Cybercrime concerns and readiness for New Zealand businesses 2014-2015

Dax Roberts
Southern Institute of Technology
Invercargill, New Zealand
dax.roberts@sit.ac.nz

Henry B. Wolfe
University of Otago
Dunedin, New Zealand
hank.wolfe@otago.ac.nz

ABSTRACT

This research considers surveys conducted on an annual basis for two years as an offshoot of previously conducted research in the field of cybersecurity awareness, training and security for New Zealand organisations. The main differences from other research in the field is that it is conducted from an academic standpoint rather than an industry or governmental perspective and is arguably more neutral because of that. The main findings are that particularly between 2014 to 2015, organisations are more concerned that cybercrime had risen, and will continue to rise, and targeted external threats are now a major concern as well. The surveys also asked if respondents believed the government was doing enough to provide protection and while in 2014 the majority did not have an opinion, in the 2015 the key finding is that organisations do not believe the government is providing enough material resources or knowledge to protect infrastructure.

Keywords: computer crime, computer security, survey, New Zealand, business, concerns, readiness, preparedness, cybercrime

1. INTRODUCTION

It has been observed that cybercrime and cyber security awareness for individuals and businesses is an important issue to government, industry and academia in New Zealand. One of the challenges this paper will address is that while both New Zealand government and industry consider and measure the threats of cybercrime for businesses, typically academia has not addressed it. As examples, Smith (2003) observed that KPMG, Ernst and Young, and Pricewaterhouse Cooper (PwC) all produce fraud related research with the use of surveys but with an industry rather than academic focus. As such those surveys do not typically have margins of error, in-depth methodologies or double-blind peer review as would be expected in academic research.

This paper addresses two challenges of prior researchers who either did not conduct their research on a consistent basis or were not consistent with their analysis methods. The results of this research are based on two surveys, one conducted in June 2014, and one conducted in June 2015. Both use a similar overall methodology as previous researchers but seeks to improve upon New Zealand research by having a larger sample size (approximately 1,000 as opposed to the typical 300-450 (Quinn, 2014, pp. 32-34) and by reporting analysis of multiple question queries such as "IT budget spent on IT security and perceived adequacy" where other researchers merely reported both observations separately. To consider the readiness of New Zealand businesses, three main types of element were considered, budget spending, attitudes towards security and practical measures such as upgrading from Windows XP and policies for using "bring your own devices" within the organisation were considered.

2. RELATED WORK

As shown in the literature review of Quinn (2014), who studied New Zealand businesses and organisations, there are a number of government and/or industry resources both in New Zealand and internationally. Those resources include the CSI/FBI (Gordon, Loeb, Lucyshyn, & Richardson, 2005) that formed the basis for Quinn's initial research but formal academic research specifically in the field was rare. Quinn (2014) conducted four surveys as part of his thesis research however they were not academically published beyond appearing in the thesis itself. As noted they were not conducted consistently on an annual basis (2005, 2006, 2007, 2010) and sometimes different months of the year (Quinn, 2014, pp. 22-25), nor were the question sets or analysis methods entirely consistent (pg. 31).

Other academic research in the field include "Modelling cybercrime and risk for New Zealand organisations" (Roberts, 2009) a PhD which shares some of the data used from Quinn's research. One of the more interesting observations from Roberts' work is that he predicts "Organised cybercrime and state-sponsored malicious cyber activity are predicted to become the predominant cyber threats over the next five to ten years" and this research takes part five years after that prediction with specific questions addressing organisational concerns of threat types, and organisational beliefs in governmental support against such threats.

Government supported organisations such as Netsafe (www.netsafe.org.nz) provide security information for a variety of end users also state that the main New Zealand sources for cybercrime research is Quinn's surveys, PwC's global surveys, and National Cyber Security Centre's Incidence reports (Hails, 2015).

