A SURVEY OF COMPUTER CRIME AND SECURITY IN SOUTH AFRICA

A. Stander, A. Dunnet, J. Rizzo

Dept Information Systems, University of Cape Town

Adrie.Stander@uct.ac.za, petitqul@gmail.com, jackalza@gmail.com

1 INTRODUCTION

Computer crime has escalated considerably over recent years and has become a very serious problem that costs governments, organisations and general computer user's significant losses annually. The Internet provides endless connectivity to billions of users around the world which has greatly influenced the flow of information. As revolutionary as this has been, the associated benefits have extended to the criminal world and allowed these miscreants to take advantage of this powerful tool to commit a host of computer crimes (Jones, 2007). Organisations relying on the Internet for daily business processes face significant challenges to ensure that their networks operate safely and that their systems continue to provide critical services even in the face of attack (Householder, Houle & Dougherty, 2002). Moreover, it has become apparent that technology and the law do not seem to go hand in hand, and instead, are grappling to find common ground (Jones, 2007).

As national computer crime statistics do not exist, the purpose of this empirical research is to produce the first South African survey on computer crime and security. By analysing the results of the national survey, a better understanding of the extent to which South African organisations are aware of and affected by computer crime can be determined. The results will also indicate the adequacy of current organisational resources, policies and procedures. South Africa's current position will be evaluated in comparison with Australia and the United States of America. Ultimately, the research aims to serve as justification for further investment in computer security technologies, as well as the

creation of or improved adherence to computer and information security policies and procedures.

2 TRENDS IN COMPUTER AND INFORMATION SECURITY

The Australian Computer Crime and Security Survey (2006) indicated that more than more than 90 percent of all respondents used anti-spam filters, anti-virus software, firewalls and access control technologies, which is consistent with results over the past four years. The British Chambers of Commerce Crime Survey (2008) found that approximately four-fifths of their respondents use anti-virus software and 77 percent use anti-spam filters to help combat computer crime.

Network-based attacks have been somewhat limited by the introduction of default firewalls in popular operating systems such as Microsoft Windows XP, as well as an increasing awareness of computer security threats and practices among organisations and general Internet users. As a result, network-based attacks have declined by a small percentage (Symantec Internet security threat report, 2008).

The SIEM (Security Information and Event Management) market is one of the fastest growing security markets, with a growth rate of more than 30 percent in 2007 and estimated revenue reaching more than $800 million in 2007 (Kavanagh & Nicolette, 2008).

The Australian Computer Crime and Security Survey (2006) indicated that almost half their respondents still do not use or follow security standards. In 2005, research indicated that more than 1300 organisations have been certified under the ISO/IEC 17799 standard and many more were in the process, making the standard the most prominent standard for IS security management (Theoharidou et al., 2005).

The British Chambers of Commerce Crime Survey (2008) found that larger organisations, typically those with more than 50 staff and turnover of £1 million or more, appear to have greater resources to be able to deal with computer crime related incidents. A majority of these organisations had formal written security plans (British Chambers of Commerce, 2008).

The CSI 2007 Computer Crime and Security Survey found that most respondents spent between 3 to 5 percent of their IT budget on security and only 9 percent of respondents spent more than 10 percent (Richardson, 2007).

3 METHODOLOGY

3.1 Research Strategy

Quantitative research in the form of a survey instrument has been used to collect the data and descriptive statistics have been used to analyse and present the data. The decision to follow a quantitative research methodology was based on the fact that the results of the survey should be a representative sample of the total population. Moreover, the nature of the data required, as well as the fact that comparisons have been drawn from similar research, meant that following a qualitative research methodology would have been inappropriate and ineffective.

3.2 Research Questions

Due to the exploratory nature of the research, research questions were derived from the literature. These questions provided a basis for the research in order to investigate possible relationships or trends with the eventual intention of discovering new theories.

3.2.1 Questions

What is the level of understanding of South African organisations with regard to the origins of computer crime?

- To what extent have South African organisations implemented and utilised the necessary resources, policies and procedures to effectively prevent and mitigate computer crime?
- What corporate policies and procedures regarding the reporting of computer crime exist within South African organisations?
- What are the perceptions of South African organisations regarding law enforcement's ability to combat computer crime?
- How are South African organisations affected by computer crime?

3.3 Sample and Respondents

The primary target respondent was a working professional who was aware of the various computer crime and security issues within his/her organisation. Typically, these were senior managers, IT administrators, IS professionals, CIOs, as well as any IT security consultants.

Simple random sampling was the primary sampling method used when selecting the sample for this survey. The survey was distributed directly, through e-mail requests to specific organisations, as well as indirectly through a web based questionnaire linked to a well known South African IT news website.

Generally it was found that only people interested in this field of research responded to the survey. A total of 60 complete responses were collected, the majority (66%) of which came from organisations with more than a hundred employees. As similar techniques were used to collect data in the Australian and United State's surveys, this was seen as representative enough to compare the local survey to those surveys. The survey went live on May 31, 2008 and was closed on August 12, 2008.

