Australian Government
Australian Institute of Criminology

The Australian Business Assessment of Computer User Security (ABACUS) survey: methodology report

Graham Challice

AIC Reports
Technical and Background Paper 32

The Australian Business Assessment of Computer User Security (ABACUS) survey: methodology report

Graham Challice

AIC Reports

Technical and
Background Paper

32

www.aic.gov.au

ISSN 1836-2052
ISBN 978 1 921532 16 0

Project no. 0133
Ethics approval no. PO114
Dataset no. 0105

Published by the Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: (02) 6260 9200
Fax: (02) 6260 9299
Email: front.desk@aic.gov.au
Website: http://www.aic.gov.au

Please note: minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **http://www.aic.gov.au**

Contents

Figures

Tables

Acknowledgments

The author would like to thank the survey participants who gave their time to respond to the survey questions and the interviewers, data entry operators, programmers and support staff who contributed to the delivery of the ABACUS project.

Introduction

This report covers the methodology of the Australian Business Assessment of Computer User Security (ABACUS) survey, including the survey instrument, sample design and selection, main data collection, and response rates. The ABACUS study was commissioned by the Australian Institute of Criminology (AIC) and involved undertaking a nationwide survey on computer security incidents against businesses. The survey defined a ‘computer security incident’ as ‘any unauthorised use, damage, monitoring attack or theft of your business information technology’.

Specifically, the survey aimed to ascertain:

- the measures Australian businesses take to prevent computer-security incidents
- the prevalence of computer-security incidents
- the types of computer-security incidents experienced by businesses
- the effects of victimisation, including financial losses, on businesses
- businesses’ responses following computer-security incidents.

The ABACUS survey was designed to produce statistically significant data on attacks on businesses’ computer security and to enable businesses to assess their computer security with the aim of preventing incidents in the future. The findings of the survey have been reported separately (see Richards 2009). They will serve to improve knowledge of the nature and dimensions of the problem and to identify risk management strategies, thereby enabling businesses to set priorities to more effectively direct scarce resources in minimising risks of computer security incidents.

Survey instrument

The ABACUS questionnaire was developed by the AIC with the assistance of a number of other parties, including:

- the Social Research Centre (SRC)
- the Technical Advisory Group (TAG)
- the Business Advisory Group (BAG).

The SRC is a private research organisation based in Melbourne, Australia, that specialises in providing research services to government agencies. The TAG and the BAG were established by the AIC to provide guidance on survey questions and other matters relating to the ABACUS study. Members of these advisory groups came from diverse backgrounds, including government agencies, peak industry bodies, universities and the private sector. The questionnaire was thus shaped with assistance from key figures from a range of relevant fields.

A number of surveys have previously looked at the problem of businesses' computer-security incidents, both in Australia and internationally (see ABS 2007; AusCERT 2006; Broadhurst et al. 2006; Computer Emergency Response Team et al. 2007; Quinn 2006; Richardson 2007). Advantages of the ABACUS survey are that it used a representative sample of businesses, and obtained enough responses to present statistically significant data on the extent and nature of the problem. Some of the ABACUS survey's questions are based on those contained in previous surveys, to enable comparisons amongst these jurisdictions.

The questionnaire asked businesses to answer 38 questions relating to computer-security incidents experienced by their business. Its main areas of focus were:

- demographic characteristics of respondents (industry sector, number of employees, annual turnover, role within the business)
- use of information technology (types of information technology used, level of knowledge of and ability to use information technology)
- measures used to prevent computer-security incidents (computer-security tools and policies used, expenditure on computer security, outsourcing of computer-security functions)
- number of computer-security incidents experienced
- types of computer-security incidents experienced (type of most significant computer-security incident, proportion of incidents perpetrated by insiders)
- effects of computer-security incidents (financial losses, other effects)
- reporting behaviours of businesses following computer-security incidents (proportions of incidents reported externally, agencies reported to, reasons for not reporting incidents).

The ABACUS questionnaire was approved by the Australian Bureau of Statistics' Statistical Clearing House, whose role it is to ensure that surveys of businesses within Australia are necessary and well-designed and place minimal burden on respondents (see http://www.sch.abs.gov.au). Due to the large sample size, the acquisition of businesses' records from the Australian Bureau of Statistics was also tabled in the Australian Parliament.

A pilot ABACUS study was undertaken in April 2007. The primary objectives of the pilot study were to test the proposed ABACUS survey instrument and methodology, to gain an insight into the likely response rate to the main survey, and to collect data for preliminary analysis.

Small, medium and large businesses from all Australian states and territories and from each of the 19 industry sectors used by ABACUS were contacted and were asked to complete the pilot questionnaire. Of 817 of these, 194 returned completed pilot questionnaires, a response rate of 24 percent.

Responses provided valuable information on a range of methodological issues, including ways to improve the survey instrument and maximise response rates. This information was used in planning the main ABACUS survey.

Participants were able to complete the questionnaire in any of three formats: on paper, on line, or by computer-assisted telephone interview (CATI). These response options were provided to assist in maximising response rates for the survey.

The questionnaire is provided for reference at Appendix 2.

Sample design and selection

Sample frame

The Australian Business Register (ABR) was used as the sample frame for the ABACUS survey. The ABR contains all businesses registered with the Australian Taxation Office as having an Income Tax Withholding role and is generally considered to equate to the population of employer businesses in Australia.

The sample frame contained details of:

- legal name
- trading name
- contact phone number
- contact fax number
- mailing address
- street address
- Australian and New Zealand Standard Industrial Classification (ANZSIC) division
- number of employees (categories)
- main state of operation
- state(s) of operation.

The ABR is held primarily for analytical and tax administration purposes, rather than for survey-research purposes. As such, there was little evidence as to the quality of some of the businesses' contact information (particularly telephone numbers).

Sample design

The Australian Bureau of Statistics' Statistical Consulting Unit (SCU) was commissioned to design the survey sample.

The target population for the ABACUS survey was defined as all Australian employer businesses, excluding defence-force establishments, private households employing staff, foreign diplomatic missions, government, and public-sector businesses. Businesses belonging to all remaining industry sectors, according to the Australian and New Zealand Standard Industrial Classification (ABS & Statistics New Zealand 2006), were considered the target population. The industry sector classifications used by the survey were thus:

- agriculture, forestry, and fishing
- mining
- manufacturing
- electricity, gas, water, and waste services
- construction
- wholesale trade
- retail trade
- accommodation and food services
- transport, postal, and warehousing
- information media and telecommunications

- financial and insurance services
- rental, hiring, and real-estate services
- professional, scientific, and technical services
- administrative and support services
- public administration and safety
- education and training
- health care and social assistance
- arts and recreational services
- other services.

A total of 20,040 units were selected. Based on the ABACUS pilot survey, conducted during 2007, a response rate of approximately 30 percent could be expected. It was therefore anticipated that approximately 6,000 completed questionnaires could be obtained from the 20,040 original sample selections, from a total population of 900,135 Australian businesses.

The sample was stratified by industry sector and business size. That is, units were selected from small, medium and large businesses and each of the 19 ANZSIC industry sectors listed above. Small businesses were defined as those with zero to 19 employees; medium businesses, as those with 20 to 199 employees; and large businesses, as those with 200 or more employees. The sample was thus stratified by 57 (3 x 19) industry-sector and employment-size groups as detailed in Table 1.

As can be seen, the 20,040 units were allocated equally among industry sectors, with a view to facilitating industry-level analysis, then proportionally by size within industry sector. A minimum of

Table 1: Number of businesses sampled, by industry sector and business size

	Small	Medium	Large	All sizes
Agriculture, forestry, and fishing	945	77	33	1,055
Mining	865	150	40	1,055
Manufacturing	829	193	33	1,055
Electricity, gas, water, and waste services	902	120	33	1,055
Construction	968	53	33	1,054
Wholesale trade	885	136	33	1,054
Retail trade	899	123	33	1,055
Accommodation and food services	795	226	33	1,054
Transport, postal, and warehousing	945	77	33	1,055
Information media and telecommunications	892	130	33	1,055
Financial and insurance services	988	33	33	1,054
Rental, hiring, and real-estate services	932	90	33	1,055
Professional, scientific, and technical services	962	60	33	1,055
Administrative and support services	879	143	33	1,055
Public administration and safety	829	193	33	1,055
Education and training	819	203	33	1,055
Health care and social assistance	912	110	33	1,055
Arts and recreation services	865	156	33	1,054
Other services	965	57	33	1,055
Total	17,076	2,330	634	20,040
As percentage of sample	85.2%	11.6%	3.2%	100.0%
As percentage of population	*89.6%*	*9.6%*	*0.7%*	*100.0%*

Table 2: Response targets, by industry sector and business size

	Small	Medium	Large	All sizes
Agriculture, forestry, and fishing	283	23	10	316
Mining	259	45	12	316
Manufacturing	249	57	10	316
Electricity, gas, water, and waste services	270	36	10	316
Construction	290	16	10	316
Wholesale trade	265	41	10	316
Retail trade	269	37	10	316
Accommodation and food services	238	68	10	316
Transport, postal, and warehousing	283	23	10	316
Information media and telecommunications	268	38	10	316
Financial and insurance services	296	10	10	316
Rental, hiring, and real-estate services	279	27	10	316
Professional, scientific, and technical services	289	17	10	316
Administrative and support services	263	43	10	316
Public administration and safety	249	57	10	316
Education and training	245	61	10	316
Health care and social assistance	273	33	10	316
Arts and recreation services	259	47	10	316
Other services	289	17	10	316
Total	5,116	696	192	6,004
Proportion of response target (percent)	85.2%	11.6%	3.2%	100.0%

10 achieved responses per cell was imposed (see Table 2), and an overall response rate of 30 percent was assumed at the cell level.

This resulted in the over-sampling of large and medium businesses, relative to their population proportion, and a commensurate under-sampling of small businesses.

Sample-list cleaning

In the process of preparing the sample list for the initial call and initial questionnaire mailing, a number of potential issues were identified.

As can be seen at Table 3, the main issues arising from list cleaning related to:

- records with tax agent details provided in either the address or telephone number fields, which resulted in a high proportion (32.7%) of duplicate entries for these variables, particularly amongst small businesses
- unusable telephone numbers (too few digits or too many digits, after attempting to backfill STD code information from address details, where these were present)
- other issues relating to duplication, record completeness, or scope status.

Of the sample records, initial list cleaning identified at least one problem in 44.1 percent.

Table 3: Outcomes of initial list cleaning

Problem	Sample records (number)	Sample records, all business sizes (percent)	Small businesses (percent)	Medium businesses (percent)	Large businesses (percent)
Duplicate phone number (tax agent number)	6,203	31.0	32.2	26.9	13.1
Tax Agent address (as identified by 'care of')	344	1.7	1.6	2.2	2.2
Unusable phone number (too few / too many digits)	1,753	8.7	9.1	6.7	7.1
Duplicate record (same trading/business name)	149	0.7	0.5	1.5	3.5
No street address (mail / potential tax agent only)	650	3.2	1.6	6.2	37.9
Incomplete address (missing street number/name)	523	2.6	2.7	2.0	1.3
Conflicting address (> one mailing address)	73	0.4	0.4	0.3	< 0.1
Overseas address	9	< 0.1	< 0.1	0.1	0.2
Sample records with at least one problem	8,847	44.1	44.4	39.9	53.6
Total sample records	20,040	100	17,076	2,330	634

Following a review of initial list-cleaning outcomes, it was agreed between the SRC and the AIC that:

- Businesses with an overseas address should be excluded (deemed out of scope) if no Australian address could be identified.
- In cases of duplicate records, the record pertaining to the larger business size and/or the industry sector with highest overall sample loss should be retained.
- There would be no courtesy call at all for small businesses (given the high proportion of small-business records with phone number difficulties, and an assumption that generically addressed, unsolicited mail could reasonably be expected to find its way to the target respondent in a small business).
- An attempt would be made to locate the mailing address and telephone numbers of medium and large businesses by manually searching the online Yellow Pages and other internet resources.
- A questionnaire would initially be mailed to all businesses (excluding those that refused to participate after the initial call), including those with a suspected incomplete address or with a known tax-agent address (in the hope that the tax agent would forward the materials to the relevant contact person at the sampled business).
- No known tax-agent numbers would be called as part of the courtesy call or telephone response maximisation phases (on the basis that it would be inappropriate to ask for forwarding information about the sampled business from the third-party tax agent).

After the initial questionnaire mailing and a review of response patterns and options for addressing non-response, it was agreed that:

- An attempt would be made to confirm addresses and backfill telephone number details for non-responding small businesses with duplicate, missing, or tax-agent telephone numbers, using Sensis's MacroMatch service, with the aim of increasing the proportion of non-respondents that could be followed up by telephone.
- A second questionnaire mailing would be undertaken for all small business non-respondents not contactable by telephone.

The main difficulty remaining after list cleaning was the list's limited capacity to enable courtesy-call and telephone non-response follow-up. These activities were to have formed key components of the response-maximisation strategy, based on the pilot ABACUS survey.

Main data collection

Overview

The essential components of the data collection methodology were unchanged from the pilot study, with an initial call to confirm and collect contact details; a survey-pack mailing; the option to complete the survey in hard copy, on line, or via computer-assisted telephone interview (CATI); and a range of telephone- and mail-based non-response follow-up activities.

Some flexibility in approach was necessary in order to address the various challenges presented by the issues associated with the quality of the sample list. A detailed description of the methodology by phase follows.

Initial call

A feature of the proposed approach for the ABACUS study was to undertake an initial call to all businesses in the sample to confirm contact details, personalise the mailed materials, and attempt to collect business profiling information to better understand scope status and non-response. In pilot testing, the response rate of businesses in which a contact person had been identified through the initial call process was considerably higher than of those sent unsolicited mail.

Due to issues arising from sample cleaning and the availability of accurate telephone numbers, it was agreed that only medium and large businesses should be included in the initial call phase. Of the 2,964 medium and large businesses sampled, three were excluded from the initial call phase due to an overseas address, 13 were excluded due to a duplicate entry, and 491 were excluded because no telephone-number details could be found using manual online company searches as described above.

The final initial call sample comprised 2,457 (82.9%) of the medium and large businesses sampled. Telephone calls were placed from 30 January to 25 February 2008.

A copy of the initial call script is at Appendix A.

Initial materials mailing

A 'best address' was identified using the address collected as part of the initial call process, the mailing address from the cleaned sample, or the street address from the cleaned sample.

As can be seen at Figure 1, in total 236 records were excluded from the initial materials mailing, including:

- overseas businesses (8)
- duplicate or incomplete address records (178)
- refusals at the initial call (35)
- businesses identified as out of scope at the initial call (15).

The mailing pack comprised a 12-page booklet, with a covering letter on the outside front cover, an instruction sheet on the inside front cover, and 10 A4 panels of survey questions, together with a glossary, confidentiality statement and sheet of frequently asked questions, and Reply Paid envelope. Mail was lodged in five batches, from 1 to 29 February 2008.

The initial batch comprised exclusively small-business records (9,497) in which the mailing details were believed to be clean (unique contact address).

The second batch comprised additional small-business records (6,481) in which the address had been updated or confirmed through the list-cleaning process described above, as well as 1,061 medium and large businesses either with updated details from initial call activity or in which manual searches had identified a mailing address but no telephone number.

The remaining batches comprised records (2,765) cleaned progressively with updated details from initial call activity and sundry address cleaning.

Appendices B, C and D contain respectively copies of the questionnaire, glossary and sheet of frequently asked questions.

Non-response telephone follow-up

A key component of the proposed response-maximisation strategy was reminder calls to non-responding businesses. The pilot ABACUS study found that this strategy was very effective in maximising response to the survey. Due to the high number of inaccurate and/or incomplete telephone contact details for businesses in the sample, an attempt was made to increase the proportion of the sample with a valid, unique telephone number through the use of MacroMatch, a Sensis service that backfills or confirms telephone numbers for a known business name and address, based on the online version of the Yellow Pages (www.yellowpages.com.au).

In total, 17,459 records were provided to MacroMatch on 8 February 2008. Of these, 4,197 (24.0%) found a match. The relatively low match rate is likely to be a product of the complexities of the matching process, in which minor differences in the presentation of the business name or address between the sample record and the Sensis record would result in a mismatch. After all telephone-number cleaning, some 5,905 sample members—almost 30 percent of the total sample—had either a duplicate number, a known tax-agent number, or a missing number, and could not be included in any subsequent telephone-based non-response follow-up.

The contact number used for telephone non-response follow-up was therefore either:

- the number collected or successfully used at the initial call,
- the new MacroMatched number, or
- the original unique telephone number as provided in the sample.

As can be seen at Figure 1, of the 17,694 non-respondents at the commencement of telephone-response maximisation, 12,880 (72.8%) were able to be followed up by telephone.

Further to the initial round of non-response follow-up telephone calls that commenced on 12 February 2008, a second round of follow-up calls to 5,477 non-responding businesses with a telephone number commenced on 26 March 2008 and continued until the cut-off for processing, approximately one month later.

In the non-response follow-up phase, a full computer-assisted telephone interview (CATI) version of the questionnaire booklet was scripted, so that businesses could be screened or complete the questionnaire by telephone as part of the non-response follow-up call if that was their preference. Given the complexity of the response options, questionnaires were not completed over the telephone except by respondents who had a copy of the glossary in front of them at the time of the call.

In most cases, the CATI version of the script was used to identify 'out of scope' businesses, and to collect data relevant to businesses that, because they had limited computing infrastructure and reported no computer-security incidents and no computer-security tools or policies, were sequenced past the majority of questions.

The telephone version of the booklet included categorised versions of Question 2, which asked respondents to indicate the number of employees their business had, and of Question 6, which asked respondents to estimate their business's annual turnover. Respondents unable or unwilling to respond to the 'open' versions of these questions were presented a categorised version of the question.

Appendix E contains a copy of the telephone non-response follow-up script.

Materials re-mailing

A bulk re-mailing of the survey pack was undertaken in two batches to 9,660 non-responding businesses, on 4 and 7 April 2008. Businesses that claimed not to have received a survey pack that were identified during telephone reminder activity, and those non-responding businesses without a valid telephone number, were included in this re-mailing. For these, a re-mailing of the survey materials was the only response-maximisation option available.

The re-mailing pack had a modified covering letter advising of the revised due date, but was otherwise identical to the initial survey pack.

In addition to the bulk re-mailing, ad hoc re-mailings were undertaken throughout the data collection period in response to requests from businesses in the sample, with a total of 10,267 survey packs being re-mailed as part of non-response follow-up activity.

Contact database maintenance

The master contact database was maintained throughout the main data collection period, using data collected from:

- the initial sample-cleaning process (identifying overseas businesses, duplicate records, and records with incomplete telephone-contact or mailing-address details)
- the mail returns logging process (accepted for processing, return to sender, refusal, out of scope)
- the final call outcome from initial call activity (contact details established, disconnected telephone number or business not known, tax agent telephone number, refusal, out of scope)
- completed online interviews
- calls to the ABACUS 1800 telephone number and emails to abacus@srcentre.com.au
- the final call outcome of reminder-call activity (telephone number disconnected or unknown, business unknown, tax-agent telephone number only, refusal, out of scope, completed CATI interview).

The contact database was used to generate lists for the various components of the projects and provide progress information and sample-yield statistics.

Sample records with a 'telephone number disconnected' outcome at the initial call were included in the initial mailing (since the address might be valid, even if the phone number had changed).

Similarly, sample records logged as 'return to sender' from mail activity were included in non-response telephone follow-up activity (since the number might still be valid even if the address had changed).

Online data collection

The online version of the questionnaire was developed directly from the final survey booklet, seeking to replicate the general 'look' of the booklet, but incorporating appropriate sequencing and input-control checks.

The online version of the questionnaire was accessible from 29 January until the cut-off for processing on 29 April 2008, using a unique login and password printed on the paper survey form or provided over the telephone during a reminder call.