Connect Smart (connectsmart.govt.nz) undertook research in both 2014 and 2015 by engaging Colmar Brunton to conduct and analyse surveys. The main difference between their research and this research is two-fold. The primary difference is that Connect Smart was interested in individuals rather than organisations and because of that they had a much larger population to draw from. As such 1876 New Zealanders participated in their research (Colmar Brunton, 2015, pg. 3) which they report has a low margin of error of approximately ±3.1%. As the participants are somewhat different in that research than in this research their findings are generally not comparable with this research.

Lucas, Drain, and Mackenzie (2014) authored the PwC 2014 "New Zealand insights into Global Economic Crime survey".

This quality assured paper appeared at the 6th annual conference of Computing and Information Technology Research and Education New Zealand (CITRENZ2015) and the 28h Annual Conference of the National Advisory Committee on Computing Qualifications, Queenstown, New Zealand, and October 6-9, 2015. Michael Verhaart, Amit Sarkar, Rosemarie Tomlinson and Emre Erturk (Eds).

While they do not explicitly mention their participant criteria, they do mention 22% of respondents were government or state owned organisations (pg. 29), and that 37% of respondent organisations had between 501-1000 employees (pg. 29) so they were studying reasonable sized organisations in the New Zealand context.

While their focus is on economic crime in general, they do consider cybercrime with findings that include “the perception of the risk of cybercrime is increasing at a faster pace than that of reported occurrences" (pg. 5) which is an important consideration for this research, both counts of actual cybercrime occurrences but also organisational perceptions of potential cybercrime and what if anything organisations do to protect themselves.

3. METHODS

A questionnaire was developed that used questions from previous researchers except where analysis or pilot testing had shown that the questions were either no longer relevant or were generally not answered. In other situations new questions were added. Examples of questions used by Quinn that were removed include question 19 from his 2005 survey (pg. 74) that asked what organisations did if they did not report intrusions to law enforcement, question 26 regarding cost benefit metrics for security funding (pg. 76) question 31 asking for specific counts of desktop operating systems used (pg. 78) and question 34 types of standards used by the organisations (pg. 79).

Previous researchers had used questions that had many rows and columns such as “technologies used” which had 30 named technologies (Digital IDs, Firewalls, Wireless as examples) and nine columns ranging from “before 1998” to “2005” which would have required respondents to have a lot of knowledge about very specific things, and take an unreasonable amount of time to answer those questions.

The 2014 survey developed for this research either dropped questions like those as too time consuming (or poorly responded to in previous versions) or feedback stated the question was not worth asking.

Questions created for the 2014 survey included asking what sort of “as a service” technologies New Zealand organisations are using, and if those services are sourced in New Zealand or not as this is expected to be a growth area in future surveys.

One of the more interesting questions not asked by Quinn as part of longitudinal studies was asking if respondents considered if organisations perceived cybercrime was on the rise and if the government was providing enough resources (either direct such as financial or indirect such as informational). Those questions were added to the 2014 survey and kept in the 2015 survey.

The key difference between 2014 and 2015 was changing the deployment method. In 2014 a paper based method was used and feedback from respondents suggested they believed more people would respond to an electronic survey. This differs from findings of Schuldt and Totten (1994) and Nulty (2008). Nulty (2008, pg. 303) in particular states roughly a 1/3 to 1/2 difference between paper based and online response rates, with online being lower than paper based. In 2015 online was trialled and while there were large savings in cost and time, the rate of actual response was half of 2014.

As with many of the previous researchers’ surveys this research was conducted as anonymous surveys and no attempts were made to track the responses back to the respondents except where respondents had explicitly stated their organisation’s name for follow up contact.

4. PARTICIPANTS

The initial 2014 survey was funded in part by a New Zealand based company who wish to remain anonymous. As such they provided funding to allow for the use of a professional mailing list which was *Data Warranted’s* mailing list. One of the appeals of the mailing list was that it was purchased as a lifetime license for the particular list, and a reasonable fee could be paid to have an updated version of it. Other benefits were that it also included email addresses which would prove useful for an electronic version of the survey. Other benefits of using a pre-generated mailing list included savings in preparation time, and being able to select specific categories of organisations to include or exclude.

