‘An annotated bibliography of multidisciplinary information security resources, for the purpose of maintaining privacy and confidentiality in New Zealand government records management.’

by

Brendan Feary

Submitted to the School of Information Management,
Victoria University of Wellington
in partial fulfilment of the requirements for the degree of
Master of Information Studies

JUNE 2013

VICTORIA UNIVERSITY OF WELLINGTON
School of Information Management

Master of Information Studies

IMPORTANT DISCLAIMER

with respect to a MIS Research Project (INFO 580)

'An annotated bibliography of multidisciplinary information security resources, for the purpose of maintaining privacy and confidentiality in New Zealand government records management.'

(hereafter referred to as 'The MIS Research Project')

being undertaken by

Brendan Feary

in partial fulfilment of the requirements of the degree of
Master of Information Studies,
School of Information Management, Victoria University of Wellington.

Topic Commencement: **Date 19 November 2012**

1. Victoria University of Wellington and its Council, its members, staff, employees, students and agents undertake no duty of care in contract, tort, or otherwise, to users (whether direct or indirect) of the MIS Research Project and make no warranties or representations of any kind whatsoever in relation to any of its contents.

2. The MIS Research Project is only made available on the basis that all users of it, whether direct or indirect, must take appropriate legal or other expert advice in relation to their own circumstances and must rely solely on their own judgement and such legal or other expert advice.

3. Under no circumstances will Victoria University of Wellington and its Council, its members, staff, employees, students or agents be liable in any way whatsoever, whether in contract, tort (including negligence), for breach of any statutory or regulatory duty (to the fullest extent permissible by law), or otherwise, to any user (whether direct or indirect) of the MIS Research Project for any loss or damage whatsoever arising directly or indirectly as a result of the use in any way of the MIS Research Project.

4. Each exclusion in the clauses of this disclaimer and each protection given by it is to be construed as a separate exclusion applying and surviving even if for any reason any of the exclusions or protections are held inapplicable in any circumstance.

i.

ABSTRACT

Research Problem

Maintaining privacy and confidentiality of data in an age of e-government and electronic recordkeeping is one of the key challenges for records management staff today. In New Zealand this issue has attracted negative attention through several recent public sector privacy and security breaches, raising questions about systemic issues, accountability, and a disconnect between strategy and implementation. How government responds will depend in large measure on the advice received regarding solutions to information security. A bibliographic gap on the relationship between records management and information security has been identified in the academic literature.

Methodology

Using targeted search strategies this annotated bibliography draws together articles from a range of journals with the aim of developing a consolidated resource for practitioners to become acquainted with the multifaceted and multidisciplinary nature of information security. The outcome is a resource directly relevant to the New Zealand context, which identifies key perspectives, relationships, technical issues, and shortcomings in research.

Results

Key findings relate to publishing trends, divided disciplines, and shortcomings in research pertaining to records management relationships with IT groups and engagement in e-government.

Implications

Includes the development of more comprehensive e-government information and security strategies, the re-examination and utilisation of existing relationships, and the strengthening of records management's position as a contributor to research and leadership in the array of possible responses to information security.

DESCRIPTORS

- Information Security;
- Records Management;
- E-Government;
- Privacy;
- Confidentiality;

ii.

ACKNOWLEDGEMENTS

I wish to acknowledge my supervisor Dr. Gillian Oliver who inspired me in the first instance to pursue a career in records management, and to pursue my interest in records continuum theory and applications. I am also grateful for the professional development and networking opportunities which have made it all come together.

I wish to acknowledge my colleagues at Archives New Zealand whose contagious enthusiasm gave me the drive and energy to get the project finished.

Finally I wish to thank my family for their motivation and support over the many years, and for putting up with my nonsensical babbling.

CONTENTS

1

INTRODUCTION

1.1 Background and New Zealand Context

Maintaining privacy and confidentiality of citizens' data in an age of e-government and electronic recordkeeping is one of the unique challenges and responsibilities of our time, and ties in with the larger issue of information security for a digital generation. One the one hand many citizens expect accessibility, enhanced services, automation, and ease of use. At the same time data is exposed to risks of malicious intent, misplacement, loss, corruption, and public exposure through the very systems and hands that manage that information for us. It is thought that the risks are well known, especially after particularly public instances of breaches in New Zealand, and subsequently awkward questions are raised when they are not being seen to be addressed adequately. This is especially so with many risks being identified in legislation by which public sector organisations are bound to comply with. These include: the Public Records Act (2005), the Privacy Act (1993), and the Official Information Act (1982), among others. Not only are legislative requirements well defined, but there are a range of supportive resources to assist in achieving compliance, such as Archives New Zealand's recordkeeping standards and the continuum resource kit (2013), as well as more specialised resources such as the DPMC Security in the Government Sector document (2002), and the GCSB New Zealand Information Security Manual (2011). There are also valuable resources provided by the Office of the Privacy Commissioner, including the Privacy Impact Assessment Handbook (OPC, 2007), and annual reports which analyse privacy breaches and the activities of the Privacy Commissioner (OPC, 2012)

The disparity between reactive responses and effective solutions to information security may well be a difference between an awareness of issues, and a deeper understanding of their social, technical, and organic complexity. New Zealand becomes a useful context through which many of these challenges can be drawn out in light of recent incidents where information has been exposed through various combinations of technological and human error. The interface between the two is as much to blame as any singular contributing element, however there are larger mechanisms and relationships at work that are at the root of the problem. It is these issues that this annotated bibliography is directed at. The perceived extent to which high profile occurrences of information security breaches and risks reflect a systemic issue should be debated as an availability heuristic, and the logic of subsequent extrapolations challenged. Recent security incidents appear to

represent an unfortunate cluster across a number of public sector organisations which have received significant media and political attention. It is the finding of this research that while information security issues are frequent, they are not systemic. Attributing blame to individual elements makes for non-constructive outcomes and patches over the real issues of dysfunction within organisations and between subject disciplines. None the less, information security breaches are valuable events to learn from, and practitioners would be well advised to examine incidents against their own organisations' measures, policies, and business functions. Recent examples from the aforementioned cluster (by no means comprehensive) include:

- Accident Compensation Corporation accidentally sending claimants' private details to the wrong recipient, for which they were criticised for an arguably slow response in the aftermath (KPMG, 23 August 2012). ACC Chairwoman Paula Rebstock told a parliamentary committee that as many as seventy-five privacy breaches occurred in a single financial quarter (Bennett, 14 February 2013). Another high profile case concerned Bronwyn Pullar, who was sent a large number of private details, including those concerning sexual abuse cases (Edwards, 24 August 2012);
- Ministry of Social Development, Work and Income New Zealand mishandled physical documents sending them to the wrong recipient (Chapman & Boyer, 24 October 2012), and blogger Keith Ng publishing the fact that public self-service kiosks allowed full, uncontrolled access to Ministry servers in spite of previously raised concerns (Chapman, Small & Field, 2 November 2012);
- Ministry of Foreign Affairs and Trade suffered a deliberate information leak of two Cabinet committee papers to Phil Goff (the opposition Labour Party foreign affairs spokesman), as a result of plans for restructuring and downsizing in the ministry (Trevett, 4 May 2012);
- A comparable risk scenario arose with the New Zealand Defence Force, after a Defence White Paper (Ministry of Defence, 2010) recommended the civilianisation of military positions budgets continued to be reduced, resulting in a significant drop in morale and an alarming number of voluntary resignations with implications for operations;
- Ministry of the Environment sent emails regarding submissions made on their website with all recipients' email addresses visible, by simple mistake of not using the blind carbon copy function to hide the details (Newstalk ZB, 29 March 2013). On another occasion the wrong letter was attached to an email (Quilliam, 6 April 2013);
- Earthquake Commission, already the focus of public frustration regarding the Christchurch earthquake recovery, sent 83,000 claimant details to the wrong recipient (Conway, 25

March 2013), which despite being protected by court injunction (Ensor, 8 April 2013) were published on a foreign website (Bennett & Tait, 12 April 2013). As a result IT systems allowing external access or communication were shut down pending an investigation (Small, Chapman, 27 March 2013; Shuttleworth, 28 March 2013);

- Bay of Plenty District Health Board staff member breached patient confidentiality by accessing clinical records and discussing patient details inappropriately in casual conversation with staff (Gillespie, 6 December 2012);
- Immigration New Zealand was revealed to have had as many as 200 privacy breaches in the last three years (from date of article), with only twelve of those people affected being informed, and ten staff losing their jobs (Levy, 22 November 2012);
- Ministry of Education's payroll system Novopay sends personal information and financial details of teachers to wrong schools amid a larger issue of pay disputes and system errors (Fletcher, 11 November 2012);
- Canterbury District Health Board investigated four clinicians for breaching patient confidentiality and privacy when they inappropriately accessed the medical records of high-profile sportsman Jesse Ryder who was hospitalised after being assaulted (Carville, 13 April 2013).

Several consistent patterns emerge from the above instances of breaches of privacy, confidentiality, and information security. Among these are:

- human error in the processing of physical documentation;
- human error in the use of common office software such as Microsoft Outlook and Excel;
- there are issues in business process design and work flow;
- predominance of operational level breaches, particularly those involved in outward focusing customer service and client communication;
- there are notable instances of malicious intent resulting typically from opportunism;
- many breaches fall under the ambit of professional misconduct;
- political situations and individual frustration are frequently major contributors to breaches;
- public exposure and breaches can be negligible in effect, but have also been demonstrated to have the potential to be extremely damaging to public image and trust in government.

Amid the media frenzy surrounding successive incidents, Prime Minister John Key made the

argument that while regrettable, privacy breaches are inevitable as a 'result of human error, not systemic failure' (Ivey, 2 April 2013). Surely human error can be systemic? This raises the question of what connotations surround the term 'systemic'. Perhaps the most pronounced are incompetence and bureaucracy, indicating a lack of resolve. However on a less emotive level it also reflects issues of frequency, scale, intent, and attitude. There are a whole range of ways in which privacy and confidentiality can be impacted, not all of which can be prevented even when anticipated. It would be a mistake to presume that people are the sole issue, and similarly that technology is the common denominator. This fails to take into account extensive interaction between the two which subsequently risks missing a valuable opportunity to enhance current information security practices through a broader implementation of skills, knowledge, and attitudes. A multi-disciplinary arrangement of information security and other supplementary research articles brought to bear on these events will assist in developing a comprehensive appreciation of the digital environment we take for granted, often not taking the time to reflect on the implications of perceiving technology as neutral.

