2007

Improving Information Security Management in Nonprofit Organisations with Action

Mark Carey-Smith
Queensland University of Technology

Karen Nelson
Queensland University of Technology

Lauren May
Queensland University of Technology

DOI: 10.4225/75/57b52bb243e30
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007.

Improving Information Security Management in Nonprofit Organisations with Action Research

Mark Carey-Smith
Karen Nelson
Lauren May
Queensland University of Technology
m.carey-smith@qut.edu.au
kj.nelson@qut.edu.au
l.may@qut.edu.au

Abstract

Information security is vital for protecting important assets of organisations, including the information resources and the organisation's reputation. In Australia, the nonprofit sector makes a significant contribution to society but is under represented in the information security literature.

This paper describes research in progress that is investigating and improving information security management in some nonprofit organisations (NPOs), which incorporates a participatory action research methodology. This approach will enhance the skill set likely to be present in Australian nonprofit organisations, producing a more sustainable solution, as well as contributing to the open literature. The Technology Acceptance Model will be utilised as a referent model to aid data analysis. This research will directly benefit the nonprofit sector by highlighting the importance and relevance of effective information security management in their organisations. It will inform the policy making process of government actors when devising policy to assist NPOs.

Keywords

Information security, information security management, action research, nonprofit organisations, technology acceptance model

INTRODUCTION

Information security is vital for protecting important assets of organisations, including the information resources and the organisation's reputation. Information security governance is an important aspect of information technology governance, which is a significant component of corporate governance (von Solms 2005). An information security management (ISM) system is an important pre-requisite in effectively managing information security processes and procedures in organisations. The importance of information security management systems is well recognised by the information security literature (for examples, see: Greene 2006; Kabay 2002; Pipkin 2000). The vast majority of the studies in this area, however, focus on ISM in large corporate or government enterprises. Most of this work involves empirical studies of implementing and managing an information security management system (ISMS) and/or an information security policy (examples include: Chang, A.J.-T. & Yeh 2006; Ericsson 2005; Fulford & Doherty 2003).

This research is concerned with improving the ISM practices of a significant component of Australian society, the nonprofit sector. The nonprofit sector makes major contributions in economic, societal and political facets of Australian life (Lyons, Mark 1999). Nonprofit organisations (NPOs) provide important support to the Australian community in the provision of services including community welfare, amateur sport, education, health, child care, religion, environmental protection, human rights and social justice. In recent years many nonprofit organisations have seen an increase in demand for services, largely due to reductions in, and outsourcing of, services by governments (Alessandrini 2002). Australian Bureau of Statistics figures for 1999-2000 (the first and last time such statistics were compiled by the ABS) show that nonprofit organisations utilised 6.8% of all employed people in Australia, contributing 4.7% or $29.7 billion to Gross Domestic Product (Australian Bureau of Statistics 2002). Nonprofit organisations also play an important role in strengthening democracy and in the creation of inclusive public policy (Maddison, Denniss & Hamilton 2004). Given the importance of nonprofit organisations for Australian society, the implications of an insecure (from an information security perspective) nonprofit sector are profound.

The ISM practices of nonprofit organisations have ramifications beyond the organisations themselves. Significant in contemporary information security is the issue of vast numbers of Internet-connected computers that can be attacked via vulnerabilities in popular operating system and application software. Computers running vulnerable software can be attacked and exploited by automated tools and combined into networks to form vast numbers of 'zombies', remotely controlled by attackers. These 'zombie armies' or 'botnets' can then be used to launch distributed denial of service attacks or send large amounts of spam as well as other nefarious activities that impact upon all Internet users, either directly or indirectly. Vinton Cerf recently warned attendees to the World Economic Forum that the issue of botnets could threaten the future viability of the Internet (Sturgeon 2007). Without effective ISM practices nonprofit organisations are likely to be part of the problem, rather than being part of the solution.

This paper sets out an approach for improving the information security management practices in nonprofit organisations. The research utilises action research as a methodology and the technology acceptance model as part of the theoretical framework underpinning the research project.

