Government Information Quarterly 32 (2015) 316–322

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Government data does not mean data governance: Lessons learned from a public sector application audit

Nik Thompson [a,*], Ravi Ravindran [b], Salvatore Nicosia [b]

[a] School of Engineering and Information Technology, Murdoch University, South Street, Murdoch, Western Australia, Australia
[b] Murdoch University, Australia

ARTICLE INFO

Article history:
Received 18 November 2014
Received in revised form 11 May 2015
Accepted 16 May 2015
Available online 4 June 2015

Keywords:
Data protection
Public sector
Governance
Case study
Data management

ABSTRACT

Public sector agencies routinely store large volumes of information about individuals in the community. The storage and analysis of this information benefits society, as it enables relevant agencies to make better informed decisions and to address the individual's needs more appropriately. Members of the public often assume that the authorities are well equipped to handle personal data; however, due to implementation errors and lack of data governance, this is not always the case. This paper reports on an audit conducted in Western Australia, focusing on findings in the Police Firearms Management System and the Department of Health Information System. In the case of the Police, the audit revealed numerous data protection issues leading the auditors to report that they had no confidence in the accuracy of information on the number of people licensed to possess firearms or the number of licensed firearms. Similarly alarming conclusions were drawn in the Department of Health as auditors found that they could not determine which medical staff member was responsible for clinical data entries made. The paper describes how these issues often do not arise from existing business rules or the technology itself, but a lack of sound data governance. Finally, a discussion section presents key data governance principles and best practices that may guide practitioners involved in data management. These cases highlight the very real data management concerns, and the associated recommendations provide the context to spark further interest in the applied aspects of data protection.

1. Introduction

The massive uptake and sheer pervasiveness of technological innovation in the private and public sectors have facilitated the creation of vast information repositories. The storage, analysis and interpretation of these repositories are only possible due to the strides in technology. This analysis and interpretation allows agencies to make faster and better informed decisions to best serve the needs of the people. However, with this data storage come concerns about privacy and security. Public concerns about large scale data collection often invoke an emotional response, as the dystopian "Big Brother" image is invoked. These concerns have generally increased over time, and the recent media attention given to the topic of government surveillance does little to allay these fears.

States have addressed these concerns with statutes designed to regulate how data is handled and thus protect the people. Indeed, for many people there is an implicit assumption that public sector agencies are capable and well equipped to handle this data with which they have been entrusted. In practice, this is not a straightforward issue. Setting aside any potential issues directly within the statutes, the key issue with technical environments is that for the statutes to be enforced adequately, data custodians must be experts in both technology as well as policy.

This paper considers the management of information assets within the public sector, with specific case references made to findings by the Western Australian (WA) Office of the Auditor General and the US Government Accountability Office. Though the affected agencies specified provide high level recommendations to any adverse findings in their own reports, this paper will provide more detailed suggestions to address the deficiencies from an organizational data management perspective.

2. Background

The WA Office of the Auditor General benchmarks selected public sector agencies primarily against the ISO 27002 international standard for Information Security (International Organization for Standardization, 2013b) while also referring occasionally to other established standards. As the standards used are international or nationally recognized, this paper will be relevant for any other organizations that have information assets to manage and protect. Furthermore, it is to be noted that many of the issues identified are not directly linked to the standards or statutes in play, but relate more to general principles of how private data should

* Corresponding author.
E-mail address: n.thompson@murdoch.edu.au (N. Thompson).

http://dx.doi.org/10.1016/j.giq.2015.05.001
0740-624X/

be handled. In a similar way to the WA Office of the Auditor General, the US Government Accountability Office refers to established legislation and standards such as the US Federal Information Security Management Act of 2002 (FISMA) when determining compliance within agencies (United States Government, 2002). FISMA recognizes the importance of data protection and mandates the protection of US federal information and information systems through various controls, including yearly audits to be conducted in federal agencies.