1.2 Purpose, Scope, Audience, Dissemination

In the larger information security and records management fields there exists a bibliographic gap. Concepts and perspectives from individual disciplines have not been adequately reconciled to facilitate practitioners from different disciplines acquiring a larger appreciation of complex privacy and confidentiality issues, nor achieve sufficient meaningful communication to develop a coordinated and shared strategy from which to address the issues at hand. Most prominent is a communication issue between IT professionals and those in records management who come from two different environments. While both the IT field and records management acknowledge that threats are generated from both social and technological issues, IT places more emphasis on well developed technology as the solution to mitigate social challenges, and records management places more emphasis on developing people to engage effectively and efficiently with technology. In both instances, technology is seen as neutral which distorts the apportioning of responsibility for maintaining privacy and confidentiality among individuals, departments, and organisations.

The purpose of this project therefore has been to produce an annotated bibliography of useful and thought-provoking articles arranged using high-level themes to structure concise annotations that both summarise and link the resources together under the umbrella of challenges faced in the New Zealand context. This has been designed to capture and evaluate a range of content dealing with such areas as: information security; privacy and confidentiality; e-government; records management; information technology; risk management; business processes; and particular sectors of government with a focus on domestic affairs involving citizens' data and information, including: health, social services, finance, justice, and citizen identity. This inevitable strays into the realm of international affairs including cloud storage and cybercrime, but always within the bibliographic structure of privacy and confidentiality. Due to limitations of what is published in New Zealand the project draws on a large degree of international material dealing with issues whose findings must be translated across to a new set of circumstances.

The scope of the bibliography is limited to a flexible parameter of articles published from the mid-1990s onwards, with a preference for more recent articles that have drawn on recent literature and are informed by recent developments in information technology and records management. The primary criteria however is always individual merit. The subjects of the articles have been selected to demonstrate a balance between comprehensiveness, and current issues. The research aim of reconciling different perspectives has inevitably resulted in a quite broad selection. The project is intended to be unique in respect of the intention to better understand what literature and themes have been published in journals, with a view to acknowledging the importance of the context that

ideas were developed in – a pre-existing, but up until now disjointed body of knowledge.

The target audience of the bibliography are those academics and professionals working from different perspectives and disciplines of information management and information security. The focus however is on people who are involved in some way with recordkeeping of government records or archives, or with responsibility for maintaining privacy and confidentiality. This includes public service workers, managers, and tertiary staff and students who examine the issues from outside the industry. While the general public are not intended as the primary users of the bibliography, it is written such that it is accessible enough for those interested to use.

Possible venues for distribution include Victoria University of Wellington's Research Archive where it will be freely available for all Information Studies staff and students, as well as others in academia and the workforce who can be directed to the repository. To promote the bibliography a submission may be made to the NZ-Records mailing list to inform the records management community, and similarly submissions made to organisations such as Records and Information Management Professionals Australasia (RIMPA) and Archives and Records Association of New Zealand (ARANZ) which may assist in reaching the target audience. Sharing the bibliography on my personal LinkedIn profile may achieve a similar effect through networking. In all cases, linking to the university repository would be the most appropriate way to provide sustained, free access.

Submission to be considered for publication in academic journals may be feasible based on the scope and topicality of:

- Records Management Journal - [ISSN 0956-5698]
- Transforming Government: People, Process and Policy - [ISSN 1750-6166]
- Information Management & Computer Security - [ISSN 0968-5227]
- Journal of Information Technology & Politics [ISSN 1933-1689X Online]

1.3 Methodology and Arrangement

The methodology for this project takes the form of bibliographic research, where relevant articles accessible through Victoria University of Wellington Library's subscriptions to academic journals have been retrieved and analysed for their relevance and utility in developing a framework through which to understand information security from different perspectives. The final objective has been to develop a broad strategy to align the perspectives with the maintenance of privacy and confidentiality in government, paying particular attention to areas which would benefit from increased attention and research.

The guiding research objectives were to:

1. Develop and communicate a conceptual and practical understanding of privacy and confidentiality as they pertain to government records management in New Zealand;
2. Compare, reconcile, and analyse the separate domains and perspectives of information security, to acquire and communicate an understanding of how they relate to one another;
3. Evaluate journal articles and periodicals for their ability to represent and inform the information security challenges to maintaining privacy and confidentiality;
4. Arrange the information resources in a manner conducive to gaining a holistic understanding of information security, while supporting the audience to access particular topics further with consideration for understanding privacy and confidentiality in New Zealand.

To access relevant articles while acquiring a comprehensive overview of what was published, search strategies were developed based on a worksheet linking multiple concepts with boolean operators. Preliminary research performed using core concepts in this manner across several journals demonstrated that a large volume of articles were available numbering in the tens of thousands, however their publication was quite dispersed over time and disciplines. It was evidently impractical and undesirable to depend on browsing alone, so the search strategies were redeveloped to reflect which industries used which terms. This enabled targeted searching and the identification of thematic clusters, several of which are represented in this bibliography. This was highly effective in overcoming obstacles such as inconsistent use of terminology, or differences between groups such as records management and information technology. Notable results were found in the Emerald, EBSCO, LISA, LISTA, and Proquest databases. The development of thematic clusters were very organic and open to change as the research progressed.

The bibliography itself has been arranged into broad, high-level themes relevant to information security and to the discourse of privacy and confidentiality in the public sector. These are:

1. Multidimensionalism and Records Management
2. Detection and Conceptualisation of the "Breach"
3. E-Government and Digital Technologies
4. Data Rights and Responsibilities
5. Technical and Specialist Perspectives
6. Information Assurance

In terms of the methodology this has been the most adaptable facet of the project, but also the most central to communicating the utility of the findings. The index in the appendix further assists user navigation of the resources by listing key descriptors of the articles (a maximum of three) with a short citation and the section of the bibliography in which the article sits.

The citation style used in this bibliography is from the American Psychological Association sixth edition citation manual (APA, 2010). Annotations take the form of a single paragraph with a limit of approximately one hundred words per entry. This was set to ensure conciseness was balanced with the need to offer insight into the applicability of concepts in the articles.

2

Note on Publishing Trends and Search Strategies

Concurrent with the separation of IT and records management in the real world, there is a matching separation in the academic literature. This is reflected in the terminology, subjects, focus of articles, preferred journals - everything. This makes searching for content on the same topic difficult because the searcher is restricted to using high level concepts (like 'information security' and 'risk management') to maintain an overlap of discussion points. For instance while searching in records management journals the term 'information security' is fairly effective. When searching in IT journals it is too broad, as the topic is broken down into areas such as networks, information systems, encryption algorithms, and so on. In fact, it was only when suggested by an associate working in government IT that I look further into 'information assurance', which opened up all sorts of doors. Anyone seeking a more comprehensive overview of the topics in this bibliography would be well directed to examine more traditional bibliographies for academic content (Dotson, 2007) or seek out online directories with dynamic content. New comers to the subject should heed the words of Privacy Commissioner Marie Shroff when commenting on the breaches at Work and Income New Zealand, when she noted that 'looking at IT security is only one part of the picture. Recent privacy breaches make it plain that a complete mind-shift is needed in some quarters' (Manhire, 2 November 2012).

3

ANNOTATED BIBLIOGRAPHY

3.1 Multidimensionalism and Records Management

Al-Rashdan, M. (2012). An analytical study of the financial intelligence units' enforcement mechanisms. *Journal of Money Laundering Control,* 15(4), 463-495.

Launching immediately into multidimensionalism, this article explores how financial intelligence units should approach the enforcement of compliance to achieve the best outcome. This is particularly salient for records management where compliance is approached typically using a soft style as opposed to tough enforcement. Instead the author advocates a qualitative approach which involves better understanding of individual cases of non-compliance and working with the organisation to meet obligations, be they legislative or guidelines. This has particular applications for enforcement of privacy in moderating over-reactions to breaches while ensuring constructive action is actually taken.

Bearman, D. (2006). Moments of risk: Identifying threats to electronic records. *Archivaria*, 62, 15-46.

Risk analysis is a critical aspect to information security. Among other benefits, it ensures a framework is in place to identify, categorise and respond to specific threats without neglecting larger strategic efforts to anticipate unknown factors and changing environments. Bearman's identification of moments of risk to digital records builds on this by essentially applying the records continuum, which highlights capture, maintenance, ingestion, access, disposal, and preservation as deserving particular attention. While based on older projects of the 1990s, it is useful for practitioners to look at their own business processes and identify their own moments of risk, either through an analysis of prior security breaches or from scratch by documenting lines of communication, access, disposal, and other criteria.

Cheng, Z. (2008). *Critical Success Factors for Enhancing Government Accountability in Relationship to Electronic Records Management Systems*. Unpublished MIS 580 Project. Victoria University of Wellington, Wellington, New Zealand.

A major objective of recordkeeping is maintaining accountability in government. While such principles remain the same whether the records are physical or digital, the measures required to meet compliance with the Public Records Act (2005) differ considerably. This MIS project argues

that implementation of electronic records management systems are of critical compliance, and identifies three critical success factors as: reliability of the system; training environment and support; and user uptake of new technology. With a continuous roll out of the latest and greatest in records management systems from vendors, government offices would benefit from paying attention to the factors that really determine success, and why.

Dotson, D. S. (2007). Information Security Resources. *Science & Technology Libraries*, 27(3), 29-51.

This annotated bibliography of information security resources limits its scope to information security articles from the previous five years of its publication, drawing on a wider range of resources than this current project. Dotson's aim in producing a bibliography was to address the needs of IT professionals to understand all of the topics of information security, however does not tailor it to meet the needs of records management. It is invaluable however as a comprehensive reference to information resources on a range of topics. Records staff seeking further information would be well advised to read further.

Duranti, L. (2010). Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. *Records Management Journal,* 20(1), 78-95.

Duranti examines the issue of digital recordkeeping with a view to establishing how systems can be used to ensure values such as reliability and authenticity can be preserved long term. In particular the need to develop a spectrum of policies, strategies and standards is identified, with attention paid to how this is to translate into practical outcomes for organisations. Consistency across industries and disciplines is argued to be key, which arguably can already be found in the International Organisation for Standards (ISO) work, which many national authorities already draw on, including Archives New Zealand.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.

This article presents the findings of a survey of information security managers in eighty-seven Norwegian organisations ranging from public agencies to power, finance, and IT. The research was conducted with a view to analysing the implementation of security measures and their effectiveness. Technical-administrative policy and procedural measures attracted particular attention. This is a valuable resource for its consideration of how a combination of measures can work together to achieve a larger objective. Perspectives on how effectiveness is measured include: risk management; economic return on investment; legal compliance; and organisational

culture. Organisations wishing to consider the comprehensiveness or effectiveness of their own measures will find the survey useful.