Figure 1: ABACUS process map, sample cleaning to initial mailing

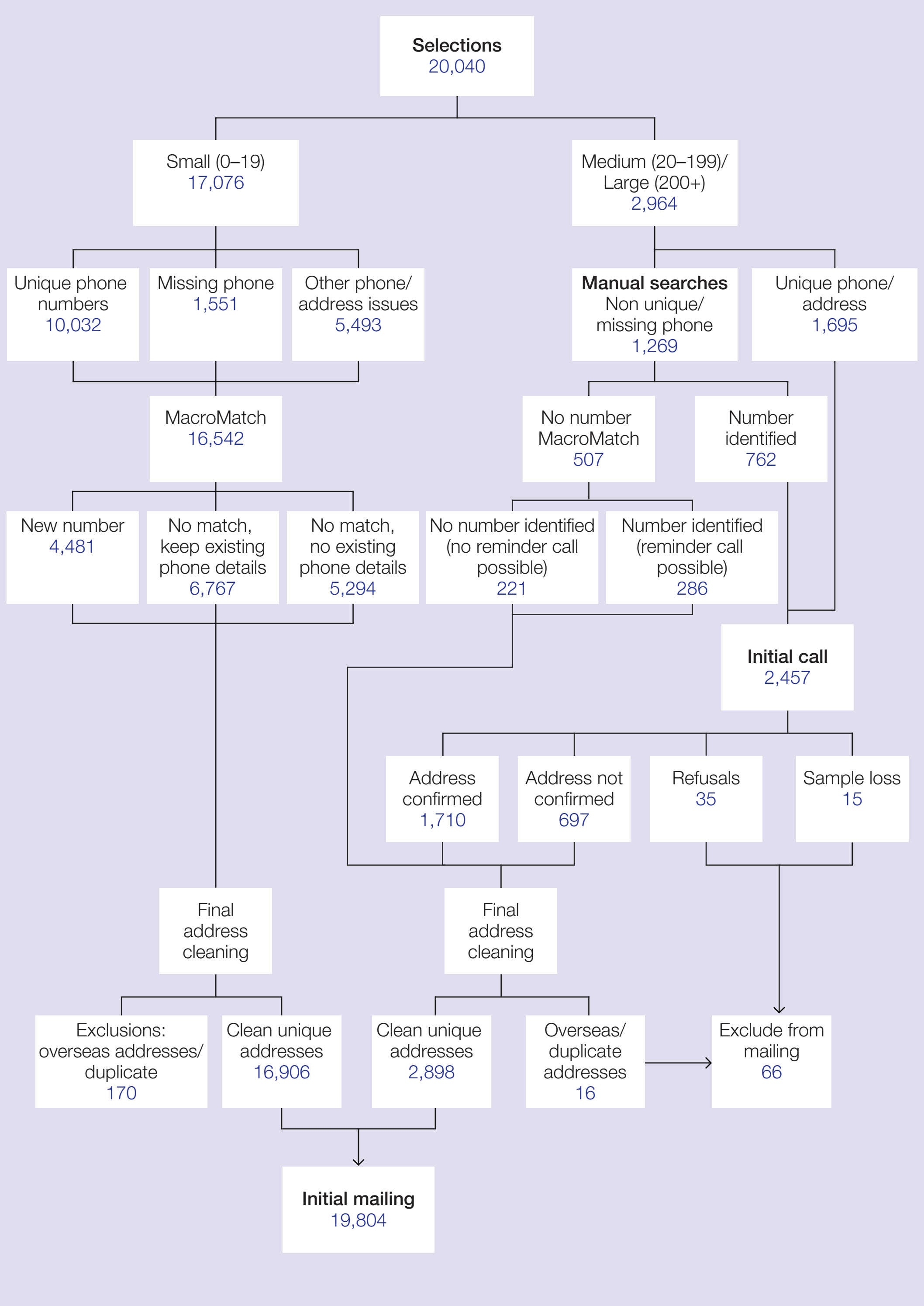
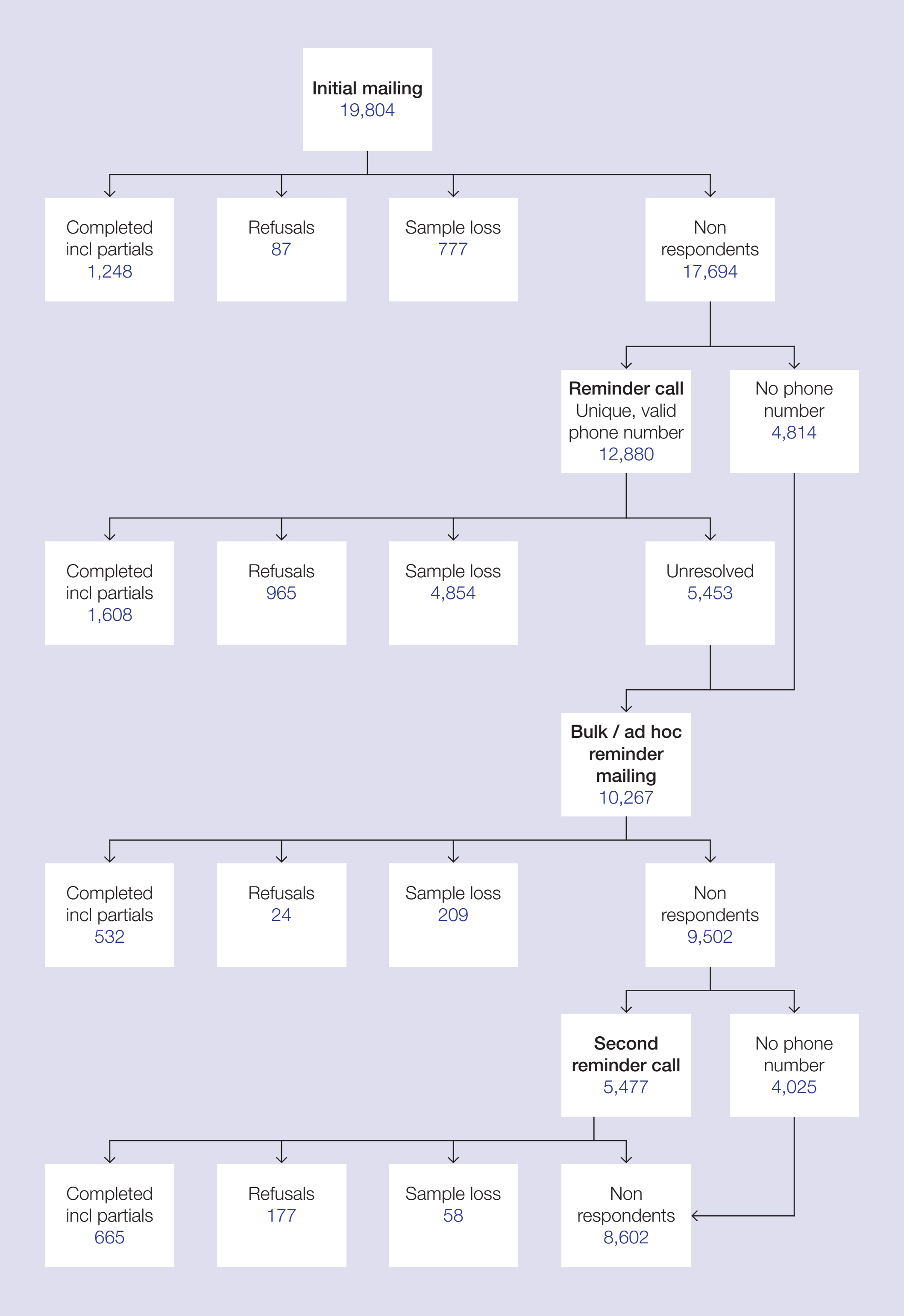

Selections 20,040
Small (0–19) 17,076
Medium (20–199)/ Large (200+) 2,964
Unique phone numbers 10,032
Missing phone 1,551
Other phone/ address issues 5,493
Manual searches Non unique/ missing phone 1,269
Unique phone/ address 1,695
MacroMatch 16,542
No number MacroMatch 507
Number identified 762
New number 4,481
No match, keep existing phone details 6,767
No match, no existing phone details 5,294
No number identified (no reminder call possible) 221
Number identified (reminder call possible) 286
Initial call 2,457
Address confirmed 1,710
Address not confirmed 697
Refusals 35
Sample loss 15
Final address cleaning
Final address cleaning
Exclusions: overseas addresses/ duplicate 170
Clean unique addresses 16,906
Clean unique addresses 2,898
Overseas/ duplicate addresses 16
Exclude from mailing 66
Initial mailing 19,804

Figure 2: ABACUS process map, non-response follow-up



Forms-based data capture

Data from completed paper returns were captured using optical mark recognition and key-from-image technologies, with a full double-key-and-verify workflow, ensuring that the data were captured exactly as recorded on the original form.

Standard methods were used to resolve, for example, multiple responses on a single-response question (by presenting an image of the question failing the input edit to the data-entry operator for resolution), with further logic edits and data cleaning undertaken at the data consolidation phase.

Data consolidation

Data from paper returns, the online survey, and telephone-based non-response activity were consolidated and cleaned according to agreed rules. This process is discussed in more detail in the following section.

Interviewer briefing and quality control

Interviewer briefing

All Social Research Centre telephone interviewers attended a comprehensive one and a half hour briefing session prior to undertaking initial call activity. The initial briefing session took place on 30 January 2008. The briefing was delivered by the SRC project manager and included:

- full details of ABACUS survey background, objectives, and methodology
- a review of all survey materials
- a detailed discussion of the likely challenges to the project, and how these might be overcome
- all aspects of administering the initial call
- practice interviewing and role play, with a focus on respondent liaison and when and how to seek full profiling information
- an outline of the sample-management protocols and the call regime that applied for the initial call.

Eight interviewers were briefed on the initial call component, with the same team undertaking non-response follow-up calls and responding to sample member queries on the 1800 number telephone hotline. A similar briefing was held before commencing the non-response follow-up activity.

Quality-control procedures

The quality-monitoring techniques applied to this project included:

- listening in, via remote monitoring, by the project manager and project supervisor to assess the ‘pitch’ of the initial call, better understand the nature of objections, and refine procedures for seeking full business profiling information
- interviewer debriefing and rebriefing after the first shift, and whenever there was important information to impart in relation to data quality; respondent liaison techniques; or technical, definitional, or process concerns relating to the survey
- an end-of-survey debriefing covering the entire process of initial call and non-response follow-up.

Response analysis

Response summary

As Table 4 indicates, there were:

- 4,000 fully responding businesses amongst those responding by mail, on line, or telephone
- 51 partially completed survey returns with insufficient data to be included in the analysis
- 1,288 refusals at any stage of the project, whether at the initial call, by calling the survey 1800 telephone number, by email, by return mail, or at the reminder call
- 8,602 non-responding businesses
- 6,099 sample records classified as unusable for a variety of reasons.

Business records were classified as unusable if:

- they related to a company based primarily outside of Australia;
- the business was no longer operating;
- the telephone number related to a private residence rather than a business;
- survey packs were marked 'return to sender';
- the business was not known at the address provided;
- the telephone number was disconnected; or
- tax-agent contact details were supplied.

The *sample yield*, which was defined as fully responding units as a percentage of *total sample*,

Table 4: Response summary

Outcome	Number	Percentage of total sample	Percentage of usable sample
Fully responding	4,000	20.0	28.7
Partially responding (not used in analysis)	51	0.3	0.4
Refusals (all types, across all stages of the project)	1,288	6.4	9.2
Non-respondents	8,602	42.9	61.7
Usable sample	*13,941*	*69.6*	*100.0*
Sample loss	6,099	30.4	
Total selections	20,040	100.0	N/A

was 20.0 percent. The *response rate*, which was defined as fully responding units as a percentage of the *usable sample*, was 28.7 percent.

Given that the scope status of some non-responding businesses was not established during survey activity, it is possible that the overall proportion of usable sample is overstated.

Response according to industry sector

Table 5 summarises response according to industry sector (based on the industry classification in the original sample record). As can be seen, sector response patterns varied considerably.

The response rate was highest for the agriculture, forestry and fishing sector, at 37.1 percent; the professional, scientific and technical-services sector, at 33.6 percent; and the education and training sector, at 32.6 percent. The response rate was lowest for the construction sector, at 19.7 percent. There was a broadly similar pattern for sample yield (fully responding units as a percentage of initial selections).

Residual non-response was fairly consistent at around 42 percent in most industry sectors. Notable exceptions included construction (49.6%), public administration and safety (47.8%) and financial and insurance services (36.1%).

Sample loss was also fairly consistent, at around 30 percent in most industry sectors, with finance and insurance services having the highest (40.3%) and health care and social assistance the lowest (24.5%) proportions of sample loss.

All industry sectors had a shortfall, relative to the target, in the number of surveys fully completed, the highest shortfalls being in construction and in public administration and safety.

Response according to business size

Table 6 summarises response according to business size. Business size was determined by the 'number of employees' category in the original sample record. As stated above, small businesses were defined as those with zero to 19 employees, medium businesses as those with 20 to 199 employees, and large businesses as those with 200 or more employees. As can be seen, there were some clear response patterns according to this characteristic.

Sample yield was highest amongst medium businesses (26.8%) and lowest amongst small businesses (18.9%). With small businesses comprising 85.2 percent of the sample, the yield amongst small business significantly skewed the overall sample yield for the project.

Refusals in medium and large businesses were almost twice as high as in small businesses. *Sample loss* amongst small businesses (33.2%) was more than twice as high as amongst medium and large businesses (15.4% and 12.0% respectively). *Non-response* was highest amongst large businesses, at 52.8 percent.

The largest shortfall, relative to the target number of interviews, occurred amongst small businesses.

Detailed response summary

Table 7 shows a detailed summary of response rates according to both business size and industry sector.

Response by sample type

Table 8 shows the breakdown of responses by initial call outcome. As was expected, the rate of response to personalised mail, in which contact with the target respondent was made as part of the initial call process (48.9%), was considerably higher than in the project over all (28.7%). The overall sample yield of this group was more than twice that of the project over all (20.0%).

The response rate for personalised mail over all, irrespective of whether contact was established with the target respondent at the initial call, was higher (39.4%) than in the project over all (28.7%). This illustrates the positive contribution of the initial call process to the overall response rate.

Although an initial call did not greatly affect the rate of response to generically-addressed mail,

Table 5: Response rates[a], by industry sector

Industry sector	Initial selections (number)	Fully responding (percent initial selections)	Refusals (all types) (percent initial selections)	Non-respondents (percent initial selections)	Sample loss (percent initial selections)	Response rate (percent contactable businesses)	Fully responding as a percentage of response target (316)
Agriculture, forestry, and fishing	1,055	27.4	3.8	42.7	26.1	37.1	91.5
Mining	1,055	22.2	7.6	38.9	31.2	32.2	74.1
Manufacturing	1,055	22.3	8.3	42.0	27.3	30.6	74.4
Electricity, gas, water, and waste services	1,055	20.5	4.5	43.2	31.5	29.9	68.4
Construction	1,054	13.8	6.5	49.6	30.1	19.7	45.9
Wholesale trade	1,054	20.9	9.8	41.6	27.4	28.8	69.6
Retail trade	1,055	17.9	7.1	43.4	31.4	26.1	59.8
Accommodation and food services	1,054	17.4	5.4	45.4	31.8	25.5	57.9
Transport, postal and warehousing	1,055	17.8	3.6	46.8	31.6	26.0	59.5
Information media and telecoms	1,055	22.9	5.2	41.2	30.0	32.8	76.6
Financial and insurance services	1,054	17.5	5.8	36.1	40.3	29.3	58.2
Rental, hiring and real estate services	1,055	17.8	7.0	42.6	32.2	26.3	59.5
Professional, scientific and technical	1,055	24.5	5.8	42.1	27.3	33.6	81.6
Administrative and support services	1,055	19.1	6.4	42.3	32.0	28.2	63.9
Public administration and safety	1,055	13.9	6.0	47.8	32.1	20.5	46.5
Education and training	1,055	23.4	6.1	41.7	28.2	32.6	78.2
Health care and social assistance	1,055	24.0	8.4	42.9	24.5	31.7	80.1
Arts and recreational services	1,054	18.7	6.3	42.5	32.4	27.7	62.3
Other services	1,055	17.3	8.5	42.8	30.8	25.1	57.9
Project total	20,040	20.0	6.4	42.9	30.4	28.7	66.7

a: Percentages of initial selections may not total 100, due to rounding and to exclusion of partially completed questionnaires

Table 6: Response rates[a], by business size

Number of employees	Initial selections (number)	Fully responding (percent initial selections)	Refusals (all types) (percent initial selections)	Non-responding (percent initial selections)	Sample loss (percent initial selections)	Response rate (percent contactable)	Fully responding as a percentage of response target (316)
Small	17,076	18.9	5.7	42.1	33.2	28.2	63.0
Medium	2,330	26.8	10.5	46.6	15.4	31.7	89.8
Large	634	24.1	10.4	52.8	12.0	27.4	79.7
Total	20,040	20.0	6.4	42.9	30.4	28.7	66.7

a: Percentages of initial selections may not total 100, due to rounding and to exclusion of partially completed questionnaires

Table 7: Response rates[a], by industry sector and business size

Business size	Initial selections (number)	Fully responding (percent initial selections)	Refusals (all types) (percent initial selections)	Non-responding (percent initial selections)	Sample loss (percent initial selections)	Response rate (percent contactable)	Fully responding as a percentage of response target (316)
Agriculture, forestry and fishing							
Small	945	27.8	3.6	41.7	26.8	38.0	92.9
Medium	77	23.4	6.5	45.5	24.7	31.0	78.3
Large	33	24.2	3.0	63.6	9.1	26.7	80.0
Mining							
Small	865	21.2	6.4	38.5	34.0	32.0	70.7
Medium	150	28.7	13.3	38.7	18.7	35.2	95.6
Large	40	20.0	12.5	47.5	17.5	24.2	66.7
Manufacturing							
Small	829	20.0	7.2	42.0	30.8	28.9	66.7
Medium	193	30.1	14.0	40.4	15.0	35.4	101.8
Large	33	33.3	3.0	51.5	12.1	37.9	110.0
Electricity, gas, water, and waste services							
Small	902	19.3	3.7	42.8	34.0	29.2	64.4
Medium	120	30.0	11.7	42.5	15.0	35.3	100.0
Large	33	18.2	3.0	57.6	21.2	23.1	60.0
Construction							
Small	968	12.8	5.8	49.9	31.4	18.7	42.8
Medium	53	34.0	15.1	34.0	17.0	40.9	112.5
Large	33	9.1	12.1	66.7	12.1	10.3	30.0
Wholesale trade							
Small	885	20.1	7.9	41.1	30.5	28.9	67.2
Medium	136	27.2	16.9	43.4	11.8	30.8	90.2
Large	33	15.2	30.3	45.5	9.1	16.7	50.0
Retail trade							
Small	899	17.4	7.1	41.0	34.4	26.4	58.0
Medium	123	21.1	7.3	57.7	13.8	24.5	70.3
Large	33	21.2	6.1	54.5	15.2	25.0	70.0
Accommodation and food services							
Small	795	16.0	4.5	43.1	36.4	25.1	53.4
Medium	226	20.8	7.1	53.5	18.1	25.4	69.1
Large	33	27.3	15.2	42.4	15.2	32.1	90.0

Table 7: continued

Business size	Initial selections (number)	Fully responding (percent initial selections)	Refusals (all types) (percent initial selections)	Non-responding (percent initial selections)	Sample loss (percent initial selections)	Response rate (percent contactable)	Fully responding as a percentage of response target (316)
Transport, postal and warehousing							
Small	945	15.9	3.2	46.9	33.9	24.0	53.0
Medium	77	39.0	7.8	40.3	13.0	44.8	130.4
Large	33	24.2	6.1	60.6	9.1	26.7	80.0
Information media and telecommunications							
Small	892	22.1	4.6	39.9	33.0	32.9	73.5
Medium	130	30.0	8.5	48.5	11.5	33.9	102.6
Large	33	18.2	9.1	48.5	24.2	24.0	60.0
Financial and insurance services							
Small	988	17.1	5.4	35.4	41.9	29.4	57.1
Medium	33	33.3	9.1	39.4	15.2	39.3	110.0
Large	33	12.1	15.2	54.5	18.2	14.8	40.0
Rental, hiring, and real-estate services							
Small	932	17.8	6.4	41.4	34.0	27.0	59.5
Medium	90	16.7	13.3	48.9	20.0	20.8	55.6
Large	33	21.2	6.1	57.6	15.2	25.0	70.0
Professional, scientific, and technical services							
Small	962	23.9	5.9	41.3	28.6	33.5	79.6
Medium	60	30.0	3.3	45.0	20.0	37.5	105.9
Large	33	30.3	6.1	60.6	3.0	31.3	100.0
Administrative and support services							
Small	879	18.2	6.3	40.4	35.0	28.0	60.8
Medium	143	24.5	6.3	52.4	16.8	29.4	81.4
Large	33	21.2	12.1	48.5	18.2	25.9	70.0
Public administration and safety							
Small	829	12.2	5.2	47.2	35.5	18.9	40.6
Medium	193	21.8	6.7	48.7	22.3	28.0	73.7
Large	33	12.1	21.2	57.6	6.1	12.9	40.0
Education and training							
Small	819	20.9	4.3	40.4	33.9	31.6	69.8
Medium	203	32.5	13.3	44.8	8.4	35.5	108.2
Large	33	30.3	6.1	54.5	9.1	33.3	100.0
Health care and social assistance							
Small	912	22.5	7.7	42.8	27.0	30.8	75.1
Medium	110	32.7	12.7	43.6	10.9	36.7	109.1
Large	33	36.4	15.2	45.5	0.0	36.4	120.0
Arts and recreation services							
Small	865	16.5	5.2	40.9	37.3	26.4	55.2
Medium	156	23.7	12.2	51.9	11.5	26.8	78.7
Large	33	51.5	6.1	39.4	3.0	53.1	170.0
Other services							
Small	965	16.5	8.4	42.4	32.5	24.4	55.0
Medium	57	22.8	10.5	47.4	14.0	26.5	76.5
Large	33	33.3	9.1	48.5	9.1	36.7	110.0
Total	20,040	20.0	6.4	42.9	30.4	28.7	66.7

a: Percentages of initial selections may not total 100, due to rounding and to exclusion of partially completed questionnaires

Table 8: Response rates[a], by sample type

Sample type	Initial selections (number)	Fully responding (percent initial selections)	Refusals (all types) (percent initial selections)	Non-responding (percent initial selections)	Sample loss (percent initial selections)	Response rate (percent contactable)
Spoke to target respondent	142	48.6	7.7	42.3	0.7	48.9
Other personalised mail	1,234	35.7	11.7	45.1	6.6	38.3
Subtotal personalised mail (initial call)	*1,376*	*37.1*	*11.3*	*44.8*	*6.0*	*39.4*
Generic mail (address confirmed)	334	22.5	17.4	37.4	21.3	28.5
Generic mail (address not confirmed)	658	17.2	5.8	55.6	20.8	21.7
Subtotal generic mail (initial call)	*992*	*19.0*	*9.7*	*49.5*	*21.0*	*24.0*
Generic mail (no initial call)	17,436	18.9	5.7	43.0	32.2	27.9
Project total	19,804	20.0	6.4	42.9	30.4	28.7

a: Percentages of initial selections may not total 100, due to rounding and to exclusion of partially completed questionnaires

Table 9: Summary of initial calls

	Sample records		Call attempts	
Call outcome	Number	Percentage of all records	Number	Percentage of all records
Collected target respondent details and profiling info	142	5.8	142	2.9
Collected target respondent details (no profiling info)	104	4.2	104	2.1
Collected target respondent details from phone answerer	1,130	46.0	1,130	23.2
Subtotal businesses able to be sent personalised mail	*1,376*	*56.0*	*N/A*	*N/A*
Refused IT Manager name (send generic pack)	334	13.6	334	6.9
Business not known at this number[a]	169	6.9	169	3.5
Tax agent number[a]	138	5.6	138	2.8
Non-contact / appointments	97	3.9	2,411	49.5
Number disconnected[a]	254	10.3	254	5.2
Subtotal generic mail	*992*	*40.4*	*N/A*	*N/A*
Fax	39	1.6	51	1.0
Refused to participate at any level	35	1.4	35	0.7
Claims to have no computers (profiling info collected)	15	0.6	15	0.3
Subtotal other outcomes	*89*	*3.6*	*89*	*1.8*
Total	2,457	100	4,872	100

a: Unusable for the purpose of additional telephone calls the overall sample loss was greatest amongst the generically-addressed mail with no initial call (32.2%). This is likely to be a factor of business size, given that this group comprised primarily small businesses (see Table 6).

