December 2005

Key Factors in E-Government Information System Security

Rodger Jamieson
Director of SEAR - Security E-Bussiness Assurance Research Group, School of Information Systems, University of New South Wales

Stephen Smith
Office of Information and Communicattion Technology, Department of Commerce

18th Bled eConference

eIntegration in Action

Bled, Slovenia, June 6 - 8, 2005

Key Factors in E-Government Information System Security

Stephen Smith

Office of Information and Communication Technology, Department of Commerce, Australia
stephen.smith@commerce.nsw.gov.au

Rodger Jamieson

Director of SEAR - Security E-Business Assurance Research Group, School of Information Systems, University of New South Wales, Australia
r.jamieson@unsw.edu.au

Abstract

This paper investigates the key drivers and key inhibitors from an Information System (IS) Security and Business Continuity Management (BCM) perspective. The research was conducted using a forum with personnel from nine government agencies with follow-up interviews with personnel from a further sixteen agencies. The study identifies key issues across a broad cross-section of government organisations. These key issues include awareness and active management support, training and appropriate funding. The issues identified are useful to management when implementing IS Security and undertaking Business Continuity Planning over e-government within agencies.

1. Introduction

Prior to e-Government, records and information were mainly stored on paper in files, filing cabinets, and vaults. Paper documents have a degree of separation between the client and the flow, storage and retrieval of documents. Manual records management systems and processes, established procedures to process and transfer documents through the system. These documents could be tracked transparently through the organisation. Hence, if tampered with, the changes would be clearly evident. These paper documents were subject to a level of security considered to be acceptable at that time. The security measures required to protect them focused mainly on the physical protection of the document and restricting permissions for people to access the records. While these

documents could be copied, the paper type, the colour and the size would be difficult to match with or replace the original. Also, copying documents is traditionally a relatively slow process.

Security threats and protective measures for these paper based systems were identified and resolved. They were written into polices and procedures, and updated over many years. This provided a degree of security for documents completely different to that of Intranet or Internet based systems which have the capability to immediately download information, giving the client (end user) the ability to copy and re-transmit this information in nanoseconds. This vulnerability exists for any organisation, whether private or public, that has a web presence (Straub et al., 1998: Backhouse et al., 2001).

Information system security has previously concentrated on confidentiality of documents stored electronically (Spinellis et al., 1999). In terms of the public perception of government organisations, security means the protection of records and data that are held for the purpose of recording, administering and monitoring the actions and policies of government agencies. This applies equally to paper documents and the data held on computer databases (Kiel, 2003). The rapid growth in the volume of information stored electronically and the uptake of e-commerce within government has heightened the need for increased security to protect the privacy of this information and prevent fraudulent activities (Bradford, 1999).

Electronic information is extremely portable and also very easy to modify. The administration, business and legal processes associated with security and protection of electronic government information have not been fully developed (Scott, 2003; Kraemer et al., 2000; Teo et al., 2003). Consequently government projects are endeavouring to develop policies and procedures to improve security (Frank, 2003). From the public's perspective, government is seen as one entity; hence a security problem within one agency may be viewed as a failure of the whole of government process. Therefore the process of maintaining and improving information security across all government agencies is viewed as an essential project. The research discussed in this paper forms part of a longitudinal action research study to help inform and improve information security across government. This paper reports on an initial research study, which involved a forum for and follow-up interviews of key agencies to determine the key drivers and inhibitors for information system security and business continuity planning (BCP) within and across government.

The ISO Standard AS/NZS ISO/IEC 17799:2001 Information technology — Code of practice for information security management contains twelve major sections which deal with information security issues. One section, Section 11, deals with Business Continuity Management (as a component of the information security issue 'availability' of information). As the agencies are required to achieve compliance with this standard, the forum questions were grouped around the eleven Information Security and one Business Continuity Management which incorporates Business Continuity Planning (BCP) sections of the standard. [It should be noted that Business Continuity Management (BCM) incorporates Business Continuity Planning, and BCP in an information technology environment is also often referred to as Disaster Recovery Planning (DRP)].