Lemieux, V. L. (2010). The records-risk nexus: exploring the relationship between records and risk. *Records Management Journal*, 20(2), 199-216.

Using the search term 'risk management' opens up an entirely new set of resources not captured by other records management terms. Lemieux promotes a measured approach to understanding risk that does not deal in absolutes or zero-tolerance policies. This is a useful paradigm shift away from public rhetoric and is substantial in reconciling difference approaches to information security, including the dynamics and practice of risk classification and responses. The article assists in understanding bibliometric trends of risk management across seven journals.

Lips, M. & Rapson, A. (2009). *Emerging Records Management in 21st Century New Zealand Government – Part 2* [Report]. Victoria University of Wellington, Wellington, New Zealand.

This report deals with the creation and management of electronic records in New Zealand government using new ICT technologies, which the authors describe as Web 2.0. Included under this category are wikis, texting, and media sharing. The objective is to determine how public service workers manage these as records by analysing specific behaviours. Since a major aspect of records management is about the behaviours of staff, this research offers valuable insights into our constantly changing digital environment. With increasing use of social media to communicate with the public, government would be well advised to consider the findings of this report with regard to updating records management training and advice.

Lips, M., Rapson, A., & Hooper, T. (2008). *Email Records Management in 21st Century New Zealand Government* [Report]. Victoria University of Wellington, Wellington, New Zealand.

The role of email management in public sector recordkeeping is examined through the lens of user behaviours and legislative compliance. The research objective is to acquire evidence of what is actually being done in New Zealand government. This complements the above bibliographic entry by Lips by building a mosaic of evidence and data for evaluation, as well as establishing a basis from which to re-evaluate the New Zealand environment in follow up research. The report is particularly valuable as an evaluation of email as an integral communication tool with its own benefits and risks. Highly relevant to recent New Zealand privacy breaches which occur with increased frequency by virtue of email use.

Olivier, M. S. (2002). Database Privacy: Balancing Confidentiality, Integrity and Availability. *SIGKDD Explorations*, 4(2), 20-27.

This article written from a computer science perspective seeks to understand how a balance between confidentiality, integrity, and availability can be achieved without significant trade-offs. Noted early in the work that the need for privacy places an added burden on database development, even impeding development in cases where availability of information is a priority. Key to finding an acceptable balance is understanding the intended purpose of the stored data, who bears the risk of exposure, and why specific elements of information are needed. These principles translate well to general records management and communication of all information. Records should be generated in the course of business activities, however the situation is rarely as clean or straightforward.

Scholl, F. & Hollander, J. (May 2003). The Changing Privacy And Security Landscape. *Business Communications Review*, 54-57.

Digital information is widely understood to pose unique challenges. This article examines those in more depth, highlighting personal privacy and information security as foremost among them, and posing several consequence scenarios of misuse, theft, and exposure within a framework of how legislation in the United States has been used to counter the threats. Specific attention is paid to the Health Insurance Portability and Accountability Act (1996), the Gramm-Leach-Bliley Act (1999), and the USA Patriot Act (2001). This offers a range of measures to examine, and offers insights into how legislation can give added impetus to compliance without becoming distracted by technical implementation or short-term issues.

Skinner, G., Han, S., & Chang, E. (2006). An information privacy taxonomy for collaborative environments. *Information Management & Computer Security*, 14(4), 382-394.

This article proposes a shared taxonomy, classification and categorisation of concepts concerning information privacy for collaborative environments. Key dimensions of privacy are identified as: the person; behaviour; communications; and data. Structural relationships and use of metadata are drawn on heavily, with a final taxonomy produced that demonstrates useful perspectives from which to design systems to protect privacy. While weighted toward a computer science conception of information privacy, the article findings have applications in analysing business functions and user behaviours for risk management and system design.

Solms, B. (2001). Information Security – A Multidimensional Discipline. *Computers & Security*, 20, 504-508.

Excellent introduction to the argument for multidimensional approach, demonstrating how several disciplines traverse perspectives and skill sets. Highlights need for: best practice guidelines and policies, standards, certification, legal compliance and interaction, governance and strategy, appreciation of human factors, monitoring, and auditing. Offers practical advice for managing comprehensive information security. Challenges preconceptions of what is being

done.

Stuart, K. & Bromage, D. (2010). Current state of play: records management and the cloud. *Records Management Journal*, 20(2), 217-225.

Explores the topic of cloud storage in records management, opening up a whole range of issues. Web 2.0 technologies are considered alongside the cloud in the context of how work processes and services can integrate, as well as generate significant and unforeseen risks. How those risks are framed are argued to be important – focusing too heavily on the technological decisions can result in misinterpreting public acceptance of what and how services are delivered, affecting perceived competency and quality of information held, used, and secured. Reinforces articles by Cullen and Reilly concerning New Zealand public perception of government competence.

Wise, P. L. (2011). *The implications of government departmental organisational structures on fulfilment of OIA obligations*. Unpublished MIS 580 Project. Victoria University of Wellington, Wellington, New Zealand.

This MIS project examines how New Zealand government organisational structure affects legislative obligations under the Official Information Act (1982) to make public records and information freely available. Key findings include patterns in pro-disclosure, attitudes to freedom of information, the effect of how accessible information is, and the importance of process, tracking systems, and decision-making. This has particular relevance for New Zealand records management information security, because the efficiency and effectiveness of the process is a major factor in determining satisfaction with compliance, the quality of information made available under the act, and the upholding of the Privacy Act (1993). Measures to ensure staff are trained in their information management responsibilities are also seen to be important to the OIA request process.

3.2 Detection and Conceptualisation of the "Breach"

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information Security and Risk Management. *Communications of the ACM*, 51(4), 64-68.

A new risk management framework is advocated here for use in evaluating information security. The article is heavily oriented towards the metrics of risk management, but none-the-less offers insights into perceived risk by highlighting the facets of expected loss, expected severe loss, and standard deviation. Lessons can be learned and applied to records management and the maintenance of privacy by making an effort to quantify particular risks faced by an organisation. The difficulty in doing so is demonstrated by the authors, who conclude that many metrics of risk analysis only offer a narrow perspective of negative outcomes, rather than considering for example the investment in information security measures.

Garrison, C. P. & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230.

This quantitative study from the United States challenges the concept of a 'breach', and finds that most incidents involve non-malicious public exposure with negligible impact on the people involved, while simultaneously acknowledging pervasive electronic threats and a wide spectrum of risks. The authors use a methodology which is slightly questionable for its subjective assessment of scale and importance of data breaches, potentially biasing the results. Questions are asked of the significance of small lapses in information security, and the idea that information security can catch all incident types and scales. In light of how prevalent minor privacy breaches are both in government and commercially, this is a particularly insightful and balanced article.

Morgan, O. J. & Welch, M. (1995). Protecting confidential computer records against careless loss. *Records Management Quarterly*, 29(3), [Online].

Discusses two older information security breaches in New Zealand at Citibank and the Securities Commission. Describes some of the legal challenges and processes involved, details of the incidents, and the subsequent call for developing security policies. They also demonstrate how an interplay between human error and technical oversight can play out in actuality, the realistic limitations and consequences of public exposure compared to the rhetoric that emerges, and how to approach such situations. It is noted that government will attempt to control public relations around such incidents, however offers little insight therein – a direction for further research and consideration.

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention

systems. *Information Management & Computer Security*, 18(4), 277-290.

This article is particularly salient to considering the exact tools, policies and measures that lead to the detection of information security breaches in a manner that is not brought to the organisation by the media. The authors highlight the importance of building a holistic approach to information security that uses ID/PSs alongside security filters and firewalls, while raising the need to develop new systems that demonstrate intelligent detection and response to known and unknown threats. The influence of risk management is evident here, as is the appreciation of multidimensionalism.

Perri, F. S. & Brody, R. G. (2012). The optics of fraud: affiliations that enhance offender credibility. *Journal of Financial Crime*, 19(4), 355-370.

Writing from the perspective of financial fraud, the authors discuss the social dynamics that are frequently central to the successful exploitation of victims. This is known as affinity fraud, and draws on factors including age, ethnicity, religion, race, and professional designations to persuade victims and develop trust. The entire concept of social trust is evident throughout intentional breaches of information security, including numerous examples in New Zealand regarding privacy. The authors also discuss the need for due diligence, pointing to the inverse effect that common security measures such as passwords and access to information systems have on staff awareness of potential threats and risks.

Sherif, J. S., Ayers, R., & Dearmond, T. G. *(2003). Intrusion detection: the art and the practice. Part 1. Information Management & Computer Security, 11(4), 175-186.*

The authors here focus on cybercrime, particularly the threat of viruses and malware, hackers who breach systems and steal information, and the general prevalence of threats that can befall any organisation. Several types of computer attacks are described, as is a brief history of milestones in computer and information security design and analysis. A dated but none-the-less useful bibliography is shared, demonstrating a classification of literature predominantly from the 1990s, in addition to the final bibliography which is quite extensive for the brevity of the article. It is important for all users of information systems to be aware of the ways in which information security can be breached, both in terms of unintentional actions and malicious attacks. While many measures exceed the skill sets of records management staff, a closer working relationship with IT to design systems and analyse business activities would be of great benefit.

Shropshire, J. (2009). A canonical analysis of intentional information security breaches by insiders. *Information Management & Computer Security*, 17(4), 296-310.

This quantitative study of intentional security breaches in the United States utilises the perspectives of crime and fraud to identify several predictors and indicators that traverse the

commercial sector to be relevant to the public sector, including factors in employee backgrounds like financial hardship, relationship strains, loss of employment, and substance abuse. Varying motivations for breaching security, privacy, and confidentiality are explored. In particular, an examination of people-based risks such as opportunism and aggrievement has many applications to the current New Zealand context (examples have included the Ministry of Foreign Affairs and Trade, the New Zealand Defence Force, and the Earthquake Commission).

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4-19.

The authors examine the diverse information security challenges faced by IT, encompassing human, organisational, and technological issues, through a set of thirty six interviews with practitioners across seventeen organisations of different sectors. Particular value can be found in analysis of how different factors interact to trigger issues. Familiar challenges include: lack of training; organisational culture; risk management; budgetary priorities; access control; management support; system complexity; and vulnerabilities. Given the relationship between records management and IT can be dysfunctional at times, collaboration on shared concerns such as these may make for stronger and more consistent information security compliance.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, 17(4), 330-340.

