Attention IT managers: Why you can’t trust security surveys

Information security is a global problem that influences all countries that are considered part of the information society. Information managers are regularly faced with a variety of security surveys showing the latest security trends. Recent security surveys show an increased concern about computer crime. The question is, how can an organisation assess and use this information, and do these surveys hold any value for managers working in the field of information security?
Introduction

The aim of this paper is to explore, from an information manager's perspective, the confusing issue of security surveys and the data that they present. The issue that information managers and information security managers face is how can this data be used to make key organisational decisions in relation to security management?

As the information society has developed and expanded, so too have concerns regarding information security. Most of these concerns have been reported via surveys. Annual or regular surveys are released by governments and organisations revealing the state of security in particular countries, for example, AusCERT (Australia), CSI/FBI (USA) and the Department of Trade and Industry (UK). Some countries have linked security issues to the development of strategies in relation to developing an information society, for example, Switzerland (Forum ICT 2007). It should be added that the information society consists of separate physical countries, and that within these separate countries organisations can have different security cultures (Hofstede 1994; Trompenaars 1997).

Various annual security surveys show that there are increased concerns about security risks and particular technologies. The growth of the Internet has resulted in associated security risks, such as online fraud, identity theft and hacking. While this new technology does bring great benefits, the major question for organisations is: How can this technology be managed securely?

This paper looks at information security practices in Australia and New Zealand based on key surveys, and determines whether security practices and issues are generic. It also suggests how organisations can use the data that is presented.

Survey results

AN AUSTRALIAN PERSPECTIVE

A survey undertaken by AusCERT during 2006 was based on the responses of 389 Australian organisations (AusCERT 2006). This was the last survey of its kind to date within Australia. Questionnaires with business reply-paid envelopes were sent to 2024 IT managers or their equivalents from a range of Australian public and private sector organisations. These managers were invited to complete the questionnaire online via a secure website, hosted by ACNielsen, or return the paper questionnaire using the reply-paid envelope. Responses were also sought from a range of private and public sector industry groups, including the Trusted Information Sharing Network (TISN), from which 19 members were invited to complete the questionnaire via the secure website. Responses to the survey totalled 389, which included 238 paper submissions and 151 online submissions. In total, the response rate to the survey was 17 per cent and all responses were anonymous (AusCERT 2006).

The major trends from the survey are listed as follows:

- 22 per cent of organisations indicated that they had experienced a security incident and the average cost of the damage was $A241,150.
- 56 per cent of respondents invested less than 5 per cent of their IT security budget on security.
- 55 per cent of respondents indicated that they had no IT staff with security qualifications.
- 34 per cent of respondents felt they were part of the Australian critical infrastructure, that is, those physical facilities, supply chains, information technologies and communication networks that if destroyed, degraded or rendered unavailable for an extended period, would adversely influence the social or economic wellbeing of the nation, or affect Australia's ability to ensure national security (TISN 2008).

The top three security incidents reported were:

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 organisations were:

- AS 17799 (2003) – 45 per cent;
- AS 7779 (2001) – 31 per cent;
- Vendor-specific standards or guides – 31 per cent;
- Industry-specific IT standards – 31 per cent;
- State government IT security standards – 18 per cent.

It was also reported that 95 per cent of respondents had media back-up procedures; 93 per cent had user access management policies; 78 per cent had an external network access policy and 72 per cent had a user responsibility policy (AusCERT 2006).

In summary, the key findings of the Australian survey were that a minority of Australian organisations find themselves victims of information security crime and suffer an average annual loss of $A241,150. The survey also showed that the majority of Australian organisations spent less than 5 per cent of their IT budget per year protecting their systems, which is an area of great concern. It was also highlighted that the biggest threat to Australian organisations comes from within the organisation itself, namely by staff misusing organisational resources. The survey also indicated that while security standards had little impact, there was a high usage of information security tools relating to technology, for example, media back-up procedures and user access management policies.

An alternative view of the survey was proposed by TISN in 2006. TISN determined that the positive trends in the survey included 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 was more than just a nuisance that wastes time and clogs up valuable server space. It was reported that 90 per cent of respondents were 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 also indicated that financial losses from both cyber-attacks and external attacks were rising. These results indicate that as organisations increase their connectivity to external networks, including the Internet, they increase their exposure to cyber-threats. Another concerning trend was the reported decrease in spending on IT security, and the reduction in levels of protective security. Given the current nature of the threat environment, the report stated “...now is not the time to be winding back on protective security counter-measures or reducing IT security budgets.”

“...THE BIGGEST SECURITY THREAT TO AUSTRALIAN ORGANISATIONS COMES FROM WITHIN THE ORGANISATION ITSELF, NAMELY BY STAFF MISUSING ORGANISATIONAL RESOURCES.”

TISN also stated that there was a significant change in the types of attacks reported. Their analysis showed that while there had been a reduction in viruses and worms, there had been an increase in Trojan attacks and root kit infections. This indicates a change in why hackers do what they do, in that they are no longer just seeking kudos from their peers, but they may also now be driven by financial gain.

A NEW ZEALAND PERSPECTIVE

In 2007, the results of the second national New Zealand computer security survey were reported. The survey results were based on the responses of 113 New Zealand computer security practitioners (Quinn 2007).

