Trends & issues
in crime and criminal justice

No. 399 September 2010

Australian Government
Australian Institute of Criminology

Computer security incidents against Australian businesses: Predictors of victimisation

Kelly Richards and Brent Davis

Foreword | *Drawing on data from the Australian Business Assessment of Computer User Security (ABACUS) survey, this paper examines a range of factors that may influence businesses' likelihood of being victimised by a computer security incident. It has been suggested that factors including business size, industry sector, level of outsourcing, expenditure on computer security functions and types of computer security tools and/or policies used may influence the probability of particular businesses experiencing such incidents. This paper uses probability modelling to test whether this is the case for the 4,000 businesses that responded to the ABACUS survey. It was found that the industry sector that a business belonged to, and business expenditure on computer security, were not related to businesses' likelihood of detecting computer security incidents. Instead, the number of employees that a business has and whether computer security functions were outsourced were found to be key indicators of businesses' likelihood of detecting incidents. Some of the implications of these findings are considered in this paper.*

Adam Tomison
Director

The Australian Institute of Criminology (AIC) recently commissioned a nationwide survey of businesses called the Australian Business Assessment of Computer User Security (ABACUS) survey (see Richards 2009). This study aimed to identify the prevalence, nature, costs and impacts of computer security incidents against Australian businesses during 2006–07. Computer security incidents were defined in the survey as *any unauthorised use, damage, monitoring attack or theft of business information technology*. Common computer security incidents include viruses and other malicious code, spyware, phishing, sabotage of network or data and denial of service attacks.

The ABACUS survey used a random, weighted sample of Australian businesses, stratified by industry sector and business size, to enable generalisations to be made about the entire population of Australian businesses. In total, 4,000 ABACUS questionnaires were completed by Australian businesses, representing a response rate of 29 percent (for a detailed discussion of the methodology of the ABACUS study see Challice (2009)).

The ABACUS study found that a majority of businesses (80%; n=2,881) that used information technology reported experiencing no computer security incidents during the 12 month period ending 30 June 2007. In the study, 'experiencing a computer security incident' meant that a business detected an incident. By definition, the survey was not able to capture incidents that businesses did not detect; the survey only capturing detected or identified computer security incidents. As a proportion of the overall sample, 12 percent (n=435) of businesses experienced one to five computer security incidents, one percent experienced six to 10 incidents (n=44) and one percent experienced more than 10 incidents (n=48). Six percent (n=212) of respondents were unable to quantify the number of computer security incidents their business had experienced.

Research has shown that businesses are concerned about the risks associated with computer security incidents and believe that victimisation is widespread (Nykodym, Taylor & Vilela 2005; Smith, Grabosky & Urbas 2004). A survey commissioned by IBM (Ho 2006) found that about half of Australian businesses perceive computer security incidents as a greater threat and more costly to their organisation than physical crime.

The literature on computer security incidents posits a range of factors as potential predictors of whether businesses experience computer security incidents. Industry sector, for example, is widely held to be a key determinant, with financial organisations deemed most likely to be targeted (IBM Global Technology Services 2008). Business size is also

commonly proposed as a factor that may determine businesses' likelihood of experiencing computer security incidents. For example, the Department of Trade and Industry (2006) found that in the United Kingdom, a higher proportion of large businesses reported experiencing malicious computer security incidents than businesses overall.

This paper provides a statistical analysis of predictors of businesses' victimisation by computer security incidents. Data from the ABACUS study (Richards 2009) suggested that some variables might influence businesses' likelihood of victimisation. The data revealed, for example, somewhat unclear relationships between the number of computer security incidents experienced and:

- expenditure on computer security;
- respondents' knowledge of information technology; and
- whether businesses outsourced any computer security functions.

Two additional variables—businesses' use of computer security tools and policies—have also been examined here, as it is their explicit purpose to limit businesses' exposure to computer security incidents.

This paper therefore examines the impact of the following factors on businesses' likelihood of experiencing a computer security incident:

- industry sector;
- business size (number of employees);
- respondents' knowledge of information technology;
- computer security tools used;
- computer security policies used;
- outsourcing of computer security measures; and
- computer security expenditure.