Focusing on the relationship between perceived technical security protection and user behaviours in compliance with security policies, this article demonstrates both an indirect and a negative direct effect where high technical protection leads to low compliance with policy. Suggested practical applications include sharing of limitations of security measures during staff training. This has particular value for records management staff and others involved in induction training for government. The authors conclude that while technical security continues to advance and adapt, human error and security behaviours continue to frustrate those measures

3.3 E-Government and Digital Service Delivery

Carter, L. & McBride, A. (2010). Information privacy concerns and e-government: a research agenda. *Transforming Government: People, Process and Policy*, 4(1), 10-13.

Reviewing major privacy studies, the authors delve into applications for e-government with the end result being a model that lists seven key factors: perceived risk; collections; error; secondary use; improper access; reputation; and third party certificate. These factors are demonstrated to be influential in citizens' confidence in government to keep their private information safe and use it appropriately. The previous privacy studies are current and relevant to e-government, making them of value to collecting further data, designing methodology, and understanding other perspectives of what factors influence confidence in government.

Chai, S., Herath, T. C., Park, I., & Rao, H. R. (2006). Repeated Use of E-Gov Web Sites: A Satisfaction and Confidentiality Perspective. *International Journal of Electronic Government Research*, 2(3), 1-22.

Building further on the theme of evaluating public confidence in e-government, this article examines further factors including the relationship between extended, repeated use of services and satisfaction, and demographic considerations that may moderate confidence levels. Such considerations are important where government is collecting and using information pertaining to finances, citizen identity, justice, and social services. The perceived need to collect information is an important factor in satisfaction for both government and the public. The overall conclusion of the study is that public buy-in is central to better development of the systems and services.

Combe, C. (2009). Observations on the UK transformational government strategy relative to citizen data sharing and privacy. *Transforming Government: People, Process and Policy*, 3(4), 394-405.

This study examines the National Pupil Database in England as an example of the Transformational Government strategy where data sharing becomes an issues of privacy. Multiple instances of legislative non-compliance in data sharing practices are demonstrated, which challenge the entire strategy of government data sharing and accessibility of information. Findings from this paper should be considered against similar initiatives proposed in New Zealand under recent restructuring and whole-of-government initiatives, particularly in the realm of government IT services and systems. Several social issues are raised around the purpose of such initiatives that are deserving of further research.

Cullen, R. (2008). Citizens' concerns about the privacy of personal information held by government: a comparative study, Japan and New Zealand. *Proceedings of the 41st*

***Hawaii International Conference on System Sciences 2008*, 1-10.**

Cullen compares privacy concerns in Japan with those in New Zealand, contributing to the debate over the role that national and social culture has on perceptions, expectations, and measures to protect or use personal information. Disparities between government, business, individual and collective perceptions of privacy are particular revealing, as is the realisation that a major preconception of e-government, that digital equates with accessible, is flawed not only in terms of variance in the population's ability to access it, but how digital governance as a whole is perceived. The question of what is accessible to whom, and for what use, is an inevitable follow up question of e-government initiatives.

Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. *Online Information Review*, 33(3), 405-421.

Similar to Cullen's (2008) article, this study explores experiences and differences between ethnic communities in New Zealand including Maori and Pacific Island groups, and citizens in Japan. This again raises individualist and collectivist differences, and differences around the conceptualisation of identity by individuals. The study is laden with useful references to pursue further with regard to privacy, trust, technology, and culture in relation to e-government. A consistent finding was that the higher the distance of power between citizens and government, the higher the mistrust of powerful organisations. Thus ethnic 'minority' groups and socially structured societies display more mistrust than those of a higher percentage ethnicity.

Cullen, R. & Reilly, P. (2008). Information Privacy and Trust in Government: A Citizen-Based Perspective from New Zealand. *Journal of Information Technology & Politics*, 4(3), 61-80.

Examines the trust relationship between New Zealand government and the public using focus groups. Two particular concerns arose, those being reluctance with technology which reflects a technological literacy and accessibility issue, and easily influenced perceptions of government employee competency. Also observed is that most participants had a limited understanding of the actual protective measures in place to secure their information and limit its use. A critical analysis of the concept of privacy, as well as useful literature review contents points to further avenues of inquiry.

Dunkerley, K., Tejay, G. (2010). Theorizing Information Security Success: Towards Secure E-Government. *International Journal of Electronic Government Research*, 6(3), 31-41.

The authors of this article examine the core issue of how to secure information systems as they become increasingly prevalent and important in the conduct of government organisations. They identify a lack of research into the relationship between organisational context and information security. Resulting from a comprehensive review of the literature, three key dimensions for

evaluating the communication of information security. These are identified as: technical, involving assurance, integrity and business enablement; semantic, involving user intention and expertise; and effectiveness, involving the communication of security benefits and user behaviours. This is useful for evaluating current organisational security policy and measures.

Lam, W. (2005). Barriers to e-government integration. *Journal of Enterprise Information Management*, 18(5), 511-530.

Using semi-structured interviews with fourteen consultants with experience in e-government projects, the author identifies and examines seventeen barriers to the success of e-government initiatives, divided into four categories: strategy, technology, policy, and organisation. Issues familiar to practitioners will include the need for ownership and governance, interoperability, standards, and the establishment of documentation surrounding privacy and data ownership. Particularly relevant to the New Zealand context is the impact of the pace of government reform in achieving integration successfully and with as few teething issues as possible. A particular emphasis is placed on the importance of stakeholder engagement at a strategic and change management level.

Lips, M., Eppel, E., Cunningham, A., & Hopkins-Burns, V. (2010). *Public Attitudes to the Sharing of Personal Information in the Course of Online Public Service Provision* [Report], Victoria University of Wellington, Wellington.

This report examines e-government from the public's perspective, with particular regard for the attitudes towards the sharing of personal information to access services. Using a combination of literature review, semi-structured interviews, and focus groups, the key findings were a generally neutral view of sharing. Consistent with other comparable research, those participants from Maori and Pasifika groups demonstrated distrust in government competence and intentions, while the general sample population were neutral or positive. A degree of privacy awareness was demonstrated in an expectation that government adhere to legislative and social obligations such as transparency and use of information for primary purpose only.

Lips, M. & Pang, C. (2008). *Identity Management in Information Age Government: Exploring Concepts, Definitions, Approaches and Solutions* [Report]. Victoria University of Wellington, Wellington.

Lips and Pang report in this study on the tendency in e-government services towards digital identity management systems to manage relationships with the public. A consistent theme in the study concerns the implications for traditional in-person processes. The application of systems in international contexts in Asia and Europe are used to establish a baseline of experiences against which New Zealand initiatives can be compared. The study focuses more on the business process side of the issue than the social implications, which highlights the need to

establish concrete measures for the protection of privacy and information.

Lomas, E. (2010). Information governance: information security and access within a UK context. *Records Management Journal*, 20(2), 182-198.

The international information security standard ISO 27001 and the records management standard ISO 15489 are the focus of this article, which argues for a risk management based records management framework to meet larger objectives with governance strategies. The proposed way in which this is to be achieved is through an integration of information security principles and requirements with the design of records management systems through the joint application of the two standards alongside aligned strategies and legislative requirements. The application of the findings of this article are particularly relevant at a strategic level where national records management standards are developed, but is also of value to records managers whose organisations implement large, complex, and numerous systems.

O'Neill, R. R. (2009). *E-Government: Transformation of Public Governance in New Zealand?* Unpublished Master's Thesis, Victoria University of Wellington, Wellington, New Zealand.

This examination of how e-government 'transformative' initiatives are being applied and the perceived impact in New Zealand is a valuable resource to compare against those predominantly international perspectives and studies. This particular article, while confirming political rhetoric concerning efficiencies, collaboration and co-production through the long-term views of senior public officials and management, also offers insights into the functionality of public office with regard to case studies, implementing technologies, and increased emphasis on information management which in turn affects conceptions of privacy, confidentiality, and security.

3.4 Data Rights and Responsibilities

Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, 16(3), 22-40.

This examination of user security behaviours, particularly moderate to risk activities, addresses the costs and impacts of such behaviour. Examples such as lapses in backing up records, insecure password and access behaviour, email security, and online financial transactions were tested in a questionnaire given to undergraduate students at two universities. Of particular utility is the decision making identified behind unsafe practices which demonstrated that being generally knowledgeable and competent computer users, and being aware of the risks, did not always coincide with safe choices. Lessons can be extrapolated to other scenarios where decision making needs to be better informed or managed to promote desired behaviours.

Banahan, B. F. & Buckovich, S. A. (2000). Patient privacy, confidentiality, and security. *Drug Topics*, 144(4), 77-86.

This article considers patient privacy in the context of the health sector, looking at the implications of increased electronic data storage and sharing to achieve both patient care and the business functions associated. Many lessons can be learned with regard to privacy and information assurance from the health sector. Perhaps among the more surprising is the networking between practices that occurs, and the implications (and patient expectations) for privacy. A theme common in healthcare is the need to share information being balanced with privacy - an issue not yet fully resolved. This article cites statistics indicating a high level of anxiety regarding secondary non-healthcare uses of their information, particularly regarding commercial access.

Dunnill, R. & Barham, C. (2007). Confidentiality and security in information. *Anaesthesia and Intensive Care Medicine*, 8(12), 509-512.

Approaching patient privacy from an information security perspective, the authors focus on three key criteria: confidentiality, integrity, and availability. This is the classic balancing act with regard to security that controls access while not unnecessarily impeding it, described as mutual incompatibility. The consequences of getting it wrong are service disruption, loss of privacy, patient harm, financial loss, and legislative non-compliance. Key observations include the control patients have over their own information and care, and open communication in that respect. Notable features of security discussed include networks, logbooks, email, and access control. Given New Zealand examples of privacy breaches in healthcare, the article strikes a

salient point in its outlining of the responsibilities of healthcare staff in information management.

Gayton, C. M. (2006). Beyond terrorism: data collection and responsibility for privacy. *VINE*, 36(4), 377-394.

The relationship between the commercial sector, public sector, and privacy rights are discussed, with an initial observation that many privacy rights issues have already been addressed through measures including legislation, standards, and professional conduct amid a larger framework of concepts. A boom in the collection of personal information by a myriad of parties forms the background to specific issues such as businesses determining the value of protecting privacy, government providing social services which are heavily dependant on personal information, and an array of breaches, disclosures and thefts of information. Refreshingly, the article finds a middle ground between tangible privacy concerns and the national security debate by examining where data accumulates and gets used most.

Harnesk, D. & Lindstrom, J. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security*, 19(4), 262-276.

This article discusses and develops a typology of security behaviours regarding information resources in a public nursing centre, and analyses 'discipline' (security management) and 'agility' (practical security in use) as important criteria for the design, implementation and management of systems and environments. The discussion is particularly relevant to balancing privacy with business functions. Advocates increased emphasis on 'human security', the integration of strategic and operational measures, further development of adaptive risk typologies and creative responses to supplement traditional policies and procedures.