Response analysis by project phase

The following sections describe patterns of response at the various stages of the ABACUS study—from the initial telephone call to non-response follow-up.

Analysis of initial call outcomes

As can be seen in Table 9, in total 4,872 initial calls were placed to the 2,457 medium- and large-businesses. Their purpose was to confirm sector and size, mailing address, and the name of the person responsible for I.T. The average number of calls placed to each business in the sample was 2.0.

The name or position title of the person responsible for information technology was collected in 1,376 cases (56.0%), including those (5.8% of total cases) in which contact was established with the target respondent.

The initial call process identified 561 records (22.8% of the total initial-call records) that did not contain telephone numbers usable for the purpose of additional telephone contact attempts (see Table 9). These were fed back into the manual search and/or MacroMatch processes for non-unique, missing and/or incorrect telephone numbers, in order to attempt to identify a valid telephone number for subsequent non-response follow-up.

Initial mailing summary

The composition and timing of the initial questionnaire mailing are summarised at Table 10.

The initial mail pack was lodged for all eligible sample members on or before 29 February 2008, giving a minimum response period before the cut-off date for processing (29 April 2008) of 38 business days.

The initial batch comprised exclusively small businesses with unique mailing addresses, with the composition of ensuing batches reflecting progress with address confirmation through the initial call process; manual address cleaning (for medium and large businesses only); and sample-record cleaning using MacroMatch.

Analysis of telephone response-maximisation activity

Non-response telephone follow-up commenced on 13 February 2008, 10 business days after the first mail packs were lodged, and continued until the close-off for data processing.

All returns received prior to the commencement of non-response follow-up activity were excluded, as were unusable numbers from the initial call. Returns received during non-response follow-up were removed from the sample on a daily basis and

Table 10: Summary of initial mailing

Batch	Initial mailing date	0 to 19	20 to 199	200 or more	Total	Response period (business days)
1	1 Feb 2008	9,497	0	0	9,497	58
2	15 Feb 2008	6,481	872	189	7,542	48
3	27 Feb 2008	769	1,380	422	2,571	40
4	29 Feb 2008	159	29	6	194	38
Total	–	16,906	2,281	617	19,804	52

Table 11: Summary of telephone non-response follow-up

	Initial reminder		Second reminder	
Call outcome	Number	Percent	Number	Percent
Questionnaire completed at reminder call	71	0.6	81	1.5
Removed from follow-up sample	273	2.1	165	3.0
Completed reminder call	2,985	23.2	2,003	36.6
Non-contact / appointments	2,992	23.2	888	16.2
Target respondent away duration	188	1.5	206	3.8
Not named business / tax agent number	3,463	26.9	692	12.6
Number disconnected	1,417	11.0	239	4.4
Fax	420	3.3	367	6.7
Refusals (all types) / claims to have no incidents	976	7.6	792	14.5
Claims to have no computers	95	0.7	44	0.8
Total sample records	12,880	100.0	5,477	100.0
Total calls placed	22,349	N/A	20,429	N/A
Average calls per sample record	1.7	N/A	3.7	N/A

Note: Initial non-responders n = 12,880

Table 12: Responses, by phase of survey

Phase	Number fully responding	Percentage of those fully responding	Number entering phase	Fully responding (percent of those entering phase)
Total	4,000	100.0		
Attributable to initial mailing	1,239	31.0	19,804	6.3
Attributable to initial-reminder calls	1,596	39.9	12,880	12.4
Subtotal initial mailing and follow-up	*2,835*	*70.9*	*19,804*	*14.3*
Attributable to reminder mailing	530	13.3	9,660	5.5
Attributable to second-reminder calls	635	15.9	5,477	11.6
Subtotal secondary mailing and follow-up	*1,165*	*29.1*	*9,660*	*12.1*

allocated the ‘removed from follow-up sample’ outcome.

As can be seen in Table 11, a total of 22,349 calls were placed to 12,880 sampled businesses for the initial non-response telephone follow-up, an average of 1.7 follow-up attempts per business. A relatively high proportion of records (37.9%) were unusable and resolved at the first call attempt. The reminder call was successfully completed in 23.2 percent of cases.

The 5,477 non-respondents at the time of the commencement of the second reminder call were followed up quite intensively, with 20,499 calls placed (an average of 3.7 calls per sampled business) and reminder calls to approximately one-third (36.6%) of cases completed.

The second round of reminder calls revealed an additional 931 unusable numbers.

The call outcomes presented in Table 11 reflect the final outcome status of the relevant telephone-reminder phase, not necessarily of the sample record.

Response analysis by phase of survey

Sample generation date and the date of completion as recorded in the master database were used to establish which phase of the project it achieved completion in.

As can be seen at Table 12, 70.9 percent of completed interviews can be attributed to the initial mailing and initial telephone follow-up phases.

Table 12 highlights the importance of intensive telephone follow-up to support the response-maximisation effort, with 55.8 percent of overall responses for ABACUS sample members attributable to telephone follow-up.

Using questionnaires whose completion was attributable to the phase as a proportion of those entering that phase as a measure of efficiency, the initial mailing and follow-up was marginally more efficient (14.3% sample yield) than the secondary mailing and follow-up (12.1% sample yield). This is consistent with other self-completion surveys undertaken by the Social Research Centre.

Non-response analysis

Part of the initial call strategy was to attempt to collect business profiling information (such as industry sector, annual turnover, use of information technology and number of employees) whenever the opportunity arose, with a view to using this information to better understand non-response.

Profiling information was collected for 142 in-scope businesses (see Table 8) at the initial call and for 316 at telephone non-response follow-up, of which 199 subsequently responded (and are excluded from this analysis).

Compared with those businesses that responded fully, non-responding businesses that were willing to provide profiling information included a higher representation of businesses with 20 or more employees, businesses with an operating revenue of $1m or more, and businesses that self-identified as being part of a critical infrastructure sector. This is broadly consistent with higher non-response from medium and large businesses as identified at Table 6.

The person from the non-responding business who provided the profiling information was also more likely to be a specialist in information technology (15.5%), with marginally higher reported information technology skills than respondents to the survey had.

There was no material difference between the proportion of those providing profiling information (78.0%) and of the responding sample (76.0%) who reported no computer-security incidents.

Refusal analysis

Table 13 summarises the point at which refusals occurred. As can be seen, almost three-quarters of total refusals (74.9%) occurred at the initial telephone reminder stage, and one in eight large businesses' refusals occurred at the initial call.

Table 13: Summary of point of refusal

Phase	Refusals by businesses of any size (column percent)	Refusals by businesses employing 0 to 19 (small) (column percent)	Refusals by businesses employing 20 to 199 (medium) (column percent)	Refusals by businesses employing 200 or more (large) (column percent)
Initial call	2.7	0.0	11.1	12.1
Initial mailing	6.8	8.3	1.2	4.5
Initial-reminder calls	74.9	72.0	84.4	83.3
Reminder mailing	1.9	2.2	0.8	< 0.1
Second-reminder calls	13.7	17.5	2.5	< 0.1
Total refusals (number)	1,288	978	244	66

Table 14: Summary of sample loss

Phase	Sample loss of all business sizes (column percent)	Sample loss of businesses employing 0 to 19 (small) (column percent)	Sample loss of businesses employing 20 to 199 (medium) (column percent)	Sample loss of businesses employing 200 or more (large) (column percent)
Initial sample cleaning / initial call	3.3	3.0	6.1	11.8
Initial mailing	12.7	11.5	29.0	25.0
Initial-reminder calls	79.6	81.2	58.5	56.6
Reminder mailing	3.4	3.2	5.8	6.6
Second-reminder calls	1.0	1.0	0.6	< 0.1
Total sample loss (number)	6,099	5,664	359	76

Of the refusals encountered during telephone reminders, approximately 70 percent were from the target respondent, the balance being 'gatekeeper' refusals.

Review of sample loss

Table 14 summarises the point at which sample loss occurred. Most (79.6%) sample loss, particularly for small business, occurred at the initial call (81.2%).

Approximately 69.6 percent of the sample loss at the initial reminder call related to a 'wrong telephone number or named business not at this number' or 'tax agent' outcome, and 28.5 percent were disconnected telephone numbers. The small residual (1.9%) related to businesses claiming not to have any computers.

Analysis by mode of response

As can be seen in Table 15, almost four-fifths (78.0%) of questionnaires were completed on paper, and almost one-fifth (18.3%) were completed on line. Only 3.8 percent were completed by computer-assisted telephone interview (CATI) at the time of the reminder call.

Mode of response depended somewhat on the basis of business size and industry sector, with a higher proportion of large businesses (38.6%), the education sector (30.4%), the professional, scientific, and technical services sector (23.6%), and the information media sector (24.4%) opting to complete the questionnaire on line.

The high proportion of completed questionnaires attributable to the second reminder call phase that were completed on line (41.9%) was to be expected, given that the interviewing team (rather than mail out an additional survey pack close to the cut-off date) actively encouraged sampled businesses to go on line.

Review of questionnaire performance

Incidence of 'don't know' and 'no answer' responses to particular questions is summarised at Table 16, providing some insight into respondents' willingness and/or capacity to answer some of the survey questions.

Questions left unanswered appeared in the paper self-completion questionnaire primarily.

Over all, the level of 'don't know' and/or 'not answered' responses is probably attributable to directing technical and specialist questions to a generalist manager or small-business respondent with only a passing knowledge of or interest in computer-security concerns.

Table 15: Mode of survey response, by business attributes or survey phase (percent)

	All modes (number)	Paper	On line	CATI
Number of employees				
0 to 19 (small)	3,222	80.2	15.6	4.2
20 to 199 (medium)	625	70.7	26.9	2.4
200 or more (large)	153	60.1	38.6	1.3
Industry sector				
Agriculture, forestry, fishing	289	84.1	9.0	6.9
Mining	234	80.3	17.9	1.7
Manufacturing	235	77.4	17.9	4.7
Electricity, gas, water & waste services	216	82.4	14.8	2.8
Construction	145	80.7	15.9	3.4
Wholesale	220	75.5	22.3	2.3
Retail	189	73.5	21.2	5.3
Accommodation and food services	183	79.8	12.0	8.2
Transport, postal and warehousing	188	81.4	13.3	5.3
Information media and telecommunications	242	74.0	24.4	1.7
Financial and insurance	184	79.9	16.3	3.8
Rental, hiring and real estate services	188	83.0	14.4	2.7
Professional, scientific and technical services	258	74.8	23.6	1.6
Administrative and support services	202	79.7	16.3	4.0
Public administration and safety	147	78.9	19.0	2.0
Education and training	247	67.6	30.4	2.0
Health care and social assistance	253	80.6	15.8	3.6
Arts and recreation	197	76.1	19.3	4.6
Other services	183	72.7	20.8	6.6
Survey phase				
Attributable to initial mailing	1,235	86.5	13.5	0.0
Attributable to initial reminder calls	1,600	81.3	14.3	4.4
Attributable to reminder mailing	514	88.1	11.9	0.0
Attributable to second reminder calls	651	45.6	41.9	12.4
Total (number)	4,000	3,118	730	152
All (percent total completed)		78.0	18.3	3.8

Table 16: Incidence of ‘don’t know’ and ‘no answer’ responses

Question	Description	Respondents encountering question (number)	Number of ‘don’t know’ or ‘no answer’ responses	Percent respondents encountering question
4	Part of critical infrastructure sector	4,000	1,470	36.8
6A	Total operating revenue	4,000	570	14.3
10	Number of security incidents	3,749	311	8.3
12	Percentage of incidents originating from person within business	871	295	33.9
13	Percentage of incidents referred to external body	871	223	25.6
14	Incident causing greatest financial loss	871	246	28.2
15	Total financial costs of all incidents	871	246	28.2
17	Issues experienced as a result of most significant incident	871	145	16.6
18	Total financial cost of most significant incident	871	232	26.6
25	Frequency of evaluating third party	529	88	16.6
27	Standards used in development of IT policies	1,764	805	45.6
28	Frequency of evaluating effectiveness of security	3,749	714	19.0
29	Method used to evaluate effectiveness	1,487	413	27.8
30	Total IT expenditure	3,749	571	15.2
31	Amount spent on computer security	3,749	716	19.1
32	Percentage of expenditure by type of security	3,749	1,710	45.6
33	Percentage increase/decrease	3,749	994	26.5
34	Incidents covered by insurance	3,749	1,360	36.3

Data preparation

Data consolidation and cleaning

Data from the initial call, paper returns, online returns, and non-response follow-up were aligned and consolidated into a single file for cleaning.

The sequencing pattern of the paper questionnaire was used to 'clean' the data. For example, if the answer to Q10 was 'None' (no computer security incidents in the reference period, with an instruction to skip to Q21), and an answer (even a zero) was given to Q15 (total costs of computer security incidents in the reference period), the response at Q15 was removed. In instances in which subsequent answers showed that a sequencing question had been missed, the response to the sequencing question was imputed. For example, if the business indicated it was required to report computer-security incidents to a law enforcement agency prior to making a claim on insurance, and Q35 was unanswered, then the answer to Q35 was backfilled to a 'Yes'.

For questions 13 and 32, the rules applied in data cleaning were:

- Where any one, or a combination, of the multiple-response variables added to 100 percent or more, the remaining multiple-response variables were set to 'zero'.
- Where any one, or a combination, of the multiple response variables added to less than 100 percent, the remaining multiple response variables were set to 'can't say'.

Approach to weighting

Australian Bureau of Statistics population counts of industry sector and number of employees (business size) were used to develop the weighting matrix for the ABACUS project. Responses to questions 1 (industry sector) and 2 (number of employees) were used to allocate each questionnaire record to a cell for weighting. Sector and employee number information not provided by the respondent was filled from the original sample record.

Some respondents provided an answer to question 1 or 2 that varied from information provided in the original sample record. In these instances, the information provided by respondents was taken to override existing information about industry sector and number of employees.

Data were weighted to represent the estimated total number of qualifying businesses in Australia, according to the Australian Bureau of Statistics.

Data delivery

Files were provided to the AIC in a STATA-compatible format, including a full code list, initially in draft format (excluding responses to verbatim questions), followed by a full file, including verbatim responses.

Summary of concerns for future surveys

Sample frame

Whilst the Australian Business Register offers comprehensive coverage, it is not maintained for research-survey sampling purposes, and a range of strategies may need to be considered if it is used for future similar surveys. These could include:

- washing selections (except those in the finance and insurance strata) against lists of known tax agents to purge the contact list of phone numbers and addresses relating to third parties such as tax agents
- providing for a more comprehensive list-preparation phase within the overall project schedule and budget
- investigating options for better matching the sample frame to existing business lists (in order that, for example, a match failure not occur because 'W.D. Smith and Sons Pty Ltd' could not be matched to 'WD Smith').

These strategies may result in a cleaner list for the commencement of data collection and reduce overall sample loss.

Methodology

Relative to similar previous studies, the ABACUS study achieved a reasonable response rate. The response rates of previous surveys have varied considerably. Rantala (2008: 2) achieved a response rate of 23 percent, Quinn (2006: 5) a response rate of 22 percent, and AusCERT (2006: 37) a response rate of 17 percent. Richardson's (2007: 27) and the Computer Emergency Response Team et al.'s (2007) American surveys appear to have achieved much lower response rates, approximately nine percent and four percent respectively. The methodological features considered to most strongly support the response-maximisation effort include:

- an accommodating approach (the option to complete the questionnaire in hard copy, on line, or by telephone)
- the initial call (as clearly illustrated in Table 9)
- intensive telephone non-response follow-up.

It is recommended that these features be retained in future similar studies.

Consideration could also be given to tailored approaches for enumerating 'difficult' industries (for example, advance letter to the Chief Executive Officer of the business and a tailored initial call script) and a tailored letter to address the 'no surveys' policy encountered occasionally when dealing with gatekeepers.

Data quality

With an ambitious data-collection agenda covering corporate, financial, specialist and technical, and strategic matters, a concern for data quality was inherent in the ABACUS study. Consideration could be given to further testing and tailoring of a number of questionnaire items and to developing strategies to improve understanding of key survey concepts by all survey respondents.

References

Australian Bureau of Statistics (ABS) 2007. *Business use of information technology 2005–06*. ABS cat. no. 8129.0. Canberra: ABS

Australian Bureau of Statistics (ABS) & Statistics New Zealand 2006. *Australian and New Zealand Standard Industrial Classification 2006*. Canberra: Commonwealth of Australia

Australian Computer Emergency Response Team (AusCERT) 2006. *2006 Australian computer crime and security survey*. Brisbane: AusCERT

Broadhurst R, Lee K, Bacon-Shone J & Zhong Y 2006. *Preliminary Report of the International Crime Victimisation Survey, 2005*. Hong Kong: Social Science Research Centre, Hong Kong University

Computer Emergency Response Team, US Secret Service, CSO Magazine and Microsoft 2007. 2007 e-crime watch survey. [accessed 7 January 2009] http://www.cert.org/archive/pdf/ecrimesummary07.pdf

Quinn KJ 2006. *Second annual New Zealand computer crime and security survey*. Dunedin: Alpha-Omega Group

Rantala R 2008. *Bureau of justice statistics special report: cybercrime against businesses, 2005*. Washington, DC: Bureau of Justice Statistics

Richards K 2009. *The Australian business assessment of computer user security: a national survey*. Research and public policy series no. 102. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/rrp/rrp102.pdf

Richardson R 2007. *2007 CSI computer crime and security survey*. San Francisco, CA: Computer Security Institute

Appendixes

Appendix A: Initial call script

ABACUS main survey—initial call script

SAMPLE VARIABLES

COMPANY_NAME

ADDRESS

SUBURB

STATE

POSTCODE

CALL OUTCOME CODES

Proceed with interview

No answer

Answering machine

FAX machine/Modem

Busy (Call back)

Appointment (hard)

Telstra message/Number disconnected

Claims to have done survey

Respondent not available/Away for duration of survey

Language difficulty, NO FOLLOW-UP

Terminated midway in survey

Stopped interview

SCREENING QUESTIONS

*(PHONE ANSWERER)

S1 Good (…). My name is (….) calling on behalf of the Australian Institute of Criminology from the Social Research Centre. We're undertaking an important national study and would like to include this business. I'd like to send some information to the person in the business responsible for I.T. Who should I address it to?

1. Continue to record contact information
2. Refuses to provide information (GO TO END1)
3. SOFT appointment—not available to confirm details now

4. HARD appointment—not available to confirm details now
5. Wants to know what it is about (GO TO EXPL1)
6. Claims to have no computers / I.T. in business (GO TO SQ9A)
7. Do not send mail (AVOID) (GO TO ALLTERM)
8. Business not known at this number
9. Phone number is not named business/is businesses tax agent/rep
10. SUPERVISOR USE ONLY—FORCING THROUGH NON CONTACTS (GO TO ALLTERM)

*(PHONE ANSWERER)

S2n Could I just record the contact name of the person responsible for IT?

1. Record Name: (COLLECT TITLE, FIRST NAME AND SURNAME IN SEPARATE FIELD)
2. (Refused)

S2p And the position title?

1. IT Manager
2. IT Director
3. Chief Information Officer
4. Other (Specify_______)
5. (Don't know)
6. (Refused)

S2c Could I just confirm the company name?

DISPLAY COMPANY NAME FROM SAMPLE

1. Company name in sample correct
2. Edit company name (Specify correct name)
3. (Refused)

S2a And the postal address:

DISPLAY ADDRESS FROM SAMPLE:

1. Address in sample is correct
2. Edit address (COLLECT STREET NUMBER AND NAME (ADDRESS LINE 1),
SUBURB AND POSTCODE IN SEPARATE FIELDS)
3. (Refused)

*(PHONE ANSWERER)

S3 INTERVIEWER ACTION: IS THE PERSON RESPONSIBLE FOR 'IT' THE PERSON YOU ARE SPEAKING TO OR IS IT SOMEONE ELSE?