THE LITERATURE

Nonprofit organisations and small to medium enterprises (SMEs) have many similarities, the major one being the relative lack of resources of much of the nonprofit and SME sectors when compared with larger corporate and government organisations. This lack of resources manifests in the level of information technology maturity found in these organisations. Generally the budgets allocated to information technology are minimal and there is usually no dedicated information technology department or personnel in smaller organisations. For an overview of the challenges faced by nonprofit organisations making effective use of information technologies see Denison, Stillman and Johanson (2007).

The similarities of NPOs and small to medium enterprises are particularly important as the academic literature examining the information security practices and needs of nonprofit organisations is extremely scarce. Hence, while the focus of this research is on nonprofit organisations, the literature concerning the information security practices of SMEs provides imperative background material. Recent research has found significant problems with information security culture, information security awareness and/or use of information security policies in SMEs in Australia (Dojkovski, Lichtenstein & Warren 2006) the United States and Europe (Dimopoulos et al. 2004), Wales (Burns, Davies & Beynon Davies 2006) and the United Kingdom (Department of Trade and Industry 2006).

There are indications that the larger the size of the organisation the more likely the organisation is to establish an ISMS (Chang, S.E. & Ho 2006; Hong et al. 2006). From this work we can assume that the relatively small size of most of the nonprofit sector means that these types of organisations are less likely to have implemented an ISMS. Industry sector is also a determining factor in the implementation of an ISMS. Sectors such as banking place relatively high importance on ISM, with a high percentage of individual financial institutions implementing their own ISMS (Chang, S.E. & Ho 2006; Hong et al. 2006). The inference from this assertion supports anecdotal evidence suggesting a widespread lack of awareness of the importance of information security in the nonprofit sector.

A number of challenges face the nonprofit sector in Australia. The legal environment for nonprofit organisations in Australia is complex and confusing (Woodward & Marshall 2004). NPOs who engage in public advocacy critical of government face particular challenges such as the threat of the loss of taxation benefits and funding (Khadem 2006; Lyons, Miriam 2005). Human and financial resources are scarce. Many NPOs are under considerable financial and operational pressures (Australian Council of Social Service 2006) and are largely or completely reliant upon volunteers for their operation (Department of Communications Information Technology and the Arts 2005). Where resources are scarce, every dollar invested in information security can be perceived as a dollar not spent in direct support of the organisational mission. This tension in allocating budgets has been made worse in recent years due to the change in government funding from mostly ongoing to mostly contract-based and outcome-focused, leaving fewer available resources for operational costs (Fitzgerald 2004). All of these factors impact upon the resources available for ISM.

Reliance upon volunteers can also lead to situations where the management of information technology resources is left up to the most technology-savvy member of the organisation, rather than trained and skilled staff as is usually the case with government and larger business enterprises. Coupled with the lack of available financial resources to engage external information technology consultants the result may be that the most important information resources of the organisation are not being managed and protected in an appropriate way. This research will examine the validity of these suppositions.

Nonprofit organisations may be at heightened risk of 'insider threat'. Insider threat refers to threats presented by legitimate users of an information system who misuse their privileges (Theoharidou et al. 2005). Human error

also accounts for a significant source of information security threats and is often undervalued as such (Im & Baskerville 2005). Smaller nonprofits may be more susceptible to such risks because of their reliance upon volunteers meaning they are unable to employ stringent recruitment practices or provide training opportunities for staff.

Research into the philanthropic behaviour of Australians has found that trust in the beneficiary organisation is an important factor to donators, particularly for more affluent people (Department of Family and Community Services 2005). Becoming the victim of a high profile information security incident could cause considerable embarrassment to a nonprofit organisation and may reduce trust in the organisation for potential donors and members. A lack of trust may decrease the willingness of donors, both individual and institutional, to part with funds. In a highly competitive donor marketplace few NPOs could afford a large decrease in donor activity.

Examples of information security incidents within any organisation are usually kept confidential, but there are some in the public domain. An example is the Web site of the nonprofit organisation ReconciliAction Network which had been displaying a message since November 2006 stating that "Our website is currently offline, after an unfortunate incident with some nasty hackers." (ReconciliAction Network 2006). Personal correspondence indicated that the organisation did not have the resources to correct the problem until mid-2007. On December 1, 2005 two human rights organisations in Canada were sent email messages with Microsoft Word attachments containing previously unknown Trojan horse attacks (Lemos 2006). The attacks were intercepted by a company providing information security services and as such were unsuccessful. The attacks, however, are an example of the complex threat environment which now confronts many nonprofit organisations.