Kemp, R. & Moore, A. D. (2007). Privacy. *Library Hi Tech*, 25(1), 58-78.

This is an indepth examination of privacy as a concept, and the justification of privacy rights with regard to philosophy, legal conception and legislation, history, and a variety of critiques from a liberal democratic perspective. Key points include: collective versus individualist cultural characteristics; separation of spheres including political, religious, and personal; motivations for desiring privacy; legislative basis; and arguments for compromising privacy for other aims, benefits, and opportunities. This article has particular application to the debate of why privacy should be important to government, what exactly is being protected and why.

Renaud, K. & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security*, 20(4), 296-311.

This phenomenological analysis of health board employee interviews in the United Kingdom

reinforces observations common across the sector that staff feel impeded and encumbered by information security policy, which is seen especially to restrict service delivery. The authors optimistically advocate mediation and avenues for reinforcing positive behaviours to reconcile staff to compliance, acknowledging culture and support as critical, however do not take the position of advocating for a change in information sharing practices or social norms such as continuation of care across multiple health providers. The article contributes to debate of balancing static requirements with functional needs for communication and access. This has applications for other government initiatives proposing increased data collection or alternative use of existing data.

Schwartz, P. M. & Janger, E. J. (2007). Notification of Data Security Breaches. *Michigan Law Review*, 105(5), 913-984.

Notification of data security breaches is an important responsibility of custodians. In the New Zealand context this relates back to the recent Immigration New Zealand privacy breaches, where the majority of those affected were not notified of that fact. There is a balancing act however: transparency of government and service delivery, versus ongoing security and trust. This reflects a commercial attitude to communication with clients (or citizens), where a breach reflects badly, perhaps disproportionately, on the organisation's competency and competitiveness.

Stahl, B. C. (2004). Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics? *Journal of Organizational and End User Computing*, 16(3), 59-77.

The ethical dilemmas of information assurance and privacy are examined here within a framework of accountability, transparency, and responsibility. The implications of being a responsible party are identified, and conclude that individuals lack the capability to address ethical issues adequately, instead requiring a collective group with governance, policy, legislation, and other professional support mechanisms in place to manage social dynamics and aforementioned framework of expectations. The article has applications in developing guidance and policies pertaining to privacy and information security in public sector organisations.

3.5 Technical and Specialist Perspectives

Dallaway, E. (2008). Information Security in Israel. *Computer Weekly*, 24-26.

Information security technologies are predominantly seen to belong to the commercial realm, and aligned with national security initiatives and expertise. This article does nothing to contradict this, however goes further to analyse the political and economic dimensions behind a surge in knowledge-services in Israel coupled with the development and implementation of high-end security technologies. A relevant relationship to be considered across all public sector initiatives is the nature of the collaboration between government and business. IT is at its core a business, which is a concept that seems to be difficult to reconcile with traditional government in-house expertise and structures. This has implications for future relationships and initiatives where privacy is involved.

Dang, T. K. & Dang, T. T. (2013). A survey on security visualization techniques for web information systems. *International Journal of Web Information Systems*, 9(1), 6-31.

At the more technical end of information security is this article on visualisation techniques for web information systems. While some research on visualisation has occurred for user interfaces and server systems, this article is a response to an identified gap in the literature. While this trend is interesting, what is more salient to this bibliography is the need to map out the structure and relationships between deployed security measures. One example of how this works in practice is in the development of security warnings for identified instances of high-risk activities, such as using unsecured networks.

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security - A survey and classification of the research area. *Computers & Security,* 30, 748-769.

This literature analysis and bibliography focused on role based access control in information security poses an alternative perspective to how access to information is determined. The traditional model of user access control is enhanced by associating individuals with a role, which itself is given particular permissions to view and write information. Not only does this allow consistent access controls at a granular level, at a business process and business activity level it allows more efficient management of permissions. While continually under development, this model is useful to understand in assessing risks to information from a user behaviour perspective, such as in records management where only certain people should be able to view human resources records, or apply disposal sentencing to digital records.

Gritzalis, D. A. (2004). Embedding privacy in IT applications development. *Information Management & Computer Security*, 12(1), 8-26.

The right to, or at minimum the expectation of privacy is one of the more entrenched ideas in the digital environment, not only in terms of personal information online but in how systems themselves take into consideration, protect, and prioritise it. Examining this situation with regard to privacy-enhancing technologies, the author develops conclusions around measures for anonymity and pseudonymity, and data protection in the forms of encryption, digital signatures, and policy. This typically relates to how the user interacts with the applications, but in terms of the mechanisms behind the application which support that. While some extents of anonymity have little application in government recordkeeping, it does raise valid questions around the documenting of personal information.

Irons, A. (2006). Computer forensics and records management – compatible disciplines. *Records Management Journal*, 16(2), 102-112.

Irons demonstrates how two different disciplines, records management and computer forensics, can work together by discussing how records management can better articulate and communicate its own conceptualisation of requirements such as evidence and monitoring, and define more precise criteria and tools to achieve this. The article raises legal disparities such as many records management concepts going untested before the courts because compliance with recordkeeping legislation is seen to be a constructive process as opposed to enforcement of rules, while computer forensics is the complete opposite and relies on stringent guidelines and processes.

Kwok, L. & Longley, D. (1999). Information security management and modelling. *Information Management & Computer Security*, 7(1), 30-40.

As information management and information security acquire a stronger profile, often under the strategic level terminology of information assurance, there is a heightened need to develop more systematic metrics and risk analysis to quantify and qualify compliance with legislation and security standards. The authors propose a risk data repository model to manage this data and information, with a view to developing an accurate picture of organisations' individual risk profiles, security management frameworks, business continuity planning, and other measures of performance that have both practical and strategic applications. The role of the information security officer is advocated as an important component of this initiative as someone who is responsible for monitoring and reporting.

Pearce, M., Zeadally, S., & Hunt, R. (2010). Assessing and improving authentication confidence management. *Information Management & Computer Security*, 18(2), 124-139.

Examining shortcomings in multi-factor authentication systems, the authors combine risk management and assurance practices to developing a new system that mitigates the risks. This article has particular application in moderate to high level security systems, for instance online

banking or similar transactions of sensitive data and information. Its relevance to privacy and confidentiality lies in new e-government initiatives that handle sensitive information en mass. A salient issue is raised that increased security does not guarantee effective protection, as measures must be considered in unison with the asset and the risks it carries.

Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, 7(1), 50-58.

Writing from a commercial IT perspective on information security and referring to somewhat dated technology implementation trends, Solms makes an excellent observation on the shared benefits and risks of information security measures, perhaps best visualised as a weak link in the chain - a weakness that may pose a threat to other systems and information. An important tool in developing consistency are standards. Key elements of those standards are identified and discussed, and are valuable for understanding how the facets of information security fit together in practice.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems*, 111(4), 570-588.

User behaviour and attitudes towards information security and privacy are a major component of an overall strategy to protect valuable information, so this study of the relationship between information security readiness and security level is a valuable tool to consider when deciding on levels of security, and what that means for effectiveness, impact on accessibility and usability of the information itself, and any factors that may affect the relationship. The authors identify an interesting factor where IT proficiency and training can temper traditional user counter-reactions to higher level security.

Swire, P. P. (2003). Efficient Confidentiality for Privacy, Security, and Confidential Business Information. *Brookings-Wharton Papers on Financial Services*, 273-310.

Building further on the theme of effective information security is the idea of efficiency. The article, focussed on financial conglomerates, translates across to e-government well given the large volumes of private and confidential data being stored, transmitted, and used every day. More specific parallels include identity theft and willingness to utilise other services on offer. As e-government initiatives multiply, momentum alone will not necessarily bring with it the trust of consistent performance. The culture of privacy protection and consistent performance found in the banking industry with regard to customers and clients is something to consider in the strategies and policies surrounding information management systems and business processes.

Valtonen, M. R. (2007). Documentation in pre-trial investigation: A study of using the records continuum model as a records management tool. *Records Management Journal*,

17(3), 179-185.

The records continuum is gaining momentum and traction as a perspective in the design of modern records management capabilities and systems, taking into account creation, capture, organisation and pluralisation. Recognising that records are living documents with changing content, multiple authors, and multiple uses is critical as electronic recordkeeping advances. This article demonstrates the consequences of continuing to perform in non-compliant ways and fail to adopt information system technologies as they emerge by examining the model in a pre-trial investigation by police. Given the security and records management benefits of digital recordkeeping, one is compelled to query the slow adoption of best practice in particular sectors.

Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security. *Journal of Organizational and End User Computing*, 16(3), 41-58.

Focusing on user authentication theory and practice, the authors consider the applications of alternative password security systems to counter the inverse relationship between quality passwords and ease of recall. The implications of resolving this dilemma are increased satisfaction from users and improved, more consistent security for organisations. Given human psychology and memory leads users to see and generate familiar patterns, the proposed system utilises this to address four key factors in information environments: multiple applications mean multiple passwords; lack of user awareness of procedures; perceived lack of compatibility with work; unrealistic perception of security and sensitivity.

3.6 Information Assurance

Colwill, C. J., Todd, M. C., Fielder, G. P., & Natanson, C. (2001). Information assurance. *BT Technology Journal*, 19(3), 107-114.

The authors of this article examine an information assurance programme with regard to defending integrated information systems and networks of national telecommunications against malicious electronic attacks. Consistent questions are asked about what is critical or vulnerable and deserving of investment, and what is not so critical. This combines business continuity planning and analysis of core business activities with the targeted delivery of risk appropriate technologies on top of baseline protection, based on an impact analysis of attacks and the implementation of security itself.

Cormack, A. (2001). Do we need a security culture? *VINE*, 31(2), 8-10.

Originating from an observation that security failures rarely affect users, Cormack challenges the mainstream opinion in information assurance with regard to the need for security culture, or a soft-approach to security. As long as users can do their work efficiently and effectively, it is argued, they are sufficiently content. The article does not put culture down completely, however argues that the criteria are in need of considerable review in terms of practical application over rhetoric. Risk management dialogue is determined to be an important factor in developing an effective security culture.

Ezingeard, J., McFadzean, E., & Birchall, D. (2005). A Model of Information Assurance Benefits. *Information Systems Management*, 22(2), 20-29.