The major trends from the survey are listed as follows:

- 87 per cent of organisations indicated that they had experienced a security incident in which the average cost of damage was $NZ13,000.
- Two-thirds of New Zealand organisations invested less than 5 per cent of their IT budget in security.
- 53 per cent of respondents indicated that they had no IT staff with security qualifications.
The top three security incidents reported were:
1) Viruses
2) Laptop or mobile asset theft
3) Insider abuse of net access or email

In terms of security standards used, the top standards used by New Zealand organisations were:
- AS/NZS ISO/IEC 17799.2001 (AS/NZS444.1) – 40 per cent;
- Other industry-specific IT standards – 35 per cent;
- Vendor-specific standards or guides – 27 per cent;
- Security in government sectors (SIGS) – 25 per cent;
- AS/NZS 17799.2.2000 (also known at AS/NZS444.2) – 18 per cent.

It was also reported that 96 per cent of respondents had media back-up procedures; 96 per cent had user access management policies; 80 per cent had an external network access policy and 76 per cent had a documented security responsibility policy (Quinn 2007).

The key findings of the New Zealand survey showed that the majority of New Zealand organisations were victims of computer crime and suffered an average loss of $NZ13,000 per year. The survey also showed that two-thirds of New Zealand organisations invested less than 5 per cent of their annual IT budget in security. New Zealand organisations' biggest security threats were from outside the organisation in the form of viruses. The survey also indicated the minimal influence of security standards.

PROBLEMS AND USAGE OF SECURITY SURVEYS

The key problem is what do these statistical trends that are reported in security surveys actually show? The statistics presented from these surveys are superficial in that there is no discussion of what the statistics and statements actually mean. Because of this, the idea of any comparison between the surveys conducted in Australia and New Zealand is unworkable.

But the value of national security surveys should not be discounted completely – just used with caution. The authors have determined that there are advantages and disadvantages of using national security surveys, which should be considered by IT managers.

One key advantage of national security surveys is that they help to raise general awareness about security issues that are either new or have become more significant over time. Security surveys also allow media organisations to report about security issues to the general populace and allow other organisations to have access to marketing information that could be used to sell or to promote products. Overall, these surveys provide a very basic snapshot of the state of security within a particular country.

However, one of the disadvantages of national security surveys is that the sample sizes used are generally very small. For example, the Australian survey discussed in this paper involved 389 organisations and the New Zealand survey involved 113 organisations. The organisations involved in the surveys are generally government and larger organisations, with little consideration given to smaller organisations. This is indeed a disadvantage as smaller organisations represent the majority of commercial organisations in these countries.

Furthermore, the questions used within the surveys may not have any relevance and the outcome of the questions may not have any meaningful impact in relation to security management. Overall, the issue of interpreting results from such surveys and determining their meaning is problematic.

Further investigation into the samples used in the AusCERT survey (AusCERT 2006) identifies interesting trends presented in Table 1. What is of interest is the relationship between response rates and industry type. While most responses came from the manufacturing sector, the sectors in which the highest response rates were expected (information technology and telecommunication) had very low rates of participation. This means that the respondent sample does not truly represent Australian industry and also raises questions about the value of a national survey. There is no discussion within the survey on whether the respondents represent large, medium, small or micro-sized
organisations, which again raises concerns about the validity of the survey findings.

The other interesting point is that the response rate to the AusCERT survey shown in Table 1 actually represents a response rate of 101 per cent.

The future of these national security surveys is currently under review. In Australia, in 2006, AusCERT spent $A44,000 on producing the national computer crime survey from funds made available by the Attorney-General's department. However, in 2007 these funds were redirected to support a larger computer crime survey that will be published in November 2008. The Australian Institute of Criminology has undertaken a new survey (Rossi 2007), but to date these results have not been released. In 2008, AusCERT released a new national survey, but this new survey was based on home usage of computers (AusCERT 2008).

### TABLE 1: PERCENTAGE OF RESPONDENTS IN AUSCERT 2006 SURVEY ACCORDING TO INDUSTRY

<table>
<thead>
<tr>
<th>RANK</th>
<th>INDUSTRY</th>
<th>PERCENTAGE OF RESPONDENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Manufacturing</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>Local government</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>Education/Research</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>State government</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Finance</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>Medical health</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>Retail</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>Transport</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>Utilities</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>Wholesale</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>Federal government</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>Personal and other services</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>Other</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>Information technology</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>Legal</td>
<td>2</td>
</tr>
<tr>
<td>16</td>
<td>Cultural and recreational services</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>Mining/Resources</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>Construction</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>Hospitality</td>
<td>2</td>
</tr>
<tr>
<td>20</td>
<td>Property and business services</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>Telecommunication</td>
<td>1</td>
</tr>
</tbody>
</table>
Conclusion

It is clear from the findings of this paper that the role of national security surveys is very limited. The results of the surveys only explain superficial detail in relation to security. Most of the results are based on basic percentages, and lack any formal statistical analysis. The surveys are also based on very small sample sizes that are not truly representative of national organisations. The data and security trends shown in these national surveys are not detailed enough to provide information managers with sufficient information to make strategic decisions or to develop new organisational policies.

References