Probability modelling

The analysis presented in this paper uses unweighted data, which is necessary in modelling analyses of this type. For more detail on the process of weighting data and the difference between weighted and unweighted data see Challice (2009) and Richards (2009). Missing answers and 'don't know' responses from all variables, except expenditure on computer security, were excluded from this analysis. As a result, the overall sample was reduced from 4,000 to 2,167. The extent of missing values differed across each of the variables, according to a range of factors, including whether a 'don't know' option was available. This is typical in surveys that investigate sensitive topic areas; missing values are particularly common for survey questions about business turnover. This paper uses models of qualitative choice which allow for analysis of the likelihood of a given explanatory variable having a significant impact on a defined dependent variable. It is important to note that in probability modelling, coefficient values represent whether the variable of interest is more or less likely than the omitted variable to impact upon the probability of a business being victimised. Where the prefix of a coefficient value is positive (+), the business is more likely to be victimised. Conversely, where the coefficient value is negative (–), the business is less likely to be victimised. The size of the coefficient does not, however, indicate the impact of the variable concerned, relative to the omitted variable, on the probability of a business's victimisation. That is, a high figure does not necessarily indicate a strong impact and a low figure does not necessarily indicate a weak impact.

Instead, odds ratios (OR) can be used to determine the impact of each variable on businesses' likelihood of being victimised by a computer security incident. For example, an odds ratio of 0.65 suggests the variable concerned is 35 percent less likely than the omitted variable (1–0.65) to lead to victimisation. Conversely, an OR of 1.65 indicates the variable concerned is 65 percent more likely (1.65–1.00) to lead to victimisation.

Another key feature of probability modelling is the requirement to select and omit a particular variable from each model. Results from the modelling analysis therefore represent the impact of the remaining variable(s) on the probability of victimisation, relative to the omitted variable.

In the current study, the selection of omitted variables was informed by the research questions driving the original study (see Richards 2009) and by existing literature on this subject area. The current study also utilises conventional statistical practice in the social sciences for evaluating the statistical significance of the modelling results—that is, results are deemed statistically significant when they have a 'probability value' of less than five percent.

The dependent variable in this study is whether the business was identified as a victim of a computer security incident during the 2006–07 financial year. The possible results were categorised as 0 for those who had not been a victim and 1 for those who had been impacted at least once that is, whether the business was aware of having been victimised. Of course, undetected incidents are not captured by this survey..

Industry sector

The ABACUS survey asked respondents from 19 industry sectors whether they had experienced a computer security incident during the previous financial year. The industry sectors surveyed were:

- agriculture, forestry and fishing;
- mining and 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; and
- other services (see Table 1).

The financial and insurance services sector was chosen as the omitted variable in this model as it is widely accepted in the literature on computer security incidents against businesses that financial sector organisations are likely targets for perpetrators of computer security incidents (see IBM Global Technology Services 2008; Symantec 2006).

As Table 1 indicates, five of the industry sectors were significantly less likely than the financial and insurance services sector to be victimised by a computer security incident during the 12 month period. These sectors

were health care and social assistance (46% less likely), arts and recreation (48% less likely), mining (50% less likely), construction (52% less likely) and other services (69% less likely).

These findings offer some support to the widespread perception that businesses from the financial services sector are more likely to be victimised. It is important to highlight, however, that a number of industry sectors were not significantly more or less likely to experience computer security incidents than businesses from the financial sector. As such, it appears that the perception of financial sector businesses as the most likely targets of computer security incidents is somewhat overstated. In addition, it is important to recognise that businesses from the financial and insurance services sector may have better computer security measures in place and may have a greater awareness of having been victimised than businesses from industry sectors with lower levels of security.

Business size

The ABACUS survey defined small businesses 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 modelling analysis by business size used medium businesses as the omitted variable. Results therefore pertain to the likelihood of small or large firms being victimised, relative to medium businesses.

As might be expected, large businesses appear more likely and small businesses less likely, to be the victims of computer security incidents than medium businesses. Large businesses were a substantial 146 percent more likely than medium businesses to be victimised. Conversely, small businesses were 29 percent less likely to be victimised. Both of these results were statistically significant and suggest that business size is a significant predictive factor in businesses' likelihood of experiencing computer security incidents.

These findings confirm results from international studies that suggest that the number of employees a business has is linked to its likelihood of experiencing a computer security incident (see Department of Trade and Industry 2006; Rantala 2008). This could suggest that larger businesses are deemed better targets by cyber criminals. Alternatively, it might suggest that larger businesses are better able to detect computer security incidents and are more aware of these incidents than their smaller counterparts.