While information assurance typically aims to coordinate and integrate the technical features of information security into policy and strategy, the authors of this article demonstrate that achieving managerial buy-in and effective delivery of the information assurance message and metrics is more difficult than would first appear. A model is proposed to structure this approach, which includes: organisational, strategic, tactical, and operational benefits arising from an investment. In addition, a useful comparison of information security with information assurance is given, demonstrating the interplay between the two.

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3), 155-176.

Building further on the well-established interplay between security, organisation and business performance, the authors propose a model of a high-potential organisation with factors indicating reception or predisposition to security implementation and decision making. Those

factors include situational awareness of threat environments, technical capacity in terms of assets and expertise, and the ability to co-ordinate an effective response to threats. As e-government initiatives and technologies become increasingly centralised, the ability to develop or embody these factors may be at risk of decline.

Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems*, 39, 463-484.

Just like any other strategy, be it information management or policy focused, testing and evaluation is critical to successful implementation and performance. One key component is the concept of the unrestricted insider, which stereotypes security threats as external. This is equally applicable to perceptions of privacy protection. However as events and this bibliography have demonstrated, many vulnerabilities and breaches arise as a direct result of supposedly unpredicted human error and other damaging user behaviours which undermine information assurance and security strategies. It can also undermine any response in that there are few deterrents to bring against internal threats, only passive or 'soft power' training and guidance.

Jalal-Karim, A. (2013). Evaluating the impact of information security on enhancing the business decision-making process. *World Journal of Entrepreneurship, Management and Sustainable Development*, 9(1), 55-64.

Delving deeper into how information security and information assurance affect decision-making is an important line of inquiry to take. One of the key findings of the article concerns the informal and inaccurate nature of decision making when it comes to a lack of access to information, whether it be unnecessarily restricted, hoarded, or some other reason that causes an impedance in the flow of information. The primary causes are identified as excessive rules and regulations, heavy handed securing of systems and communications, culture, and disengaged management. The author concludes that addressing these areas to achieve the correct balance and environment will improve informed decision-making.

Pathari, V. & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*, 20(4), 264-280.

Making information security policy and documentation link with the implementation of controls and other technologies is a major part of quality information assurance. The purpose of the article is to advise on the analysis of security statements in order to determine areas of importance and priority. Another key measure is whether statements are driving or receiving in nature, meaning for instance a receiving statement depends on the fulfilment of other requirements to fulfil its own. The worst case scenario is where a policy document is orphaned, with no implementation around it. This can lead to misleading confidence and assurance when

management look at information security strategy, not realising the disconnect with actual implementation.

Rathmell, A. (1998). Information warfare and sub-state actors: An organisational approach. *Information, Communication & Society*, 1(4), 488-503.

Certainly at the extreme end of information security, 'information warfare', or in more conventional terms things like cyber attacks and theft, rarely affect the average citizen. Privacy is more frequently breached by the custodian of the data than any external threat. Yet increasingly the actions of sub-state actors (such as transnational and national criminal groups, hackers, and highly competitive commercial, industrial, and financial organisations) are affecting the privacy of individuals' data. Given government is increasingly maintaining digital records and increasingly rely on networks, they are a prime target for this type of activity. Records management can play a part in information security through the effective control of sensitive records and ensuring users understand and are capable of adhering to security advice.

Rogers, L. R. (2004). *Principles of Survivability and Information Assurance*. Carnegie Mellon University, Pittsburgh, PA, United States of America. 1-6.

This article considers information assurance from the perspective of survivability and continuation of services in the event of a myriad of scenarios where things can go wrong. Proposing a combination of organisational policy driving decisions; risk analysis and management; identification and documentation of all data, systems, users, and infrastructure; and valuation of assets to determine and prioritise survivable units. A major feature of information assurance is determined to be effective communication and targeted messages.

Schou, C. D. & Trimmer, K. J. (2004). Information Assurance and Security. *Journal of Organizational and End User Computing*, 16(3), i-vii.

Schou and Trimmer have a go at describing what information assurance means at the strategic, operational, and implementation levels. While the high level features are covered well, they identify the risk of disconnect and inconsistency with implementation, or the level and quality of protection that is expected but cannot be guaranteed in confidence levels. They highlight the foundation of information security well as being about awareness training, education, and culture, with technology being a capstone (or keystone) to the structured relationships between levels of information assurance. This article is one of several in a special edition which are included in this bibliography.

Wilbanks, L. (2008). Need to Share vs. Need to Assure. *IT Pro.* May/June 2008, 64-65.

This conversational article makes observations about work practices and personal behaviours of staff, and how they align (or do not align) with larger strategic goals like information assurance.

The need to balance efficient and effective information systems with security requirements raises yet again the apparent dichotomy between security and access. This is an attitude that needs to be addressed at multiple points of opportunity, such as induction of staff, in-house training and development, working with IT and systems, and designing work processes (among others). The conclusion of the author concerns the sharing of responsibility for achieving what are organisational aims, not just those for individual groups or staff.

Winjum, E. & Molmann, B. K. (2008). A multidimensional approach to multilevel security. *Information Management & Computer Security*, 16(5), 436-448.

Looking at the applications of multi-level security is a key discussion that records management staff need to engage in with regard to their security and privacy obligations. Understanding how information is arranged and used through the mapping of business activities is the first step in deciding what records require protection, what will be most effective, the impacts, and how the process of applying and reviewing security is to be managed. It can be a mistake to apply overly complicated systems when fewer levels would achieve the same result. Using the common set of: unclassified, confidential, secret, top secret, the authors demonstrate that a great degree of security in fact comes from defining roles and processes as it does from ascribing a security level to records at a singular level.

4

Directions for Future Research

- Information Security and Information Assurance: the appropriation of terminology and concepts from vendors and the IT industry lend themselves to further research, including the relationship with upper management.
- Relationships between IT and Records Management in the public sector: with regard to their relative positions of influence and expertise. This may include areas of current co-operation, and areas where there could, or should, be increased collaboration.
- Risk Analysis and Management: the theoretical and practical applications of this tool kit to information security, records management, and business processes.
- Comprehensive case study research into New Zealand instances of privacy breaches and information security failures.

5

Conclusions

Bibliographic gaps in academic literature can reflect several things. In the case of this bibliography, the gap is characterised by a separation of professionals, ideas, tools, and perspectives. Everyone wants information to be safe and secure, particularly their own private or confidential data. This expectation is amplified in the possession of a government steering towards initiatives which rely on the uptake of electronic recordkeeping and service delivery. What this means in practice however reflects the disparity between public attitudes and government business activities, between strategy and implementation, subject matter experts and end users.

This bibliography has addressed the gap to some modest degree by advocating a multidimensional approach to information security, and calling for the re-examination of existing relationships to adapt and engage in current issues surrounding the performance of information security, particularly between information technology professionals, records management, and those involved in business process. The New Zealand government's track record in maintaining the safety and privacy of records is looking fairly poor at the present time due to a number of breaches and leaks which have raised questions of whether the situation is systemic and rampant. The short answer to which is no. There is no single factor that is behind the exposure of private records - even human error is insufficient in describing the medley of circumstances.

How government now responds to the situation will depend in large measure on the advice received through key channels, including the Privacy Commissioner and the Chief Information Officer at a strategic level, and from subject matter experts at an operational level. The effectiveness of any response is difficult to pre-determine. If this bibliography demonstrates anything it is that the strategies exist and the technologies exist, but there is a lack of synergy and a lack of consistency in performance, and not just in terms of practice but in the underlying theories and structures too. The key lesson to take away from this resource is that while technology is inherently neutral, we endow it with qualities through our applications and behaviours. Understanding that at both macro and micro levels will determine future developments in this field.

6

Index

Governance	O'Neill, R.R. (2009)	3.3
Health Sector	Banahan, B.F., et al. (2000)	3.4
	Dunnill, R. & Barham, C. (2007)	3.4
	Renaud, R. & Goucher, W. (2012)	3.4
Identity Management	Lips, M. & Pang, C. (2008)	3.3
Implementation	Dallaway, E. (2008)	3.5
	Hall, J.H., et al. (2011)	3.6
	Hamill, J.T., et al. (2005)	3.6
	Pathari, V. & Sonar, R. (2012)	3.6
Information Assurance	Colwill, C.J., et al. (2001)	3.6
	Cormack, A. (2001)	3.6
	Dotson, D.S. (2007)	3.1
	Ezingeard, J., et al. (2005)	3.6
	Hamill, J.T., et al. (2005)	3.6
	Pathari, V. & Sonar, R. (2012)	3.6
	Rogers, L.R. (2004)	3.6
	Schou, C.D., et al. (2004)	3.6
	Stahl, B.C. (2004)	3.4
	Wilbanks, L. (2008)	3.6
Information Security	Aytes, K. & Connolly, T. (2004)	3.4
	Banahan, B.F., et al. (2000)	3.4
	Bodin, L.D., et al. (2008)	3.2
	Dallaway, E. (2008)	3.5
	Dang, T.K. & Dang, T.T. (2013)	3.5
	Dotson, D.S. (2007)	3.1
	Dunkerley, K. & Tejay, G. (2010)	3.3
	Dunnill, R. & Barham, C. (2007)	3.4
	Fuchs, L., et al. (2011)	3.5
	Garrison, C.P. & Ncube, M. (2011)	3.2
	Hall, J.H., et al. (2011)	3.6
	Harnesk, D. & Lindstrom, J. (2011)	3.4
	Jalal-Karim, A. (2013)	3.6
	Kwok, L. & Longley, D. (1999)	3.5
	Patel, A., et al. (2010)	3.2
	Pearce, M., et al. (2010)	3.5
	Renaud, R. & Goucher, W. (2012)	3.4
	Schwartz, P.M., et al. (2007)	3.4
	Sherif, J.S., et al. (2003)	3.2
	Solms, R. (1999)	3.5
	Sun, J., et al. (2011)	3.5
	Warkentin, M., et al. (2004)	3.5
	Werlinger, R., et al. (2009)	3.2
	Winjum, E., et al. (2008)	3.6
	Zhang, J., et al. (2009)	3.2
Information Systems	Carter, L. & McBride, A. (2010)	3.3
	Cheng, Z. (2008)	3.1
	Colwill, C.J., et al. (2001)	3.6
	Dang, T.K. & Dang, T.T. (2013)	3.5
	Dunkerley, K. & Tejay, G. (2010)	3.3