1. PERSON CURRENTLY SPEAKING TO (GO TO S6)
2. SOMEONE ELSE

*(PHONE ANSWERER)

S4 Could you put me through to <NAME RECORDED AT S2n>, so I can check that the material we'll be mailing is relevant to your business? It will only take a couple of minutes.

INTERVIEWER NOTE: TAKE CARE NOT TO COME ACROSS AS BEING PUSHY. IF RESPONDENT SOUNDS ANNOYED/BUSY CHOOSE OPTION 3—DID NOT PURSUE COLLECTING SCREENING INFORMATION FROM RESPONDENT

1. Continue (GO TO S5a)
2. Phone answerer refused to pass on to named person/person responsible for IT (GO TO END2)
3. Did not pursue collecting screening information from phone answerer (GO TO END2)

*(PERSON RESPONSIBLE FOR IT)

S5a Good (…). My name is (….) calling on behalf of the Australian Institute of Criminology from the Social Research Centre. We're undertaking an important national study on the prevalence and types of computer security incidents that impact on Australian businesses and would like to include this business.

REFER CHEAT SHEET FOR EXPLANATION OF PURPOSE OF SURVEY, ETC

1. Continue
2. Wants to know what it is about (GO TO EXPL1)
3. Claims to have no computers / I.T. in business (GO TO SQ9B)

S5b Would it be ok if I asked you a few quick questions just to check that the study is relevant to your business? It should only take a minute or so.

INTERVIEWER NOTE: TAKE CARE NOT TO COME ACROSS AS BEING PUSHY. IF RESPONDENT SOUNDS ANNOYED/BUSY CHOOSE OPTION 3—DID NOT PURSUE COLLECTING SCREENING INFORMATION FROM RESPONDENT

1. Continue (GO TO Q1)
2. Does not have time to answer questions (GO TO END2)
3. Did not pursue collecting screening information from person responsible for IT (GO TO END2)
4. Do not send mail (AVOID) (GO TO ALLTERM)

*(PHONE ANSWERER IS PERSON RESPONSIBLE FOR IT)

S6 Would it be ok if I asked you a few quick questions now to check if the material we would like to mail out is relevant to your business? It should only take a minute or so.

INTERVIEWER NOTE: TAKE CARE NOT TO COME ACROSS AS BEING PUSHY. IF RESPONDENT SOUNDS ANNOYED/BUSY CHOOSE OPTION 3—DID NOT PURSUE COLLECTING SCREENING INFORMATION FROM RESPONDENT

1. Continue (GO TO Q1)
2. Refused/didn't have time to answer questions (GO TO END2)
3. Did not pursue collecting screening information from person responsible for IT (GO TO END2)
4. Do not send mail (AVOID) (GO TO ALLTERM)

EXPL1 The Australian Institute of Criminology is undertaking an important national study on the prevalence and types of computer security incidents that impact on Australian businesses.

IF NECESSARY: The mail pack we would like to send will have all the details. It includes a short questionnaire that can be completed on line, mailed back or by phone.

REFER CHEAT SHEET FOR EXPLANATION OF PURPOSE OF SURVEY, ETC

1. Snap back to previous question

*(PHONE ANSWERER CLAIMS TO HAVE NO COMPUTERS)

SQ9A Which of the following types of information technologies (IT) did your business use during the 12-month period ending 30th June 2007?

(MULTIPLES ACCEPTED)

READ OUT

1. Personal computers (GO TO S1)
2. Laptops (GO TO S1)
3. Smart phones (phones that have the capacity to send and receive emails and access the internet) (GO TO S1)
4. Other wireless devices (GO TO S1)
5. Local area network (GO TO S1)
6. Wide area network (GO TO S1)
7. Virtual private network (GO TO S1)
8. Other (Specify) (GO TO S1)
9. None (GO TO PQ)

*(NEW RESPONDENT—PERSON RESPONSIBLE FOR IT CLAIMS TO HAVE NO COMPUTERS)

SQ9B Which of the following types of information technologies (IT) did your business use during the 12-month period ending 30th June 2007?

(MULTIPLES ACCEPTED)

1. Personal computers (GO TO S5b)
2. Laptops (GO TO S5b)
3. Smart phones (phones that have the capacity to send and receive emails and access the internet) (GO TO S5b)
4. Other wireless devices (GO TO S5b)
5. Local area network (GO TO S5b)
6. Wide area network (GO TO S5b)
7. Virtual private network (GO TO S5b)
8. Other (Specify) (GO TO S5b)
9. None (GO TO PQ)

PQ Ok, well could I just ask a couple of very quick questions about the business to help us understand the types of business that do NOT use computers?

1. Continue (GO TO Q1)
2. Refused to answer profiling questions (RECORD AS Q9=9 AND GO TO END3)

*(PERSON RESPONSIBLE FOR IT)

Q1 What is your main line of business?

PROBE AS NECESSARY: What type of business or service do you provide?

1. Agriculture, Forestry and Fishing
2. Mining
3. Manufacturing
4. Electricity, Gas, Water and Waste Services
5. Construction
6. Wholesale trade
7. Retail trade
8. Accommodation and Food Services
9. Transport, Postal and Warehousing
10. Information Media and Telecommunications
11. Financial and Insurance Services
12. Rental, Hiring and Real Estate Services
13. Professional, Scientific and Technical Services
14. Administrative and Support Services
15. Public Administration and Safety
16. Education and Training
17. Health Care and Social Assistance
18. Arts and Recreational Services
19. Other Services (Specify)
20. (Don’t know)

*(PERSON RESPONSIBLE FOR IT)

Q2 Which of the following categories best describes the total number of employees on the Australian payroll of your business as at 30th June 2007?

READ OUT

1. No employees
2. 1—4
3. 5—19
4. 20—199
5. 200+
6. (Don’t know)

*(PERSON RESPONSIBLE FOR IT)

Q3 In which state or territory was THE MAJORITY of your business's staff employed during the 12-month period ending 30th June 2007?

(SINGLE RESPONSE)

DISPLAY STATE FROM SAMPLE RECORD

INTERVIEWER: IF "CAN'T SAY" RETURN STATE FROM SAMPLE RECORD

1. New South Wales
2. Victoria
3. Queensland
4. Western Australia
5. South Australia
6. Tasmania
7. Northern Territory
8. Australian Capital Territory

*(PERSON RESPONSIBLE FOR IT)

Q4 Is your business considered to be part of a critical infrastructure sector according to the Trusted Information Sharing Network (TISN)?

1. Yes
2. No (GO TO Q6a)
3. Don't know (GO TO Q6a)

*(PERSON RESPONSIBLE FOR IT)

Q5 To which ONE of the following TISN critical infrastructure sectors does your business belong?

READ OUT

1. Banking and Finance
2. Transport and Distribution
3. Emergency Services
4. Energy
5. Food Supply
6. Health
7. Government Services
8. Communications
9. (Not applicable)

Q6 (EXACT TURNOVER) DELETED

*(PERSON RESPONSIBLE FOR IT)

Q6a Which of the following best describes the turnover of your business during the 12-month period ending 30th June 2007?

1. Less than $100,000
2. $100,000 to less than $500,000

3. $500,000 to less than $1 million
4. $1 million to less than $10 million
5. $10 million to less than $1 billion
6. $1 billion or more
7. (Don't know)

*(PERSON RESPONSIBLE FOR IT)

Q7a How would you rate your LEVEL OF KNOWLEDGE to use information technologies? Would you say…

READ OUT

1. Very low
2. Low
3. Moderate
4. High, or
5. Very high
6. (Can't say)

*(PERSON RESPONSIBLE FOR IT)

Q7b How would you rate YOUR ABILITY TO USE information technologies?

READ OUT

1. Very low
2. Low
3. Moderate
4. High, or
5. Very high
6. (Can't say)

*(PERSON RESPONSIBLE FOR IT)

Q8 Which ONE of the following best describes your ROLE within the business?

INTERVIEWER NOTE: WE ARE NOT SEEKING A POSITION TITLE, JUST A ROLE DESCRIPTION TO IDENTIFY WHETHER THE RESPONDENT HAS A SPECIALIST IT ROLE OR NOT

READ OUT

1. Owner / director / CEO / MD
2. General management / operations management
3. CFO / financial management
4. CIO / IT management
5. Fraud / security control
6. Other (Specify)

PREQ9(1) IF SQ9A=9 (PHONE ANSWERER STATES BUSINESS HAS NO COMPUTERS) GO TO END3.

PREQ9(2) IF S3=2 (NEW RESPONDENT IS RESPONSIBLE FOR IT) AND SQ9B=9 (HAS NO COMPUTERS) GO TO END3.

PREQ9(3) IF SQ9A= 1 TO 8 OR SQ9B=1 TO 8 (BUSINESS USES COMPUTERS), AUTOFILL Q9 AND THEN GO TO Q10.

*(NOT ASKED SQ9A OR SQ9B)

Q9 Which of the following types of information technologies (IT) did your business use during the 12-month period ending 30th June 2007?

(MULTIPLES ACCEPTED)

READ OUT

1. Personal computers
2. Laptops
3. Smart phones (phones that have the capacity to send and receive emails and access the internet)
4. Other wireless devices
5. Local area network
6. Wide area network
7. Virtual private network
8. Other (Specify)
9. None (GO TO END3)

*(PERSON RESPONSIBLE FOR IT)

Q10 How many computer security incidents, if any, did your business experience during the 12-month period ending 30th June 2007? A computer security incident is defined as “any unauthorised use, damage, monitoring, attack or theft of your business information technology”.

INTERVIEWER NOTE: Each incident should only be counted once, for example any worm or virus that could be classified as a computer security incident should only be counted as a single attack, not once per infected machine.

1. None
2. One or more (Specify) [ALLOWABLE RANGE 1 TO 99999]
3. (Don’t know)
4. (Refused)

*(PERSON RESPONSIBLE FOR IT)

Q22 Were any of the computer security measures of your business outsourced to a third party during the 12-month period ending 30th June 2007?

1. Yes
2. No
3. (Don’t know)
4. (Refused)

*(PERSON RESPONSIBLE FOR IT)

Q22a Thank you for that. Yours is definitely one of the businesses we would like to include in the study.

1. Continue

PREQ22B IF S3=2 (DIFFERENT PERSON RESPONSIBLE FOR IT).

*(DIFFERENT PERSON RESPONSIBLE FOR IT)

Q22b Before I go, can I quickly just confirm your contact details?

***PROGRAMMER NOTE**: Display contact details here for confirmation (and editing) if necessary.
Confirm Name: [TITLE, FIRST NAME AND SURNAME IN SEPARATE FIELDS]
Confirm Address: [STREET NUMBER AND NAME, SUBURB AND POSTCODE IN SEPARATE FIELDS]
Collect Phone Number: DISPLAY PHONE NUMBER FROM SAMPLE AND EDIT AS
NECESSARY (AREA CODE: ALLOWABLE RANGE= 2 DIGITS (02–08), PHONE NUMBER: ALLOWABLE RANGE=8 DIGITS]

END You will receive materials in the next week or so. Thanks again for your time.

END1 Thank you for your time.

END2 That's fine—thank you very much for your time today. We will send out the material in the next week or so.

END3 (That's all I need to ask you. The mail we were going to send out related to computer security. As you do not use the types of computer equipment I just read out—there is no need to send out the material). Thanks anyway.

ALLTERM

1. Refuses to provide contact information (send mail materials to "The IT Manager" at company name and address as per sample) (S1=2)
2. Refuses to participate at any level (do not send mail) (S1=6, S5b=4, S6=4) (GO TO RR1)
3. Contact details of person responsible for IT collected from phone answerer (S4=2, S4=3) (send mail materials to named contact person)
4. Person responsible for IT does not have time to provide profiling info (S5b=2, S5b=3, S6=2, S6=3) (send mail materials to named contact person)
5. Claims to have no computers in company—no profiling information (PQ=2)
6. Claims to have no computers in company—profiling information collected (SQ9A=9 OR SQ9B=9 AND PQ NOT 2) OR (Q9=9)
7. Full profiling information collected (send mail materials to named contact person) (Q22a=1)
8. Business not known at this number
9. Phone number is not named business/is businesses tax agent/rep
10. Non contacts (S1=10)

*(REFUSES TO PARTICIPATE AT ANY LEVEL)

RR1 OK, that's fine, no problem, but could you just tell me the main reason you do not want to participate, because that's important information for us?

1. Other (SPECIFY_______)

OUTPUT—CONSOLIDATED FILE OF “BEST CONTACT NAME AND ADDRESS”

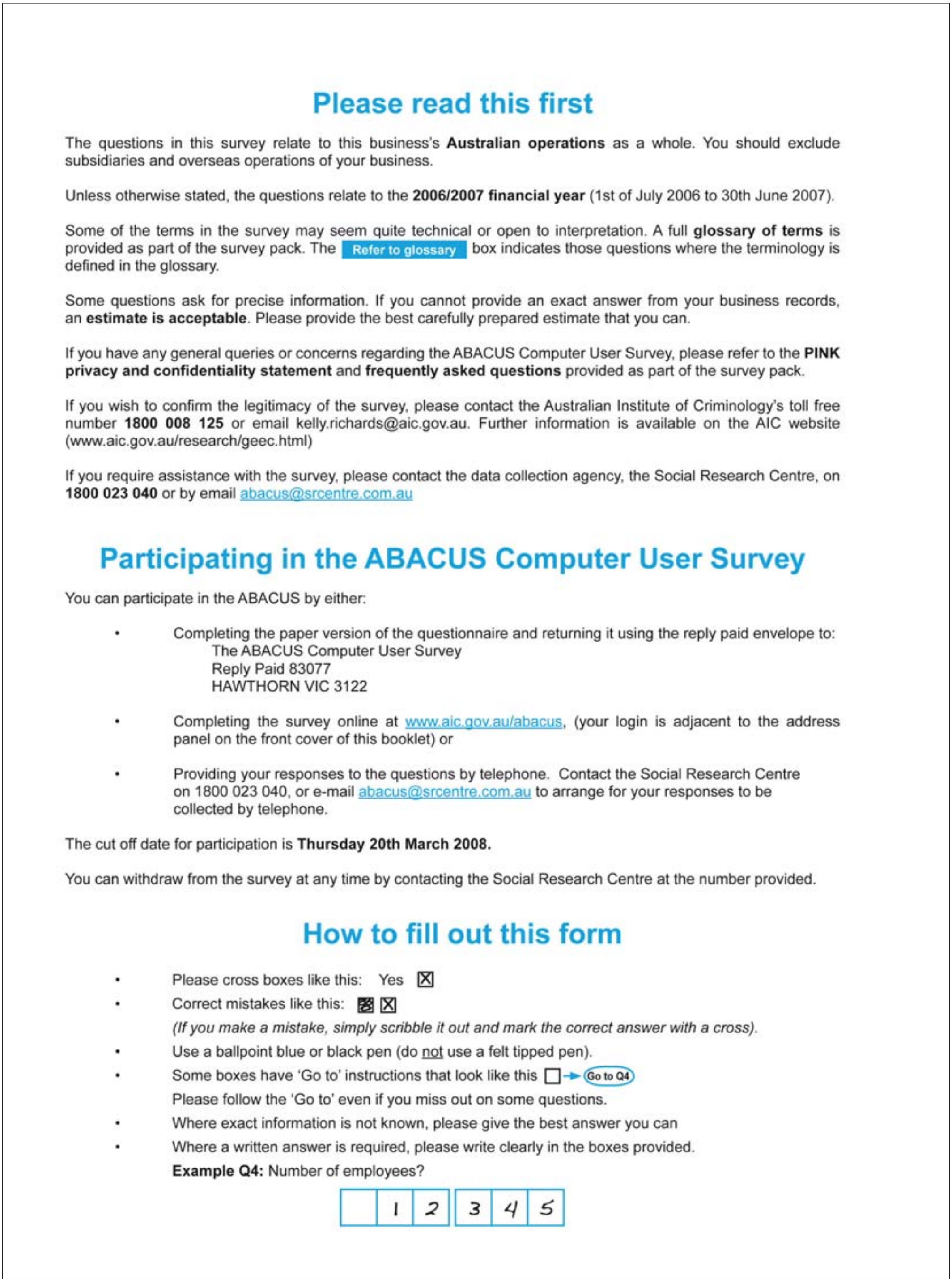
CONTACT NAME (from Q22b, else S2n, else blank)

POSITION TITLE (from S2p, else “The IT Manager”)

COMPANY NAME (from S2c, else Company name in sample record)

CONTACT ADDRESS (from Q22b, else S2a, else Address in sample record).

Appendix B: Questionnaire



Please read this first

The questions in this survey relate to this business's **Australian operations** as a whole. You should exclude subsidiaries and overseas operations of your business.

Unless otherwise stated, the questions relate to the **2006/2007 financial year** (1st of July 2006 to 30th June 2007).

Some of the terms in the survey may seem quite technical or open to interpretation. A full **glossary of terms** is provided as part of the survey pack. The Refer to glossary box indicates those questions where the terminology is defined in the glossary.

Some questions ask for precise information. If you cannot provide an exact answer from your business records, an **estimate is acceptable**. Please provide the best carefully prepared estimate that you can.

If you have any general queries or concerns regarding the ABACUS Computer User Survey, please refer to the **PINK privacy and confidentiality statement** and **frequently asked questions** provided as part of the survey pack.

If you wish to confirm the legitimacy of the survey, please contact the Australian Institute of Criminology's toll free number **1800 008 125** or email kelly.richards@aic.gov.au. Further information is available on the AIC website (www.aic.gov.au/research/geec.html)

If you require assistance with the survey, please contact the data collection agency, the Social Research Centre, on **1800 023 040** or by email abacus@srcentre.com.au

Participating in the ABACUS Computer User Survey

You can participate in the ABACUS by either:

- Completing the paper version of the questionnaire and returning it using the reply paid envelope to:
  The ABACUS Computer User Survey
  Reply Paid 83077
  HAWTHORN VIC 3122
- Completing the survey online at www.aic.gov.au/abacus, (your login is adjacent to the address panel on the front cover of this booklet) or
- Providing your responses to the questions by telephone. Contact the Social Research Centre on 1800 023 040, or e-mail abacus@srcentre.com.au to arrange for your responses to be collected by telephone.

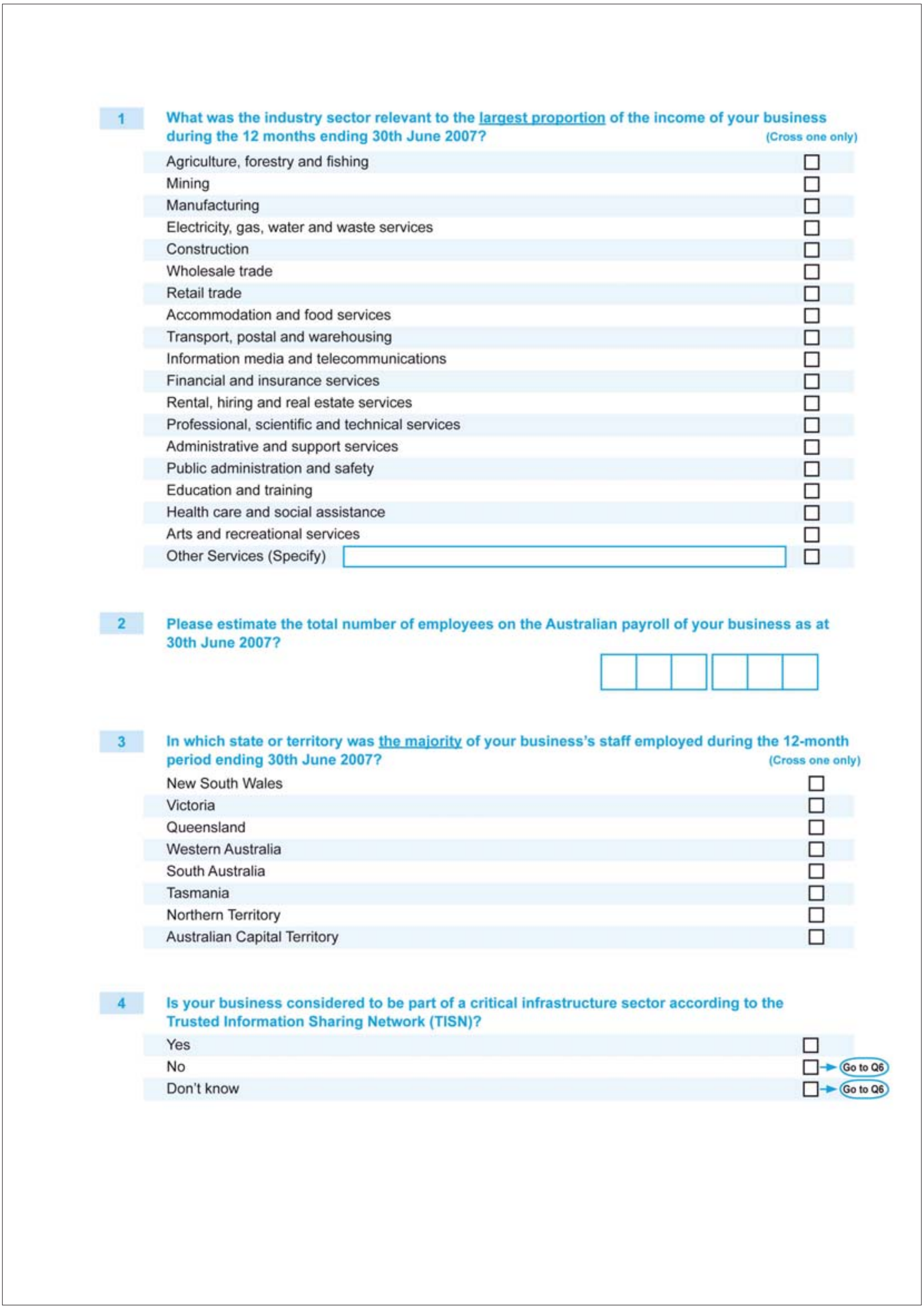
The cut off date for participation is **Thursday 20th March 2008.**

You can withdraw from the survey at any time by contacting the Social Research Centre at the number provided.