The ISO 27002 standard is a code of practice for information security; as such it contains a large number of best practices and controls which may be implemented to support the development of organizational security standards. These controls are placed into groupings to identify relevant subject areas in familiar domains such as physical and environmental security, HR security, asset management and communications security. As ISO 27002 is not a management standard it is not possible to obtain certification to this standard, instead it is to be considered complementary to the ISO 27001 — Information Security Management certification (International Organization for Standardization, 2013a) as it provides greater detail and specifications of controls. In Western Australian public sector agencies, compliance with these standards is not mandatory, however as the framework is internationally recognized and proven, it forms a useful baseline against which auditing and evaluation may be performed. A further benefit of using such widely recognized standards is the fact that there is often a relatively direct mechanism by which to map between controls in the various standards. For instance, a mapping has already been created across ISO27001/27002, the SANS 20 Critical Security controls and the NIST SP 800-53 (Johnson, 2013).

On March 27, 2007, Justice (Commissioner) Kevin Hammond of the WA Corruption and Crime Commission (CCC) made what is considered by many as a landmark frank and honest statement about the behavior of some senior public servants in Western Australia. Justice Hammond stated "*it is clear there are many quite influential public officers who wouldn't recognise a conflict of interest if it walked up and kicked them in the backside*" (Hammond, 2007). In a report to the WA Parliament in 2010, the CCC reported on the alleged access of a confidential information system by an Associate to a Judge of the District Court of Western Australia. The Judge's Associate had numerous associations with drug dealers and had inappropriately accessed information from the Court's information systems. This report re-emphasized the CCC view that that there was no such thing as an innocuous enquiry of a confidential database when the persons driving the enquiry are operating with criminal intent (Parliament of Western Australia, 2010). In a similar vein, the US Government suffered a historically significant and embarrassing security leak when a relatively junior US service officer, Bradley Manning was able to access and subsequently release thousands of US government classified documents in 2010.

The above examples are indicative of the scale and potential for breaches within the public sector. The WA Office of the Auditor General has made many findings and recommendation on the behavior and practices of public sector agencies in managing their information assets. The US Government Accountability Office in Sept 2013 found that almost all of the major federal agencies had flaws with their controls in detecting and limiting access to information systems (US Government Accountability Office, 2013).

There is an expectation from the community that information collected, accessed and used by public sector agencies will be protected and also used only for the purpose it was intended. There is also a community expectation that there will be standards, practices and procedures in relation to data access, data privacy, data security and data disposal with overarching data governance in place.

The following sections of this paper will discuss some examples of improper practices identified by WA Office of the Auditor General in the area of controlling and protecting information assets specifically in an information systems environment. These examples are gleaned from the Information Systems Audit Report (Western Australian Auditor General, 2013) which details an application audit conducted on five applications at four agencies. The audit process for these business applications involved a systematic review of the documentation and operational aspects of the applications to provide assurance in the following domains:

1. Policies and procedures.
2. Data preparation (input and processing).
3. Interface control suitability to enforce data quality requirements.
4. Maintenance of master data files.
5. Audit trail of activities.
6. Segregation of duties (staff must perform duties relevant to their role only).
7. Backup and recovery provisions in the event of system malfunction or disaster.

The agencies were selected due to the fact that inappropriate management or controls in these agencies would cause a significant impact. The four agencies chosen were Western Australia Police, Department of Finance, Department of Mines and Petroleum and Department of Health (2 applications). While there were minor issues identified in all of the agencies, the cases presented in subsequent sections will elaborate on the findings in two of these agencies as these are particularly problematic and very relevant to the data management focus of this paper. The paper will go on to introduce some high level recommendations and potential solutions to mitigate the effect of these issues.

Although the case study primarily uses examples from the WA Public Sector, it is not implied that the problem is unique to Western Australia. It is the strong belief of the authors that the issues reported are consistent across the globe and the recommendations may serve as a guide to IT practitioners in various industries when they evaluate their data management protocols.

3. The importance of data protection

Data management is defined within the DAMA Data Management Body of Knowledge (DAMA-DMBOK) as the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information asset (Mosley, Brackett, Earley, & Henderson, 2009).

There is a justifiably strong emphasis on the protection of information assets within DAMA-DMBOK. Public sector agencies in the course of their work routinely collect a vast amount of information relating to organizations, partner agencies and of course individuals. The Western Australia Police Service for example maintains details of the criminal activity, allegations, and investigations on many individuals within Western Australia, as well as detailed historical records, the integrity of which is crucial in order for the Police Service to fulfill their duties. Using this agency as an example, unauthorized access of their information holdings may have the potential impact of:

- Causing reputational and physical damage to individuals or organizations.
- Tipping off individuals to ongoing investigations.
- Causing loss of confidence in the officers of the service.
- Creating operational delays and inefficiencies due to internal reviews and investigations.