The focus of this research was New Zealand businesses only and the following types of organisation were excluded: schools and academic institutions, and government organisations with the main reason being that those organisations are likely to be resourced in different ways for their cyber security defences.

In both 2014 and 2015 the same mailing list was used which was not updated between the deployment times. This was primarily for consistency so that the same group were potentially surveyed. There were a total of 932 organisations listed in the mailing list, and all those in the list were sent a paper based version of the survey (with a postage paid return envelope) in 2014, and an electronic version was emailed in the 2015 version. The 2014 survey was open for one month June 1st (based on when the surveys were expected to arrive) to June 30th, and the 2015 survey was initially open from June 1st to June 15th which was then extended June 22nd.

ANZSIC codes are “Australia New Zealand Standard Industrial Classification” codes which are broken down to 3 or more levels. As an example the top level code is a letter (P is Education) and the remaining levels are numbers. For a tertiary institute Level 1 would be P, the Level 2 representation would be P81, Level 3 would be P810, and Level 4 would be P810100 for Technical and Vocational Education and Training or P810200 for Higher Education.

In 2014, the respondents were comprised of 16 different top level ANZSIC codes and 7 organisations stated they were “other” and in 2015 respondents came from 13 different top level ANZSIC codes and 6 organisations stating they were “other”. Table 1 shows the three main respondent types by ANZSIC code and also includes organisations that selected “Other”.

Table 1 Main respondents by ANZSIC code 2014 and 2015

ANZSIC code	**2014**	**2015**
C Manufacturing	19.7%	12.1%
I Transport	10.0%	10.6%
M Professional Services	9.2%	15.2%
No code given: “Other”	5.4%	9.1%

Top level codes only were asked as level 4 codes could easily uniquely identify certain respondents. An additional open ended question was added if respondents did want to either name themselves directly, or include a level 3 or level 4 ANZSIC code.

5. DATA ANALYSIS

One potential challenge with surveys is determining what constitutes a valid response. Ideally a response would be valid if every question that could be answered was answered. For the 2014 survey, the paper based version was 12 pages, it was considered that if the first 6 pages (demographics, views on current and future cyber security risks, and government resourcing) and the final page (the ANZSIC organisational code for the respondent) were filled in, it would be a valid survey. A 2015 response was deemed to be valid based on the same criteria of specific questions answered. The data processing was done by using SPSS version 22, and all percentages are the "valid percent" to one decimal place unless otherwise stated. "Valid percent" means that only valid responses for that particular question are reported.

The main difference between the 2014 and 2015 surveys was their deployment (paper based vs. electronic). The response rate for the 2014 survey was 7 surveys returned unopened as "return to sender" giving a "bounce back" rate of less than 1% and a total 132 valid responses (14.2%).

The response rate for the 2015 survey was 223 responses "return to sender" (this figure covers those who had an out of office response which means the person may or may not be responding within the survey timeframe), those where the original recipient was no longer working for the organisation and where either internet mailing issues prevented the email from being delivered or the address was not deemed valid. This represents a bounce-back rate of 23.9%. There were a total of 66 valid responses (9.3% when considering surveys that were not bounced back) which is somewhat lower than 2014. It is noted that the Connect Smart survey ran at roughly the same time and some organisations may have not decided to respond to our survey due to having answered that survey or other related surveys in the same timeframe.

Overall the margins of error for the two samples are ±7.9% for the 2014 survey and ±11.4% for the 2015 survey with the 95% confidence level. This is not seen as an overall problem for comparisons of questions such as Question 11 (both 2014 and 2015) of "Do you believe cybercrime against New Zealand has increased over the last 24 months?". The sample size and margin of error does become a potential issue when considering the number of respondents from specific organisational types as reported in Table 1 such as "C Manufacturing" in 2014 had 26/132 respondents (19.7%) vs. 8/66 (12.1%), and "M Professional services" had 12/132 responses (9.2%) in 2014, and 10/66 (15.2%) in 2015. On the surface the percentage of Professional services responses appears to have increased but in reality it is functionally the same between 2014 and 2015. Where this is a potential issue for analysis or presentation it has been noted.