How to fill out this form

- Please cross boxes like this: Yes ☒
- Correct mistakes like this: ▨ ☒
  (If you make a mistake, simply scribble it out and mark the correct answer with a cross).
- Use a ballpoint blue or black pen (do not use a felt tipped pen).
- Some boxes have 'Go to' instructions that look like this □ → Go to Q4
  Please follow the 'Go to' even if you miss out on some questions.
- Where exact information is not known, please give the best answer you can
- Where a written answer is required, please write clearly in the boxes provided.
  Example Q4: Number of employees?

	1	2	3	4	5



1 **What was the industry sector relevant to the largest proportion of the income of your business during the 12 months ending 30th June 2007?** (Cross one only)

Agriculture, forestry and fishing □
Mining □
Manufacturing □
Electricity, gas, water and waste services □
Construction □
Wholesale trade □
Retail trade □
Accommodation and food services □
Transport, postal and warehousing □
Information media and telecommunications □
Financial and insurance services □
Rental, hiring and real estate services □
Professional, scientific and technical services □
Administrative and support services □
Public administration and safety □
Education and training □
Health care and social assistance □
Arts and recreational services □
Other Services (Specify) ______ □

2 **Please estimate the total number of employees on the Australian payroll of your business as at 30th June 2007?**

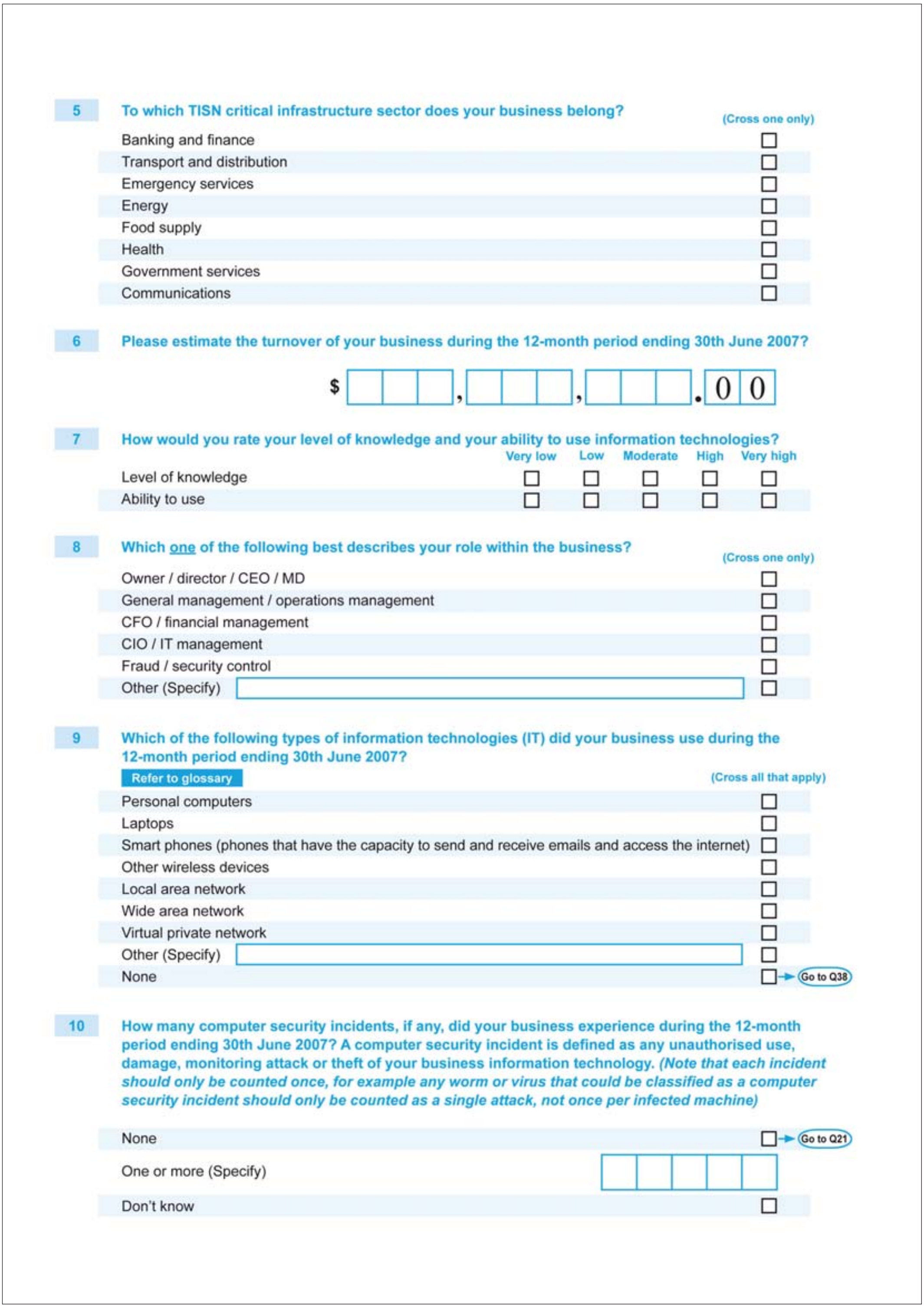
□□□□□□

3 **In which state or territory was the majority of your business's staff employed during the 12-month period ending 30th June 2007?** (Cross one only)

New South Wales □
Victoria □
Queensland □
Western Australia □
South Australia □
Tasmania □
Northern Territory □
Australian Capital Territory □

4 **Is your business considered to be part of a critical infrastructure sector according to the Trusted Information Sharing Network (TISN)?**

Yes □
No □ → Go to Q6
Don't know □ → Go to Q6



5 To which TISN critical infrastructure sector does your business belong?

(Cross one only)

Banking and finance □
Transport and distribution □
Emergency services □
Energy □
Food supply □
Health □
Government services □
Communications □

6 Please estimate the turnover of your business during the 12-month period ending 30th June 2007?

$ □□□,□□□,□□□.00

7 How would you rate your level of knowledge and your ability to use information technologies?

	Very low	Low	Moderate	High	Very high
Level of knowledge	□	□	□	□	□
Ability to use	□	□	□	□	□

8 Which one of the following best describes your role within the business?

(Cross one only)

Owner / director / CEO / MD □
General management / operations management □
CFO / financial management □
CIO / IT management □
Fraud / security control □
Other (Specify) ____________ □

9 Which of the following types of information technologies (IT) did your business use during the 12-month period ending 30th June 2007?

Refer to glossary

(Cross all that apply)

Personal computers □
Laptops □
Smart phones (phones that have the capacity to send and receive emails and access the internet) □
Other wireless devices □
Local area network □
Wide area network □
Virtual private network □
Other (Specify) ____________ □
None □ → Go to Q38

10 How many computer security incidents, if any, did your business experience during the 12-month period ending 30th June 2007? A computer security incident is defined as any unauthorised use, damage, monitoring attack or theft of your business information technology. *(Note that each incident should only be counted once, for example any worm or virus that could be classified as a computer security incident should only be counted as a single attack, not once per infected machine)*

None □ → Go to Q21
One or more (Specify) □□□□□
Don't know □

11 **What types of computer security incidents did your business experience during the 12-month period ending 30th July 2007?**

Refer to glossary

(Cross all that apply)

Insider abuse of access □

Theft or loss of hardware □

Virus or other malicious code □

Spyware □

Phishing □

Denial of service attack □

Sabotage of network or data □

Unauthorised network access □

Theft or breach of proprietary or confidential information □

Incident involving this business's web application □

Other (Specify) ________ □

Don't know □

12 **Of all computer security incidents that your business experienced in the 12-month period ending 30th June 2007, what percentage originated from a person or persons within your business?**

% Internally originating incidents □□□

Don't know □

13 **What percentage of all computer security incidents that affected your business during the 12 months ending 30th June 2007 was referred to each of the following?**

	Complete for each	Don't know
Police	□□□ %	□
Non-police enforcement / regulatory agency	□□□ %	□
An external computer security incident response team e.g. AusCERT	□□□ %	□
Lawyer/s for civil action	□□□ %	□
Electronic payment provider e.g. Visa, MasterCard	□□□ %	□
Other (Specify) ________	□□□ %	□
Dealt with internally - not referred to a third party	□□□ %	□

14 **Which one of the following best describes the computer security incident that caused the greatest financial loss to your business during the 12-month period ending 30th June 2007?**

Refer to glossary

(Cross one only)

Insider abuse of access □

Theft or loss of hardware □

Virus or other malicious code □

Spyware □

Phishing □

Denial of service attack □

Sabotage of network or data □

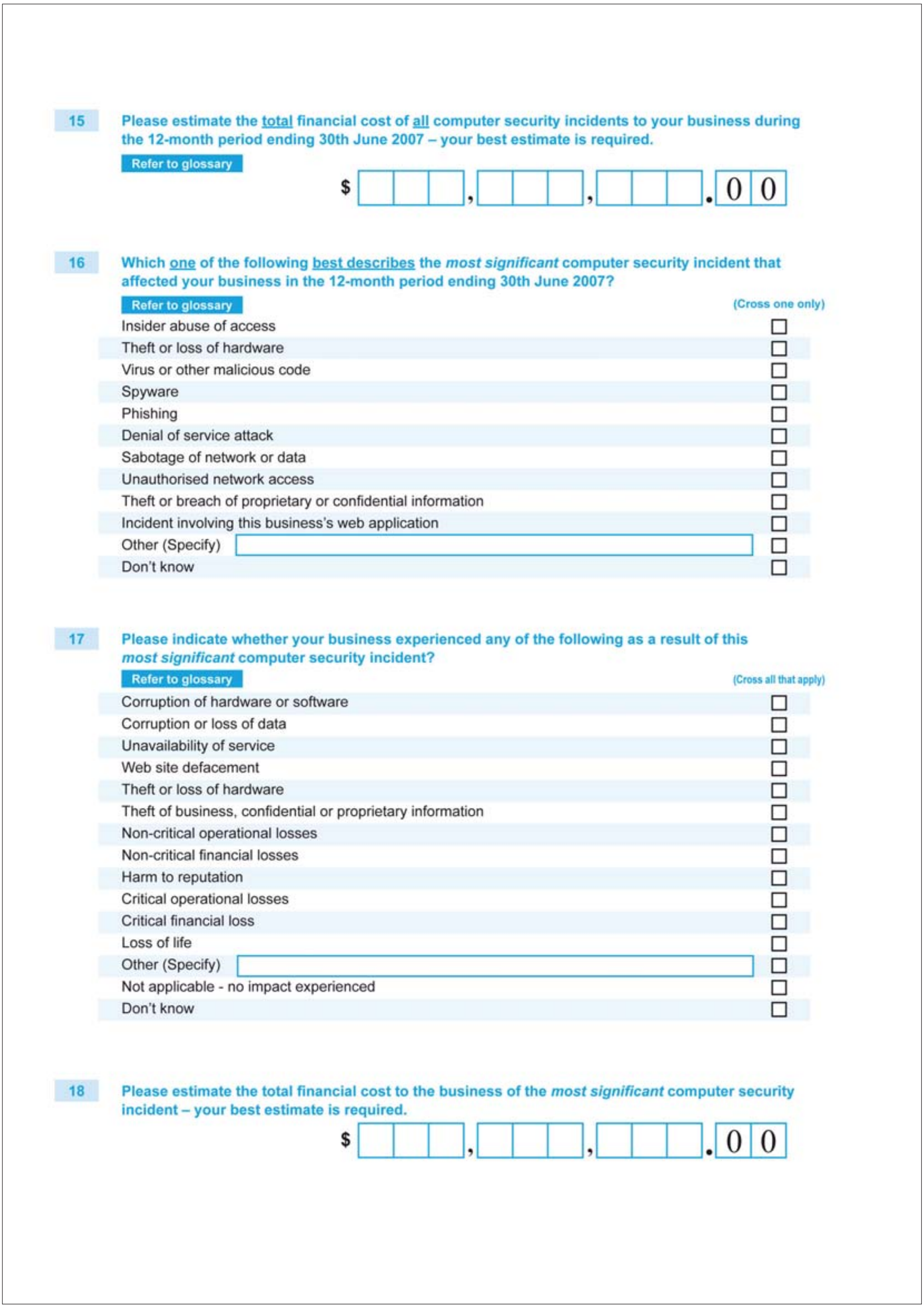
Unauthorised network access □

Theft or breach of proprietary or confidential information □

Incident involving this business's web application □

Other (Specify) ________ □

Don't know □



15 **Please estimate the total financial cost of all computer security incidents to your business during the 12-month period ending 30th June 2007 – your best estimate is required.**

Refer to glossary

$ □□□,□□□,□□□.0 0

16 **Which one of the following best describes the *most significant* computer security incident that affected your business in the 12-month period ending 30th June 2007?**

Refer to glossary

(Cross one only)

Insider abuse of access □
Theft or loss of hardware □
Virus or other malicious code □
Spyware □
Phishing □
Denial of service attack □
Sabotage of network or data □
Unauthorised network access □
Theft or breach of proprietary or confidential information □
Incident involving this business's web application □
Other (Specify) ________ □
Don't know □

17 **Please indicate whether your business experienced any of the following as a result of this *most significant* computer security incident?**

Refer to glossary

(Cross all that apply)

Corruption of hardware or software □
Corruption or loss of data □
Unavailability of service □
Web site defacement □
Theft or loss of hardware □
Theft of business, confidential or proprietary information □
Non-critical operational losses □
Non-critical financial losses □
Harm to reputation □
Critical operational losses □
Critical financial loss □
Loss of life □
Other (Specify) ________ □
Not applicable - no impact experienced □
Don't know □

18 **Please estimate the total financial cost to the business of the *most significant* computer security incident – your best estimate is required.**

$ □□□,□□□,□□□.0 0

19 **For the *most significant* computer security incident that affected your business during the 12-month period ending 30th June 2007....**

a. Which of the following actions were taken, and

b. How satisfied was your business with the outcome obtained as a result of reporting

19a **Action taken** (Cross all that apply)

19b **Satisfaction with outcome** (Cross one only)

	Action taken	Very dissatisfied	Dissatisfied	Neither satisfied nor dissatisfied	Satisfied	Very satisfied	Can't say	
Reported to police	□	□	□	□	□	□	□	Go to Q21
Reported to non-police enforcement / regulatory agency	□	□	□	□	□	□	□	
Reported incidents to an external computer security incident response team e.g. AustCERT	□	□	□	□	□	□	□	
Reported incidents to lawyer for civil action	□	□	□	□	□	□	□	
Reported to an electronic payment provider e.g. Visa, MasterCard	□	□	□	□	□	□	□	
Other (Specify) ________	□	□	□	□	□	□	□	
Only dealt with internally	□	□	□	□	□	□	□	Go to Q20

20 **Which of the following were reasons why your business chose *not* to report the most significant computer security incident to a third party?**

	(Cross all that apply)
Negative publicity	□
Business was not explicitly targeted e.g. worm	□
Nothing to gain	□
Did not think to report	□
Incident outside jurisdiction of law enforcement	□
Did not want data or hardware seized as evidence	□
Did not know who to contact	□
Incident not serious enough to report	□
Competitors would use to their advantage	□
Dealt with internally	□
Fear of reprisals	□
Fear of repeat victimisation	□
Other (Specify) ________	□
Don't know	□

21 **Which of the following computer security measures did your business use during the 12-month period ending 30th June 2007?**

Refer to glossary

	(Cross all that apply)
No computer security tools or procedures were used	□
Physical security	
Keeping servers in secure rooms	□
Limiting access to workstations	□
Physically securing laptop computers	□
Physically securing wireless devices	□
Physical security used but unable to specify	□
Other (Specify)	□
Cryptographic & authentication tools	
Digital Certificates	□
Biometrics	□
Smartcards	□
Security tokens (other than smartcards)	□
Password verification	□
Single sign on	□
Encryption of data	□
File integrity assessment tool	□
Encrypting removable data storage devices	□
Cryptographic and authentication tools used but unable to specify	□
Other (Specify)	□
Anti fraud & malware tools	
Anti-spam filters	□
Anti-virus software	□
Anti-spyware software	□
Anti-phishing software	□
Anti-fraud and malware technologies used but unable to specify	□
Other (Specify)	□
Detection & monitoring tools	
Internet content / image filtering or monitoring	□
Intrusion detection system	□
Intrusion prevention system	□
Detection and monitoring tools used but unable to specify	□
Other (Specify)	□
Security Management Tools	
Endpoint security client software	□
Firewall	□
Vulnerability management system	□
Provisioning system	□
Security compliance tools	□
Instant messaging security solutions	□
Manual patch management	□
Automated patch management	□
Configuration management	□
Security management technologies used but unable to specify	□
Other (Specify)	□
Other measures (Specify)	□
Don't know	□

22 **Were any of the computer security measures of your business outsourced to one or more third parties during the 12-month period ending 30th June 2007?**

Yes □

No □ → Go to Q26

Don't know □ → Go to Q26

23 **Were any of the third parties based primarily in a country other than Australia?**

Yes □

No □

Don't know □

24 **How were the outsourced computer security measures reviewed or evaluated?**

Refer to glossary

(Cross all that apply)

Security audit by internal staff □

Security audits by external businesses □

Security compliance check □

Other (Specify) ________ □

Third party performance was evaluated but unable to specify □

Don't know □

Not reviewed or evaluated □ → Go to Q26

25 **Approximately how often was the work of this third party evaluated or reviewed?** (Cross one only)

Weekly □

Monthly □

Quarterly □

Biannually □

Annually □

Ad hoc □

Other (Specify) ________ □

Don't know □

26 **What type of computer security related <u>policies</u> did your business have during the 12-month period ending 30th June 2007?** (Cross all that apply)

Refer to glossary

Did not have any computer security policies □ → Go to Q28

Staff/user related policies

Employee education and awareness program □

Segregation of duties □

System content monitoring □

Wireless technology acceptable use policy □

IT acceptable use policies □

Mobile policies (such as mandatory encryption of data stored on mobile devices) □

User access management □

Background checks □

Mandatory reporting of misuse / abuse of computer equipment □

Documented standard operating procedures □

Monitor internet connections □

Account / password management policies □

Staff / user related policy used but unable to specify □

Other (Specify) ________ □

Security testing policies

System penetration testing □

System audit policies □

Risk assessment policies □

Security testing policy used but unable to specify □

Other (Specify) ________ □

Continued over page.....