Defining Nonprofit Organisations

Nonprofit organisations are referred to by a variety of different, sometimes conflicting, terms. The group of NPOs in Australia can be collectively referred to by a number of terms, including the nonprofit sector, the voluntary sector, the third sector (as distinct from the government and business sectors) or civil society. This variety of terms can be explained by Lyons' contention that "people identify with and generalize about fields of activity far more easily than types of organization" (Lyons, Mark 1998).

In Australia the term 'nonprofit organisation' has not been defined in legislation. Over time a common law definition has been established and has been administratively adopted by the Australian Taxation Office (Sheppard, Fitzgerald & Gonski 2001). This definition is set out in *Tax basics for non-profit organisations* published by the Australian Taxation Office:

> The Tax Office accepts an organisation as non-profit where its constituent or governing documents prevent it from distributing profits or assets for the benefit of particular people – both while it is operating and when it winds up. ...A non-profit organisation can still make a profit, but this profit must be used to carry out its purposes and must not be distributed to owners, members or other private people (pp.1-2, Australian Taxation Office 2005).

The International Classification of Nonprofit Organizations (ICNPO) was developed by the John Hopkins Comparative Nonprofit Sector Project by Salamon and Anheier (1996). The definition of what constitutes a nonprofit organisation that will be adopted in this research is the ICNPO system. The attributes identified (organised, private, self-governing, non-profit-distributing and voluntary) are the most appropriate for this research. The ICNPO definition clarifies important distinctions between organisational types that are *prima facie* quite different. For example there are obvious differences between the information security needs and governance requirements of a credit union, a university and an environmental advocacy group, though all could be described in some circumstances as nonprofit organisations. According to the ICNPO definition however, only the environmental advocacy group would satisfy all the criteria.

The Action Research Methodology

This research project is designed around an action research methodology. Action research (AR) has a dual approach: "action in practice and knowledge generation through rigorous research." (p.160, Oosthuizen 2002). Susman and Evered (1978) add a third aim of AR, "to develop the self-help competencies of people facing problems." (p.588, 1978). This third aspect is more important in AR projects that have an emphasis on sustainability of the problem solution – the ability of the participants to continue to improve their situation without external 'expert' assistance. It is an important goal of this research.

AR involves the researcher becoming part of the research study and working with the research participants to enact change. Greenwood and Levin (2007) describe action research as consisting of three aspects which should be in balance: action – "[AR] aims to alter the initial situation of the group, organization, or community in the direction of a more self-managing, liberated and sustainable state" (p.6); research – "We believe that AR is one

of the most powerful ways to generate new research knowledge." (p.7); and participation – "…AR is a participatory process in which everyone involved takes some responsibility." (p.7).

AR is an appropriate method for information systems research as it "produces highly relevant research results, because it is grounded in practical action, aimed at solving an immediate problem situation while carefully informing theory" (p.1, Baskerville 1999). AR places emphasis on democratic processes in the framing and conduct of the research project (Greenwood & Levin 2007), making it appropriate for nonprofit organisations which often use democratic internal processes. One of the important attributes of nonprofit organisations that differentiates them from small businesses is their "bias toward informality, participation and consensus" (p.1, Allison & Kaye 2003).

AR is conducted in process cycles. A typical AR project involves a number of cycles of action and critical reflection and is highly flexible (Oosthuizen 2002). Using short, multiple cycles, with the accompanying opportunities for repeated critical reflection and repeated attempts to disprove the interpretations arrived at in earlier analyses should produce increased rigour in the research results (Dick 2000). Susman and Evered (1978) describe AR as a cyclical process consisting of five phases: diagnosing, action planning, action taking, evaluating, and specifying learning, as represented in Figure 1. The Susman and Evered model will be utilised in this research. The completion of each of the five phases offers an opportunity for critical reflection which will result in greater rigour than if less critical reflection was conducted.