Table 1 Modelling results, by sector

	n	OR	CI[a]	p
Accommodation/food services	71	0.59	0.27–1.27	0.18
Administrative/support services	84	0.94	0.48–1.83	0.85
Agriculture, forestry/fishing	196	0.72	0.41–1.26	0.25
Arts/recreational services	129	0.52	0.27–1.00	0.05**
Construction	138	0.48	0.25–0.93	0.03**
Education/training	110	1.05	0.57–1.92	0.89
Electricity, gas, water/waste services	83	0.54	0.26–1.14	0.11
Financial/insurance services (omitted variable)	118	–	–	–
Health care/social assistance	174	0.54	0.30–0.98	0.04**
Information media/telecommunications	85	0.58	0.28–1.20	0.14
Manufacturing	132	0.75	0.41–1.38	0.36
Mining	104	0.50	0.25–1.01	0.05**
Other services	45	0.31	0.10–0.95	0.04**
Professional, scientific/technical services	180	0.86	0.49–1.50	0.59
Public administration/safety	52	0.86	0.39–1.90	0.71
Rental, hiring/real estate	71	0.79	0.38–1.63	0.52
Retail trade	193	0.57	0.32–1.01	0.06
Transport, postal/warehousing	105	0.71	0.37–1.36	0.30
Wholesale trade	97	0.68	0.35–1.34	0.27
McFadden R-squared				0.01
LR statistic				20.71
Probability(LR stat)				0.29
Akaike information criterion				0.93
Schwarz criterion				0.98

a: The column CI in this and the following Tables refers to the 95 percent confidence interval for the estimate of the odds ratio

**=statistically significant at p≤0.05

Source: AIC, ABACUS 2008 [computer file]

Knowledge of information technology

Respondents to the ABACUS survey were asked to rate their own level of knowledge of information technology as *very low*, *low*, *moderate*, *high* or *very high*.

The probability modelling analysis found that those with very low knowledge of information technology were least likely to have identified computer security incidents (see Table 3). Respondents who rated their knowledge as very low were 77 percent less likely than those with moderate knowledge (the omitted variable) to identify a computer security incident during the year. Conversely, respondents who rated themselves as having a low level of knowledge were 51 percent less likely than those with moderate knowledge to be victimised.

Those with high knowledge and very high knowledge were substantially more likely (24% and 82% respectively) to identify being the victims of a computer security incident.

These results were statistically significant, with the exception of those respondents who rated their knowledge as high (which approached statistical significance at 10%).

In one sense, these findings may seem counterintuitive. That is, it might be expected that those respondents who experienced low levels of computer knowledge to have been victimised more frequently than those who rated their knowledge as high or very high. It is important to note, however, that respondents with low levels of computer knowledge may represent businesses with limited information technology infrastructure.

Table 2 Modelling results, by business size

	n	OR	CI	p
Small	1,786	0.71	0.523–0.956	0.02**
Medium (omitted variable)	308	–	–	–
Large	73	2.46	1.43–4.24	0.00**
McFadden R-squared				0.013
LR statistic				25.797
Probability (LR stat)				0.000
Akaike information criterion				0.917
Schwarz criterion				0.924

**=statistically significant at p≤0.05

Source: AIC, ABACUS 2008 [computer file]

Table 3 Modelling results, by respondents' knowledge of information technology

	n	OR	CI	p
Very low	603	0.23	0.06–0.97	0.04**
Low	211	0.49	0.30–0.81	0.01**
Moderate (omitted variable)	1,121	–	–	–
High	187	1.24	0.96–1.60	0.10
Very high	45	1.82	1.27–2.61	0.00**
McFadden R-squared	0.02			0.02
LR statistic	32.24			32.24
Probability(LR stat)	0.00			0.00
Akaike information criterion	0.92			0.92
Schwarz criterion	0.93			0.93

**=statistically significant at p≤0.05

Source: AIC, ABACUS 2008 [computer file]

Those who experienced higher levels of knowledge, however, may work for businesses with substantial information technology infrastructure. Such businesses may be likely to be both more likely targets of computer security incidents and better able to detect such incidents. In addition, higher levels of information technology knowledge may result in better computer security practices and therefore an increased awareness of computer security incidents.

Computer security tools

ABACUS respondents were asked to indicate the types of computer security tools their business had used during the 2006–07 financial year. Computer security tools were grouped into physical security tools, cryptographic and authentication tools, anti-fraud and malware tools, detection and monitoring tools, and security management tools and were defined as follows:

- *physical security tools*—devices such as locks that are used to secure computer hardware;
- *cryptography*—the process of scrambling plain text into cipher text (encryption) and then back again (decryption);
- *authentication tools*—hardware or software designed to verify the identity of a user, process or device;
- *anti-fraud and malware tools*—software or hardware designed to prevent fraud or malware affecting a system or network;
- *detection and monitoring tools*—software or hardware designed to monitor the use of a specific computer system or network; and
- *security management tools*—software or hardware designed with the goal of managing and improving the security of computer systems or networks.