6. FINDINGS

Table 2 considers the direct comparison with the 2014 and the 2015 results for singular questions of interest. The "positive" answer has been added to the question, so if organisations have been a victim of cybercrime, it has been presented in the table. Where interesting or unexpected results have been encountered (such as question 13, "Does the government provide enough resources?") more than one option has been presented with the relevant answer in italics.

Table 2 2014 and 2015 single question comparisons

Question number	Question	2014	2015
8	Percentage of IT budget spent on IT Security *3-5%*	20.9%	13.6%
8	Percentage of IT budget spent on IT Security *Unknown*	23.3%	36.4%
11	Has cybercrime *increased* in the last 24 months?	63%	78%
12	Will cybercrime *increase* in the next 24 months?	75.8%	87.9%
13	Does the government provide enough resources to protect the national cyber infrastructure? *Yes*	9.2%	12.1%
13	Does the government provide enough resources to protect the national cyber infrastructure? *Unknown*	62.3%	43.9%
14	Does the government provide enough information to business on how to protect corporate cyber infrastructure? *Yes*	9.2%	21.2%
14	Does the government provide enough information to business on how to protect corporate cyber infrastructure? *Unknown*	42.%	21.2%
15	Does your organisation invest the appropriate amount on security awareness training? *No*	55%	65.2%
25	Has your organisation been a *victim* of cybercrime?	11.5%	12.1%

6.1 Observations on specific findings for single question queries

As a note, the questions regarding a 24 month period were used as this will be part of a year on year longitudinal study and allow analysis across longer timeframes.

Despite the difference in sample sizes, one of the more interesting findings is that respondents' attitudes to if government provides resources (question 13) and information (question 14) has changed between the years from "Unknown" to a more definitive answer generally which is "No". Initially it was likely this could be explained by Connect Smart's own research (Colmar Brunton, 2015) in that it would expected most organisations would have heard of Connect Smart and other government initiatives, however their actual findings were approximately only 4% of respondents had heard of Connect Smart's campaign (pg. 20).

The other main findings include that organisations are generally spending the same percentage of their IT budget on security despite their concerns that cybercrime will increase, and that organisations are definitely not investing enough in security awareness training.

Findings not included in Table 2 show that in 2015, 42.4% of organisations did not allow "bring your own device" (BYOD) and of those who did allow BYOD the results are split reasonably evenly between the organisations supporting any device an employee uses versus organisations only supporting specifically named devices. These findings were not included in Table 2 as those specific questions were new to 2015 but will be kept going forward.

Table 3 Computer Threats comparison 2014 and 2015

Category	**2014**	**2015**
Generic External such as viruses, malware	**72.0 %**	**69.7 %**
Unpredictable natural disasters such as earthquake	**47.0 %**	**48.5 %**
Random internal such as employee mistake	**44.7 %**	34.8%
Targeted internal attacks by employees such as data theft	20.5 %	36.4%
Random external attacks such as cyber vandalism	22.0 %	27.3%
Targeted external attacks such as hackers or industrial espionage	36.4 %	**51.5%**
Other	1.5%	1.5%

The respondents were asked to rank the three main threats they were concerned about based on seven possible types which are presented in Table 3. The three most common responses for each year have been **bolded** in Table 3 for clarity. As a note because respondents could select up to three types, the percentages do not add to 100% (or 300% as although no respondent picked more than 3, some selected only one or two). The question was asked this way as previous researchers had either asked organisations to rank all seven in order (which resulted in it either not being answered or only some answers given ranks) or used an open ended question approach that meant having to recode the answers and getting inconsistent ranges of answers. Some organisations would only give one or two concerns whereas others would include six of more concerns.

The most likely reasons for this are that generic external threats such as viruses and malware cannot easily be guarded against, as they are always changing. Likewise unpredictable natural disasters can reasonably affect most organisations in New Zealand either directly such as fire or earthquake, or indirectly by affecting supply chain infrastructure or roads and the like. The rise of targeted external attacks is considered due in part to the rise of ransomware attacks (Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015) and the rise in prominence those attacks are being reported in the media.