4 RESULTS AND FINDINGS

4.1 Who We Asked

Survey respondents represent a broad range of industry sectors which include organisations from both the public and private sectors. Over 14 different industry sectors are represented. The industries with the greatest representation are the Information Technology sector (33 percent); the financial sector (18 percent); and the national or provincial government sector (15 percent). In terms of employee numbers and gross annual income/expenditure, most respondents that completed the survey belong to small to medium-sized organisations.

Respondents were grouped by job description. Twenty percent of respondents were senior executives with the titles chief executive officer (CEO) (10 percent), chief information officer (CIO) (8 percent), chief security officer (CSO) (2 percent) or chief information security officer (CISO) (5 percent). The single largest category of respondents (13 percent) had the job title of security officer. An additional 12 percent of

respondents had the title of systems administrator, 7 percent of respondents had the title of IT support, while 43 percent had various other titles

4.2 Readiness to Protect

This national survey cannot measure organisations' readiness to protect their IT systems merely based on responses to a few questions about the use of security technologies, policies and procedures, IT security standards and the level of training and education of personnel responsible for managing these systems. It does, however, seek to raise awareness about some of the essential elements which may contribute to an organisation's security posture and readiness to protect their systems.

4.3 Security technologies used

Respondents were asked to identify the types of security technology used by their organisations. Nearly all respondents reported the use of anti-virus software (98 percent), logins and passwords (97 percent), and firewalls (93 percent). The USA and Australian respondents matched the SA result of 98 percent for anti-virus software, yet exceeded reported usage of firewalls with 97 percent and 98 percent, respectively. In contrast, there was a significant difference in the usage of logins and passwords between SA and the two countries. Furthermore, Australian organisations place much more emphasis on access control (90 percent) compared to South Africa (57 percent). Other noticeable differences between the three countries include the reported usage vulnerability management technologies, as well as the fact that SA organisations reported the highest usage of biometrics.

4.4 Security evaluation

Although organisations are implementing various security technologies, it is important to note whether or not they are verifying that these security technologies are properly in place and effective on an ongoing basis. Fifty-three percent of SA respondents and 63 percent of USA respondents reported that their organisations perform security audits conducted by their internal staff, making security audits the most popular technique in the evaluation of the effectiveness of information security. The SA percentage for each technique is less than that of the USA, with the exception of e-mail monitoring software. The use of other techniques, such as automated

tools and Web activity monitoring software, are clearly also prevalent. Regarding security audits by external organisations and penetration testing by internal staff, the USA results exceeded the SA results by 20 percent and 26 percent, respectively.

4.5 Computer security policies and standards used

Among the four Readiness to Protect factors (technologies, policies, standards and training) the most significant in terms of lack of adherence, is the proportion of organisations that use or follow various IT security related standards. There was a considerable difference between the responses of SA and Australia. SA reported a 68 percent adherence or usage of IT security related standards, with 32 percent of respondents indicating the usage of ISO/IEC 17799 standard

4.6 Spending

Respondents were asked whether their organisation has increased expenditure on computer security in the last 12 months as a result of concerns about the adequacy of computer security within their organisation. Fifty-seven percent of SA organisations increased their IT security spending in the last 12 months for these reasons, compared to 50 percent of Australian organisations. However, this should not necessarily be interpreted as meaning that 43 percent of SA organisations were satisfied with their current IT security spending levels. Approximately 35 percent of SA respondents did not know what proportion of their organisational IT budget was allocated to IT security,

4.7 Outsourcing

Respondents were asked several questions pertaining to their IT security personnel, including the extent to which the computer security function of the organisation is outsourced. Fifty percent of SA organisations reported that their security function was not outsourced, as opposed to 61 percent of USA organisations.

4.8 Training and Awareness

Regarding training, qualifications and certifications of IT security personnel, respondents were questioned on each of these aspects. In the area of IT tertiary qualifications, SA reported 57 percent of their personnel had tertiary IT qualifications and 30 percent had no formal qualifications

but more than 5 years IT security experience. Australia reported significantly higher numbers regarding vendor IT certification and ad hoc IT security courses.

Training staff adequately in IT security is an important part of the security agenda. Respondents were asked what percentage of the total IT budget their organisations allocate to awareness training where most SA and Australian respondents indicated this was less than 1 percent. While 30 percent of SA organisations reported that their organisations do not use awareness training and a further 22 percent do not measure the effectiveness of awareness training, many reported the use of volume and type of incidents or of help desk issues as indicators. Thirty-two percent of USA organisations reported the use of mandatory written or digital tests.

4.9 Computer Crime, Attack and Abuse Trends

Respondents were asked whether they had experienced one or more electronic attacks in the last 12 months. Forty-five percent of SA organisations said “Yes”. Notably, the USA and SA responses were fairly similar, yet the Australian responses differed significantly. Respondents who indicated that they had experienced one or more electronic attacks in the last 12 months were then asked to report the approximate number of these electronic attacks. Most respondents for SA, the USA and Australia reported between 1 and 5 attacks within the last 12 months. Both SA and Australian respondents reported that more attacks came from the inside as opposed to the outside.