The Western Australian Planning Commission as another example maintains details of future plans. Within the repositories of this agency lie details of potential land and building deals, preferred contractors and details of tenders. Should this information fall into the wrong hands, it may have the potential impact of:

- Individuals or companies taking advantage of insider information to benefit financially from land procurement.

- Loss of confidence in the Planning Commission and its work.
- Delays in vital planning work due to court action and investigations.

As seen, various public sector agencies hold crucial information repositories, the integrity and security of which directly affect their ability to perform their duties. The nature of the information repositories is diverse, and different agencies may hold quite different information — however these are all unified by the same principles, that the information must be safeguarded and protected adequately in order to prevent severe repercussions.

Within the Western Australian Public Sector, the State Records Act 2000 governs public sector agencies' recordkeeping practices. Under the Act, the WA State Records Commission produces legally binding principles and standards to govern agencies' recordkeeping practices (State Records — Government of Western Australia, 2013).

4. Case study 1: Firearms Management System

The Western Australia Police is responsible for maintaining and securing the Firearms Management System (FMS) that contains the license information for all registered Western Australians with a firearm license. Information is collected via a paper based application submitted to the WAP through the Australia Post. Firearm ownership is tightly regulated, and in accordance with the Firearms Act 1973, an owner of a firearm must present written permission from a property owner to satisfy the genuine reason for an applicant to use a firearm for recreational shooting. An exception to this documentation requirement is if the individual himself is the owner of a suitable property for the category of firearm being licensed. The police may then request further evidence or inspect the property to ascertain suitability. In all cases, applicants must also complete firearm awareness training and submit to a probity check to consider if the person is a fit and proper person to be granted a license. Furthermore, licenses from other jurisdictions, i.e. other states in Australia are not recognized.

Through the course of the OAG audit, a number of alarming findings were made. These included:

a) Firearms were not being reliably recovered from deceased estates. Sometimes the FMS would not update a deceased license holder until 280 days after the fact, which left the firearms unaccounted for during this time.
b) Applicants were submitting template copies of property owner permissions to own firearms on specific properties. The FMS had no way of comparing property owner permission letters to identify repetition or forgery. This led to the audit revealing that one property owner had provided property letters to over 270 applicants in a little over a year, enabling many of these to subsequently acquire firearm licenses.
c) The system reported firearm possession by people assessed as unfit to have a firearm. Up to 50% of these individuals labeled “unfit” did not actually possess a firearm, yet the system was not being updated to reflect these changes. This obscured the valid data, making it difficult for officers to produce usable reports of “unfit” firearm holders.
d) Manual processing was required, even for basic correct operation of the FMS. This is a common source of data entry issue and administrative errors call into question the integrity of data.

4.1. Findings

The audit revealed an alarming lack of control over data input, processing and reporting. As a result the auditors reported that they had no confidence in the accuracy of basic information on the number of people licensed to possess firearms or the number of licensed or unlicensed firearms in Western Australia. In the absence of reliable information, the local authorities are unable to effectively manage firearm licensing and regulation in the state.

4.2. Recommendations

Specific and automated processes need to be implemented to support the integrity and timely input of information into Firearms Management Systems. This is the only way to ensure that firearms can be suitably managed. This could be enacted by strengthening the data governance in the form of formalized policies and procedures which take into account the entire data life cycle including both automated and manual tasks. This will ensure that information updates are propagated in a timely fashion and that the integrity of the data is preserved, regardless of which part of the system it lies in. A complementary step would be to implement more specific data security management controls in the form of change control logging of applications and back end servers and rigid system authorization access controls to ensure accountability of data updates.

5. Case study 2: Emergency Department Information System (EDIS)

The Emergency Department Information System (EDIS) is a system utilized by the Department of Health to capture patient data in real-time and to support emergency departments' operations. The system collects personal patient data, time of admittance, arrival mode, diagnosis, outcome, and discharge information. This data can be used with other patient data to evaluate trends, percentages of output or transfers within given time standards, and re-admittance statistics (Western Australian Auditor General, 2013). This system is based upon the widely used and mature iSoft Emergency Department platform (Computer Sciences Corporation, 2014).