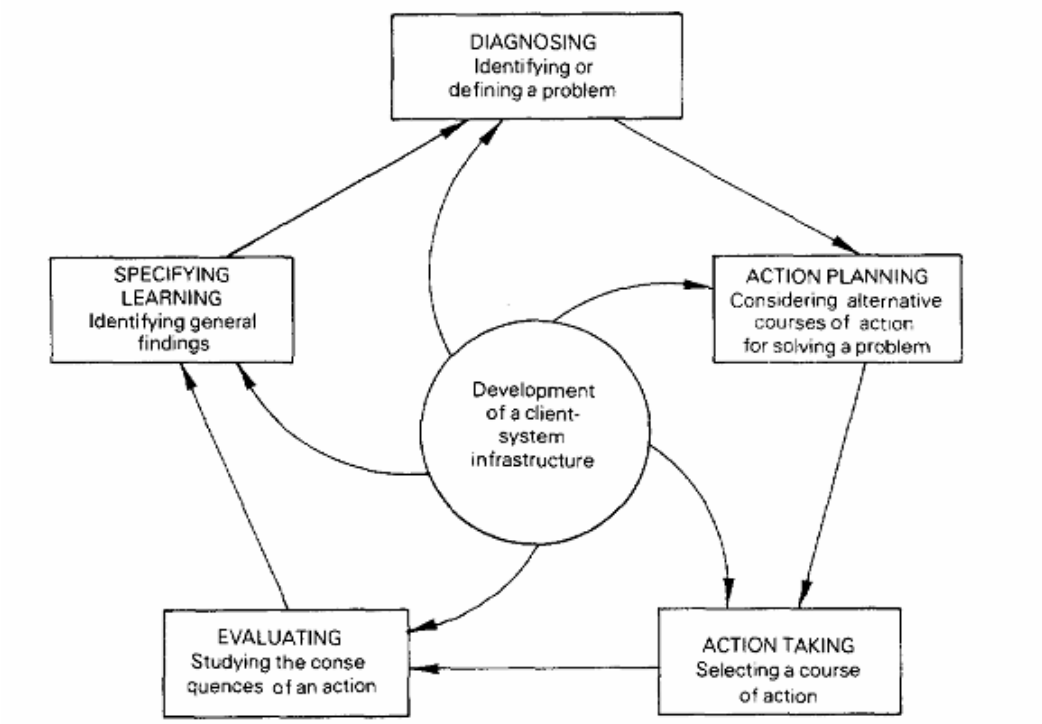

Figure 1: The cyclical nature of action research (p.588, Susman & Evered 1978)

The Technology Acceptance Model

To aid the evaluating and specifying learning phases of the AR cycle, the Technology Acceptance Model will be utilised as a referent model. The Technology Acceptance Model (TAM) was proposed by Davis (1989) as a model to explain why users accept or reject information technology.

TAM is based on the premise that two particular aspects of how users perceive a new information technology application will heavily influence their acceptance of it. The two aspects are the users' *perceived usefulness* and *perceived ease of use* of the new application. Perceived usefulness is defined by Davis as "the degree to which a person believes that using a particular system would enhance his or her job performance" (p.320, 1989). Perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free of effort" (p.320, Davis 1989). Perceived usefulness has a direct effect on users' behavioural intention to use the system, while perceived ease of use has indirect effects via its effect on perceived usefulness and users' attitudes. The intention to use then impacts upon actual use of the system, which is a measure of the success of the system. Davis also recognised that additional, external variables may have an impact on users' perceptions.

TAM has been applied in many studies in information systems research and has been found to be an accurate and robust model (Hsi-Peng Lu 2005). The vast majority of these studies have involved collection of data using quantitative methods, usually questionnaire-based surveys as employed by Davis in the original study (examples include: Adamson & Shine 2003; Brown et al. 2002; Hsi-Peng Lu 2005; James et al. 2006; Johnson 2005). However, some researchers of technology acceptance have found that qualitative methods of data collection are better suited to their research environments (examples include: Behrens et al. 2005; Benamati & Rajkumar 2002; Johnson 2005). Qualitative data gathering methods will be deployed in this research as these methods are seen as the most appropriate for understanding the complex and interactive factors affecting the information security management practices that occur in organisations.

In this research TAM will be used as a referent model to analyse the data collected during the AR interventions in the participant organisations. The insights gained will result in a greater understanding of critical success factors and will enrich the ongoing development of the theoretical framework that underpins the research project.