6.2 Multiple question analysis

This section considers a number of questions that can only be answered by considering multiple questions together. As such the main questions are

- IT budget spent on IT security and perceived adequacy
- IT budget spent on security and being a victim of cybercrime
- Types of organization and their IT security spending
- Security awareness training and organisational factors
- Types of organisation and being a victim of cybercrime
- Upgrading from Windows XP and being a victim of cybercrime

6.2.1 Spending on security and perceived adequacy

As Table 2 previously showed, in 2014 most organisations stated they spent 3-5% of their IT budget on IT security which remained the most common response in 2015 excluding "unknown". Table 4 then considers those organisations that responded "yes" to question 9 (is your organisation's spending on IT security adequate?") and the amount they were spending on IT security (question 8).

Table 4 Comparison of IT budget spent on IT Security and belief it is Adequate 2014 and 2015

Percent spent on IT security	**2014 (n=81)**	**2015 (n=27)**
<1%	43.8%	40.0%
1-2%	44.0%	28.6%
3-5%	63.0%	22.2%
6-7%	70.0%	100%
8-10%	80.0%	60%
>10%	100.0%	66.7%
Unknown percentage spent	66.7%	41.7%

A key observation from Table 4 is that in 2014, 81 respondents (61.4%) answered that the portion of IT budget on security was adequate whereas in 2015 only 27 respondents (40.9%) answered that the portion spent on security was adequate. This in itself fits with earlier findings that 2015 respondents felt cybercrime had risen and will continue to rise (Table 2). The percentages are presented as reported (rather than recoded), as banding was used instead of making it an open ended question to allow for easier comparison between these surveys and previous researchers.

The second observation is that in 2014 generally as the percentage spent on IT security increased, the more likely an organisation was to feel their spending was adequate. The 2015 findings are less clear because as an example only one organisation responded that their budget percentage of IT was 6-7% and because they thought it was adequate that result was reported as 100% for that category.

6.2.2 IT spending on Security and being a victim of cybercrime

Following from those findings it is possible to consider "does the percentage of IT budget spent on security relate to the likelihood of the organization being a victim of cybercrime?" This question needed a high response rate from two specific survey questions: organisations being able to specify their IT security budget (as a percentage), and organisations being victims of cybercrime.

As the overall response rate for being a victim of cybercrime was functionally 12% for both years, it made it difficult to accurately measure factors such as question 8 ("Percentage of budget spent on IT security") without running into margin of error concerns. The frequencies (after recoding) show however that organisations who spent 0-5% of their budget on IT security were much more likely to have been victims of cybercrime. A second caveat with this data is that many of the respondents to question 8 in general selected "Unknown". This can be explained as the respondent could have been a systems administrator and not a chief technology officer or a manager or they did not want to answer the question.

6.2.3 Organisational budget spent on IT security

Table 5 Organisation type (ANZSIC code) spending on Security as a percentage of IT budget

Percentage of IT budget	2014 (as percentages)			2015 (as percentages)		
Recoded	**C**	**I**	**M**	**C**	**I**	**M**
0-5 %	69.3	61.5	33.3	37.5	71.4	50
6-10 %	7.7	0.00	33.3	25	14.3	0
10+ %	11.5	7.7	8.4	0	0	10
Unknown	11.5	30.8	25.0	37.5	14.3	40

Table 5 presents the three main respondent organisational types based on their ANZSIC code (presented in Table 1) and the percentage of IT budget spent on security. Due to the number of possible answers for question 8 (percentage spent on security) it has been recoded appropriately to three main fields, and unknown has been left.

As with other observations, the 2015 values are not entirely consistent with the 2014 values because of a lower response rate in 2015 which in turn can make it difficult to interpret. However these values are useful when considering 6.2.5 organisational type and being a victim of cybercrime.