	Gritzalis, D.A. (2004)	3.5
	Harnesk, D. & Lindstrom, J. (2011)	3.4
	Skinner, G., et al. (2006)	3.1
	Wilbanks, L. (2008)	3.6
	Wise, P.L. (2011)	3.1
Information Warfare	Rathmell, A. (1998)	3.6
Intrusion Detection & Prevention	Patel, A., et al. (2010)	3.2
	Sherif, J.S., et al. (2003)	3.2
Investment	Ezingeard, J., et al. (2005)	3.6
Knowledge Management	Gayton, C.M. (2006)	3.4
Law Enforcement	Valtonen, M.R. (2007)	3.5
Motivation	Shropshire, J. (2009)	3.2
Multi-Level Security	Winjum, E., et al. (2008)	3.6
Multidimensionalism	Solms, B. (2001)	3.1
	Winjum, E., et al. (2008)	3.6
Obstacles	Lam, W. (2005)	3.3
Performance	Hall, J.H., et al. (2011)	3.6
Politics	Dallaway, E. (2008)	3.5
Privacy	Banahan, B.F., et al. (2000)	3.4
	Carter, L. & McBride, A. (2010)	3.3
	Chai, S., et al. (2006)	3.3
	Combe, C. (2009)	3.3
	Cullen, R. (2008)	3.3
	Cullen, R. (2009)	3.3
	Cullen, R. & Reilly, P. (2008)	3.3
	Dunnill, R. & Barham, C. (2007)	3.4
	Gayton, C.M. (2006)	3.4
	Gritzalis, D.A. (2004)	3.5
	Harnesk, D. & Lindstrom, J. (2011)	3.4
	Kemp, R. & Moore, A.D. (2007)	3.4
	Lips, M. & Pang, C. (2008)	3.3
	Lips, M., et al. (2010)	3.3
	Olivier, M.S. (2002)	3.1
	Renaud, R. & Goucher, W. (2012)	3.4
	Scholl, F. & Hollander, J. (2003)	3.1
	Skinner, G., et al. (2006)	3.1
	Stahl, B.C. (2004)	3.4
	Swire, P.P. (2003)	3.5
Public Relations	Morgan, O.J., et al. (1995)	3.2
Quality Assurance	Wilbanks, L. (2008)	3.6
Records Continuum	Valtonen, M.R. (2007)	3.5
Records Management	Bearman, D. (2006)	3.1
	Duranti, L. (2010)	3.1
	Irons, A. (2006)	3.5
	Lips, M. & Rapson, A. (2009)	3.1
	Lips, M., et al. (2008)	3.1
	Lomas, E. (2010)	3.3
	Stuart, K. & Bromage, D. (2010)	3.1
	Valtonen, M.R. (2007)	3.5
	Wise, P.L. (2011)	3.1
Risk Analysis	Bearman, D. (2006)	3.1
	Bodin, L.D., et al. (2008)	3.2

	Lemieux, V.L. (2010)	3.1
	Zhang, J., et al. (2009)	3.2
Risk Management	Aytes, K. & Connolly, T. (2004)	3.4
	Bodin, L.D., et al. (2008)	3.2
	Garrison, C.P. & Ncube, M. (2011)	3.2
	Hagen, J.M., et al. (2008)	3.1
	Kwok, L. & Longley, D. (1999)	3.5
	Lemieux, V.L. (2010)	3.1
	Lomas, E. (2010)	3.3
	Patel, A., et al. (2010)	3.2
	Perri, F.S. & Brody, R.G. (2012)	3.2
	Rogers, L.R. (2004)	3.6
	Stuart, K. & Bromage, D. (2010)	3.1
	Sun, J., et al. (2011)	3.5
	Werlinger, R., et al. (2009)	3.2
Security Breach	Garrison, C.P. & Ncube, M. (2011)	3.2
	Morgan, O.J., et al. (1995)	3.2
	Schwartz, P.M., et al. (2007)	3.4
	Shropshire, J. (2009)	3.2
Security Measures	Hagen, J.M., et al. (2008)	3.1
Standards	Lomas, E. (2010)	3.3
	Scholl, F. & Hollander, J. (2003)	3.1
	Solms, R. (1999)	3.5
Strategy	Ezingeard, J., et al. (2005)	3.6
	Hamill, J.T., et al. (2005)	3.6
	Jalal-Karim, A. (2013)	3.6
	Rathmell, A. (1998)	3.6
	Solms, B. (2001)	3.1
	Swire, P.P. (2003)	3.5
Sub-State Actors	Rathmell, A. (1998)	3.6
Survivability	Rogers, L.R. (2004)	3.6
Taxonomy	Skinner, G., et al. (2006)	3.1
User Behaviour	Aytes, K. & Connolly, T. (2004)	3.4
	Cormack, A. (2001)	3.6
	Lips, M. & Rapson, A. (2009)	3.1
	Lips, M., et al. (2008)	3.1
	Schou, C.D., et al. (2004)	3.6
	Werlinger, R., et al. (2009)	3.2
	Zhang, J., et al. (2009)	3.2
Visualisation	Dang, T.K. & Dang, T.T. (2013)	3.5
Web 2.0	Lips, M. & Rapson, A. (2009)	3.1
	Stuart, K. & Bromage, D. (2010)	3.1

7

References

[*material cited in body*]

Al-Rashdan, M. (2012). An analytical study of the financial intelligence units' enforcement mechanisms. *Journal of Money Laundering Control,* 15(4), 463-495.

American Psychological Association. (2010). *Publication manual of the American Psychological Association* (6th ed). Washington DC, United States: American Psychological Association.

Archives New Zealand. (2013). *Guidance and Standards.* Retrieved 24 January 2013, from http://archives.govt.nz/advice/guidance-and-standards.

Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, 16(3), 22-40.

Banahan, B. F. & Buckovich, S. A. (2000). Patient privacy, confidentiality, and security. *Drug Topics*, 144(4), 77-86.

Bearman, D. (2006). Moments of risk: Identifying threats to electronic records. *Archivaria*, 62, 15-46.

Bennett, A. (2013, 14 February). ACC privacy breaches still 'unacceptably high'. *NZ Herald*. Retrieved 20 February 2013, from http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10865475.

Bennett, A. & Tait, M. (2013, 12 April). Blogger defies court order on EQC. *NZ Herald*. Retrieved 12 April 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10877018.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information Security and Risk Management. *Communications of the ACM*, 51(4), 64-68.

Carter, L. & McBride, A. (2010). Information privacy concerns and e-government: a research agenda. *Transforming Government: People, Process and Policy*, 4(1), 10-13.

Carville, O. (2013, 13 April). Ryder's medical files spied on. *Stuff.co.nz*. Retrieved 14 April 2013, from www.stuff.co.nz/national/health/8545410/Ryders-medical-files-spied-on.

Chai, S., Herath, T. C., Park, I., & Rao, H. R. (2006). Repeated Use of E-Gov Web Sites: A Satisfaction and Confidentiality Perspective. *International Journal of Electronic Government Research*, 2(3), 1-22.

Chapman, K. & Boyer, S. (2012, 24 October). Privacy blunders mount at WINZ. *Stuff.co.nz*. Retrieved 15 January 2013, from http://www.stuff.co.nz/national/politics/7854125/Privacy-blunders-mount-at-Winz.

Chapman, K., Small, V., & Field, M. (2012, 2 November). Minister: Kiosks 'an atrocious operation'. *Stuff.co.nz*. Retrieved 15 January 2013, from http://www.stuff.co.nz/national/politics/7898326/Report-damns-ministry-over-security-breaches.

Cheng, Z. (2008). *Critical Success Factors for Enhancing Government Accountability in Relationship to Electronic Records Management Systems*. Unpublished MIS 580 Project. Victoria University of Wellington, Wellington, New Zealand.

Colwill, C. J., Todd, M. C., Fielder, G. P., & Natanson, C. (2001). Information assurance. *BT Technology Journal*, 19(3), 107-114.

Combe, C. (2009). Observations on the UK transformational government strategy relative to citizen data sharing and privacy. *Transforming Government: People, Process and Policy*, 3(4), 394-405.

Conway, G. (2013, 25 March). EQC privacy breach affects 83,000. *Stuff.co.nz*. Retrieved 25 March 2013, from http://www.stuff.co.nz/business/rebuilding-christchurch/8469811/EQC-privacy-breach-affects-83-000.

Cormack, A. (2001). Do we need a security culture? *VINE*, 31(2), 8-10.

Cullen, R. *(2008). Citizens' concerns about the privacy of personal information held by government: a comparative study, Japan and New Zealand. Proceedings of the 41st Hawaii International Conference on System Sciences 2008, 1-10.*

Cullen, R. (2009). Culture, identity and information privacy in the age of digital government. *Online Information Review*, 33(3), 405-421.

Cullen, R. & Reilly, P. (2008). Information Privacy and Trust in Government: A Citizen-Based Perspective from New Zealand. *Journal of Information Technology & Politics*, 4(3), 61-80.

Dallaway, E. (2008). Information Security in Israel. *Computer Weekly*, 24-26.

Dang, T. K. & Dang, T. T. (2013). A survey on security visualization techniques for web information systems. *International Journal of Web Information Systems*, 9(1), 6-31.

Department of the Prime Minister and Cabinet. (2002). *Security in the Government Sector*. Retrieved 16 August 2012, from New Zealand Security Intelligence Service: http://www.nzsis.govt.nz/publications/Security_in_the_Government_Sector_2002.pdf.

Dotson, D. S. (2007). Information Security Resources. *Science & Technology Libraries*, 27(3), 29-51.

Dunkerley, K., Tejay, G. (2010). Theorizing Information Security Success: Towards Secure E-Government. *International Journal of Electronic Government Research*, 6(3), 31-41.

Dunnill, R. & Barham, C. (2007). Confidentiality and security in information. *Anaesthesia and Intensive Care Medicine*, 8(12), 509-512.

Duranti, L. (2010). Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. *Records Management Journal,* 20(1), 78-95.

Edwards, B. (2012, 24 August). Political round-up: Is Bronwyn Pullar a hero? *NZ Herald*. Retreived 30 August 2012, from http://www.nzherald.co.nz/opinion/news/article.cfm?c_id=466&objectid=10829239.

Ensor, B. (2013, 8 April). Halt to leaked EQC details. *Stuff.co.nz*. Retrieved 12 April 2013, from http://www.stuff.co.nz/national/8524059/Halt-to-leaked-EQC-details.

Ezingeard, J., McFadzean, E., & Birchall, D. (2005). A Model of Information Assurance Benefits. *Information Systems Management*, 22(2), 20-29.

Fletcher, K. (2012, 11 November). Security fears in teachers' pay leak. *Stuff.co.nz*. Retrieved 15 January 2013, from http://www.stuff.co.nz/national/education/7933869/Security-fears-in-teachers-pay-leak.

Fuchs, L., Pernul, G., & Sandhu, R. (2011). Roles in information security - A survey and classification of the research area. *Computers & Security,* 30, 748-769.