Some researchers have extended TAM to include additional factors that influence behaviour in the form of external variables. For example, Johnson (p.116, 2005) defines a number of external variables that may influence investment in information security. The external variables which are expected to impact upon users' perceptions of an ISMS are likely to be different aspects of users' perceptions and experiences with information security. This will be brought to light in the conduct of semi-structured interviews with the members of the participant organisations as well as via ongoing participant observation and analysis of relevant paperwork such as information security policy documents and meeting minutes.

IMPLEMENTING AN INFORMATION SECURITY MANAGEMENT SYSTEM USING AR

The AR project being conducted in this study is the implementation of information security management systems in a number of nonprofit organisations. This constitutes a change process to be implemented in a number of organisations to address identified problems with the ISM practices in the organisation.

There will be two or three interventions conducted in this AR project. The first of these is currently underway in its initial stages. Each intervention will be conducted at a different nonprofit organisation and will consist of a series of AR cycle iterations (sometimes referred to as AR spirals). It is likely that the first intervention will consist of two or three iterations, with the final phase of specifying learning in the final iteration providing input to the diagnosing phase of the next intervention. In this manner the lessons learned from the first intervention will be used to revise and 'sharpen' the model that will emerge during the AR project. The model will then be deployed in the next intervention and will undergo further revision and improvement based upon the knowledge that emerges from subsequent AR cycles.

A Hybrid Model Based on AS/NZS ISO/IEC 17799

ISM standards are important documents that aid the development and maintenance of ISM practices in organisations (von Solms 2005). The AS/NZS ISO/IEC 17799:2006 standard (hereafter referred to as 17799) is a commonly deployed example (Standards Australia/Standards New Zealand 2006). Considerable information security knowledge is needed to carry out the activities identified in many of the steps in 17799. It is very unlikely that the skills and knowledge needed would be present in many nonprofit organisations (NPOs) except for the larger, better resourced organisations. The question that arises from this assumption is where are these skills going to come from if there are insufficient funds to pay for them? Or is there a less demanding method for NPOs to 'do it themselves'? This research will design and implement a hybrid model for implementing an ISMS utilising an AR methodology, making use of a skill set more likely to be present in NPOs.

Benefits

The use of an AR methodology in a number of NPOs will be of benefit in the following ways. Firstly, the multiple AR iterations in each intervention and the multiple AR interventions will result in greater rigour and 'transferability'. Transferability, in Lincoln and Guba's terminology (1985), refers to the extent to which the knowledge generated in a study can be applied elsewhere. This quality is particularly important in research projects such as this where one of the goals is the generation of useful knowledge for the practitioner community (in this case, information security professionals implementing ISMS). As this project involves transfer of knowledge gained from one site (the first NPO) to at least one other site, transferability will be a vital part of the project design.

Secondly, the AR methodology will be participatory by design. This will ensure two important aspects of the project are realised: participant engagement and participant education. The research participants will be engaged to a significant extent, which should contribute to the success of the project through participants' commitment (sometimes referred to as buy-in). The participants will be educated via the experiential learning that will take place through their participation in the entire process. This will result in participants gaining a greater awareness of the importance of information security and practical skills that contribute to the sustainability of the solution. There is little to be gained if the solution falls apart after a period of time due to the inability of the organisation to manage their own information security needs.

In a broader sense, this research will be of benefit in the following ways:

- It will directly benefit the NPO sector by highlighting the importance of ISM and by providing guidelines which are practical and appropriate.
- It will make a contribution to both the open literature and the professional practice of information security practitioners by helping improve upon the existing dearth of information on practical implementations of information security in NPOs.
- It will inform the policy making process of government actors when devising policy to assist NPOs.

Methodology Summary

During the AR interventions, data will be collected via participant observation, semi-structured interviews with participants, seeking feedback from participants on ongoing findings and through paperwork generated during the intervention and already existing prior to the intervention, such as existing information security policy documents. This triangulation of different data sources will contribute to the rigour of the research (Dick 1999). The purpose of the data collection is to build up the richness of the theoretical framework that informs and supports the research and to gain as thorough an understanding as possible of how the information security management practices of nonprofit organisations can be improved.