6.2.4 Security awareness training and organisational factors

The respondents in general did not feel that their organisations were providing enough security awareness training (Table 2). When considering the organisational type of the respondent, no particular organisation in either 2014 or 2015 stood out as being particularly "good" at providing the appropriate amount of security awareness training which suggests this needs to be improved across all organisations based on ANZSIC code.

When considering the percentage of IT budget spent on security and investment in security awareness training however, those who felt their organisations were spending enough of the budget in security also felt their organisation was investing enough in security awareness training.

6.2.5 Organisational type and being a victim of cybercrime

Table 6 Organisation type (ANZSIC code) and victim of cybercrime

	2014 (as percentages)			2015 (as percentages)		
Response	**C**	**I**	**M**	**C**	**I**	**M**
Yes	19.2	8.3	8.3	12.5	14.3	10.0
No	80.8	83.4	75.0	87.5	85.7	90.0
Unknown	0.0	8.3	16.7	0.0	0.0	0.0

Table 6 presents the three main organisational types and of those who reported being victims of cybercrime. Unknown has been included as some organisations either responded they knew they had had financial losses but could not identify it as purely cybercrime (such as someone using a stolen credit card to purchase goods from an organisation's website which the respondent stated was regular theft rather than a cybercrime) or that they knew they had been a victim of crime but had not isolated the specific cause. Because of the overall low amount of reported cybercrime (11%) these results are more for illustrative purposes that the three main respondent types were not particularly more likely to be victims of cybercrime than not. Looking at the other respondents however showed that Accommodation (ANZSIC code H) had the largest problem with cybercrime and Electricity (ANZSIC code D) also reported cybercrime. The key note is that in 2014 only three Accommodation organisations responded (two in 2015) and only eight Electricity in 2014 (one in 2015) which while below the margin of error does suggest an area for further review given the very large number of accommodation service organisations in New Zealand and the critical role that the Electricity sector plays in New Zealand.

6.2.6 Upgrading from Windows XP and being a victim of cybercrime

A question this survey considered was if organisations who had been victims of cybercrime (question 25) had upgraded from Windows XP (question 17) or not. Windows XP had an end of support date of April 2014 which was two months before the 2014 survey was deployed and prior research suggested that most but not all respondents would be using Windows XP in the year prior to the 2014 survey. The results of Q17 showed that 69.3% of respondents had upgraded from Windows XP before responding to the survey, and 3 respondents (2.4%) stating they would not be updating their Windows XP clients. Feedback and observation showed that a number of organisations still use legacy software and need to have systems like Windows XP. No respondent stated that they did not use Windows XP. The 2015 results somewhat confirmed the timeframe information with 66.7% saying they had updated 12 months or more from the 2015 survey date. Of the remaining 33%, 13.6% stated they were still in the process of upgrading and the other 19.4% had updated sometime in the last 12 months (between the 2014 and 2015 surveys).

Those results were then cross tabulated with the organisations who had stated they were a victim of cybercrime in 2014 and 2015. In 2014 there were 14 victims of cybercrime, of which 10 had already upgraded from Windows XP (of a total of 87 organisations who had upgraded) giving a percentage of 11.5%, with the remaining 4 either in progress, within the next 6 months (from the 2014 survey date) or unknown.

With the 2015 results 8 organisations stated they had been a victim of cybercrime, and this was evenly split between those who had upgraded from Windows XP over 12 months ago, and those who were in the process of upgrading. By itself this is an interesting observation but not necessarily useful, a better way of considering it is, 44 organisations had upgraded Windows XP more than 12 months ago, and only 4 of those had been victims (9.1%) versus 4 organisations in the process of upgrading windows XP of 9 organisations were victims of cybercrime (44.4%). Arguably the survey could have asked if using Windows XP was the sole cause of the cybercrime event, however prior research showed that often organisations did not know the cause or could not trace it to a particular event, or did not wish to divulge it. In future surveys, upgrading form XP will be changed to the most appropriate operating systems, and a simple tick box will be added asking if the operating system being out of support range was the most likely cause of the cybercrime.