The focus of AS/NZS ISO/IEC 17799:2001 is to protect security of information by providing a set of recommendations (in effect controls and best practices) for situations that are applicable for E-commerce and also E-government. With the increasing volume of business being conducted between organisations over electronic networks it is essential that a trusted relationship be established between the stakeholders trading together. One such scheme is for all parties to agree on an appropriate standard and adopt it, adhere to its principles and move to accreditation [The standard in this case is AS/NZS7799.2.2003].

A number of frameworks have been developed and tested since the 1970s to quantify and manage the issue of information system security. Australia's standard for Information Security Management (AS/NZS7799: 2000) and the second part Information security management Part 2: Specification for information security management systems (AS/NZS7799.2.2003), provide a framework and set of recommendations in a risk management context.

The second part of the Australian Standard, AS/NZS7799.2.2003, is an adoption of the British standard BS 7799.2:2002 Information security management systems, Part 2: Specification with guidance for use.

The first part, AS/NZS7799: 2000, has been revised for application to e-Commerce, and was re-branded from its original publication as AS/NZS 4444: 1996. The current standard (first part) for Information System Management is Information technology— Code of practice for information security management - AS/NZS ISO/IEC 17799:2001 with an amendment in 2004, redesignated from AS/NZS7799: 2000 The latest version is acknowledged as a generic guide for the establishment and implementation of a process such as information system security management and information system risk management.

Certification is possible for '7799' and is recognised internationally (under ISO 17799). There are, however, very few organisations that can offer this service, currently only two within Australia. The adoption of standards is becoming increasingly important to establish benchmarks and assurance for organisations and clients that conduct business on-line. An additional benefit of certification to this standard is its regular (6 monthly) audit reviews which ensure certification to the standard is maintained, thus providing extra rigor and assurance regarding security compliance.

From a global perspective, all Government priorities are generally to fulfil the following objectives:

- Improving service delivery - to tangibly improve service delivery and satisfy the highest service priorities of people, businesses, communities and employees by redirecting resources to priority services.
- Getting value for money from the public purse - Government expects agencies to operate within their budgets, rigorously pursue efficiencies, streamline regulatory systems and cut "red tape".
- Aligning supporting government agendas - Government wants to ensure that public sector planning, investment and management strategies align with its goals and that agencies work together to achieve the Government's priorities (OICT, 2004).

These objectives are used to drive the delivery of several services through different delivery channels and are made available to ensure that they function for people, businesses, communities and employees. Agencies and clusters take a systematic approach to obtaining regular feedback from users to be better informed about people's needs and expectations. Regularly refreshing this knowledge and using it in tandem with other research is a prerequisite for identifying Information and Communication Technology (ICT) based service delivery solutions.

1.1 Definitions of IS Security and BCP

IS Security (ISS) is effective implementation of policies to ensure the confidentiality, availability and integrity of information and assets is protected from theft, tampering, manipulation or corruption. BCP (which is incorporated in BCM) is planning to mitigate

the adverse effects of an unexpected catastrophe, which may result in the loss of services, operations or information for a period of time. Some explanation of these terms is provided below.

"Information systems security is the protection of information systems against unauthorized access to or modification of information whether in storage, processing, or transit, and against denial of service to authorized users, including those measures necessary to detect, document, and counter such threats" (NSTISSC, 1999, p4).

Business Continuity Management (BCM) is defined as a "holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, band and value creating activities (Business Continuity Institute & BSI Standard PAS 56)" (Worthington, 2005).

The term Business Continuity Planning (BCP) is defined by Gartner as:

- "Planning for the continuation of business operations in the event of a disaster
- Ensure that critical business activities are maintained or restored as quickly as possible
- Focused on a prioritized resumption of the most critical business functions" (Gartner, 2002 p9)

IS Security has previously concentrated on confidentiality of information stored electronically. The rapid growth in the volume of such information and the uptake of e-Commerce within organisations has heightened the need for increased security to protect the privacy of this information and prevent fraudulent activities (Spinellis, 1999).

