2007

The Impact of Security Surveys within Australia and New Zealand

Matthew J. Warren
Deakin University

Shona Leitch

DOI: 10.4225/75/57b553a5b8764
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007

The Impact of Security Surveys within Australia and New Zealand

Matthew J. Warren and Shona Leitch
School of Information Systems,
Faculty of Business and Law,
Deakin University,
Burwood, Victoria, Australia, 3217
mwarren@deakin.edu.au
shona@deakin.edu.au

Abstract

Information security is portrayed as a global problem that impacts all countries that are considered as part of the Information Society. Recent surveys show that there are increased concerns about computer crime. The paper will focus upon recent national security surveys from Australia and New Zealand and the trends that this research shows. Is it fair to assume the security practices are the same all over the world? The paper looks at security practices from a number of different countries perspectives and shows that security practices are not generic and vary from country to country. The paper will also evaluate the worth that National Security Surveys have in the field of Information Security Surveys.

Keywords

Computer Security, Security Practices, Australia, New Zealand and Survey.

INTRODUCTION

Information security is portrayed as a global problem that impacts all countries that are considered as part of the Information Society. Numerous annual security surveys show that there are increased concerns about security risks with Information Society or particular technologies. The growth of the Internet has resulted in the development of the Information Society and with the new society comes new associated security risks such as on-line fraud, identity theft, hacking. etc.

As the Information Society has developed, so has the concerns raised regarding security, these concerns have been reported via the use of surveys. Annual or regular survey surveys are released by governments and organizations showing the state of security in particular countries, examples include, AusCERT (Australia), CSI/FBI (USA), Department of Trade and Industry (UK), etc. Some countries have linked security issues into the development of strategies in relation to developing an Information Society for example Switzerland (Forum ICT, 2007).

The virtual information society consists of physical countries all over the world. Within these separate countries organizations have different cultures (Hofstede,1994; Trompenaars,1997). The paper looks at security practices from Australia and New Zealand based upon these key surveys and tries to determine whether security practices and issues are not generic and vary from country to country.

SURVEY RESULTS

This section will analyse the latest national security surveys from Australia and New Zealand in order to determine what the key security trends and issues are.

AUSTRALIAN PERSPECTIVE

A survey was undertaken by AusCERT during 2006 and was based upon the responses of 389 Australian organizations (AusCERT, 2006).

Survey questionnaires with business reply-paid envelopes were sent to 2,024 IT managers or their equivalents from a range of Australian public and private sector organisations. These enterprises were invited to complete the survey on-line via a secure web site, hosted by ACNielsen, or return the paper questionnaire via the reply-paid envelope. Responses were also sought from a number of private and public sector industry groups, including the Trusted Information Sharing Network (TISN), 19 members were invited to complete the survey via the secure web site. Responses to the survey totalled 389, which included 238 paper submissions and 151 on-line submissions. In total the response rate to the survey was 17%. All responses were anonymous (AusCERT, 2006).

The major trends from the survey, included (AusCERT, 2006):

- 22% of organizations indicated that they had experienced a security incident an the average cost in damage was A$241,150;
- 56% of respondents invested under 5% of their IT security budget on security;
- 55% of the respondents indicated that they no IT staff with any security qualifications;
- 34% of respondents feet that they are part of the Australian Critical Infrastructure.

The top three security incidents reported were (AusCERT, 2006):

1. Insider abuse of Internet access, email or computer system resources;
2. Laptop Theft;
3. Virus or Worm infection.

In terms of security standards used, the top standards used by Australian companies were (AusCERT, 2006):

- AS 17799 - 45%;
- AS 7779 - 31%;
- Vendor specific standards or guides - 31%;
- Industry specific IT standards - 31%;
- State government IT security standards - 18%.

Of the respondents, they reported that 95% have media back-up procedures, 93% have user access management policies, 78% have external network access policy and 72% have a user responsibility policy (AusCERT, 2006).

In summary, the key findings of the Australian survey are that the minority of Australian organizations are victims of crime and suffer an average loss of A$241,150. The survey also shows that the majority of Australian companies spend less than 5% of their budget per year protecting their systems. Australian companies biggest security threats are from within the organization by staff misusing organizational resources. The survey also indicates the low impact of security standards but indicate a high usage of Information Security tools relating to technology, for example media back-up procedures, user access management policies, etc.

An alternative view of the survey put forward by Trusted Information Sharing Network (TISN) (TISN, 2006) was that the positive trends of the survey are a marked reduction in the number of reported cyber-attacks, and a rise in the number of organisations that were free from detected internal attacks. Participants in the survey also recognised that spam is more than just a time wasting, in-box clogging nuisance that takes up valuable server

space. Ninety per cent reported using spam filters, not only to stop junk email, but also to protect systems against malware and cyber-attacks.

The TISN view of the report (TISN, 2006) also indicates that financial losses from both cyber-attacks and external attacks are rising. These results indicate that as organisations increase their connectivity to external networks, including the Internet, they increase their exposure to cyber-threats. A concerning trend is the reported decrease in spending on IT security, and the reduction in levels of protective security. Given the nature of the threat environment, the report states '… now is not the time to be winding back on protective security counter-measures or reducing IT security budgets.'

The TISN view also stated that there was a significant change in types of attacks reported (TISN, 2006). While there has been a reduction in viruses and worms, there has been an increase in trojan attacks and rootkit infections. This indicates a change in why hackers do what they do. They are no longer just seeking kudos among their peers—now they are driven by financial gain.