5.1. Findings

The audit found that the EDIS implementation in Western Australia included very limited system controls to detect and prevent users from gaining unauthorized access to confidential information. EDIS did not require validation of the identity of each person making clinical data entries, as possibly the implementers considered speed or ease of use to be more important than authentication constraints. As a result of this, individual staff interactions with the system could not be identified. Therefore, the Department of Health could not determine which medical staff member was responsible for clinical data entries made in EDIS or for data entry mistakes that may have resulted in adverse patient care.

5.2. Recommendations

The information workflow needs to be refined to include appropriate change management controls so that unauthorized or inappropriate changes are prevented or at least tracked after the initial entry of data into EDIS. This is achievable by requesting these features to be implemented in the supporting software itself, after which time the usage policy may be updated to reflect the new requirement. The implementation of this feature would also require changes at an operational level, as staff would be required to follow a revised data entry procedure. At an administrative level, an overhaul of the authentication mechanisms is required to integrate existing authentication (e.g. staff ID card) into the information workflow in EDIS. This will facilitate the required individual logging of activities and changes made in the records system. Alerts may be set up for the relevant data managers or health department nominee to monitor activities and changes made in domains that may be considered to be high risk.

The necessity for individual logging of user activities will also require users to comply with an organizational password policy. The high risks associated with unaccountable or anonymous access to this critical information system may be mitigated by appropriate access policies,

including password policies. Further operational level changes could be considered for preventative and detective controls including routine audits to help limit any further unauthorized access or disclosure of patient records.

6. Observations

These case studies do not represent isolated, uncommon occurrences, but are rather indicative of more widespread data management issues within large agencies. In many cases, agencies start with adequate plans, but struggle to ensure compliance with the policies and standards laid out during project design. Compliance is also affected by the often lack of appreciation of the need to protect their information assets. Thus, risks may be taken with critical pieces of information simply because their value is not understood. Even in the absence of wrongdoing, lax information security practices can cast doubt on the quality of the data.

An interesting commonality is present in the details of the two cases. The weaknesses do not appear to arise from existing business rules or from the capabilities of technology itself, but rather from the unique arrangement of these components into a particular implementation. By attempting to retro-fit incomplete or improperly configured technical solutions without considering the wider organizational data management landscape, the overall integrity of the data is impacted throughout its life cycle. Table 1 summarizes the findings of the application audit organized by the same seven knowledge areas listed above.

Of the above knowledge areas, issues were noted in data preparation, interface controls, audit trail and segregation of duties — all of which are indicative of the state of data governance in the respective agencies. Noteworthy issues were not specified in the other knowledge areas of business rules, master file maintenance or backup and recovery.

In the public sector, business rules are often the subject of substantial refinement and years of iteration. Furthermore they are often based on existing statutes as the agencies are already likely to be experienced in handling the very same information albeit in hard copy form. In the policy and procedures domain, the business rules themselves are not the issue but rather the application rules and the workflow surrounding particular technical solution. The maintenance of master records and files is also acceptable in many cases; once again this is likely to be transference of well understood techniques that have been previously applied to traditional record systems. These best practices originate from business record keeping regulations (e.g. State Records — Government of Western Australia, 2013) as well as the operational brief of database administrators whose sole charge is to ensure that database is running and operational at all times. In the same way, other operational database administration tasks such as backup and recovery are often handled satisfactorily too. There are a tried and tested set of technologies and strategies that any sufficiently well-funded organization may apply to ensure that data is backed up, safe and recoverable.

What has been demonstrated is a distinct lack of proper data governance. Data governance is a set of processes that ensures that important data assets are formally managed throughout the enterprise (Mosley et al., 2009). Within the WA Public Sector, the Australian Government Information Security Manual serves as a standard for the security of government information systems (Australian Signals Directorate, 2014). The WA Auditor General expects the WA Public Sector agencies to follow the principles of the Information Security Manual which lays out in detail the mandatory controls required to ensure sound data management. However as evidenced by the above case studies, in reality this expectation is not met.

7. Data governance

Data governance may be considered as a central data management function in that its influence is felt within all IT and data management disciplines. The activities undertaken through a data governance initiative provide the checks and balances which change how all of the other functions are performed. In short, data governance is simply the "government" of data and focuses exclusively on the management of data assets. To carry this analogy further — data governance may be seen to operate on several key principles.