The objective of information security is to preserve an organisation's information assets and the business processes they support in the context of (Bell, 2001):

- Confidentiality - ensuring that information is only available to the people and systems authorised to receive it. Information may be confidential for many reasons including privacy, commercial or political;
- Integrity - ensuring that information is only changed by people and systems authorised to make changes to it; and
- Availability - ensuring that information and information processing systems are available when information is required (Evans, 2003).

These objectives originate from and are consistent with OECD publications dating back to the early 1990's and also the subsequent (and current) ISO/IEC, BS, Australian information and other international security standards, guidelines and handbooks.

At any time an organisation can experience a disruption to its business operations beyond its control. It may be a major incident with lasting effects such as a flood or fire or may be shorter in duration due to an event such as a power failure or denial of access to critical offices or systems.

An organisation can limit the impact of such events through contingency planning including the development of a BCP. A BCP is a critical component of IT security in general and information security management systems (ISMS) in particular.

A BCP includes the process of planning to create a state of readiness which will provide an immediate response to a disaster affecting a business unit or the IT environment of an agency. A Disaster Recovery Plan (DRP) consists of documented procedures for the

management and recovery of the critical IT services of an agency should an unscheduled disruption occur. It allows for orderly and timely recovery of the IT processing capabilities. For the purposes of this paper, BCP encompasses DRP and both are components of BCM.

Increasing complexity and dependency on IT by government agencies, the prevalence of computer hackers, terrorist threats and the introduction of legislation relating to protection of Government records has raised the importance of IT Security and Information System Security Management for the Government and its agencies. Although the AS/NZS ISO/IEC 17799:2001 standard primarily refers to information and systems security (ISS) it includes BCM and the related BCP as an important section. This means that adequate BCM and BCP provisions must be in place to enable the agencies to recover from any type of disaster that affects continuity of core government business.

2. Research Methods

A forum was conducted on the 4th April 2003 at the Office of Information Technology, to determine the key drivers and key inhibitors to Information System Security and Business Continuity Management (incorporating BCM and BCP). At the end of the forum, a disaster scenario formed the basis of a roundtable discussion. Eleven representatives from nine government agencies, with both technical and management backgrounds, attended the forum. The agencies ranged in size from small agencies (< 350 staff for example Arts and Ports), through medium sized agencies (350-1000 staff, such as Agriculture and Justice), to large agencies (over 1000 staff members, for example Commerce and Health). These agencies included health, justice, education, Of these agencies, one had achieved certification to the AS/NZS ISO/IEC 17799:2001 standard, one had not yet started their certification process and the others were in the process of achieving certification.

The process whereby the research forum involved a focus group is one the most common methods of qualitative research (Blaikie, 2000; Ross, 2004). A Delphi rating technique was also used to rank and rate issues raised in the forum. Schmidt et al. (2001) used this technique during their research to identify software project risks. It was determined to be a useful way to rank issues that were identified during a brainstorming session. Forum attendees consisted of nine IS Security Managers who were involved in a series of question-focused, scenario-based activities guided by a facilitator. The advantage of this group discussion forum method is that it enabled participates to firstly brainstorm ideas, and then discuss the ideas prior to rating and ranking the issues disclosed. The forum created an atmosphere that allowed for open interaction and stimulating discussion, and provided a flexible environment in which to discover the perceptions and experiences of the individual participants. The forum also uncovered concepts and generated new ideas on the topics being discussed.

The original drivers and inhibitors were taken from suggestions by each participant. Each participant was asked to prepare at least one driver and one inhibitor for both ISS and BCP. In an exchange of ideas around the table each participant proposed ideas which were documented on a whiteboard and the process was repeated until all participants' ideas had been documented. The completed list was discussed, duplicates eliminated, then ranked and rated, and the process and was then repeated for inhibitors and again for BCP.

The focus of the forum and follow-up interviews was to determine the key drivers and key inhibitors of IS Security and BCM (incorporating BCP) from a whole of government perspective. This research project is essential for government as it highlights a range of difficulties faced by agencies when charged with the responsibility to improve/implement

their ISS and BCP processes. The forum identified and allowed the discussion of initiatives developed within the individual agencies that should be of benefit across government and improve information security.