The Technology Acceptance Model will be utilised to aid in the analysis of the data with particular reference to NPO staff members' attitudes towards and perceptions of information security. It is likely that there will emerge a number of external attributes that contribute to the perceptions of information security held by NPO staff members. From informal discussions the researcher has held with members of the NPO sector common themes have emerged. These include the tension between allocating budgets for operational and mission-critical areas, perceived inconvenience of the effects of information security technologies and lack of awareness of the importance of information security in general, let alone the need for ISM. These themes will be explored further through the methods discussed above.

Preliminary Findings

To date a number of semi-structured interviews have been conducted with staff members (paid and volunteer staff) from a variety of nonprofit organisations to gather their experiences and perceptions of information security. A number of themes have emerged from these interviews.

One consistent topic is the lack of planning and coordination of information security practices in NPOs. Information security solutions are implemented in an ad-hoc fashion and not based on an information security risk assessment. This problem appears to be present in organisations largely reliant upon volunteers as well as better-funded organisations with paid information technology staff. It also appears to exist across the nonprofit sector to include service-type organisations such as those providing health-related services, as well as advocacy-type organisations such as human rights and environmental organisations.

Another topic is the lack of awareness present in NPOs of the importance of information security. One person with approximately twenty years of experience working in the nonprofit sector with approximately thirty different organisations stated: "I could probably list on one hand the number of conversations I've been on on this topic [information security] at team meetings, staff meetings and board meetings of NGOs in twenty years." Part of the reason for this lack of awareness may be the tension that exists in many NPOs between fulfilling the mission of the organisation and expending resources on supporting infrastructure such as information technology in general and information security in particular. When organisations are financially stretched they are forced to prioritise their efforts on core issues and information security does not appear to be one of them. Another factor that may be particularly effective in organisations that are largely volunteer-based are the reasons for people volunteering in the first place; they are there for reasons that are meaningful for them, not because they get paid. In the words of one NPO staff member: "This is the type of organisation that attracts people who have a crystal in their pocket and like to sit around and hold hands."

In addition to the preliminary data findings, there have been some lessons learnt in the work conducted thus far in the first intervention. To date the development of the client-system infrastructure (negotiation of project parameters etc.) and the first phase (problem diagnosis) have been completed. These activities have generated insights into the frustrations that can occur in conducting research with nonprofit organisations from within a framework of a university. The NPO where the first intervention is taking place is largely volunteer-based and consists of a relatively informal and decentralised management structure. This can lead to delays in decision-making as the individuals that constitute a decision-making body may have difficulty attending meetings due to other commitments. When the principal researcher was unsuccessfully attempting to get a decision-making process expedited one of the organisation members provided him with some useful advice: "…it will take as long as it takes. Understandably you might require it sooner but things take as long as they take - it really depends on when decision makers are meeting." This incident shows it is important to align the expectations of the researcher with the realities of the participant organisation. As the old saying goes, patience is a virtue.

CONCLUSION

Effective ISM is critical in ensuring important assets of organisations, such as information and reputation, receive appropriate protection. In Australia, the nonprofit sector makes a significant contribution to society but is under represented in the information security literature. This paper has set out a plan of action to investigate how ISM practices of a small number of NPOs can be improved by a combination of an existing ISM standard, ISO/IEC 17799, a participatory methodology in action research, and a theoretical framework for the study that includes the Technology Acceptance Model. A small number of AR interventions will be carried out in NPOs, producing a refined model of an ISMS that is more appropriate for nonprofit organisations.

REFERENCES

Adamson, I. & Shine, J. (2003) Extending the New Technology Acceptance Model to Measure the End User Information Systems Satisfaction in a Mandatory Environment: A Bank's Treasury, *Technology Analysis & Strategic Management*, vol. 15, no. 4, pp. 441 - 455.

Alessandrini, M. (2002) A fourth sector: The impact of neo-liberalism on non-profit organisations, paper presented to Australasian Political Studies Association Jubilee Conference, Canberra, Australia, 2-4 October, 2002.

Allison, M. & Kaye, J. (2003) *Reference Article: Characteristics of Nonprofit Organizations -- Implications for Consultation*, viewed February 1 2007, URL http://www.nten.org/uploads/transferpodolsky02.pdf

Australian Bureau of Statistics (2002) *Non-Profit Institutions Satellite Account*, Australian Bureau of Statistics.

Australian Council of Social Service (2006) *Australian Community Sector Survey 2006*, Australian Council of Social Service.