New Zealand Perspective

In 2007 the results of the second national New Zealand Computer Security survey was reported and based upon 2006 results. The 2007 survey results were based upon the responses of 113 New Zealand computer security practitioners (Quinn, 2007). This section of the paper is based upon the results of the New Zealand Computer Security Survey (Quinn, 2007).

The major trends from the survey, included:

- 87% of organizations indicated that they had experienced a security incident, the average cost in damage was NZ$13,000;
- Two-thirds of New Zealand organisations invest less than 5% of their IT budget in security;
- 53% of the respondents indicated that they had no IT staff with any security qualifications.

The top three security incidents reported were:

- Viruses;
- Laptop or mobile asset theft;
- Insider abuse of Net access or email.

In terms of security standards used, the top standards used by New Zealand companies were:

- AS/NZS ISO/IEC 17799.2001 (AS/NZS444.1) - 40%;
- Other Industry specific IT standards - 35%;
- Vendor specific standards or guides - 27%;
- Security in Government Sectors (SIGS) - 25%;
- AS/NZS 17799.2.2000 (aka AS/NZS444.2) - 18%.

Of the respondents, they reported that 96% have media back-up procedures, 96% have user access management policies, 80% have external network access policy and 76% have documented security responsibility policy (Quinn, 2007).

The key findings of the New Zealand survey are that the majority of New Zealand organizations are victims of computer crime and suffer an average loss of $NZ13,000 per year, the survey also shows that two-thirds of New Zealand organizations invest less than 5% of their IT budget in security. New Zealand companies biggest

security threats are from outside the organization in the form of viruses. The survey also indicated the low impact of security standards.

PROBLEMS AND USAGE OF SECURITY SURVEYS

The major trends from the Australian AusCERT survey, indicated that (AusCERT, 2006):

- 22% of organizations indicated that they had experienced a security incident an the average cost in damage was A$241,150;
- 56% of respondents invested under 5% of their IT security budget on security;
- 55% of the respondents indicated that they no IT staff with any security qualifications;
- 34% of respondents feet that they are part of the Australian Critical Infrastructure.

The major trends from the New Zealand National Security survey, indicated that (Quinn, 2007):

- 87% of organizations indicated that they had experienced a security incident, the average cost in damage was NZ$13,000;
- Two-thirds of New Zealand organisations invest less than 5% of their IT budget in security;
- 53% of the respondents indicated that they had no IT staff with any security qualifications.

The problem is what does these statistical trends actually show. The statistics put forward are superficial and there is no discussion of what the statistics and statements represented actually mean within the surveys. Because of the superficial way that the statistics are used within the surveys, the idea of any comparison between surveys of different countries is unworkable.

But the role of national security surveys should not be discounted completely, they should be used with caution. The authors have determined that there are advantages and disadvantages of using such national security surveys.

The advantages of such national security surveys include:

- that they help to raise general awareness about particular security issue, these security issues could be new or have become a greater issue;
- it would allow media organizations to report about security issues to the general populace;
- It would allows organizations to have marketing information that they could use to sell or promote products;
- it provides a very basic snapshot of the state of security within a particular country.

The disadvantages of such national security surveys include:

- for national security surveys the same sample size used are very small for example Australia 389 organizations and New Zealand 113 organizations;
- the organizations involved in the survey focus upon government and larger organizations, smaller organizations do not play a key role in the survey participants even though they represent the majority of commercial organizations;

- the questions used within the survey may not have any relevance and the outcome of the questions may not have any meaningful impact and would not have an impact in relation to security management;

- there is an issue of interpreting results from such a survey and determine their meaning.

The future of these national security surveys are under review. In 2006 it cost AusCERT $44,000 to produce the national computer crime survey, which provided local up to date information on network attacks over the previous 12 months. These funds were made available from the Federal Attorney General's department. However, this year those funds have been redirected to support a larger computer crime survey that will be published in November. The new survey is being undertaken by the Australian Institute of Criminology (Rossi, 2007).

CONCLUSION

In the author's opinion the role of national security surveys are very limited. The results of the surveys contain only superficial detail. Most of the results are based upon basic percentages and lack any formal statistical analysis. The surveys are also based upon very small sample sizes. The issue is how can a national survey be based upon such small samples? For example, New Zealand's was based on113 responses.

Only time will tell if there is any future for national security surveys in providing detailed information or whether they just provide the media will simple security snapshots.

REFERENCES

AusCERT (2006) *2006 Australian Computer Crime and Security Survey*, AusCERT, Australia, ISBN: 1-86499-849-0.

CCIP (2006) CCIP (Critical Centre for Infrastructure Protection) e-Bulletin, Issue 23, August, New Zealand.

Forum ICT (2007) *Information Society in Switzerland*, Forum ICT 21, Switzerland.

Hofstede, G (1994) *Cultures and organizations – Software of the mind*,

Harper Collins Publishers, London, UK.

TISN (2006) CIP Newsletter - Trusted Information Sharing Network, Vol 3, No 3, Australia.

Trompenaars, F; Hampden-Turner, C (1997) *Riding the waves of culture* (2:nd edition),McGraw-Hill, New York, United States.

Rossi, S. (2007) AusCERT no longer defined by THAT survey, Computer World, 21st May.

University of Otago (2007) Press Release - IT management practices inadequate to preserve forensic evidence, 26th September, New Zealand.

Quinn, K (2007) *Second annual New Zealand computer crime and security survey*. Alpha-Omega Group, Dunedin, New Zealand, ISBN 11774207.

COPYRIGHT