Data related policies

Media backup procedures □

Management of removable computer media storage devices □

Protection of electronic account information e.g. customer account details □

Data related policy used but unable to specify □

Other (Specify) ______ □

Incident response policies

Use of incident response team □

Business continuity policy □

Forensic plan □

Incident management procedures □

Incident response policy used but unable to specify □

Other (Specify) ______ □

External business policies

Payment system supplier policies □

Other supplier determines policies □

External business policy used but unable to specify □

Other (Specify) ______ □

Wireless security policies

Secure placement of access points □

Name of network changed from default □

Encrypted signals □

Connections restricted to known devices only □

Wireless monitoring □

Wireless computer security policies used but unable to specify □

Other (Specify) ______ □

Other policies (Specify) ______ □

Don't know □

27 **Which of the following IT standards were used in the development of your business's current IT policies** **(Cross all that apply)**

AS / NZS ISO / IEC 17799:2005 - Code of practice for information security management □

AS / BS7799.2:2003 - Information security management □

ACSI 33 – Australian Government Information Security Manual □

HB 231 2003 Information Security Risk Management □

HB 171:2003 – Guidelines for management of IT evidence □

RFC 2196 – Site security handbook □

ISO/IEC 13335 – 1:2004 Information technology. Guidelines for the management of IT security □

State government IT Security standard □

Other (Specify) ______ □

Don't know □

No standards used □

28 **How often was the effectiveness of your business's computer security evaluated during the 12-month period ending 30th June 2007?** **(Cross one only)**

Frequency (Specify) ______ □

Don't know □

Computer security was not evaluated □ → Go to Q30

29 **Which of the following methods did your business use to evaluate the effectiveness of its computer security measures during the 12-month period ending 30th June 2007**

Refer to glossary

	(Cross all that apply)
Security audit by internal staff	□
Security audits by external businesses	□
Automated tools	□
Email monitoring software	□
Web activity monitoring software	□
Other (Specify) ________________	□
Don't know	□

30 **Please estimate the total IT expenditure for your business during the 12-month period ending 30th June 2007 – your best estimate is required.**

Refer to glossary

$ □□□,□□□,□□□.0 0

31 **Please estimate the total amount spent on computer security measures by your business during the 12-month period ending 30th June 2007 – your best estimate is required.**

$ □□□,□□□,□□□.0 0

32 **What percentage of expenditure on computer security measures during the 12-month period ending 30th June 2007 was for each of the following?**
Please refer to Q21 for examples of what is included in each category listed below

	Complete for each	Don't know
Physical security	□□□ %	□
Cryptographic and authentication tools	□□□ %	□
Anti fraud and malware technologies	□□□ %	□
Detection and monitoring tools	□□□ %	□
Security management technologies	□□□ %	□
Other (Specify) ________________	□□□ %	□

33 **Compared with expenditure on computer security measures in the previous financial year (i.e. ending June 2006), did expenditure on computer security measures in the 12-month period ending 30th June 2007 increase, decrease or stay the same?**

Increase	□□□ %
Decrease	□□□ %
Stayed the same	□
Don't know	□

34 **Which of the following types of computer security incidents are covered by your business's computer security insurance policy?**

Refer to glossary

(Cross all that apply)

Insider abuse of access □
Theft or loss of hardware □
Virus or other malicious code □
Spyware □
Phishing □
Denial of service attack □
Sabotage of network or data □
Unauthorised network access □
Theft or breach of proprietary or confidential information □
Incident involving this business's web application □
Other (Specify) ________ □
Don't know □ → Go to Q37
No computer security incidents are covered by this business's insurance □ → Go to Q37

35 **Did your business make any claims on its insurance policies for losses due to computer security incidents during the 12-month period ending 30th June 2007?**

Yes □
No □ → Go to Q37
Don't know □ → Go to Q37

36 **Were you required to report computer security incidents to a law enforcement agency prior to making a claim against your insurance?**

Yes □
No □
Don't know □

37 **Are you familiar with any of the following awareness raising initiatives?**

(Cross all that apply)

Stay Smart Online http://www.staysmartonline.gov.au □
Scamwatch http://www.scamwatch.gov.au □
FIDO http://www.fido.gov.au □
The Australian High Tech Crime Centre http://www.ahtcc.gov.au □
AusCert http://www.auscert.org.au □
Stay Safe Online http://www.staysafeonline □
Other (Specify) ________ □
Not aware of any of these initiatives □

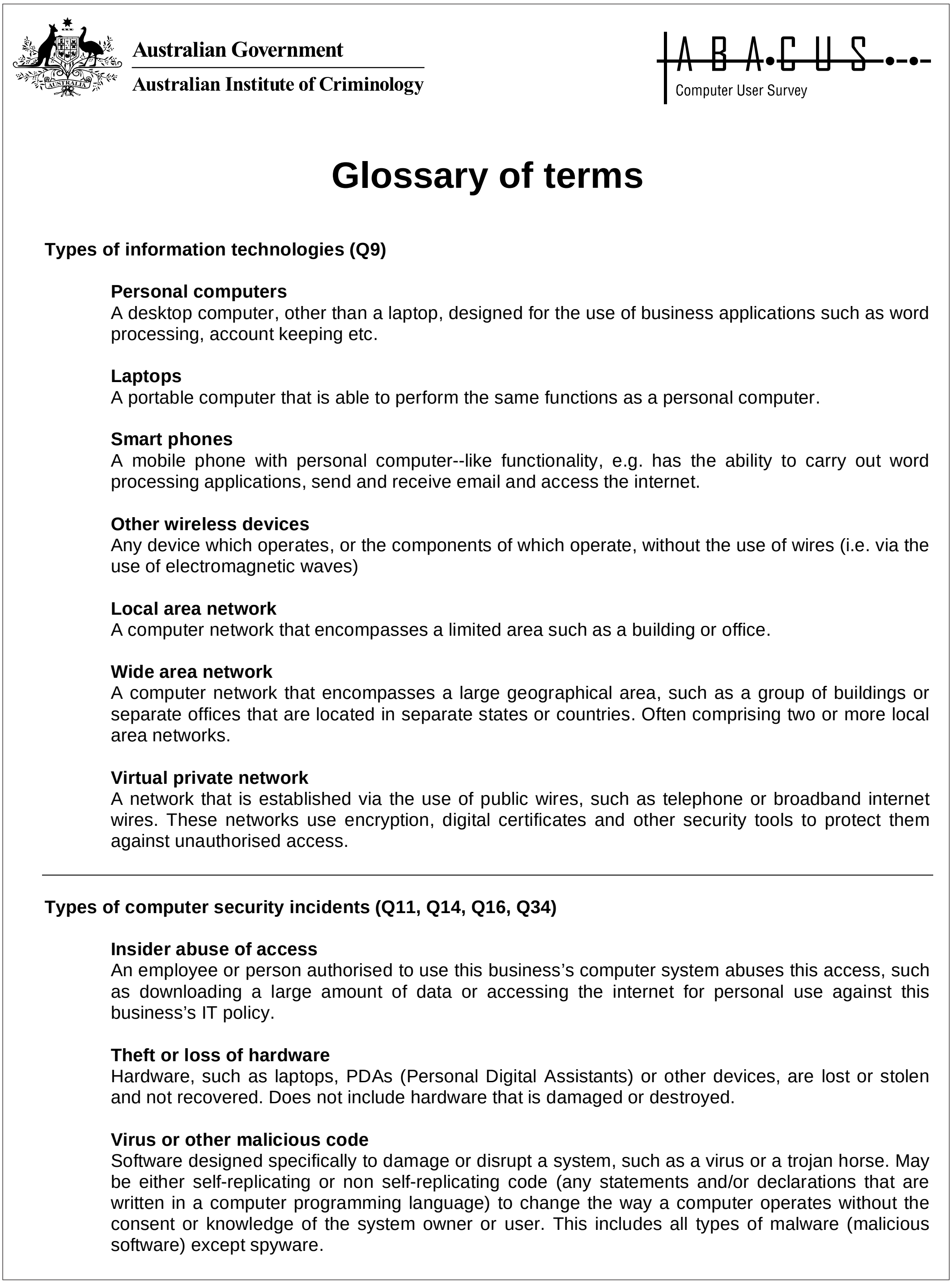
38 **Please provide an estimate of the time taken to complete this form** Hrs □□ Mins □□

This includes time actually spent reading the instructions, working on the questions and sourcing the information, and any time spent by other employees in collecting and providing the information

Thank you for taking the time to complete this survey.
Please return it in the reply paid envelope to:

The ABACUS Computer User Survey
Reply Paid 83077
HAWTHORN VIC 3122

Appendix C: Glossary



Australian Government
Australian Institute of Criminology

ABACUS
Computer User Survey

Glossary of terms

Types of information technologies (Q9)

Personal computers
A desktop computer, other than a laptop, designed for the use of business applications such as word processing, account keeping etc.

Laptops
A portable computer that is able to perform the same functions as a personal computer.

Smart phones
A mobile phone with personal computer--like functionality, e.g. has the ability to carry out word processing applications, send and receive email and access the internet.

Other wireless devices
Any device which operates, or the components of which operate, without the use of wires (i.e. via the use of electromagnetic waves)

Local area network
A computer network that encompasses a limited area such as a building or office.

Wide area network
A computer network that encompasses a large geographical area, such as a group of buildings or separate offices that are located in separate states or countries. Often comprising two or more local area networks.

Virtual private network
A network that is established via the use of public wires, such as telephone or broadband internet wires. These networks use encryption, digital certificates and other security tools to protect them against unauthorised access.

Types of computer security incidents (Q11, Q14, Q16, Q34)

Insider abuse of access
An employee or person authorised to use this business's computer system abuses this access, such as downloading a large amount of data or accessing the internet for personal use against this business's IT policy.

Theft or loss of hardware
Hardware, such as laptops, PDAs (Personal Digital Assistants) or other devices, are lost or stolen and not recovered. Does not include hardware that is damaged or destroyed.

Virus or other malicious code
Software designed specifically to damage or disrupt a system, such as a virus or a trojan horse. May be either self-replicating or non self-replicating code (any statements and/or declarations that are written in a computer programming language) to change the way a computer operates without the consent or knowledge of the system owner or user. This includes all types of malware (malicious software) except spyware.

Types of computer security incidents (Q11, Q14, Q16, Q34) (continued)

Spyware
Software designed to collect information from a computer secretly and send it elsewhere (e.g. key loggers) or change settings and interfere with the performance of a compromised computer.

Phishing
Assuming the identity of a legitimate organisation or website using forged email, fraudulent websites or other instant messaging communication forums such as MSN, to persuade others to provide information – usually personal financial, such as credit card numbers, account user names and passwords, social security numbers – for the purpose of using it to commit fraud.

Denial of service attack
An attack aimed at specific web sites by flooding the web server with repeated messages, depleting the system resources and denying access to legitimate users.

Sabotage of network or data
Intentional destruction of, or damage to, a computer network or to data stored on a network or stand alone computer.

Unauthorised network access
Obtaining access to a restricted computer network, without providing adequate credentials such as logon name and password.

Theft or breach of proprietary or confidential information
The unauthorised access to, and/or, use, viewing, duplication, distribution or theft of, proprietary or confidential information. *Proprietary information* is information relating to or associated with this business's product, business or activities. It includes, but is not limited to, items such as trade secrets, research and development and financial information.

Incident involving the business's web application
Any malicious or destructive incident that involves this business's website. This might include placing unauthorised information on a website or preventing it from being used as intended.

Financial loss (Q14) and financial cost (Q15)

Financial cost and financial loss (as relating to either a specific computer security incident or all computer security incidents) should include all costs associated with the incident/s. These may include aspects such as the direct financial cost of the incident, staff costs in repairing the damage caused, loss of revenue due to the incident or any other cost that was a direct result of the incident. Do not include computer security measures implement before or after the incident accorded.

Most significant incident (Q16 to Q20)

The most significant incident is the one that your business regards as causing the greatest negative effect or loss. Such incidents may include ones that caused the greatest financial loss, caused damage to your business's reputation and/or other negative effects.

Computer security incident outcomes (Q17)

Corruption of hardware of software
Damage to computer hardware or software that renders it, in part or in whole, non-operational.

Corruption or loss of data
Damage to or interference with data that renders it, in part or in whole, non-operational.

Unavailability of service
Making the operations of your business either in part or in whole unavailable.

Computer security incident outcomes (Q17) (continued)

Web site defacement
Damage caused to a public web site that limits or prevents its intended use.

Theft or loss of hardware
(Refer definition at Q11, Q14, Q16, Q34 above).

Theft of business, confidential or proprietary information
(Refer definition at Q11, Q14, Q16, Q34 above).

Non-critical operational losses
A disruption to your business that did not cause suspension or severe damage to your business's operations.

Non-critical financial losses
Loss of money or value to your business that did not cause a severe negative alteration to your business's financial state.

Harm to reputation
The reduction in confidence in your business or an increase in negative association with your business.

Critical operational losses
A disruption to your business that caused suspension or severe damage to your business's operations.

Critical financial loss
Loss of money or value to your business that causes severe negative alteration to your business's income or assets.

Loss of life
The death of a person who was, or was not, an employee of your business.

Computer security measures (Q21)

Physical security
Using devices, such as locks, to secure computer hardware

Cryptographic and authentication tools
Cryptography is a means of scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called 'encryption'), then back again (known as 'decryption') – this enables securing of private information sent through public networks by encrypting it in a way that makes it unreadable to anyone except the person or persons holding the mathematical key or knowledge to decrypt the information..

Authentication software or hardware is designed to verify the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Digital certificates
Electronic documents signed by a trusted Certification Authority (CA) which identifies the key holder and the affiliated business entity, binds the key holder to a public/private key pair, and contains other information required by the certificate profile (e.g. X.509, a commonly used ITU-T standard for public key infrastructure).

Biometrics
The use of a person's physical or behavioural characteristics as a form of identification and authentication. It includes, but is not limited to, retinal scans, finger/hand scans, keyboard ballistics, handwriting etc.

Computer security measures (Q21) (continued)

Smartcards
Smartcards, also known as chip cards, are plastic cards containing integrated circuits for information system access and identification and the holding of digital credentials and electronic value tokens.

Security tokens (other than smartcards)
Hardware devices designed to provide two-factor authentication by generating a one-time authentication key – in addition to a password or pin – which allows access to a network or system resources.

Password verification
The use of a password that is linked to an individual user account which allows access to network or system resources.

Single sign on
An identity management mechanism that allows account holders to authenticate themselves once when accessing inter-connected network and system resources.

Encryption of data
The process of scrambling or encoding of information to ensure that only the intended recipient (holding the corresponding decryption key or password) can read the information.

File integrity assessment tool
Software or hardware used to verify the integrity of the files' contents (i.e. to determine if a file has been modified).

Encrypting removable data storage devices
The process of scrambling or encoding of information on removable storage devices (such as USB drives or removable hard drives) to ensure that only the intended recipient (holding the corresponding decryption key or password) can read the information.

Anti fraud and malware tools
Software or hardware designed to prevent fraud or malware (such as viruses) affecting a system or network.

Anti-spam filters
Software or hardware designed to identify, block and manage unsolicited email messages that are often used to commit fraud.

Anti-virus software
Software tools designed to identify, thwart and eliminate malicious code (i.e. virus, Trojans and worms) from a system, incoming email message, etc.

Anti-spyware software
Software designed to detect and remove spyware from a system (refer Q11, Q14, Q16, Q34 above for a definition of spyware).

Anti-phishing software
Software designed to detect and prevent phishing attacks and the fraud that results from them. They can include Uniform Resource Locator (URL) blockers and fraud detection technologies. (refer Q11, Q14, Q16, Q34 above for a definition of phishing).

Detection and monitoring tools
Software or hardware designed to monitor the use of a specific computer system or network.

Internet content filtering / image filtering or monitoring
Software or hardware designed for monitoring and limiting access to inappropriate information or data configured according to the organization's security policy.

Computer security measures (Q21) (continued)

Intrusion detection system
Software applications designed to protect backbone services by detecting inappropriate, incorrect, or anomalous activities that cannot usually be detected by a conventional firewall.

Intrusion prevention system
Software or hardware designed to protect computers from exploitation by identifying and blocking potentially malicious activity in real-time.

Security management tools
Software or hardware designed with the specific goal of managing and improving the security of computer systems and networks.

Endpoint security software
Endpoint security software, a suite of software and hardware, designed to work to prevent security breaches (e.g. data leakages) and to conform to defined enterprise and desktop security policies at endpoints. The latter can be an individual computing or storage device such as a client workstation for a network or personal computing device including laptops, desktops and PDAs (Personal Digital Assistant).

Firewall
Software or hardware, designed for the protection of a network from unauthorised access, which permits, denies or provides proxy data connections configured according to the organization's security policy.

Vulnerability management system
A process in which vulnerabilities are found and fixed and vulnerable systems are shielded. It includes configuration policy compliance, threat information, asset clarification, prioritisation and workflow.

Provisioning system
Provisioning systems allows the management of user accounts and user profiles that are linked to a person across an IT environment through a combination of user roles and business rules.

Security compliance tools
Software applications that enforce corporate and/or regulatory policies and standards.

Instant messaging security solutions
Software applications that enforce instant messaging (IM) usage policies such as the types of IM applications and IM attachments which are allowed.

Manual patch management
The process of controlling the deployment and maintenance of interim software releases (e.g. software updates) and security patches into production environments.

Automated patch management
The process of patch management, with minimal human intervention, that enables automated analysis targeting and distribution of granular level patches (individual patches vs. large service packs) and rapid quality-assurance testing.

Configuration management
The establishment of approved changes to the configuration of a computer system or network and the interrelation between system components.

Computer security policies (Q26)

Staff related policies
Any computer security policy that is directed at the staff of this business.

Employee education and awareness program
Courses, seminars and other activities that are designed to increase the awareness and understanding of the business's employees of issues relating to computer security.

Segregation of duties
Where no individual has control over two or more phases of a transaction or operation within a business environment, designed to prevent fraud.

System content monitoring
A system designed to specifically monitor information that is coming in and/or going out to/from this business's systems.

Wireless technology acceptable use policy
A policy that clearly defines what type of use is acceptable for this business's wireless technology, i.e. acceptable download limits for wireless device.

IT acceptable use policies
A policy that clearly defines what type of use is acceptable for this business's information technology, e.g. acceptable levels of personal use.

Mobile policies (such as mandatory encryption of data stored on mobile devices)
A policy that specifically relates to the use of mobile devices, such as PDAs (Personal Digital Assistants). These types of polices can mandate what type of data may be stored on these devices or data that is required to be encrypted.

User access management policies
A policy that governs access rights (privileges) of individuals on your business's systems. These may also include the appropriate access rights of individuals to be recorded in an Access Control List.

Background checks
A policy that requires verification of information provided by employees of this business, such as checking for a criminal history prior to offering a candidate a position with this business.

Mandatory reporting of misuse / abuse of computer equipment
Policies that require a person to report misuse or abuse of computer equipment as soon as they become aware of it. This may include situations where an individual uses this business's system to download large amounts of personal data or access illegal or offensive content.

Documented standard operating procedures
A set of written instructions that governs the appropriate use of this business' information technologies.

Monitoring internet connections
A policy that governs how individual users' internet activity is monitored.

Account/password management policies
A policy that specifically relates to users' account and password information. These may include mandatory password lengths or frequency of password renewal.

Security testing policies

System penetration testing
A method to evaluate the security of a computer, system or network by simulating an electronic attack (i.e. an attack by a hacker).

Computer security policies (Q26) (continued)

System audit policies
Policies mandating audits of this business's computers, including issues such as the frequency and type of audits carried out and details of those responsible for undertaking those audits. This is a measurable technical assessment of a network, system or application.

Risk assessment policies
Policies that govern the type and frequency of risk assessment of this business. Risk assessment is a process where the magnitude of potential loss and the probability it will occur are measured.

Data related policies
Any polices that relate to the handling, storage and security of data for this business.

Media backup procedures
Set policies and procedures that govern how the backup of data is recorded, stored and the frequency with which the backup occurs.

Management of removable computer media storage devices
Policies and procedures that govern if, how and when removable computer media devices can be used. For the purpose of this survey a removable computer media storage device is a device that connects either physically or wirelessly to another host or client device and allows the exchange of data between the two devices (e.g. USB drive or a removable hard drive, but excluding CDs, DVDs and Diskettes).

Protection of electronic account information
Policies relating to the protection of customer, client or partner business information, such as credit card and personal details.

Incident response policies
Incident response policies include any policies that govern what responses are appropriate after a computer security incident has occurred.

Use of incident response team
Does this business use consultants, not comprised of employees of this business, to investigate and respond to computer security incidents.

Business continuity policy
A policy or plan that allows a business to conduct its normal operations in the event of computer systems being non-operational or being severely impeded in their operation.

Forensic plan
A policy or set of guidelines that governs the preservation of digital evidence following a computer security incident.

Incident management procedures
A policy or set of guidelines that dictates a standard procedure for dealing with computer security incidents.

External business policies

Payment system supplier policies
Policies that your business is required to follow in order to use an external payment system provider (such as Paypal or credit card payments).

Other supplier determines policies
Policies that your business is required to follow in order to conduct business or use the services of another business.

Computer security policies (Q26) (continued)

Wireless security policies
Wireless security policies govern what types of security practices are used for the protection of data that is stored and transferred between wireless devices (refer Q7 for definition of wireless)

Secure placement of access points
Placement of wireless access points in a secure location, such as ceiling or on a high wall.

Name of network changed from default
Changing the default (original) name of the network to a unique name.

Encrypted signals
All signals sent by both wireless hosts and connecting devices are sent in an encrypted format.

Connections restricted to known devices only
Only hardware devices that have been "set up" as part of the wireless network are able to access the network.

Wireless monitoring
Monitoring content that is sent and received by a wireless device.

Computer security and outsourcing evaluation methods (Q24, Q29)

Security audit by internal staff
A measurable technical assessment of a network, system or application that is carried out by a staff member of this business.

Security audits by external businesses
A measurable technical assessment of a network, system or application that is carried out a person who is not a staff member of this business, e.g. a consultant.

Security compliance check
A form of assessment used to check a variety of security issues in terms of their compliance with a policy or guideline.

Automated tools
The use of software to monitor and report on the status of, and changes to files and settings on individual systems, networks, servers etc.