Firstly there is a responsibility for legislative functions (including standards documentation and policies), judicial functions (the process of addressing problems or breaches) and executive functions (administration and ongoing service provision). These responsibilities are shared across various organizational units in keeping with overall data governance principle of shared decision making. Secondly, data governance operates at multiple levels. In the same way that state and local governments operate in their own spheres — data governance includes broader organizational (i.e. state) governance as well as local level policy making and planning. Finally, there is a separation of duties between organizational units. Checks and balances may therefore be provided as activities such as legislative or executive functions are carried out by different stakeholders.

Coordination of decision making in data (and in the more general IT) governance structures may be seen as a hierarchical arrangement in which superiors delegate to and communicate their wishes to their subordinates, who in turn delegate their control and so on. Information flows from top to bottom and vice versa (Peterson, 2004). The four major roles are those of the executive sponsor, the chief steward, and the business and technical data stewards (Weber, Otto, & Österle, 2009). These roles are detailed in Table 2.

Table 1
Cross-case comparison.

	Firearm Management System	Emergency Department Information System
Policies and procedures	Business rules are acceptable. (Dictated by Firearms act) Application rules are not satisfactory, e.g. system only updates for renewals, and not when firearm holders are deceased.	Business rules are acceptable.
Data preparation (input/output/processing)	Numerous weaknesses leading the auditors to conclude that they have no confidence in the data.	Numerous weaknesses which affect clinical work practices and the integrity of the data
Interface controls	Issues include the lack of ability to produce basic reports on properties.	Issues include the lack of change tracking. Thus unauthorized or inappropriate changes are possible after initial entry.
Master file maintenance	No issues noted.	No issues noted.
Audit trail	Issues include the need or workarounds and manual processing to effectively operate. This threatens the integrity of data and makes the system harder to audit due to double-handling of the same data.	Issues include limited system controls existing to detect and prevent users from gaining unauthorized access to confidential information. The application is configured with minimal logging; therefore individual activity may not be audited.
Segregation of duties	Issues found. These include lack of application policies to log access, changes or to review database usage. Activity is only logged at the application level and not at the database level, therefore it is possible that role based access is not enforced appropriately.	Issues found. As there are no useful activity logs, it is not possible to link access (authorized or otherwise) to staff. There is also no application requirement for staff to verify ID when making clinical entries, therefore it is possible that access of staff is not appropriately segregated.
Backup and recovery	No issues noted.	No issues noted.

Table 2
Major data governance roles.
Adapted from Weber et al., 2009.

Role	Description	Organizational position
Executive sponsor	Provides funding, strategic direction, advocacy and oversight (English, 2009; Newman & Logan, 2006)	Executive or upper management (e.g. the organizations CIO)
Chief steward	Enforces standards and puts the decisions of any governance board or committee into practice (Dyché & Levy, 2011; Marco, 2006)	Senior manager — see organizational position for stewards below.
Business and technical data steward	Details corporate wide standards and policies for his or her own area of responsibility. This can take a business or technical perspective, in which the technical stewards also contribute further information including standardized definitions and system details (Dyché & Levy, 2011)	Business stewards are recruited from a relevant business unit or department. Technical stewards must possess IT skill and therefore often originate from the IT department.

Research into the more general domain of IT governance is relatively mature, with several decades of publications behind it. However it is of note that the domain of IT governance does not fully encompass all of the required principles for successful data governance (Wende, 2007). Specifically, the formula for data governance success requires close collaboration between business leaders and the technical professionals — something which is often lacking.

Many major data governance issues may be remedied by relatively few key governance principles. For the purposes of discussion, these will be broadly addressed in terms of people, standards and compliance.

7.1. People

The leadership and vision of a Chief Information Officer are crucial for ensuring the success of any data governance initiative. An effective leader, who clearly communicates and directs the direction of the organization can accomplish things that would be impossible otherwise. This person is responsible for implementing data governance related decisions, and serves as a high level point of contact for business leaders to report to. Depending on the scale of the organization, a dedicated data governance office may be established. This will provide support for the activities of data stewards at all levels. Data stewardship is primarily a means of acknowledging formal accountability for the control of certain data assets. A data steward is not an IT representative, but rather a subject matter expert, or stakeholder with an existing interest in the data. Data stewards manage data assets on behalf of others, and represent the interests of all stakeholders, not just the group from which they are recruited. This does not fix a single point of responsibility, but conveys the idea that government officials and organizations are responsible for the care and protection of all information, regardless of its original source (Dawes, 2010). For instance, in the case of the Firearms Management Service, an ideal choice of data steward would be a law enforcement professional who interacts with the FMS on a regular basis, understands the data and appreciates the need for improvement and data quality. He or she may then work with higher level policy makers to establish formal strategies and later to ensure that they are implemented.