Respondents reported their opinions regarding suspected motives for electronic attacks that harmed the confidentiality, integrity or availability of network data or systems in the last 12 months. SA respondents reported foreign government political advantage (28 percent), illicit financial gain (25 percent) and indiscriminate random acts (22 percent) as the most common suspected motives. Australian respondents suspected that illicit financial gain (27 percent) was amongst the main motives, but reported personal grievance (31 personal) and other political interest (55 percent) as more common motives of electronic attacks.

Regarding the types of electronic attack, computer crime, or computer access misuse or abuse - SA, the USA and Australia responses were mostly similar. SA organisations were most able to detect computer

facilitated fraud (60 percent), whilst the USA and Australia mostly detected a degradation of network performance associated with heavy network scanning (59 percent and 62 percent respectively).

Respondents were also asked which of these types of electronic attacks, computer crime, or computer access misuse or abuse, caused their organisations financial loss in the past 12 months. Computer facilitated financial fraud was the main cause of financial loss for both SA (53 percent) and Australian (69 percent) organisations.

4.10 Cost

In order to approximate the cost of computer crime, respondents were asked to provide estimated Rand values that their organisations lost in total due to various types of electronic attack, computer crime, computer access misuse, or abuse within the last 12 months. Bearing in mind that these figures were rough guesses, losses estimated totalled R57.8 million. Of the total estimated loss, R50.1 million was due to unauthorised access to information by insiders. Theft of other computer hardware devices, telecommunications fraud, sabotage of data or networks, laptop theft, as well as DOS attacks, all had figures which exceed R1 million.

4.11 Reporting Behaviours and Attitudes

Beyond computer crime, attack and abuse trends, respondents were asked whether they shared information on these intrusions with law enforcement and legal counsel, who they reported these incidents to, and more generally, what, the outcome was when incidents were reported. Most SA (30 percent), USA (30 percent) and Australian (69 percent) organisations chose not to report one or more incidents to anyone outside their organisations, followed closely by reporting one or more incidents to a law enforcement agency. SA respondents also indicated the reporting of incidents to legal counsel for civil remedy (23 percent), as well as to their organisations' external auditor (17 percent).

When respondents were asked about the most important reasons why their organisation chose not to report computer crime, the results yielded a strong contrast of results between Australia and the other two countries. Most SA respondents reported that civil remedy seemed best (33 percent), or that they did not believe that law enforcement agencies were capable of apprehending the perpetrators (27 percent), or merely that the incident was

not serious enough to report (27 percent). Similarly, most Australian respondents (76 percent) did not believe that law enforcement agencies were capable of apprehending the perpetrators, yet 74 percent indicated that negative publicity was also an important reason.

In cases where the electronic attacks or other forms of computer crime were reported, SA (25 percent) and Australian (49 percent) respondents stated that the crime was investigated but the lack of evidence prevented charges being laid. Only 15 percent of SA respondents and 19 percent of Australian respondents reported that the investigations resulted in a charge/charges being laid.

5 CONCLUSION

As a developing country, the national economy will become increasingly reliant on IT infrastructure and e-commerce for critical activities. Future growth may be hindered by the constantly evolving threat of computer crime, and thus it imperative that South African organisations are made aware of and become more knowledgeable of the origins and consequences of computer security issues, in the hope that further investment will be made into computer and information security for improvement. Moreover, those responsible for computer and information security should be able to justify new investments in new technologies and awareness training, as well as be able to understand the economic, financial, and risk management aspects of computer security. *Risk intelligent* organisations must be able to identify changes, threats or vulnerabilities in the landscape as they become visible.

6 REFERENCES

Australian computer crime and security survey. (2006). Retrieved April 4, 2008, from http://www.auscert.org.au/images/ACCSS2006.pdf

British Chambers of Commerce. (2008). *The invisible crime: A business crime survey*. Retrieved April 14, 2008, from http://www.britishchambers.org.uk/67982192431433336 51/crime.html

Campbell, K., Gordon, L.A., Loeb, M.P. & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11(3), 431 – 446. Retrieved April 18, 2008, from SSRN database.

Householder, A., Houle, K. & Dougherty, C. (2002). Computer attack trends challenge Internet security. *Computer*, 35(4), 5-7. Retrieved April 10, 2008, from IEEE database.

Jones, B. R. (2007). Comment - virtual neighborhood watch: Open source software and community policing against cybercrime. *Journal of Criminal Law & Criminology*, 97(2), 601-629.

Kavanagh, K. M. & Nicolette, M. (2008). *Magic quadrant for security information and event management.* Gartner RAS Core Research Note G00156945.

Richardson, R. (2007). *CSI computer crime and security survey*. Retrieved March 29, 2008, from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Symantec Internet security threat report. (2007). Retrieved March 31, 2008, from http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

Taylor,M., Haggerty, J. & Gresty,D. (2007). The legal aspects of corporate computer forensic investigations. *Computer Law & Security Report*, 23(6), 562 – 566. Retrieved April 18, 2008, from ScienceDirect database.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, 24(6), 472-484. Retrieved March 29, 2008, from ScienceDirect database.