The research questions addressed by this study include:

1. What do you see as the key drivers for successful IS Security for your agency?
2. What do you see as the key inhibitors to successful IS Security for your agency?
3. What do you see as the key drivers for BCP to work in your agency?
4. What do you see as the key inhibitors to successful BCP for your agency?

The issues raised in the forum were scaled by their rank and ratings:

- Rank – ranking order of preference (1,2,3…n). This task required the participant to order the issues from the most important (numbered '1') to the lease important issue in the sequence. The analysis involved sorting the ranking issued from the most to least important.
- Rating – involved estimating the magnitude of importance of each issue. This task required the participant to estimate the degree of importance of the individual issue. The scale used was a Likert Scale ranging from '7' being the most important to '1' being very unimportant. The analysis involved averaging the ratings across all the participants the sorting them in reverse order from the most to least important, thus the issue with an average closest to '7' was then rated the most important issue.

The follow-up interview questions were based on the outcomes of the forum and the agencies were selected from all agencies within government and stratified into one of three groups:

- Agencies with established policies, procedures and practices sufficient enough to achieve certification to AS/NZS ISO/IEC 17799:2001 within the next few months.
- Agencies with developing policies, procedures but are not prepared enough for certification within the next 12 months.
- Agencies who made limited progress towards certification and would be unlikely to achieve certification.

An additional 16 agencies were interviewed using the questions developed from the forum. The results from these questions will be discussed in the following sections.

3. Information System Security

3.1 Key Drivers for Successful IS Security

The first focus question discussed at the forum related to identifying key drivers for IS Security. The participants identified the key drivers, which are set out in Table 1. These are the major factors which should contribute to successful IS Security processes within government agencies (Baird et al, 2002).

Table 1 shows the average rankings of these key drivers and the average importance ratings given by the participants to each driver.

Table 1: Key Drivers For Successful IS Security

Key Drivers For Successful IS Security	Average Rank[1]	Ranked Importance Rating[2]	Average Rating[3]
Active support of senior management	1	1	6.6
Commitment of funding	2	2	6.2
Protection of information assets	3	3	6.1
Statutory / legislative requirements	4	7	5.6
Staff awareness & training	5	5	5.7
Maintain integrity of electronic records	6	4	5.7
Negative experience(s) can drive change	7	11	5.0
Compliance with standards e.g. AS/NZS ISO/IEC 17799:2001	8	8	5.3

The issues transcribed from the forum are an accurate summary of the discussion that took place. All issues were rated above 4.3 (> moderately important) indicating that all of these issues are worth considering by management as factors that drive successful ISS processes within e-government. In order to differentiate between issues, ranking was carried out which revealed the three major issues (refer to Table 1) that are key to successful IS Security processes. These are:

- the active support of management
- sufficient funding
- staff awareness and training.

Comments from the participants emphasise these issues. The important elements of the comments raised in the forum on the need for Senior Management Support include:

> *"... supported by senior management ... the resources are given to you and it's an achievable outcome ..."* (Participant 10)

The 'active support of management' was ranked the most important issue and rated number 1 in priority. The need for Management support is essential and necessary as it is senior management that is ultimately accountable and charged with the task of initiating and supporting important projects with adequate funding and resources. The ranking of this issue so highly in this forum indicates that, although IS security concerns have been recognised by the IT department for many years, senior management has yet to fully appreciated the importance of IS Security processes within the business framework. The failure of senior management to fully support IS security processes is limited by the expectation of the outcome measured against the performance of other projects within the organisation. It may be difficult for management to approve ongoing funding for IS security projects that are not understood or appreciated as being a necessity (that is, of high risk), nor as generating profit or reducing costs.

1 Rank (of the order assigned by each participant, averaged, then ordered).

2 Rating [of the importance ranking (1-7 for each issue raised). This is the sum of this data, in ascending order of the average).