7.2. Standards

Standards and policies are very often the first thing that springs to mind when the term data governance is mentioned. Policies are statements describing the fundamental rules applicable to the use of any organizational resource. In the context of data, this will include rules as to how data will be acquired, translated, stored, secured and made available to legitimate users. Standards describe how to do something, for example the minimum requirements for security or network access. Policies on the other hand explain which activities are permitted or otherwise. Topics covered may include low level aspects such as the data architecture, but also operational matters such as quality expectations, security rules, privacy policies and how and if the data is to be shared. These documents are generally drafted by data management professionals and are tailored to the unique needs of the project or organization. However, there are numerous existing industry standards and best practices which provide guidance and an adequate baseline. In fact, the sheer volume and availability of knowledge in this area mean that there is little excuse for an organization to not have adequate standards. Once put in place, these standards must be adequately communicated and explained to users to ensure compliance, and regular audits must ensure that they are being followed adequately. The case studies above suggest that issues only become apparent if the system is thoroughly audited, therefore simply having an adequate set of standards and policies may not be sufficient unless compliance is evaluated.

7.3. Compliance

No industry or department is exempt from governmental or industry regulations, however these have little value unless there are measures to adequately track and ensure compliance. In many cases, the nature of the industry means that there are already well established and rigid rules as to how data is to be handled and processed. Furthermore, there may be an understanding that compliance is compulsory with possible penalties for non-compliance. Constraints on how data is handled may come from several areas such as proprietary business concerns, legislation, or industry regulation. These must be balanced to ensure that legitimate data access needs are supported. However, as information workers inside government agencies may often freely interact with large repositories of confidential data on a daily basis, there is a potential for the value and sensitive nature of the information to be forgotten. Data governance guides how controls are implemented and also provides mechanisms to monitor compliance and benchmark against established baselines. To ensure compliance, checks and balances must be built into the routine work processes to reinforce correct behavior. Furthermore, periodic auditing must be conducted to establish a benchmark of the agency's current compliance level.

8. Discussion

Many of the stated standards, polices and mandates are significant documents involving many hours to digest and comprehend. The challenge facing the public sector is that these policies and standards are not easily understood by the majority of public sector workers. The younger work force, who readily shares personal information with their friends and even strangers in today's culture of social media and blogging arguably might not fully understand the concept of information confidentiality.

The principle of protecting the information worker from themselves is often suggested for public sector agencies. Certainly, the literature supports the view that human factors constitute a major threat to computer security, and comprehensive security models now include the human element as a vital aspect of IT security that must be controlled and secured (Islam & Dong, 2008). The acknowledgement of the risks introduced by human factors is not simply limited to the academic community — criminals are also aware of this factor. In fact, according to the 2013 annual data breach report, 29% of the data breaches investigated were found to have leveraged social tactics – the human factor –

in circumventing data security (Verizon, 2013). Attackers have evolved their focus from technical weaknesses toward human vulnerabilities and unfortunately research and industry practices have not adapted at the same pace (Hong, 2013). It is becoming apparent, that "the human factor is the Achilles heel of information security" (Gonzalez & Sawicka, 2002), and successful data governance hinges on an understanding of human factors.

At an operational level, activities such as more stringent access management and ensuring routine audits may yield benefits. Although it can be argued that many activities simply address the symptoms rather than isolating the root causes of the issues. Based on these authors' experience in data management in large public and private sector agencies, three best practices have been identified that may enhance the potential for success. These are outlined below.