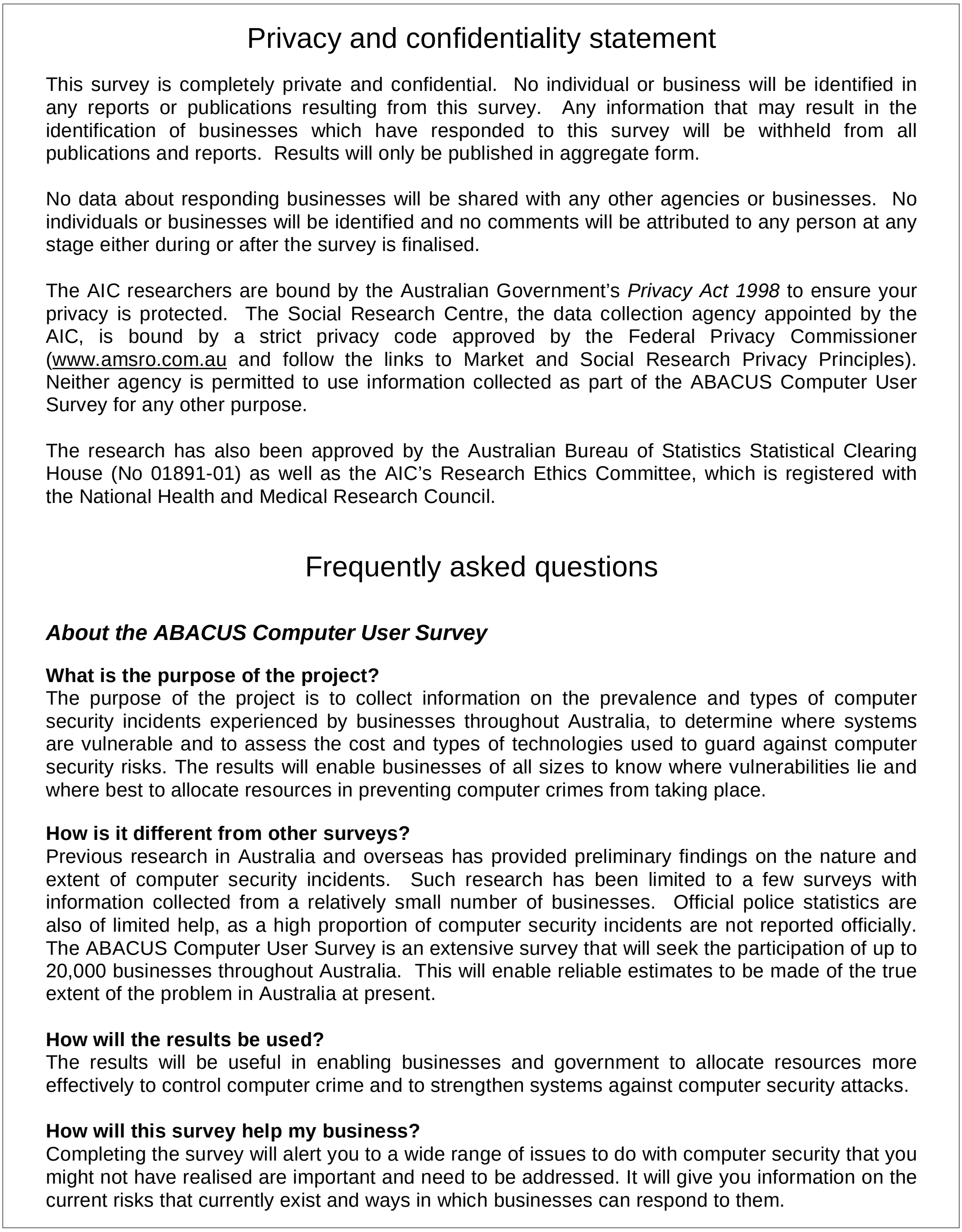
E-mail monitoring software
Software that is designed to monitor the email activity of users.

Web activity monitoring software
Software that is designed to monitor the web activity (sites visited etc) of a specific user or users.

IT expenditure (Q30)

IT expenditure includes all types of expenditure relating to your business's information technology. These may include the cost of IT training, software and hardware and salaries for IT staff.

Appendix D: Frequently asked questions sheet



Privacy and confidentiality statement

This survey is completely private and confidential. No individual or business will be identified in any reports or publications resulting from this survey. Any information that may result in the identification of businesses which have responded to this survey will be withheld from all publications and reports. Results will only be published in aggregate form.

No data about responding businesses will be shared with any other agencies or businesses. No individuals or businesses will be identified and no comments will be attributed to any person at any stage either during or after the survey is finalised.

The AIC researchers are bound by the Australian Government's *Privacy Act 1998* to ensure your privacy is protected. The Social Research Centre, the data collection agency appointed by the AIC, is bound by a strict privacy code approved by the Federal Privacy Commissioner (www.amsro.com.au and follow the links to Market and Social Research Privacy Principles). Neither agency is permitted to use information collected as part of the ABACUS Computer User Survey for any other purpose.

The research has also been approved by the Australian Bureau of Statistics Statistical Clearing House (No 01891-01) as well as the AIC's Research Ethics Committee, which is registered with the National Health and Medical Research Council.

Frequently asked questions

About the ABACUS Computer User Survey

What is the purpose of the project?
The purpose of the project is to collect information on the prevalence and types of computer security incidents experienced by businesses throughout Australia, to determine where systems are vulnerable and to assess the cost and types of technologies used to guard against computer security risks. The results will enable businesses of all sizes to know where vulnerabilities lie and where best to allocate resources in preventing computer crimes from taking place.

How is it different from other surveys?
Previous research in Australia and overseas has provided preliminary findings on the nature and extent of computer security incidents. Such research has been limited to a few surveys with information collected from a relatively small number of businesses. Official police statistics are also of limited help, as a high proportion of computer security incidents are not reported officially. The ABACUS Computer User Survey is an extensive survey that will seek the participation of up to 20,000 businesses throughout Australia. This will enable reliable estimates to be made of the true extent of the problem in Australia at present.

How will the results be used?
The results will be useful in enabling businesses and government to allocate resources more effectively to control computer crime and to strengthen systems against computer security attacks.

How will this survey help my business?
Completing the survey will alert you to a wide range of issues to do with computer security that you might not have realised are important and need to be addressed. It will give you information on the current risks that currently exist and ways in which businesses can respond to them.

Who is funding this survey?
The ABACUS Computer User Survey is being paid for out of an Australian Government fund that is drawn from assets confiscated from criminals in the past. It is being carried out by the Australian Institute of Criminology (www.aic.gov.au), Australia's national centre for research into crime and justice matters, with the assistance of the Social Research Centre (www.srcentre.com.au), a private research organisation based in Melbourne, which specialises in providing research services to government agencies. The Social Research Centre is responsible for collecting ABACUS data from participating businesses and providing a **de-identified** data file to the AIC researchers who will analyse the data and write-up the results of the study.

Who can I contact if I have questions?
If you wish to confirm the legitimacy of the survey, please contact the Australian Institute of Criminology's toll free number **1800 008 125** or email kelly.richards@aic.gov.au. Further information is available on the AIC website (www.aic.gov.au/research/geec.html)

If you require assistance completing the survey, please contact the data collection agency, the Social Research Centre, on **1800 023 040** or by email abacus@srcentre.com.au

About ABACUS participants

Who is taking part in the study?
Up to 20,000 businesses of all sizes and from all industry sectors across Australia will be approached as part of the ABACUS Computer User Survey.

We are a small business with minimal IT infrastructure. Why should we take part?
It is important for businesses of all types and sizes to take part, so we can understand how computer crime affects the whole business sector in Australia. Even if you only use a computer for preparing accounts, word processing or managing your contacts, we would still very much appreciate your participation.

What will my business get in return for participating?
The results of the study will be published in 2008 and you will find out information on the scale of computer security issues throughout Australia, as well as how they affect specific industry sectors and different business types.

How was my business selected?
Your company was randomly selected from the Australian Bureau of Statistics Business Register to represent similar organizations within your industry sector across Australia. Your participation is crucial to ensure that the snapshot taken of computer security issues accurately reflects what is happening within your industry sector as well as across Australia as a whole. Prior to approaching any businesses the AIC had to undergo a rigorous approval process with the Australian Bureau of Statistics, Statistical Clearing House to ensure that the questionnaire met with expectations regarding business surveys.

Am I required to take part?
Participation in the ABACUS Computer User Survey is voluntary, but the importance of having your business represented as a part of this study cannot be stressed enough. Your participation is crucial to ensure that the snapshot taken of computer security issues accurately reflects what is happening within your industry sector as well as across Australia as a whole.

Which other companies are taking part?
The sample consists of thousands of companies across all business sectors. They range in size from small companies with just a few employees to large, nationally recognized conglomerates. The identity of all sampled companies is confidential and will not be made public.

Appendix E: Non-response follow-up script

ABACUS main survey—2nd reminder call script

NOTE: questionnaire version used for last round of reminder calls (when too close to end of fieldwork period to re-send pack).

S1 Good (...) my name is (...). I'm calling on behalf of the Australian Institute of Criminology from the Social Research Centre. May I please speak to (name on sample/IT MANAGER)?

EXPLAIN IF NECESSARY: We recently invited (name on sample/IT Manager) to participate in an important national study currently being conducted by the Australian Institute of Criminology to examine the extent and impact of computer user security incidents.

1. Continue with named contact person/IT Manager
2. HARD—Make appointment to speak with named contact person/IT Manager (RECORD NAME AND SCHEDULE APPOINTMENT)
3. SOFT—Make appointment to speak with named contact person/IT Manager (RECORD NAME AND SCHEDULE APPOINTMENT)
4. (SUPPRESS CODE) CALLED 1800 NUMBER TO COMPLETE SURVEY OVER PHONE (GO TO S3B)
5. Refused to pass on to named person (GO TO PROFILE)

S1a We recently sent you a mail pack which included information about an important national study currently being conducted by the Australian Institute of Criminology to examine the extent and impact of computer user security incidents. The mail pack was addressed to (you/the IT Manager).

IF THINKS SURVEY DOES NOT APPLY TO BUSINESS, SAY: If that's the case then we would still like to collect some information which will take 1–2 minutes of your time. Would it be alright to ask these quick questions now to profile your business for our study? IF YES, SELECT CODE 8 (NOT SURE WHETHER APPLIES) AT NEXT QUESTION FOR PROFILING QUESTIONS.

Firstly, did you receive the mail pack?

IF NECESSARY: The pack included a short questionnaire that could be mailed back completed on line, or by phone.

1. Yes
2. No (GO TO S3A2)
3. Refuses to participate (GO TO PROFILE)

*(RECEIVED CENSUS PACK)

S2 That's great. Have you had the chance to complete it as yet?

1. Yes, completed hardcopy (not yet mailed back) (GO TO S4)
2. Yes, completed hardcopy and mailed back (GO TO END2)
3. Yes, completed online (GO TO END2)
4. No, not yet completed (GO TO S4)
5. Would like to complete on the phone (GO TO S3b)
6. Would like to complete online (GO TO S3A)
7. No, do not intend/refuse to complete (GO TO PROFILE)
8. Not sure whether applies to me—haven't had any computer security incidents/don't use computers (GO TO S5)

*(NOT RECEIVED MAIL PACK)

S3a2 That's OK, we can organise for you to complete the survey either online or over the phone.

IF NOT ALREADY MENTIONED: Just to give you a little more information about the project: The study, called the ABACUS Computer User Survey is being undertaken to enhance the understanding of computer security issues facing businesses today and will assist in informing suitable risk management strategies. This will help businesses such as yours to be well-informed so that you are able to set priorities and better target scarce resources to maximise your business's security. Participation in the study is expected to take up to 20 minutes. More information including frequently asked questions and privacy provisions that apply to the study is available on our website at www.srcentre.com.au/respondents under ABACUS.

Would you prefer to complete the study online or over the phone?

1. Complete online
2. Complete over the phone (GO TO S3b)
3. Not sure whether applies to me—haven't had any computer security incidents/don't use computers (GO TO S5).

*(PREFER TO COMPLETE ONLINE)

S3a You can complete the survey online by going to www.aic.gov.au/abacus and your login is (WEB LOGON ID FROM SAMPLE). You will be prompted to select a password prior to beginning the survey so you can go back to it at a later time—if you don't have time to complete the survey in one sitting.

1. Recorded web site address and username (GO TO S4)
2. Would prefer to complete over the phone (GO TO S3B)
3. Refuses to participate (GO TO PROFILE—THEN ALLTERM)

*(PREFER TO COMPLETE OVER THE PHONE)

S3b That's fine. We can call you back to complete the survey over the phone when you have a copy of the glossary which includes the key aspects of the terminology used in the study. You will need to refer to the glossary when answering some of the questions.

You can download the glossary, from our website www.srcentre.com.au/respondents under ABACUS.

1. Complete survey on phone now—respondent has a copy of the glossary questionnaire in front of them (GO TO Q1)
2. Call back at another time (record name and schedule appointment)
3. Refuses to participate (GO TO PROFILE—THEN ALLTERM)

*(NOT YET COMPLETED QUESTIONNAIRE)

S4 As we would like to include as many businesses as possible in the survey to ensure that the information collected accurately reflects what is happening across Australia, the cut off date for participation has been extended to Friday April 11. If you require any assistance with the survey you can contact us on 1800 023 040.

If you prefer I can provide you with details to complete the survey online.

IF PREFERS TO COMPLETE SURVEY ONLINE, SAY: You can complete the survey online by going to www.aic.gov.au/abacus and your login is (WEB LOGON ID FROM SAMPLE). You will be prompted to select a password prior to beginning the survey so you can go back to it at a later time—if you don't have time to complete the survey in one sitting.

1. Continue (GO TO END2—THEN ALLTERM)

*(HAVEN'T HAD ANY COMPUTER SECURITY INCIDENTS/DON'T USE COMPUTERS)

S5 If that's the case, it will only take a few minutes to complete over the phone. Do you have time to run through it now?

1. Complete on phone—continue now (GO TO Q1)
2. Complete on phone—call back (record name and schedule appointment)
3. Refuses to participate (GO TO PROFILE)

*(REFUSES TO PARTICIPATE)

PROFILE. Would it be ok if I asked you a few quick questions so that we can understand more about the businesses that did not participate in the survey?

1. Continue (GO TO PQ1)
2. Refused to answer profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ1 What was the industry sector relevant to the LARGEST PROPORTION of the income of your business during the 12 months ending 30th June 2007?

AID IF NECESSARY

1. Agriculture, forestry and fishing
2. Mining
3. Manufacturing
4. Electricity, gas, water and waste services
5. Construction
6. Wholesale trade
7. Retail trade
8. Accommodation and food services

9. Transport, postal and warehousing

10. Information media and telecommunications

11. Financial and insurance services

12. Rental, hiring and real estate services

13. Professional, scientific and technical services

14. Administrative and support services

15. Public administration and safety

16. Education and training

17. Health care and social assistance

18. Arts and recreational services

19. Other services (Specify)

20. (Don’t know)

21. Refused to answer question

22. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ2 Please estimate the total number of employees on the Australian payroll of your business as at 30th June 2007?

1. Number of employees provided [ALLOWABLE RANGE=0–999999] [Go to PQ3]

2. Don’t know

3. Refused to answer question

4. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ2a Which of the following categories best describes the total number of employees on the Australian payroll of your business as at 30th June 2007?

READ OUT

1. No employees

2. 1—4

3. 5—19

4. 20—199

5. 200+

6. Don’t know

7. Refused to answer question

8. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ3 In which state or territory was THE MAJORITY of your business’s staff employed during the 12-month period ending 30th June 2007?

DISPLAY STATE FROM SAMPLE RECORD

INTERVIEWER: IF “CAN’T SAY” RETURN STATE FROM SAMPLE RECORD

1. New South Wales
2. Victoria
3. Queensland
4. Western Australia
5. South Australia
6. Tasmania
7. Northern Territory
8. Australian Capital Territory
9. Refused to answer question
10. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ4 Is your business considered to be part of a critical infrastructure sector according to the Trusted Information Sharing Network (TISN)?

1. Yes
2. No [Go to PQ6]
3. Don’t know [Go to PQ6]
4. Refused to answer question [GO TO PQ6]
5. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ5 To which TISN critical infrastructure sector does your business belong?

AID IF NECESSARY

1. Banking and finance
2. Transport and distribution
3. Emergency services
4. Energy
5. Food supply
6. Health
7. Government services
8. Communications
9. (Don’t know)
10. Refused to answer question
11. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ6 Please estimate the turnover of your business during the 12-month period ending 30th June 2007?

1. Total turnover provided—up to $100 million [ALLOWABLE RANGE=1–99999999] [Go to PQ9]
2. Total turnover provided—more than $100 million [SPECIFY AMOUNT IN TEXT] [Go to PQ9]
3. Don’t know

4. Refused to answer question
5. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ6a Which of the following best describes the turnover of your business during the 12-month period ending 30th June 2007?

READ OUT

1. Less than $100,000
2. $100,000 to less than $500,000
3. $500,000 to less than $1 million
4. $1 million to less than $10 million
5. $10 million to less than $1 billion
6. $1 billion or more
7. Don't know
8. Refused to answer question
9. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(REFUSED, AGREED TO ANSWER PROFILING QUESTIONS)

PQ9 Which of the following types of information technologies (IT) did your business use during the 12-month period ending 30th June 2007? (MULTIPLES ACCEPTED)

READ OUT

1. Personal computers (GO TO END2)
2. Laptops (GO TO END2)
3. Smart phones (phones that have the capacity to send and receive emails and access the internet) (GO TO END2)
4. Other wireless devices (GO TO END2)
5. Local area network (GO TO END2)
6. Wide area network (GO TO END2)
7. Virtual private network (GO TO END2)
8. Other (Specify) (GO TO END2)
9. None (GO TO END2)
10. Refused to answer question (GO TO END2)
11. Refused to answer ANY FURTHER profiling questions (GO TO END2)

*(ALL)

Q1 What was the industry sector relevant to the LARGEST PROPORTION of the income of your business during the 12 months ending 30th June 2007?

AID IF NECESSARY

1. Agriculture, forestry and fishing
2. Mining
3. Manufacturing
4. Electricity, gas, water and waste services

5. Construction

6. Wholesale trade

7. Retail trade

8. Accommodation and food services

9. Transport, postal and warehousing

10. Information media and telecommunications

11. Financial and insurance services

12. Rental, hiring and real estate services

13. Professional, scientific and technical services

14. Administrative and support services

15. Public administration and safety

16. Education and training

17. Health care and social assistance

18. Arts and recreational services

19. Other services (Specify)

20. (Don't know)

*(ALL)

Q2 Please estimate the total number of employees on the Australian payroll of your business as at 30th June 2007?

1. Number of employees provided [ALLOWABLE RANGE=0–999999] [Go to Q3]

2. Don't know

*(DON'T KNOW NUMBER OF EMPLOYEES)

Q2a Which of the following categories best describes the total number of employees on the Australian payroll of your business as at 30th June 2007?

READ OUT

1. No employees

2. 1—4

3. 5—19

4. 20—199

5. 200+

6. Don't know

*(ALL)

Q3 In which state or territory was THE MAJORITY of your business's staff employed during the 12-month period ending 30th June 2007?

DISPLAY STATE FROM SAMPLE RECORD

INTERVIEWER: IF "CAN'T SAY" RETURN STATE FROM SAMPLE RECORD

1. New South Wales

2. Victoria

3. Queensland
4. Western Australia
5. South Australia
6. Tasmania
7. Northern Territory
8. Australian Capital Territory

*(ALL)

Q4 Is your business considered to be part of a critical infrastructure sector according to the Trusted Information Sharing Network (TISN)?

1. Yes
2. No [Go to Q6]
3. Don't know [Go to Q6]

*(PART OF A CRITICAL INFRASTRUCTURE SECTOR)

Q5 To which TISN critical infrastructure sector does your business belong?

AID IF NECESSARY

1. Banking and finance
2. Transport and distribution
3. Emergency services
4. Energy
5. Food supply
6. Health
7. Government services
8. Communications
9. (Don't know)

*(ALL)

Q6 Please estimate the turnover of your business during the 12-month period ending 30th June 2007?

1. Total turnover provided—up to $100 million [ALLOWABLE RANGE=1–99999999] [Go to Q7]
2. Total turnover provided—more than $100 million [SPECIFY AMOUNT IN TEXT] [Go to Q7]
3. Don't know

*(DON'T KNOW TOTAL OPERATING REVENUE)

Q6a Which of the following best describes the turnover of your business during the 12-month period ending 30th June 2007?

READ OUT

1. Less than $100,000
2. $100,000 to less than $500,000
3. $500,000 to less than $1 million
4. $1 million to less than $10 million
5. $10 million to less than $1 billion

6. $1 billion or more

7. Don't know

*(ALL)

Q7a How would you rate your LEVEL OF KNOWLEDGE to use information technologies? Would you say…

READ OUT

1. Very low
2. Low
3. Moderate
4. High, or
5. Very high
6. (Can't say)

*(ALL)

Q7b How would you rate YOUR ABILITY TO USE information technologies?

READ OUT

1. Very low
2. Low
3. Moderate
4. High, or
5. Very high
6. (Can't say)

*(ALL)

Q8 Which ONE of the following best describes your role within the business?

READ OUT

1. Owner / director / CEO / MD
2. General management / operations management
3. CFO / financial management
4. CIO / IT management
5. Fraud / security control
6. Other (Specify)

*(ALL)

Q9 Which of the following types of information technologies (IT) did your business use during the 12-month period ending 30th June 2007? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO GLOSSARY (Q9)

READ OUT

1. Personal computers
2. Laptops
3. Smart phones (phones that have the capacity to send and receive emails and access the internet)

4. Other wireless devices

5. Local area network

6. Wide area network

7. Virtual private network

8. Other (Specify)

9. None [Go to Q38]

PREQ10 IF S5=1(NOT SURE WHETHER SURVEY APPLIES TO BUSINESS) AND Q9=1–8 (USES IT) ASK QCHECK, ELSE GO TO Q10

*(NOT SURE WHETHER SURVEY APPLIES TO BUSINESS)

QCHECK. Your business qualifies to participate in the survey. The survey takes approximately 15 minutes, depending on your answers, are you willing to complete the survey now or would you prefer I called back at another time?

1. Complete survey on phone now—respondent has a copy of the glossary questionnaire in front of them (GO TO Q10)

2. Complete survey online (GO TO S4B)

3. Complete hardcopy questionnaire (GOTO S4B)

4. Soft appointment—Make appointment to speak with named contact person/IT Manager

(RECORD NAME AND SCHEDULE APPOINTMENT)

5. Hard appointment—Make appointment to speak with named contact person/IT Manager

(RECORD NAME AND SCHEDULE APPOINTMENT

6. Refuses to participate (GO TO END2—THEN MARK ON ALLTERM [BUSINESS QUALIFIES

—REFUSES TO COMPLETE (QCHECK=3]

*(COMPLETE SURVEY ONLINE OR HARDCOPY AT QCHECK)

S4B The cut off date for participation has been extended to Friday April 11. If you require any assistance with the survey you can contact us on 1800 023 040.