For a detailed glossary of terms used in the ABACUS study see Challice (2009).

The probability modelling analysis indicates that businesses that used security management tools, and detection and monitoring tools were more like to experience computer security incidents (128% more likely and 63% more likely than those without any security tools respectively).

This may indicate that commonly used computer security tools, such as firewalls, intrusion detection systems and intrusion prevention systems, were effective tools for detecting computer security incidents against businesses during the 2006–07 financial year. As noted above, businesses with more robust computer security infrastructure in place may be more likely to detect computer security incidents.

Outsourcing of computer security

ABACUS respondents were asked to indicate whether their business had outsourced any computer security measures during the 2006–07 financial year.

Table 4 Modelling results, by type of computer security tools used

	n	OR	CI	p
Physical security	1,252	0.92	0.71–1.19	0.51
Cryptographic/authentication	1,429	1.12	0.84–1.50	0.44
Anti-fraud/malware	1,971	1.57	0.81–3.03	0.18
Detection/monitoring	989	1.63	1.27–2.09	0.00**
Security management	1,708	2.28	1.50–3.46	0.00**
No security tools (omitted variable)	124	–	–	–
McFadden R-squared				0.04
LR statistic				71.34
Probability (LR stat)				0.00
Akaike information criterion				0.90
Schwarz criterion				0.91

**=statistically significant at p≤0.05

Source: AIC, ABACUS 2008 [computer file]

The modelling analysis found that outsourcing of computer security functions played an important role in determining whether a business identified as a victim of a computer security incident.

Businesses that outsourced one or more computer security functions were 110 percent more likely than those that did not outsource any computer security to identify as having experienced a computer security incident during the year. This is a key finding of this analysis of the ABACUS data.

It is widely believed that outsourcing computer security functions can result in weakened security for businesses' information technology systems (Choo, Smith & McCusker 2007 ; Ernst and Young 2009). The analysis suggests that this belief may be well-founded. However, an alternative interpretation of this finding is that outsourced computer security providers may be more likely to detect computer security incidents, leading to higher rates of reported incidents.

Computer security policies

ABACUS respondents were also asked to indicate the types of computer security policies their business had used during the 2006–07 financial year. Computer security policies were grouped into:

- *staff/user-related policies*—security policies that are directed at the staff of a business;
- *security-testing policies*—such as system audit policies or risk assessment policies;
- *data-related policies*—polices related to the handling, storage and security of data for a business;
- *incident response policies*—policies that govern appropriate responses after a computer security incident has occurred;
- *external business policies*—such as payment system supplier policies; and
- *wireless security policies*—policies that govern which types of security practices are used for the protection of data that is stored and transferred between wireless devices.

The analysis shows that different computer security policies have statistically significantly different impacts on the likelihood of a business becoming a victim of a computer security incident. Businesses with staff/user-related policies were 92 percent more likely than those with no security policies (the omitted variable) to experience a computer security incident. Businesses with wireless policies were 47 percent more likely to experience a computer security incident. By contrast, businesses that used external business security policies were 32 percent less likely than those without any security policies to be victimised.

Expenditure on computer security

Finally, the ABACUS survey asked respondents about their total expenditure on computer security during the 2006–07 financial year.

In contrast to the other variables examined in the modelling reported in this study (which used categorical data), information on computer security spending was collected as continuous data. That is, business respondents were asked to provide a dollar estimate of their expenditure, rather than merely indicate which broad expenditure bracket their business belonged to.

The modelling utilised two measures of computer security spending:

- information technology security expenditure as a proportion of total information technology expenditure; and
- information technology security expenditure as a proportion of total turnover.

In both cases, computer security spending had no practical impact on the likelihood of a business being victimised by a computer security incident (the OR in both cases was 1.00). Only the former (information technology security expenditure as a proportion of total information technology expenditure) was statistically significant ($p<0.01$).

Conclusion

The explanatory power of each of the models reported in this study (the share of the variance in the dependent variable explained by the independent variable(s)) was quite small, as can be seen in the McFadden R-squared figure in each Table.

Considered as a whole, the variables analysed—industry sector, business size, respondents' knowledge of information technology, types of computer security tools used, types of computer security policies used, whether businesses outsourced computer security functions and businesses' information technology security expenditure as a proportion of total information technology expenditure—explain 8.6 percent of businesses' likelihood of experiencing a computer security incident. Although the model left a substantial proportion of the variance associated with experiencing a computer security incident unexplained, this is still an encouraging result for this modelling design.