Firstly, keep it simple. Policy documents and warnings need to be presented in simple language with clear examples of breaches and consequences. Users often rely on existing mental models and heuristics when faced with warnings. In short, if they are able to work unhindered even after ignoring the warning or policy then they may continue to persist in the unsafe behavior (Bravo-Lillo, Downs, & Komanduri, 2011). Security should not be an abstract concept, but be something that is relatable and easily linked to the user's own day to day activities. For instance, explaining the impact of an information leak may be more convincing than simply stating that information sharing is not allowed. Legal departments may weigh in on this matter as there is some thought that condensed or simplified standards and polices may limit the agency's ability to prosecute a staff member for illegal activity. However we believe that prevention is better than prosecution and stopping many from inadvertently committing a possibly criminal act is a worthy goal to achieve. By providing different perspectives on a single policy document (e.g. Highlights, Main policy document & Quick reference guide), a satisfactory balance between comprehensiveness and understandability may be reached.

Secondly, compliance should be easier than non-compliance. We acknowledge that this is easier said than done, but it is an aim to strive for. In a busy and stressful work environment, users very often default their behavior to the easiest option. This is recognized as a factor involved when users assess security risks. For instance, when assessing an appropriate course of action to follow, users will often subconsciously assess the cost of the action and thus influence their behavioral intention (Rogers, 1975). If the cost (in this case, time taken or difficulty) to act in a secure manner outweighs the benefits, then users are less likely to perform the secure action. A large suite of access and information monitoring tools are available which can streamline legitimate access of data and thus guide users toward a more secure and controlled "default" behavior.

Thirdly, reinforce the positive. Organizational policies tend to focus on negative behavior but do not recognize the good work of many. Positive reinforcement will provide a friendly way to remind users that their actions are potentially monitored and audited and that as individuals, their actions do count. Furthermore, the creation of an appropriate security culture within the organization will influence the actions of entire teams. According to Technology Threat Avoidance Theory (Liang & Xue, 2010), when users lack knowledge the social environment provides cues to action. Furthermore, the social environment creates a normative influence which encourages users to behave in a manner which is consistent with the rest of the group. Therefore this group influence may yield significant improvements in terms of overall organizational compliance.

9. Conclusions

This paper has presented findings from a recent application audit of public sector business systems conducted by the Western Australian (WA) Office of the Auditor General. The audit revealed weaknesses in many of the knowledge areas including data preparation, interface controls, audit trail and segregation of duties. What is conspicuous in these findings is the commonality that these knowledge areas have: They are all domains which would be directly influenced, improved and monitored by a sound data governance initiative.

The case study examples in this paper focused on public sector agencies as they are typically required to provide more transparency and are subject to mandated audits to evaluate their compliance with policies and standards. Private corporations, on the other hand are commonly far less transparent with knowledge of audits or data breaches, often only submitting information when specifically directed or due to legislative requirements.

Members of the public have a reasonable expectation that their private data will be protected, but in reality this expectation is not met. Public sector agencies should aspire to be the "Gold Standard", and use their highly visible position to establish themselves as industry leaders. This will encourage private corporations to follow suit and aim to conform to the standards set by the public sector.

A crucial side to any standardization or compliance exercise is that of auditing. These cases are indicative of the nature of problems that remained undetected until externally audited. The only unsolvable issues are those which have not been detected yet. Therefore an important lesson for current systems and policies is that robust and transparent auditing and evaluation must be routinely conducted.

Finally, these findings highlight the dangers of a disconnect between organizational policy and the specific technical systems in place. Very often technical solutions are put into place without considering the wider governance and policy framework (or vice versa), thus resulting in a dangerous separation. A successful solution will be tailored to the unique organizational context and will be the result of a strong partnership between IT professionals and those who work with the data. IT professionals with sound understanding of data management in all its facets (governance, development, security or operations) must inform and enforce what is required to protect data integrity to allow it to work for organizations as a benefit; not as a hindrance. Perhaps what Justice (Commissioner) Kevin Hammond should have said on March 27, 2007 was: "it is clear there are many quite influential public officers who should really have listened to their experts and put in viable solutions instead of ones that will simply set them up to fail".

References

Australian Signals Directorate (2014). *ISM — Information security manual Retrieved June 12, 2014* .

Bravo-Lillo, C.C., Downs, L., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, *9*(2), 18–26.

Computer Sciences Corporation (2014). iSoft Emergency Department. Retrieved 12 Nov, 2014, from http://www.isofthealth.com/en/Solutions/Department/Emergency.aspx

Dawes, S.S. (2010). Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, *27*(4), 377–383.

Dyché, J., & Levy, E. (2011). *Customer data integration: Reaching a single version of the truth*, *vol. 7*, John Wiley & Sons.