Australian Taxation Office (2005) *Tax basics for non-profit organisations*, NAT 7966-06.2005, Australian Taxation Office.

Baskerville, R.L. (1999) Investigating information systems with action research, *Communications of the Association for Information Systems*, vol. 2, no. 3, pp. 1-5.

Behrens, S., Jamieson, K., Jones, D. & Cranston, M. (2005) Predicting System Success using the Technology Acceptance Model: A Case Study, paper presented to 16th Australasian Conference on Information SystemsPredicting Success using TAM, Sydney, Australia.

Benamati, J. & Rajkumar, T.M. (2002) The application development outsourcing decision: An application of the technology acceptance model, *The Journal of Computer Information Systems*, vol. 42, no. 4, pp. 35-43.

Brown, S.A., Massey, A.P., Montoya-Weiss, M.M. & Burkman, J.R. (2002) Do I really have to? User acceptance of mandated technology, *European Journal of Information Systems*, vol. 11, no. 4, pp. 283-295.

Burns, A., Davies, A. & Beynon Davies, P. (2006) A study of the uptake of Information Security Policies by small and medium sized businesses in Wales, paper presented to Global Conference on Emergent Business Phenomena in the Digital Economy, Tampere, Finland, November 28th - December 2nd, 2006.

Chang, A.J.-T. & Yeh, Q.-J. (2006) On security preparations against possible IS threats across industries, *Information Management & Computer Security*, vol. 14, no. 4, pp. 343-60.

Chang, S.E. & Ho, C.B. (2006) Organizational factors to the effectiveness of implementing information security management, *Industrial Management & Data Systems*, vol. 106, no. 3, pp. 345-61.

Davis, F.D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, vol. 13, no. 3, pp. 318-40.

Denison, T., Stillman, L. & Johanson, G. (2007) The Australian Non-profit Sector and the Challenge of ICT, *First Monday*, vol. 12, no. 5.

Department of Communications Information Technology and the Arts (2005) *Information and Communications Technology Transforming the Nonprofit Sector*, Department of Communications Information Technology and the Arts.

Department of Family and Community Services (2005) *Giving Australia: Research on Philanthropy in Australia*, Department of Family and Community Services.

Department of Trade and Industry (2006) *Information Security Breaches Survey 2006*, Department of Trade and Industry (United Kingdom).

Dick, B. (1999) Sources of rigour in action research: addressing the issues of trustworthiness and credibility, paper presented to Association for Qualitative Research Conference "Issues of rigour in qualitative research", Melbourne, Australia, July 6-10, 1999.

Dick, B. (2000) *Beginners' Guide to action research*, viewed February 18 2007, URL http://www.scu.edu.au/schools/gcm/ar/arp/guide.html.

Dimopoulos, V., Furnell, S.M., Jennex, M. & Kritharas, I. (2004) Approaches to IT Security in Small and Medium Enterprises, paper presented to 2nd Australian Information Security Management Conference, Perth, Australia.

Dojkovski, S., Lichtenstein, S. & Warren, M.J. (2006) Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises, paper presented to 5th European Conference on Information Warfare and Security, Helsinki, Finland, 1-2 June, 2006.

Ericsson, G.N. (2005) Management of information security for an electric power Utility-on security domains and use of ISO/IEC17799 standard, *Power Delivery, IEEE Transactions on*, vol. 20, no. 2, pp. 683-690.

Fitzgerald, R. (2004) *Not for Profit, Not for Volunteers*, Australian Broadcasting Corporation, June 27, 2004, Radio Programme, URL http://www.abc.net.au/rn/talks/bbing/stories/s1143837.htm.

Fulford, H. & Doherty, N.F. (2003) The application of information security policies in large UK-based organizations: an exploratory investigation, *Information Management & Computer Security*, vol. 11, no. 3, pp.106-114.

Greene, S.S. (2006) *Security Policies and Procedures: Principles and Practises*, 1st edn, Pearson Prentice Hall, New Jersey.

Greenwood, D. & Levin, M. (2007) *Introduction to Action Research: Social Research for Social Change*, 2nd edn, Sage Publications, Inc., Thousand Oaks, California.

Hong, K.-S., Chi, Y.-P., Chao, L.R. & Tang, J.-H. (2006) An empirical study of information security policy on information security elevation in Taiwan, *Information Management & Computer Security*, vol. 14, no. 2, pp. 104-15.