It is also important to note that the absolute contributions of each of these factors varied

Table 5 Modelling results, by type of computer security policy used

	n	OR	CI	p
Staff/user-related policies	2,167	1.92	1.28–2.87	0.00**
Security testing policies	2,167	0.89	0.62–1.29	0.55
Data-related policies	2,167	1.23	0.81–1.87	0.32
Incident response policies	2,167	1.33	0.92–1.92	0.13
External business policies	2,167	0.68	0.46–1.01	0.06
Wireless security policies	2,167	1.47	1.07–2.02	0.02**
No computer security policies (omitted variable)	–	–	–	–
McFadden R-squared				0.04
LR statistic				84.25
Probability (LR stat)				0.00
Akaike information criterion				0.89
Schwarz criterion				0.91

**=statistically significant at $p \leq 0.05$

Source: AIC, ABACUS 2008 [computer file]

Dr Kelly Richards is a Research Analyst with the Australian Institute of Criminology

Dr Brent Davis is Research Manager of the Modelling and Forecasting program with the Australian Institute of Criminology

General editor, *Trends & issues in crime and criminal justice* series: Dr Adam M Tomison, Director, Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

Project no. 0133

noticeably. The types of computer security policies used (4.2%) and the types of computer security tools used (3.6%) had the greatest explanatory power.

Whether businesses outsourced computer security functions (1.7%), respondents' knowledge of information technology (1.6%), business size (1.3%) and industry sector (1%) explained less of the variance in businesses' experiences of computer security incidents. Importantly, businesses' computer security expenditure explained just 0.5 percent of the variance. It should be noted that these individual contributions total 13.9 percent—well above the combined total of 8.6 percent. This is due to a degree of co-linearity among some of the variables, which is to be expected in an analysis of this kind. A correlation analysis found notable levels of practical and statistical significance between, for example, industry sector and business size, industry sector and types of computer security policies used, business size and respondents' knowledge of information technology and business size and types of computer security tools used.

Overall, the variables considered in the ABACUS survey, and analysed in detail here, therefore appear to explain only a small fraction of businesses' likelihood of becoming a victim of a computer security incident.

This finding suggests that many of the factors widely considered to influence businesses' probability of being victimised—including industry sector, use of computer security tools and outsourcing—are of less importance than previously thought. A range of variables other than those explored in the ABACUS study and analysed in detail in this paper may determine businesses' likelihood of becoming the victim of a computer security incident.

Nonetheless, the findings presented here suggest that in relation to preventing computer security incidents, businesses might consider the following strategies:

- maintaining tight regulatory controls over computer security functions that are outsourced. Although the heightened risk of victimisation among businesses that outsourced computer security functions may be a result of these businesses having greater detection capabilities, a range of risks also have been associated with outsourcing, and businesses should be aware of these (Choo, Smith & McCusker 2007; Colwill & Gray 2007); and
- ensuring that basic computer security tools, such as firewalls, intrusion detection and intrusion prevention systems are in place and up-to-date.

Acknowledgements

The ABACUS study was funded under the Attorney-General's Department's Proceeds of Crime fund.

References

All URLs correct as at 21 June 2010

Challice G 2009. *The Australian business assessment of computer user security (ABACUS) survey: Methodology report*. Technical and background paper series no. 32. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tbp/21-40/tbp032.aspx

Choo R, Smith R & McCusker R 2007. *Future directions in technology-enabled crime: 2007–09*. Research and public policy series no. 78. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

Colwill C & Gray A 2007. Creating an effective security risk model for outsourcing decisions. BT Technology Journal 25(1): 79-87

Department of Trade and Industry 2006. *Information security breaches survey 2006: Technical report*. London: Department of Trade and Industry

Ernst and Young 2009. Outpacing change: Ernst & Young's 12th annual global information security survey. http://www.ey.com/Publication/vwLUAssets/12th_annual_GISS/$FILE/12th_annual_GISS.pdf

Ho A 2006. *Global business security survey: Key highlights*. http://business.singtel.com/upload_hub/singtel_hk/EB-IBM.pdf

IBM Global Technology Services 2008. *IBM internet security systems x-force 2007 trend statistics*. Somers, NY: IBM Corporation

Nykodym N, Taylor R & Vilela J 2005. Criminal profiling and insider cyber crime. *Computer Law & Security Report* 21: 408–414

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

Richards 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/current%20series/rpp/100-120/rpp102.aspx

Smith R, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Symantec 2006. *Symantec internet security threat report: Trends for January 06–June 06*. Cupertino, CA: Symantec