3 Average Rating (The sum of the average ratings across all participants in descending order of the average).

> *"... the reason management support is lacking in many projects is the poor explanation of the issues and benefits middle management provide to senior management ..."* (follow up interview)

> *"... most business cases for security upgrades are poorly structured and written and do not clearly explain the benefits of security and the tasks to be carried out ..."* (follow up interview)

Following on from the issue of Senior Management Support is the 'Statutory/Legal requirements' which not only affect the integrity of the business but may place legal obligations on a Director/CEO and other senior managers of an organisation.

> *"... (the) main driver is reducing our agency exposure, whether it's our losses, legal liability, downtime or service loss ..."* (Participant 1)

This issue of reducing agency exposure has major implications across the whole of an organisation as the exposures may lead to a loss of confidential information, a loss of reputation and/or financial losses. This in turn may result in systems having to be temporarily removed from public access until solution patches are applied or law enforcement services investigate any alleged security breaches. If service level agreements have been established a loss of service may result in contractual penalties or legal action.

Another major issue identified is the issue of 'Awareness and Training'.

> *"... Staff awareness and training, ... people need to know what is expected of them and they (need) to know the basis of the issues of security so they know what they have to contend with and what is expected of them... we need to make them aware and do what's necessary so that we all know where we stand ..."* (Participant 9)

With regular changes in the workforce it is difficult to maintain a functional pool of knowledge regarding the safe and effective operation of business systems. As new staff commence their duties most of the knowledge conveyed by colleagues is about the operational processes rather than concentrating on the security components of the business processes. Until a staff member has been through orientation and received the necessary security training, the risk of unsafe business processes is increased. When staff are fully trained, it is crucial that they are aware of the responsibilities and accountabilities of their role.

3.2 Key Inhibitors to Successful IS Security Processes

The second focus question discussed related to identifying key inhibitors to successful IS Security processes. The participants identified the following key inhibitors, which are set out in Table 2. These are the major factors which would inhibit successful IS Security processes within government agencies.

Table 2 shows the average rankings of these key inhibitors and the average importance ratings given by the participants to each inhibitor.

Table 2: Key Inhibitors to Successful IS Security Processes

Key Inhibitors to Successful IS Security Processes	Rank	Rating	Av. Rating
Security needs to part of the development process Lack of management awareness	1	1	6.7
Lack of security awareness and training for all staff	2	3	6.0
Lack of allocated funds due to low priority	3	4	5.9
No negative experiences so it is assumed that everything is ok	4	8	5.4
Resistance to set up a uniform user interface across the organisation	5	2	6.2
Lack of consistency of risk management processes across the breadth of organization	6	5	5.7
Expectation of users to be able to access all information when they want.	7	17	4.7
Security perceived as hindering productivity	8	6	5.7

Once again all inhibitors raised rated above 4.6 (> moderately important) and hence all should be considered, as key factors that may inhibit successful IS security processes within government agencies. The major issue identified as an inhibitor is the issue of 'Management Awareness'. This issue scored the highest in 'Rating' and was also 'Ranked' the most important.

"Lack of awareness that information generated belongs to the organisation ... " (Participant 4)

The awareness of information as an important resource not only needs to be recognised by staff but also by senior management. The collection and processing of any information collected by an organisation will inturn be subsequently used by them or other organisations to make decisions about their customers and services. These decisions can be business, financial, personal and may even have life threatening consequences. The protection of this information from fraudulent or accidental tampering or loss is vital and is clearly a responsibility of management.

"... the perception or assumption with security is that it is solely an IT responsibly rather than recognising that it affects the whole business ..." (Participant 6)

This quote reinforces the previous comments where management needs to be aware of the significance of the relationship between business processes and the IT departments in terms of responsibility for information security. Just because the IT department develops/operates the business systems, the information contained within belongs to the organisation. Therefore, security of business information cannot be solely to the responsibility of the IT department.

"... IS security is a necessary evil which hindered productivity ..." (Participant 1)

This comment is one of the most common complaints levelled at IT security processes from the operational areas. It is probably also true, effective security has to be protective and therefore intrusive to some degree to offer an appropriate level of protection. One of

the aims of a security system designer is to try to make security as easy and practical as possible to implement and use, even though the back end development systems can be quite complex.