Garrison, C. P. & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230.

Gayton, C. M. (2006). Beyond terrorism: data collection and responsibility for privacy. *VINE*, 36(4), 377-394.

Gillespie, K. (2012, 6 December). Major privacy breach at Bay of Plenty DHB. *NZ Herald*. Retrieved 15 January 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10852380.

Government Communications Security Bureau. (2011). *New Zealand Information Security Manual*. Retrieved 16 August 2012, from http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf.

Gritzalis, D. A. (2004). Embedding privacy in IT applications development. *Information Management & Computer Security*, 12(1), 8-26.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3), 155-176.

Hamill, J. T., Deckro, R. F., & Kloeber, J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems*, 39, 463-484.

Harnesk, D. & Lindstrom, J. (2011). Shaping security behaviour through discipline and agility: Implications for information security management. *Information Management & Computer Security*, 19(4), 262-276.

Irons, A. (2006). Computer forensics and records management – compatible disciplines. *Records Management Journal*, 16(2), 102-112.

Ivey, S. (2013, 2 April). PM: Privacy breaches are inevitable. *NZ Herald*. Retrieved 2 April 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10874977.

Jalal-Karim, A. (2013). Evaluating the impact of information security on enhancing the business decision-making process. *World Journal of Entrepreneurship, Management and Sustainable Development*, 9(1), 55-64.

Kemp, R. & Moore, A. D. (2007). Privacy. *Library Hi Tech*, 25(1), 58-78.

KPMG. (2012, 23 August). Independent Review of ACC Privacy and Information Security [Press Release]. *Scoop*. Retrieved 24 January 2013, from http://www.scoop.co.nz/stories/PO1208/S00351/independent-review-of-acc-privacy-and-information-security.htm.

Kwok, L. & Longley, D. (1999). Information security management and modelling. *Information Management & Computer Security*, 7(1), 30-40.

Lam, W. (2005). Barriers to e-government integration. *Journal of Enterprise Information Management*, 18(5), 511-530.

Lemieux, V. L. (2010). The records-risk nexus: exploring the relationship between records and risk. *Records Management Journal*, 20(2), 199-216.

Levy, D. (22 November 2012). Immigration staff axed over privacy breaches. *Stuff.co.nz*. Retrieved 22 January 2013, from http://www.stuff.co.nz/national/politics/7981525/Immigration-staff-axed-over-privacy-breaches.

Lips, M., Eppel, E., Cunningham, A., & Hopkins-Burns, V. (2010). *Public Attitudes to the Sharing of*

Personal Information in the Course of Online Public Service Provision. [Report], Victoria University of Wellington, Wellington, New Zealand.

Lips, M. & Pang, C. (2008). *Identity Management in Information Age Government: Exploring Concepts, Definitions, Approaches and Solutions* [Report]. Victoria University of Wellington, Wellington, New Zealand.

Lips, M. & Rapson, A. (2009). *Emerging Records Management in 21st Century New Zealand Government – Part 2.* [Report]. Victoria University of Wellington, Wellington, New Zealand.

Lips, M., Rapson, A., & Hooper, T. (2008). *Email Records Management in 21st Century New Zealand Government* [Report]. Victoria University of Wellington, Wellington, New Zealand.

Lomas, E. (2010). Information governance: information security and access within a UK context. *Records Management Journal*, 20(2), 182-198.

Manhire, T. (2012, 2 November). Privacy breaches make it plain a complete mind-shift is needed. *Issue Listener Plus*. Retrieved 15 January 2013, from http://www.listener.co.nz/commentary/the-internaut/privacy-breaches-make-it-plain-a-complete-mind-shift-is-needed/.

Ministry of Defence. (2010). *Defence White Paper 2010*. Retrieved 15 January 2013, from http://www.defence.govt.nz/pdfs/defence-review-2009-defence-white-paper-final.pdf.

Morgan, O. J. & Welch, M. (1995). Protecting confidential computer records against careless loss. *Records Management Quarterly*, 29(3), [Online].

Newstalk ZB. (2013, 29 March). Another government agency apologises for privacy breach. *NZ Herald*. Retrieved 7 April 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10874338.

Office of the Privacy Commissioner. (2007). *Privacy Impact Assessment Handbook*. Retrieved 15 January 2013, from http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf.

Office of the Privacy Commissioner. (2012). *Annual Report 2012*. (ISSN 1179-9846 Online). Retrieved 15 January 2013, from http://privacy.org.nz/assets/Files/Reports-to-ParlGovt/2012-OPC-Annual-Report.pdf.

Official Information Act. (1982). Retrieved 24 January 2013, from http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html.

Olivier, M. S. (2002). Database Privacy: Balancing Confidentiality, Integrity and Availability. *SIGKDD Explorations*, 4(2), 20-27.

O'Neill, R. R. *(2009). E-Government: Transformation of Public Governance in New Zealand?* Unpublished Master's thesis, Victoria University of Wellington, Wellington, New Zealand.

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, 18(4), 277-290.

Pathari, V. & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*, 20(4), 264-280.

Pearce, M., Zeadally, S., & Hunt, R. (2010). Assessing and improving authentication confidence management. *Information Management & Computer Security*, 18(2), 124-139.

Perri, F. S. & Brody, R. G. (2012). The optics of fraud: affiliations that enhance offender credibility. *Journal of Financial Crime*, 19(4), 355-370.

Privacy Act. (1993). Retrieved 15 January 2013, from http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

Public Records Act. (2005). Retrieved 15 January 2013, from http://www.legislation.govt.nz/act/public/2005/0040/latest/DLM345529.html.

Quilliam, R. (2013, 6 April). Another Govt privacy breach. *NZ Herald*. Retrieved 7 April 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10875826.

Rathmell, A. (1998). Information warfare and sub-state actors: An organisational approach. *Information, Communication & Society*, 1(4), 488-503.

Renaud, K. & Goucher, W. (2012). Health service employees and information security policies: an uneasy partnership? *Information Management & Computer Security*, 20(4), 296-311.

Scholl, F. & Hollander, J. (May 2003). The Changing Privacy And Security Landscape. *Business Communications Review*, 54-57.

Schou, C. D. & Trimmer, K. J. (2004). Information Assurance and Security. *Journal of Organizational and End User Computing*, 16(3), i-vii.

Schwartz, P. M. & Janger, E. J. *(2007). Notification of Data Security Breaches. Michigan Law Review, 105(5), 913-984.*

Sherif, J. S., Ayers, R., & Dearmond, T. G. *(2003). Intrusion detection: the art and the practice. Part 1. Information Management & Computer Security, 11(4), 175-186.*

Shropshire, J. (2009). A canonical analysis of intentional information security breaches by insiders. *Information Management & Computer Security*, 17(4), 296-310.

Shuttleworth, K. (2013, 28 March). EQC's IT systems frozen. *NZ Herald*. Retreived 29 March 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10874231.

Skinner, G., Han, S., & Chang, E. (2006). An information privacy taxonomy for collaborative environments. *Information Management & Computer Security*, 14(4), 382-394.

Small, V. & Chapman, K. (2013, 29 March). EQC email system shut down. *Stuff.co.nz*. Retrieved 29 March 2013, from http://www.stuff.co.nz/national/politics/8485413/EQC-email-system-shut-down.

Solms, B. (2001). Information Security – A Multidimensional Discipline. *Computers & Security*, 20, 504-508.

Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, 7(1), 50-58.

Stahl, B. C. (2004). Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics? *Journal of Organizational and End User Computing*, 16(3), 59-77.

Stuart, K. & Bromage, D. (2010). Current state of play: records management and the cloud. *Records Management Journal*, 20(2), 217-225.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems*, 111(4), 570-588.

Swire, P. P. (2003). Efficient Confidentiality for Privacy, Security, and Confidential Business Information. *Brookings-Wharton Papers on Financial Services*, 273-310.

Torrie, B. (2013, 24 March). Online medical records possible life-saver. *Stuff.co.nz*. Retreived 25 March 2013, from http://www.stuff.co.nz/technology/digital-living/8465512/Online-medical-records-possible-life-saver.

Trevett, C. (2012, 4 May). Ministry and commission to investigate foreign service leaks. *NZ Herald*. Retrieved 15 January 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10803425.

Valtonen, M. R. (2007). Documentation in pre-trial investigation: A study of using the records continuum model as a records management tool. *Records Management Journal*, 17(3), 179-185.

Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the Check-Off Password System (COPS): An Advancement in User Authentication Methods and Information Security. *Journal of Organizational and End User Computing*, 16(3), 41-58.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational,

and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4-19.

Wilbanks, L. (2008). Need to Share vs. Need to Assure. *IT Pro.* May/June 2008, 64-65.

Winjum, E. & Molmann, B. K. (2008). A multidimensional approach to multilevel security. *Information Management & Computer Security*, 16(5), 436-448.

Wise, P. L. (2011). *The implications of government departmental organisational structures on fulfilment of OIA obligations*. Unpublished MIS 580 Project. Victoria University of Wellington, Wellington, New Zealand.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, 17(4), 330-340.

8

Bibliography

[*material not cited in body*]

Committee on National Security Systems, United States of America. (2010, 26 April). *National Information Assurance (IA) Glossary* (Report No. CNSSI 4009). Retrieved 19 January 2013, from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

Gombodorj, E. (2011). *A Post Implementation Review of the Success of an e-Government Portal Project. MIM592 Research* Paper. Unpublished Master's Thesis, Victoria University of Wellington, Wellington, New Zealand.

Kidd, R. (2012, 28 October). Privacy breaches keep pouring in. *Stuff.co.nz*. Retrieved 15 January 2013, from http://www.stuff.co.nz/national/politics/7873352/Privacy-breaches-keep-pouring-in.

Quilliam, R. (2013, 22 May). Kiwis lose confidence in safety of private information. *NZ Herald*. Retrieved 25 May 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10885327.

Quinn, K.J.S. (2010). *New Zealand Computer Crime and Security Survey*. Retrieved 20 October 2012, from Internet New Zealand: http://internetnz.net.nz/sites/default/files/workstreams/2010_nz_computer_crime__security_survey.pdf.

Shuttleworth, K. (2012, 24 October). Bennett says privacy failures 'one-off'. *NZ Herald*. Retrieved 15 January 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10842525.

Trevett, C. (2012, 6 December). New MSD kiosks to roll out in May. *NZ Herald*. Retrieved 15 January 2012, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10852366.

Trevett, C. (2012, 7 December). Ministry vows to fix flaws. *NZ Herald*. Retrieved 15 January 2013, from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10852497.

Final Word Count

[*for content through sections 1 to 5*]

**

11,776