7. CONCLUSIONS

The main conclusion to draw from this research is that organisations are consistently reporting cybercrime victimhood at approximately 12% between these surveys (2014, 2015), and that much like Lucas et al. (2014) the perception of being at risk from cybercrime is rising much more quickly than the occurrences of cybercrime.

Importantly when considering concerns and readiness for New Zealand organisations, respondents believed cybercrime had increased and will be increasing in the next 24 months, and that more organisations had a firm opinion that government was not doing enough in the form of resources or knowledge on how to protect against cybercrime. Related to this, organisations generally did not feel their organisations were spending enough on security if the percentage of budget devoted to security was 5% or less, and most organisations did not feel their organisation was investing enough into security awareness training.

This research also asked what the main threats organisations were concerned about, with viruses and malware (generic external threats) being of most concern from previous research and consistently across both years of this research, and the impact of unpredictable natural disaster also being a concern. This is partly expected given the 2011 Christchurch Earthquakes and the ongoing issues arising from it. The third biggest concern changed between 2014 and 2015 however with the rise of external targeted attacks such as hackers or industrial espionage being a much larger concern in 2015.

It is likely by addressing the other concerns raised in this research (organisation security spending, governmental protections and the like) that the rise of hackers and hacking attacks can be mitigated whereas concerns such as unpredictable natural disaster cannot. In case of natural disaster organisations can be better prepared for the aftermath by having disaster recovery plans, backup, and access to specific business resources to ensure business continuity.

8. FUTURE WORK

The two main aspects of future work for this research is conducting the same style of questionnaire on an annual basis which would address the key shortcomings of previous research. Although feedback in 2014 suggested that paper based was a “waste of resources” and that certain respondents “only ever respond to electronic surveys”, the 2015 response rate was lower than 2014. In 2016 the survey will be paper based again and one of the aims will be to determine if that has an effect on response rate.

A second area of future work is considering specific case studies of organisations to better address the aspects of “why” certain views changed. In particular both questions 13 and 14 asked about government provision of resources and information for protecting cyber infrastructure. The observation is that organisations felt government was not providing enough, and a good follow up would be determining if organisations expect government to provide this to organisations or not.

A third area of interest is measuring how organisations were spending their IT security budget as many of the victims of cybercrime were spending 5% or less of their IT budget on security and determining if that money could be spent better, or if more money was definitely needed to be spent.

REFERENCES

Colmar Brunton. (2015). Cyber security behaviours and campaign awareness for 'Connect Smart'2015 Retrieved from: http://www.connectsmart.govt.nz/assets/Uploads/Colmar-Brunton-Connect-Smart-Research-2015.pdf

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI computer crime and security survey*: Computer Security Institute San Francisco, CA.

Hails. (2015). The top 3 cyber security threats for NZ small businesses: #ConnectSmart. Retrieved 3/8/2015, from http://blog.netsafe.org.nz/2015/06/23/the-top-3-cyber-security-threats-for-nz-small-businesses-connectsmart/

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. Paper presented at the *Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference*, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings.

Lucas, Drain, & Mackenzie. (2014). New Zealand insights from PwC's 2014 Global Economic Crime survey (pp. 36). Retrieved from http://www.pwc.co.nz/PWC.NZ/media/pdf-documents/publications/pwc-global-economic-crime-survey-new-zealand-supplement-feb-2014-final2.pdf: PricewaterhouseCoopers.

Nulty, D. D. (2008). The adequacy of response rates to online and paper surveys: what can be done? *Assessment & Evaluation in Higher Education, 33(3),* 301-314.

Quinn, K. (2014). *Identification and analysis of security risks in New Zealand information technology*. Master’s thesis, University of Otago.

Roberts, C. (2009). *Modelling cybercrime and risk for New Zealand organisations.* Doctoral thesis, University of Otago

Schuldt, B. A., & Totten, J. W. (1994). Electronic mail vs. mail survey response rates. *Marketing Research, 6(1),* 3-7.

Smith, R. (2003). Methodological Impediments to Researching Serious Fraud in Australia and New Zealand. Paper presented at the Evaluation in *Crime and Justice: Trends and Methods Conference*. Canberra