"... Different size agencies have different needs..." (follow up interview)

The policies developed by central government tend to place all agencies in the same category and fail to recognise the variation in size, function and critically of agencies. The initiatives of central agency policy should account for the variations in agencies trying to comply with their directives.

4. Business Continuity Planning (BCP)

4.1 Key Drivers Business Continuity Planning (BCP)

The third focus question discussed at the forum relate to identifying key drivers for BCP. The participants identified the following key drivers, which are set out in Table 3. These are the major factors, which should contribute to successful BCP processes within government agencies.

Table 3 shows the average rankings of these key drivers and the average importance ratings given by the participants to each driver.

Table 3: Key Drivers for BCP Processes to Work in Your Agency

Key Drivers for BCP Processes To Work In Your Agency	Rank	Rating	Av. Rating
Recognise that business is the driver not information technology	1	1	6.9
Standards and legislation for vital records may be enforceable	2	5	5.9
Use experienced external consultants to improve skilling of staff	3	3	6.1
Previous negative experience	4	4	6.0
Assigning appropriate levels of authority	5	2	6.2
Integration of organisational and community needs if applicable	7	6	5.8
To protect critical information	6	9	5.3
BCP processes to encompass the "whole" organisation (planning phase for response and recovery)	8	7	5.8

All factors raised were rated above 4.7 (> moderately important) indicating that all of these issues are worth considering by management as factors that drive successful BCP processes within e-government. Once again the ranking in the table differentiates between the issues. The most common issue on BCP Process Drivers was based on the following comment:

" ... That the business is the driver of BCP and not IT driving that ..." (Participant 9)

Businesses need to be fully attentive of the union between the business and the BCP processes. This means that the business should not isolate itself from being a stakeholder in the BCP processes and allow the IT department to lead the BCP processes. Although

the development of a BCP is usually charged to the IT department, it will become an IT Disaster Recovery Plan (DRP) unless business and management are serious about having an active role in its development, testing and review.

"…. when you read 7799 (AS/NZS7799) it clearly says that BCP is an integral component of gaining that certification …" (Participant 3)

Essentially an effective level of security includes an effective and tested BCP.

"…. it not an imaginary concept, it is a real and pragmatic approach to managing their business in a day-to-day environment …" (Participant 4)

BCP is not a document that is quickly assembled, with a report to management that the task of BCP is now completed. BCP is dynamic and involves the active participation of the entire organisation. It is more about the culture of the process to create an effective process rather than just a document. It also requires continual updates, testing and, as such is a 'living' document.

4.2 Key Inhibitors to Successful Business Continuity Processes

The last focus question that was discussed relates to identifying key inhibitors to BCP Processes. The participants identified the following key inhibitors, which are set out in Table 4. These are the major factors, which may contribute to inhibiting successful to BCP processes within government agencies.

Table 4 shows the average rankings of these key inhibitors and the average importance ratings given by the participants to each inhibitor.

Table 4: Key Inhibitors to Successful BCP Processes

Key Inhibitors to Successful BCP Processes	Rank	Rating	Av. Rating
Lack of awareness	1 ◄⟷►	1	6.7
Failure to recognise that the business is the driver not information technology	2 ◄⟷►	2	6.3
Failure to understand where IT fits into the business model	3 ◄⟷►	3	6.1
Lack of allocated and availability of funds for clearly identifiable business plans	4 ◄⟷►	4	5.9
Training at all levels to increase awareness	5 ◄⟷►	5	5.9
Lack of capacity / resources to test BCP	6	6	5.9
Lack of current and appropriate BCP processes	7	8	5.6
Incomplete 'asset register' & other information that 'hooks' into the plan	8	10	5.6

All BCP inhibitors raised rated above 4.8 (> moderately important) and hence all should be considered as key factors that may inhibit successful BCP processes within government agencies. Once again the awareness issue has been raised as one of the key inhibitors for BCP processes within agencies. In this research question, "Awareness" was both rated and ranked as number 1.