Hsi-Peng Lu, C.-L.H.H.-Y.H. (2005) An empirical study of the effect of perceived risk upon intention to use online applications, *Information Management & Computer Security*, vol. 13, no. 2, pp. 106-120

Im, G.P. & Baskerville, R.L. (2005) A longitudinal study of information system threat categories: the enduring problem of human error, *SIGMIS Database*, vol. 36, no. 4, pp. 68-79.

James, T., Pirim, T., Boswell, K., Reithel, B. & Barkhi, R. (2006) Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model, *Journal of Organizational and End User Computing*, vol. 18, no. 3, pp. 1-24.

Johnson, A. (2005) The Technology Acceptance Model and the Decision to Invest in Information Security, paper presented to The 2005 Southern Association of Information Systems Conference.

Kabay, M.E. (2002) Security Policy Guidelines, in S. Bosworth & M.E. Kabay (eds), *Computer Security Handbook*, 4th edn, John Wiley & Sons, New York, pp. 28.1-28.12.

Khadem, N. (2006) *Bid to strip green groups' tax status*, The Age, viewed January 8 2007, URL http://www.theage.com.au/news/national/bid-to-strip-green-groups-tax-status/2006/08/08/1154802891527.html.

Lemos, R. (2006) *Targeted Trojan attacks on the rise*, viewed February 16 2007, URL http://www.securityfocus.com/news/11418.

Lincoln, Y. & Guba, E. (1985) *Naturalistic Inquiry*, Sage Publications, Beverly Hills, California.

Lyons, Mark. (1998) *Defining the Nonprofit Sector: Australia*, The John Hopkins Institute for Policy Studies.

Lyons, Mark. (1999) Australia's non-profit sector, in W. McLennan (ed.), *1999 Year Book of Australia*, Australian Bureau of Statistics, pp. 546-52.

Lyons, Mirriam. (2005) *Taxing times for outspoken charities*, New Matilda, viewed May 18 2007, URL http://www.newmatilda.com/home/articledetail.asp?ArticleID=737.

Maddison, S., Denniss, R. & Hamilton, C. (2004) *Silencing Dissent: Non-government organisations and Australian democracy*, Discussion Paper Number 65, The Australia Institute.

Oosthuizen, M.J.H. (2002) Action Research, in K. Williamson (ed.), *Research methods for students, academics and professionals: information management and systems*, 2nd edn, Centre for Information Studies, Charles Sturt University, Wagga Wagga, pp. 159-75.

Pipkin, D. (2000) *Information Security - Protecting the Global Enterprise*, 1st edn, Prentice Hall PTR, New Jersey.

ReconciliAction Network (2006) *ReconciliAction Youth Network*, viewed May 23 2007, URL http://www.reconciliaction.org.au/.

Salamon, L.M. & Anheier, H.K. (1996) *The International Classification of Nonprofit Organizations - ICNPO. Revision 1.0*, The John Hopkins Institute for Policy Studies, Baltimore.

Sheppard, I., Fitzgerald, R. & Gonski, D. (2001) *The Report of the Inquiry into the Definition of Charities and Related Organisations*, Charities Definition Inquiry.

Standards Australia/Standards New Zealand (2006), *AS/NZS ISO/IEC 17799:2006 Information technology—Security techniques—Code of practice for information security management*, Standards Australia/Standards New Zealand.

Sturgeon, W. (2007) *Botnets could eat the Internet*, Zdnet Australia, viewed February 21 2007, URL http://www.zdnet.com.au/news/security/soa/_Botnets_could_eat_the_Internet_/0,130061744,339273256,00.htm .

Susman, G.I. & Evered, R.D. (1978) An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly*, vol. 23, no. 4, pp. 582-603.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005) The insider threat to information systems and the effectiveness of ISO17799, *Computers & Security*, vol. 24, no. 6, pp. 472-84.

von Solms, B. (2005) Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, vol. 24, no. 2, pp. 99-104.

Woodward, S. & Marshall, S. (2004) *A Better Framework: reforming not-for-profit regulation*, The Centre for Corporate Law and Securities Regulation, Faculty of Law, The University of Melbourne.

COPYRIGHT