English, L.P. (2009). *Information quality applied: Best practices for improving business information, processes and systems*. Wiley Publishing.

Gonzalez, J. J., & Sawicka, A. (2002). A framework for human factors in information security. *In International Conference on Information Security, Rio de Janeiro*. World Scientific and Engineering Academy.

Hammond, K. (2007). Corruption, Integrity & the Public Sector. Retrieved 1 Jan, 2014, from http://www.ccc.wa.gov.au/Publications/Reports/Speeches/Speech%20by%20Commissioner%20Kevin%20Hammond%20%E2%80%93%20to%20IPAA.pdf

Hong, J. (2013). Computer Security needs refocus, and be nice about it. *Communications of the ACM*, *56*(6), 10–11.

International Organization for Standardization (2013a). ISO/IEC 27001 — Information security management. Retrieved 2nd June 2014, from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

International Organization for Standardization (2013b). ISO/IEC 27002 — Security techniques — Code of practice for information security controls. Retrieved 2nd June 2014, from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533

Islam, S., & Dong, W. (2008). Human factors in software security risk management. *In Proceedings of the first international workshop on Leadership and management in software architecture, Leipzig, Germany* (pp. 13–16). ACM.

Johnson, B. (2013). Mapping the SANS 20 to NIST 800-53 to ISO 27002. Retrieved Nov 14, 2014, from http://systemexperts.com/media/pdf/SystemExperts-SANS20-1.pdf

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.
Marco, D. (2006). Metadata management & enterprise architecture. *DM Review*, *16*(10), 17.
Mosley, M., Brackett, M., Earley, S., & Henderson, D. (2009). *The DAMA guide to the Data Management Body of Knowledge*. NJ, USA: Technics Publications, LLC.
Newman, D., & Logan, D. (2006). *Governance is an essential building block for enterprise information management*. Stamford, CT, 4: Gartner Research.
Parliament of Western Australia (2010). Corruption and Crime Commission Report on the Investigation of Alleged Public Sector Misconduct in Relation to the Activities of an Associate to a Judge of the District Court of Western Australia — Report No. 8. Retrieved Jan 01, 2014, from http://www.ccc.wa.gov.au/Publications/Reports/Published%20Reports%202010/Precis%20of%20Report%20on%20Activities%20of%20Associate%20to%20a%20Judges%20of%20the%20DCWA.pdf
Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, *21*(4), 7–22.
Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, *91*(1), 93.
State Records — Government of Western Australia (2013). Recordkeeping policies and standards. Retrieved 1 July, 2013, from http://www.sro.wa.gov.au/state-recordkeeping/recordkeeping-policies-and-standards
United States Government (2002). Federal Information Security Management Act (FISMA). Retrieved 12 July, 2014, from http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
US Government Accountability Office (2013). Federal Information Security: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness. Retrieved 2 Feb, 2014, from http://www.gao.gov/products/GAO-13-776
Verizon (2013). *Industry Data Breach Report.* Retrieved 2nd April, 2014, from http://www.verizonenterprise.com/DBIR/2013/.
Weber, K., Otto, B., & Österle, H. (2009). One size does not fit all — A contingency approach to data governance. *Journal of Data and Information Quality (JDIQ)*, *1*(1), 4.
Wende, K. (2007). A model for Data Governance-Organising accountabilities for Data Quality Management. *In 2007 Australasian conference on Information Systems, Queensland, Australia* (pp. 417–425). AIS.
Western Australian Auditor General (2013). Information Systems Audit Report. Retrieved October 11th, 2014, from https://audit.wa.gov.au/wp-content/uploads/2013/06/report2013_11.pdf

Nik Thompson is the Academic Chair of Cyber Forensics and Information Security at Murdoch University in Western Australia. He holds MSc and PhD degrees from Murdoch University and teaches in the area of Computer Security and Data Resource Management. His research interests include affective computing, human–computer interaction and information security.

Ravi Ravindran is the Director for Business Systems in the Western Australia Department of Corrective Services. He has extensive career experience in various public sector agencies, specifically focusing in data management and control.

Salvatore Nicosia is a Postgraduate in the School of Engineering and IT at Murdoch University. His career includes diverse roles ranging from many years on deployment with the United States Armed Forces to more recent academic appointments teaching at Murdoch University.