"…. lack of awareness of the need at an executive level because of the perception of no real risk …." (Participant 1)

Some risk managers would rate the chance of a catastrophic event occurring to an organisation, requiring the implementation of their BCP, as once in a lifetime. This however, does not absolve management of the responsibility of preparing a BCP to deal with a catastrophic event occurring.

"…. lack of capacity to test 24/7 …" (Participant 3)

There can be a lack of resources or capacity within the business or IT systems to fully test an organisation's BCP processes. Some business systems cannot be shut down or switched off-line to be tested because they are mission critical or sometimes have potentially life threatening consequences. It then becomes a management decision to determine the appropriate BCP testing strategy based upon the associated risks of the organisation.

"… you can have a plan that covers every aspect of your business …" (Participant 6)

This comment may be a little optimistic, but in the event of a disaster, which requires the implementation of the BCP processes, all major aspects of the business need to be addressed by the plan. This is usually determined by an appropriate business impact analysis (BIA) being undertaken.

"… using a BCP video in induction training …" 200 eyes looking at security is better than 2 IT eyes…." (follow up interview)

This comment highlights the issues of staff awareness and staff induction being a good start point for this initiative. However, BCP processes are usually not the only issue discussed at induction. Other strategies need to be implemented to ensure BCP processes have a high profile within the agency.

5. Discussion and Limitations

There is a very good correlation between the 'ranked' order and the 'rating' order of the top 5 issues raised at the forum. The correlation can be seen in the connectivity (arrows) between the ranking and rating columns of Tables 1 to 4. This further reaffirms the importance of the issues raised and the reliability of the individual measures of the ranking and rating.

One major limitation of the initial study is that it only focused on the practices of nine government agencies. However, the additional sixteen agencies that participated in the follow-up interviews give a more representative result as these agencies were stratified in terms of progress towards AS/NZS ISO/IEC 17799:2001 certification rather than grouping by agency staff numbers. Also, it should be noted that only high-level issues were covered and while these issues were significant, the purpose was to identify them. Exploring these issues in greater detail and linking them to agency certifications remains an area for future research.

Other issues for further consideration are that there is no overall corporate governance for the whole of Government. Also, each agency has the autonomy to set their individual processes and to achieve certification to AS/NZS ISO/IEC 17799:2001.

6. Conclusion and Future Directions

The purpose of this paper was to determine the key issues that exist with IS Security and BCP processes for Whole of Government and then rank and rate them accordingly. The summary of the main issues across the four focus questions of the forum and follow-up interviews includes the majority of the four following issues:

1. Training
2. Management Support
3. Budget / Cost / Resources
4. Awareness

While not all of these overall issues are applicable to all organisation or agencies, they would appear to be relevant to a large number of organisations as key drivers or key inhibitors in respect of IS Security and BCP processes.

The positive effects from successful IS Security and BCP programs in organisations should result in the ability to obtain and maintain the support and understanding of Management.

The forum results reinforce the requirement that BCP processes should be an integral part of the business plans of every organisation, and not an IT 'add on'. Even though IT is often the champion and custodian of the BCP process, this does not imply that the IT department is the driving force behind its development, maintenance and ongoing testing nor is the IT Department solely responsible and accountable for these processes.

This study highlights the perception of IS Security and BCP issues within government organisations. The second phase of this e-government research program was to expand the coverage of the forum, by interviewing more government agencies, using the same set of four research questions and allowing them to rate and rank the issues raised by this forum. The next phase of this research program is to expand the coverage of the forum and interview government agencies and organisations, that are also attempting to achieve certification to AS/NZS ISO/IEC 17799:2001 and determine the key drivers and inhibitors with agencies certified to AS/NZS ISO/IEC 17799:2001.

In conclusion, running the same exercise with non-government agencies that are also attempting to achieve certification to AS/NZS ISO/IEC 17799:2001 would be beneficial as a comparative study and should be of practical assistance to private sector organisations.

References

AS/NZS ISO/IEC 17799 (2001): "2001: Information technology - Code of practice for information security management", Standards Australia.

AS/NZS ISO/IEC 17799 (2004):"2001/Amdt 1-2004: Information technology - Code of practice for information security management", Standards Australia.