1. Continue (GO TO END2)

*(ALL)

Q10 How many computer security incidents, if any, did your business experience during the 12 month period ending 30th June 2007? A computer security incident is described as any unauthorised use, damage, monitoring, attack or theft of your business information technology.

Each incident should only be counted once, for example any worm or virus that could be classified as a computer security incident should only be counted as a single attack, not once per infected machine.

1. None (Go to Q21)

2. Number of computer security incidents provided [ALLOWABLE RANGE=1–99999]

3. Don’t know

*(HAD COMPUTER SECURITY INCIDENT)

Q11 What types of computer security incidents did your business experience during the 12-month period ending 30th June 2007? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO GLOSSARY (Q11)

AID IF NECESSARY

1. Insider abuse of access
2. Theft or loss of hardware
3. Virus or other malicious code
4. Spyware
5. Phishing
6. Denial of service attack
7. Sabotage of network or data
8. Unauthorised network access
9. Theft or breach of proprietary or confidential information
10. Incident involving this business's web application
11. Other (Specify)
12. Don't know

*(HAD COMPUTER SECURITY INCIDENT)

Q12 Of all computer security incidents that your business experienced in the 12-month period ending 30th June 2007, what percentage originated from a person or persons WITHIN YOUR BUSINESS?

1. Percentage internally originating incidents provided [ALLOWABLE RANGE=0–100]
2. Don't know

*(HAD COMPUTER SECURITY INCIDENT)

Q13 What percentage of all computer security incidents that affected your business during the 12 months ending 30th June 2007 was referred to each of the following?

(STATEMENTS)

a. Police

b. Non-police enforcement/regulatory agency

c. An external computer security incident response team e.g. AusCERT

d. Lawyer/s for civil action

e. Electronic payment provider e.g. Visa, MasterCard

f. Other (Specify)

g. Dealt with internally—not referred to a third party

(RESPONSE FRAME)

1. Provided percentage [ALLOWABLE RANGE 0–100]
2. Don't know

****PROGRAMMER CHECK**—Q13 A-G SHOULD ADD TO NO MORE THAN 100%

*(HAD COMPUTER SECURITY INCIDENT)

Q14 Which ONE of the following BEST DESCRIBES the computer security incident that caused the greatest financial loss to your business during the 12-month period ending 30th June 2007?

RESPONDENT SHOULD REFER TO GLOSSARY (Q14)

READ OUT

1. Insider abuse of access
2. Theft or loss of hardware
3. Virus or other malicious code
4. Spyware
5. Phishing
6. Denial of service attack
7. Sabotage of network or data
8. Unauthorised network access
9. Theft or breach of proprietary or confidential information
10. Incident involving this business's web application
11. Other (Specify)
12. (Don't know)

*(HAD COMPUTER SECURITY INCIDENT)

Q15 Please estimate the TOTAL financial cost of ALL computer security incidents to your business during the 12-month period ending 30th June 2007?

IF RESPONDENT HESITATES, SAY: What's your best estimate?

RESPONDENT SHOULD REFER TO GLOSSARY (Q15)

1. Total cost of all computer security incidents provided—up to $100 million [ALLOWABLE RANGE=1–99999999]
2. Total cost of all computer security incidents provided—more than $100 million [SPECIFY AMOUNT IN TEXT]
3. Don't know

*(HAD COMPUTER SECURITY INCIDENT)

Q16 Which ONE of the following BEST DESCRIBES the MOST SIGNIFICANT computer security incident that affected your business in the 12-month period ending 30th June 2007?

RESPONDENT SHOULD REFER TO GLOSSARY (Q16)

READ OUT

1. Insider abuse of access
2. Theft or loss of hardware
3. Virus or other malicious code
4. Spyware
5. Phishing
6. Denial of service attack
7. Sabotage of network or data
8. Unauthorised network access
9. Theft or breach of proprietary or confidential information

10. Incident involving this business's web application
11. Other (Specify)
12. (Don't know)

*(HAD COMPUTER SECURITY INCIDENT)

Q17 Please indicate whether your business experienced any of the following as a result of this MOST SIGNIFICANT computer security incident? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO GLOSSARY (Q17)

READ OUT

1. Corruption of hardware of software
2. Corruption or loss of data
3. Unavailability of service
4. Web site defacement
5. Theft or loss of hardware
6. Theft of business, confidential or proprietary information
7. Non-critical operational losses
8. Non-critical financial losses
9. Harm to reputation
10. Critical operational losses
11. Critical financial loss
12. Loss of life
13. Other (Specify)
14. (Not applicable—no impact experienced)
15. (Don't know)

*(HAD COMPUTER SECURITY INCIDENT)

Q18 Please estimate the total financial cost to the business of the *most significant* computer security incident?

IF RESPONDENT HESITATES, SAY: What's your best estimate?

1. Financial cost provided—up to $100 million [ALLOWABLE RANGE=1–99999999]
2. Financial cost provided—more than $100 million [SPECIFY AMOUNT IN TEXT]
3. Financial cost never estimated by the business
4. Don't know

*(HAD COMPUTER SECURITY INCIDENT)

Q19a Which of the following actions were taken for the MOST SIGNIFICANT computer security incident that affected your business during the 12 month period ending 30th June 2007?

READ OUT

1. Reported to police
2. Reported to non-police enforcement/regulatory agency
3. Reported incidents to an external computer security incident response team e.g. AusCERT

4. Reported incidents to lawyer for civil action
5. Reported to an electronic payment provider e.g. Visa, MasterCard
6. Other (Specify)
7. Dealt with solely internally

*REPEAT Q19B FOR EACH 1 TO 7 SELECTED IN Q19A

*(REPORTED INCIDENT EXTERNALLY)

Q19b How satisfied was your business with the outcome obtained as a result of (DISPLAY STATEMENT)

Would you say …very satisfied, satisfied, neither satisfied nor dissatisfied, dissatisfied or very dissatisfied

(STATEMENT)

a. Reporting this incident to the police [ONLY DISPLAY IF Q19A=1]

b. Reporting this incident to non-police enforcement/regulatory agency [ONLY DISPLAY IF Q19A=2]

c. Reporting this incident to an external computer security incident response team e.g. AusCERT [ONLY DISPLAY IF Q19A=3]

d. Reporting this incident to the lawyer for civil action [ONLY DISPLAY IF Q19A=4]

e. Reporting the incident to the electronic payment provider e.g. Visa, MasterCard [ONLY DISPLAY IF Q19A=5]

f. Other [ONLY DISPLAY IF Q19A=6]

g. Dealt with solely internally [ONLY DISPLAY IF Q19A=7]

(RESPONSE FRAME)

1. Very dissatisfied
2. Dissatisfied
3. Neither satisfied nor dissatisfied
4. Satisfied
5. Very satisfied
6. Can’t say

PREQ20 IF Q19A=7 (DEALT WITH SOLELY INTERNALLY) CONTINUE, ELSE GO TO Q21

*(DEALT WITH SOLELY INTERNALLY)

Q20 Which of the following were reasons why your business chose NOT to report the most significant computer security incident to a third party? (MULTIPLES ACCEPTED)

READ OUT

1. Negative publicity
2. Business was not explicitly targeted e.g. worm
3. Nothing to gain
4. Did not think to report
5. Incident outside jurisdiction of law enforcement
6. Did not want data or hardware seized as evidence
7. Did not know who to contact

8. Incident not serious enough to report

9. Competitors would use to their advantage

10. Dealt with internally

11. Fear of reprisals

12. Fear of repeat victimisation

13. Other (Specify)

14. (Don’t know)

*(ALL)

Q21 Which of the following computer security measures did your business use during the 12-month period ending 30th June 2007? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO HARDCOPY QUESTIONNAIRE AND GLOSSARY (Q21),

AID IF NECESSARY

1. No computer security tools or procedures were used

2. PHYSICAL SECURITY—Keeping servers in secure rooms

3. PHYSICAL SECURITY—Limiting access to workstations

4. PHYSICAL SECURITY—Physically securing laptop computers

5. PHYSICAL SECURITY—Physically securing wireless devices

6. PHYSICAL SECURITY—Physical security used but unable to specify

7. PHYSICAL SECURITY—Other (Specify)

8. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Digital certificates

9. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Biometrics

10. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Smartcards

11. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Security tokens (other than smartcards)

12. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Password verification

13. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Single sign on

14. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Encryption of data

15. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—File integrity assessment tool

16. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Encrypting removable data storage devices

17. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Cryptographic and authentication tools used but unable to specify

18. CRYPTOGRAPHIC & AUTHENTICATION TOOLS—Other (Specify)

19. ANTI FRAUD AND MALWARE TOOLS—Anti-spam filters

20. ANTI FRAUD AND MALWARE TOOLS—Anti-virus software

21. ANTI FRAUD AND MALWARE TOOLS—Anti-spyware software

22. ANTI FRAUD AND MALWARE TOOLS—Anti-phishing software

23. ANTI FRAUD AND MALWARE TOOLS—Anti fraud and malware technologies used but unable to specify

24. ANTI FRAUD AND MALWARE TOOLS—Other (Specify)

25. DETECTION AND MONITORING TOOLS—Internet content / image filtering or monitoring

26. DETECTION AND MONITORING TOOLS—Intrusion detection system

27. DETECTION AND MONITORING TOOLS—Intrusion prevention system

28. DETECTION AND MONITORING TOOLS—Detection and monitoring tools used but unable to specify

29. DETECTION AND MONITORING TOOLS—Other (Specify)

30. SECURITY MANAGEMENT TOOLS—Endpoint security client software

31. SECURITY MANAGEMENT TOOLS—Firewall

32. SECURITY MANAGEMENT TOOLS—Vulnerability management system

33. SECURITY MANAGEMENT TOOLS—Provisioning system

34. SECURITY MANAGEMENT TOOLS—Security compliance tools

35. SECURITY MANAGEMENT TOOLS—Instant messaging security solutions

36. SECURITY MANAGEMENT TOOLS—Manual patch management

37. SECURITY MANAGEMENT TOOLS—Automated patch management

38. SECURITY MANAGEMENT TOOLS—Configuration management

39. SECURITY MANAGEMENT TOOLS—Security management technologies used but unable to specify

40. SECURITY MANAGEMENT TOOLS—Other (Specify)

41. Other measures (Specify)

42. Don't know

*(ALL)

Q22 Were any of the computer security measures of your business outsourced to one or more third parties during the 12-month period ending 30th June 2007?

1. Yes

2. No (Go to Q26)

3. Don't know (Go to Q26)

*(COMPUTER SECURITY MEASURES OUTSOURCED)

Q23 Were any of the third parties based primarily in a country other than Australia?

1. Yes

2. No

3. Don't know

*(COMPUTER SECURITY MEASURES OUTSOURCED)

Q24 How were the outsourced computer security measures reviewed or evaluated? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO GLOSSARY (Q24)

1. Security audit by internal staff

2. Security audits by external businesses

3. Security compliance check

4. Other (Specify)

5. Third party performance was evaluated but unable to specify

6. Don't know

7. Not reviewed or evaluated (Go to Q26)

*(COMPUTER SECURITY MEASURES OUTSOURCED REVIEWED/EVALUATED)

Q25 Approximately how often was the work of this third party evaluated or reviewed?

1. Weekly
2. Monthly
3. Quarterly
4. Biannually
5. Annually
6. Ad hoc
7. Other (Specify)
8. Don't know

*(ALL)

Q26 What type of computer security related POLICIES did your business have during the 12-month period ending 30th June 2007? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO HARDCOPY QUESTIONNAIRE AND GLOSSARY (Q26)

AID IF NECESSARY

1. Did not have any computer security polices (Go to 28)
2. STAFF USER RELATED POLICIES—Employee education and awareness program
3. STAFF USER RELATED POLICIES—Segregation of duties
4. STAFF USER RELATED POLICIES—System content monitoring
5. STAFF USER RELATED POLICIES—Wireless technology acceptable use policy
6. STAFF USER RELATED POLICIES—IT acceptable use policies
7. STAFF USER RELATED POLICIES—Mobile policies (such as mandatory encryption of data stored on mobile devices)
8. STAFF USER RELATED POLICIES—User access management
9. STAFF USER RELATED POLICIES—Background checks
10. STAFF USER RELATED POLICIES—Mandatory reporting of misuse/abuse of computer equipment
11. STAFF USER RELATED POLICIES—Documented standard operating procedures
12. STAFF USER RELATED POLICIES—Monitor internet connections
13. STAFF USER RELATED POLICIES—Account/password management policies
14. STAFF USER RELATED POLICIES—Staff/user related policy used but unable to specify
15. STAFF USER RELATED POLICIES—Other (Specify)
16. SECURITY TESTING POLICIES—System penetration testing
17. SECURITY TESTING POLICIES—System audit policies
18. SECURITY TESTING POLICIES—Risk assessment policies
19. SECURITY TESTING POLICIES—Security testing policy used but unable to specify
20. SECURITY TESTING POLICIES—Other (Specify)
21. DATA RELATED POLICIES—Media backup procedures

22. DATA RELATED POLICIES—Management of removable computer media storage devices

23. DATA RELATED POLICIES—Protection of electronic account information e.g. customer account details

24. DATA RELATED POLICIES—Data related policy used but unable to specify

25. DATA RELATED POLICIES—Other (Specify)

26. INCIDENT RESPONSE POLICIES—Use of incident response team

27. INCIDENT RESPONSE POLICIES—Business continuity policy

28. INCIDENT RESPONSE POLICIES—Forensic plan

29. INCIDENT RESPONSE POLICIES—Incident management procedures

30. INCIDENT RESPONSE POLICIES—Incident response policy used but unable to specify

31. INCIDENT RESPONSE POLICIES—Other (Specify)

32. EXTERNAL BUSINESS POLICIES—Payment system supplier policies

33. EXTERNAL BUSINESS POLICIES—Other supplier determines policies

34. EXTERNAL BUSINESS POLICIES—External business policy used but unable to specify

35. EXTERNAL BUSINESS POLICIES—Other (Specify)

36. WIRELESS SECURITY POLICIES—Secure placement of access points

37. WIRELESS SECURITY POLICIES—Name of network changed from default

38. WIRELESS SECURITY POLICIES—Encrypted signals

39. WIRELESS SECURITY POLICIES—Connections restricted to known devices only

40. WIRELESS SECURITY POLICIES—Wireless monitoring

41. WIRELESS SECURITY POLICIES—Wireless computer security policies used but unable to specify

42. WIRELESS SECURITY POLICIES—Other (Specify)

43. Other policies (Specify)

44. Don’t know

*(ALL)

Q27 Which of the following IT standards were used in the development of your business current IT policies? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO HARDCOPY QUESTIONNAIRE, AID IF NECESSARY

1. AS/NZS ISO/IEC 17799:2005—Code of practice for information security management

2. AS/BS7799.2:2003—Information security management

3. ACSI 33—Australian Government Information Security Manual

4. HB 231 2003 Information Security Risk Management

5. HB 171:2003—Guidelines for management of IT evidence

6. RFC 2196—Site security handbook

7. ISO/IEC 13335 -1:2004 Information technology. Guidelines for the management of IT security.

8. State government IT Security standard

9. Other (Specify)

10. Don’t know

11. No standards used

*(ALL)

Q28 How often was the effectiveness of your business's computer security evaluated during the 12 month period ending 30th June 2007?

1. Frequency (Specify)
2. Don't know
3. Computer security was not evaluated (Go to Q30)

*(EVALUATED COMPUTER SECURITY)

Q29 Which of the following methods did your business use to evaluate the effectiveness of its computer security measures during the 12-month period ending 30th June 2007? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO HARDCOPY QUESTIONNAIRE AND GLOSSARY (Q29).

AID IF NECESSARY

1. Security audit by internal staff
2. Security audits by external businesses
3. Automated tools
4. E-mail monitoring software
5. Web activity monitoring software
6. Other (Specify)
7. (Don't know)

*(ALL)

Q30 Please estimate the TOTAL IT EXPENDITURE for your business during the 12-month period ending 30th June 2007?

IF RESPONDENT HESITATES, SAY: What's your best estimate?

RESPONDENT SHOULD REFER TO GLOSSARY (Q30)

1. Total IT expenditure provided—up to $100 million [ALLOWABLE RANGE=1–99999999]
2. Total IT expenditure provided—more than $100 million [SPECIFY AMOUNT IN TEXT]
3. Don't know

*(ALL)

Q31 Please estimate the TOTAL AMOUNT SPENT ON COMPUTER SECURITY MEASURES by your business during the 12-month period ending 30th June 2007?

IF RESPONDENT HESITATES, SAY: What's your best estimate?

1. Total amount spent on computer security measures provided—up to $100 million

   [ALLOWABLE RANGE=1–99999999]

2. Total amount spent on computer security measures provided—more than $100 million

   [SPECIFY AMOUNT IN TEXT]

3. Don't know

*(ALL)

Q32 What percentage of expenditure on computer security measures during the 12-month period ending 30th June 2007 was for each of the following?

RESPONDENT SHOULD REFER TO Q21 FOR EXAMPLES OF WHAT IS INCLUDED IN EACH CATEGORY

(STATEMENTS)

a. Physical security

b. Cryptographic and authentication tools

c. Anti fraud and malware technologies

d. Detection and monitoring tools

e. Security management technologies

f. Other (Specify)

(RESPONSE FRAME)

1. Provided percentage [ALLOWABLE RANGE 0–100]
2. Don't know

**PROGRAMMER CHECK—Q13 A–G SHOULD ADD TO NO MORE THAN 100%

*(ALL)

Q33 Compared with expenditure on computer security measures in the PREVIOUS FINANCIAL YEAR (i.e. ending June 2006), did expenditure on computer security measures in the 12 month period ending 30th June 2007 increase, decrease or stay the same?

1. Percentage increase provided [ALLOWABLE RANGE 1–1000]
2. Percentage decrease provided [ALLOWABLE RANGE 1–1000]
3. Stayed the same
4. Don't know

*(ALL)

Q34 Which of the following types of computer security incidents are covered by your business's computer security insurance policy? (MULTIPLES ACCEPTED)

RESPONDENT SHOULD REFER TO GLOSSARY (Q34)

1. Insider abuse of access
2. Theft or loss of hardware
3. Virus or other malicious code
4. Spyware
5. Phishing
6. Denial of service attack
7. Sabotage of network or data
8. Unauthorised network access
9. Theft or breach of proprietary or confidential information
10. Incident involving this business's web application
11. Other (Specify)
12. Don't know (Go to Q37)
13. No computer security incidents are covered by this business's insurance (Go to Q37)

*(COMPUTER SECURITY INCIDENTS COVERED BY INSURANCE POLICY)

Q35 Did your business make any claims on its insurance policies for losses due to computer security incidents during the 12-month period ending 30th June 2007?

1. Yes
2. No (Go to Q37)
3. Don't know (Go to Q37)

*(MADE CLAIM ON INSURANCE POLICY)

Q36 Were you required to report computer security incidents to a law enforcement agency prior to making a claim against your insurance?

1. Yes
2. No
3. Don't know

*(ALL)

Q37 Are you familiar with any of the following awareness raising initiatives?

READ OUT

1. Stay Smart Online http://www.staysmartonline.gov.au
2. Scamwatch http://www.scamwatch.gov.au
3. FIDO http://www.fido.gov.au
4. The Australian High Tech Crime Centre http://www.ahtcc.gov.au
5. AusCERT http://www.auscert.org.au
6. Stay Safe Online http://www.staysafeonline.info
7. Other (Specify)
8. (Not aware of any of these initiatives)

*(ALL)

Q38 Thinking about the time you just spent and including any other time spent reading the instructions, working on the questions and sourcing the information AND any other time spent by other employees in collecting and providing the information. How much time have you spent on this questionnaire?

1. Record hours [ALLOWABLE RANGE 0.0–20.0] (ALLOW DECIMALS)
2. Record minutes [ALLOWABLE RANGE 0–60]
3. Don't know

END1 Thank you for your time in completing the ABACUS Computer User Survey. Your input will benefit in the understanding of cybercrime and its prevention.

END2 Thanks for your time

Allterm DISPLAYED IN DONE REPORT

1. Phone number is not named business/is businesses tax agent/rep (S1=4)
2. Phone answerer refused to pass on to named person/IT manager (S1=5)
3. Named person/IT manager refuses to participate (S1a=3)
4. Not received mail pack—refuses to participate (S1a=2 and S3a2=1 and S3a=3) or (S1a=2 and S3a2=2 and S3b=4)
5. Received mail pack—refuses to participate (S2=7)

6. Hasn’t had any incidents/doesn’t use computers—refuses to participate (S5=4)

7. Refuses to complete online or over phone (S1a=1 and S2=5 and S3b=4) or (S1a=1 and S2=6 and S3a=3)

8. Completed reminder call (S4=1)

9. Completed hardcopy and mailed back (S2=2)

10. Called 1800 number (S1=6)

11. Completed via phone during reminder (Q38=1,2,or 3)

METHOD RECORD:

1. Questionnaire completed over the phone with respondent

2. Data entry of hardcopy questionnaire (HIDE THIS CODE SO IT IS NOT VISIBLE TO INTERVIEWERS).

AIC Reports
Technical and Background Paper 32

Australia's national research and
knowledge centre on crime and justice

www.aic.gov.au