It subsumes the coverage of questions 6 and 8 in NZCASS 2006.

The other estimates

Table C1 shows NZCASS 2006 estimates alongside those from other surveys.

Table C1 NZCASS 2006 estimates of e-crime compared to other estimates

	NZCASS 2006	Statistics New Zealand	British Crime Survey	US National Crime Victimisation Survey	Auckland University Survey
Computer e-crime					
Computer virus, worm, or spyware	53%	17% Causing damage or loss	27% Virus only		62%
Hacking	6%		2%		
Offensive web material	15%		25% Receipt and unintentional encounter		
Fraud over the computer	1.8%	1.1% Causing loss			
Harassing emails	10%		12%		
Mobile phone e-crime					
Offensive calls or texts	8%		9% Offensive or harassing		
Harassing mobile phone messages	5%	4% Slightly more restricted			
Identity theft					
Card misuse	2.3%		4%		
Identity theft	2.8%		2% Different form of question	3% Broader range of questions, but over shorter time frame.	

Corp 331
ISBN 978-0-478-29042-X

MINISTRY OF
JUSTICE
Tāhū o te Ture

newzealand.govt.nz