AS/NZS 7799 (2000): "2000 - Information technology -- Code of practice for information security management", Standards Australia.

AS/NZS 7799.2 (2003): "2003 - Information Security Management -- Part 2: Specification for Information Security Management Systems", Standards Australia.

Backhouse, J., & Dhillon, G., (2001): Current direction in IS security research: towards socio-organizational perspectives, Information Systems Journal, Vol. 11, pp. 127-153.

Baird, A. Jamieson, R. & Cerpa, N., (2002): Development of a Framework for Risks and Security in B2C E-Business, in Monteiro J L, Swatman P M C, Tavares L V, (eds), Towards the Knowledge Society: eCommerce, eBusiness and eGovernment, Kluwer Academic Publishers, pp. 399-414.

Bell, G. (2001): Information Security Risk and Assessment, 2001 UNC Charlotte Symposium on Information Security and Privacy, http://www.sis.uncc.edu/LIISP/slides01/Greg-Bell.pdf (Accessed 28 April 2005).

Blaikie, N., (2000): "Designing Social Research", Oxford: Polity Press, Blackwell Publishers Ltd, Oxford UK.

BS 7799-2 (2002): "2002 : Information security management. Specification with guidance for use", Standards Australia.

Evans, N., (2003): "Information Security Guideline for NSW Government – Part 1 Information Security Risk Management", Office of Information and Communication Technology Sydney, http://www.oict.nsw.gov.au/pdf/4.4.16.IS1.pdf (Accessed 28 April 2005).

Frank, D., (2003): Policy would secure users, transactions, Federal Computer Week, Falls Church, Jan 27, Vol. 17, No. 2, p 10.

Ross, K. L., (2004): "Foundationalism and Hermeneutics", http://www.friesian.com/hermenut.htm (Accessed 28 April 2005).

Gartner, (2002): Executive Presentation of Business Recovery Planning, Ney York State Forum, 02 Consulting, http://www.nysfirm.org/documents/ppt/bc_02/8-13GartnerBCP%20Pres.ppt (Accessed 28 April 2005).

Kraemer, K. L., and Dedrick, J., (2000): "European E-Commerce Report", Working Paper Center for Research on Information Technology and Organizations". University of California, Irvine, August 2000. http://www.crito.uci.edu/git/publications/pdf/european-e-commerce-report2.pdf (accessed 28 April 2005).

NSTISSC (1999): "National Security Telecommunications and Information Systems Security Committee (NSTISSC)" NSTISSI No. 4009 National Information Systems Security (INFOSEC) Glossary, January, p 4.

OICT, (2004): "Office of Information and Communications Technology - connect.NSW: an Internet Strategy for NSW", http://www.oict.nsw.gov.au/content/1.3.1.Imp_Frame_Summary.asp (Accessed 28 April 2005).

Schmidt, R., Lyytinen, K., Keil M., Cule P., (2001): Identifying Software Project Risks: An international Delphi Study, Journal of Management Information Systems, Spring, Vol. 17, No. 4, pp 5-36.

Scott, R.W., (2003): Planners need to plan for disaster, Accounting Today, New York, Jan 2003, pp. 18-20.

Spinellis, D., Kokolakis, S., Gritzalis, S., (1999): Security requirements, risks and recommendations for small enterprise and home-office environments, Information Management & Computer Security, Vol. 7, No. 3, pp. 121-128.

Straub, D. W., & Welke, R. J., (1998): Coping with Systems Risk: Security Planning Models for Management Decision-Making, MIS Quarterly, Vol. 22, No. 4, December 1998, pp. 441-469.

Teo, H. H., Wei, K. K., and Benbasat, I., (2003): Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective, Management Information Systems Quarterly Vol. 27, No. :1, pp. 19-49.

Worthington, J., (2005): Flying Blind, Risk Management, Issue 16, April, pp 16-17.

Acknowledgements

The authors wish to acknowledge the assistance and cooperation of participants at the e-Government IS Security Forum, held at the Office of Information Technology in April 2003, to identify key research issues in the e-government IS Security and Business Continuity Planning process areas.