BUSINESS
SCHOOL

THE UNIVERSITY OF
SYDNEY

BUSINESS INFORMATION SYSTEMS

Business Information Systems (BIS) is an exciting, fast changing field. In today's world BIS professionals and graduates play a key role in enabling organisations to meet their strategic goals, drive business innovation and assist businesses to comply with increasingly complex legal requirements.

An understanding of BIS is important to the work of all business professionals including: executive managers who determine the organisation's strategic direction; information professionals who design and deliver new information services; accounting and financial managers who use information systems for financial management and business reporting; and marketing and sales managers who use information systems to track customer buying patterns and to promote new products.

Employers are looking for employees who understand both business and technology issues and have the skills and knowledge to contribute to the shaping of their organisation's BIS strategy and planning.

Established in 2002, the Discipline of Business Information Systems at the University of Sydney Business School, is a multidisciplinary team with a strong commitment to practice based industry-relevant teaching and research.

Our research focuses on:

- Information systems strategy
- Project & change management
- Information policy and knowledge management
- Information risk, assurance and
- Governance
- Enterprise systems and business
- Process management
- Technology driven business
- Innovation
- Government information systems
- Decision support and business intelligence systems.

We offer degree programs at both undergraduate and postgraduate level that are accredited by the Australian Computer Society (ACS).

Managing Identities:
from government e-commerce
to national security

Dr. Philip Seltsikas

BIS WP2009-01

BUSINESS INFORMATION SYSTEMS
WORKING PAPER SERIES

ISSN 1837-1744

Managing Identities:
from government e-commerce to national security

Abstract
This paper is concerned with the challenges and issues facing US State and Federal government in attempting to develop, implement and maintain electronic identity management systems. Primary data was collected from four key stakeholders in two US States and from five key stakeholders at the US Federal government (two 'agencies'). A qualitative analysis identifies four dominant themes and a trend that is shifting government identity management efforts from supporting government e-commerce transactions to improving national security. Central to this trend are key structural changes in the Federal management and budgeting of identity management initiatives. Projects that involved multi-million dollar investments in facilitating government e-Commerce transactions appear to have lost momentum, putting those huge investments at risk. Furthermore, the research findings suggest that US government electronic identity implementers depend heavily on exogenous standards, with anecdotal evidence indicating that this may be a very risky approach.

Keywords: e-Government, identity management, e-Commerce, government security, US Federal Government, US State governments

Introduction

This paper presents research results from a study conducted in the USA that sought to understand the key challenges and issues facing State and Federal government in their efforts to develop and implement 'identity management', policies, systems and technologies. Identity management (IdM) is concerned with the creation and processing (authentication) of citizens, businesses and governments' digital identities. IdM has received little attention in academic literature of a non-technical nature (Mahmood et.al., 2008), and even less so when we look at the e-Government literature.

The need for understanding and facilitating secure electronic identification of persons (natural or legal) is manifest. When traditional government transactions are 'moved' to the e-Government setting (Dearstyne 2001; Layne & Lee 2001), the remoteness of the users who are normally 'transacting' using the Internet or other electronic means produces a strong requirement to ensure that the person (natural or legal) transacting on-line is indeed who they say they are.

Governments continue to invest heavily in programmes and projects to facilitate and foster the adoption of their on-line services. The aims of this research were to develop an understanding of the critical issues facing Federal and State government in the USA with respect to their implementation of IdM technologies and policies. In doing so, the results highlight four information management themes that represent government challenges for IdM. The research process involved nine interviews with senior government officials at both State and Federal level. It was conducted at the end of 2008. Due to the sensitivity of the data to the respondents, their anonymity was assured, and the results have been necessarily generalized in this paper.

Identity Management in Government

The management of electronic identity (or Identity Management, IdM) has been high on the agenda of most governments for the last five to ten years. The 'market' for secure IdM solutions seems to be very large indeed, particularly if industry analysts' forecasts are correct. The Stanford Group (2007), for example, estimates annual spending in the US on government IdM-related initiatives for the period 2004-2011 to be almost US$9,480 million. In the USA, there has been a considerable effort to 'solve' the IdM security problem for e-Government. In 2004, the Federal US Government started a Pan-US presidential project to research, develop and implement an architecture for the management of IdM that was designed to support 26 core e-Government applications (e-Authentication, GSA, 2006). Holden & Millet (2005) had noted the requirement for 'electronic authentication' in e-Government. They highlight the fact that electronic IdM is not simply a technological solution, but a "balance between access, security, authentication, and privacy" (ibid, p. 367).

In Europe, and other countries there have also been initiatives similar to those in the USA. The European Commission has funded research to design a secure architecture for cross-border IdM at a pan-European level. Otjacques et al. (2008) provide a comparison of individual IdM approaches across 18 of the 25 EU member states, focusing particularly on the use of Single Identification Numbers (SINs).

The topic of 'electronic identity' is sparsely referenced in the Information Systems (IS) academic literature and is mostly found in the more technical computing journals that deal with the underlying security technologies such as 'cryptography' (see for example, Miyata et.al. 2006). Context and use (from an IS perspective) are rarely considered in depth. Published research directly related to the topic of this paper is sparse, especially in the established IS journals.

In reviewing the IS literature for relevant existing knowledge, several studies are notable. Gil Garcia et.al (2007) look at issues surrounding management and benefits expectations in e-government projects where disparate stakeholders are required to collaborate to exchange information. This relates to the *context* of IdM as identity information is often 'managed' across disparate (and often normally unrelated) entities.

Pavlou et.al (2007) deal with the problem of uncertainty in online relationships. This is an area which IdM tries to mitigate through both technical and non-technical means. Pavlou et.al. argue that online relationships between buyers and sellers (presumably unknown communicating entities) can be better understood if they are viewed as "agency relationships" and that "perceived uncertainty is a barrier to online transactions" (p. 131).

Hui et.al. (2007) explore aspects relating to user's attitudes with respect to 'privacy' in using an online web-site and imparting personal data. Their work empirically demonstrates that on-line users really do care about how their personal data (including identity data) is 'managed' on-line.

Carter & Bélanger (2005) have produced a 'model of e-government adoption' that showed 'trustworthiness' to be an important factor to citizen uptake of government services. In Carter & Bélanger's work trustworthiness can be influenced by a 'privacy statement' on the on-line service website. As IdM technologies also have the potential to influence trustworthiness Carter & Bélanger's work can be used as a starting point.

Moon & Norris (2005) examine a wide range of factors that may impact upon the implementation of e-government initiatives and find that 'managerial orientation' and 'government capacity' can have effect. Their work indicates that studies concerning the implementation of e-government need to consider multiple possible factors, many of which are "institutional and environmental"; factors which may not be directly related to technology.

Straub & Welke (1998) explore the issue of IS security and propose a risk management analysis approach for the protection of a corporation's information assets. IdM policies and systems are similarly concerned with risk management in the specific domain of authorisation, authentication and identification.

In recent years a variety of technologies have been developed to provide and manage the security of online identity data. These include PKI (Public Key Infrastructure), smartcards, and identity federation standards such as Shibboleth (Miyata et. al. 2006), used in identity federations in higher education (e.g. Athens authentication, 2008); the security assertion markup language (SAML) (Miyata et. al. 2006), and WS-* (ibid.). It is not the aim of this paper to review the multitude of technologies, emerging standards and legislation surrounding IdM, but it should be noted that these multiple technologies have failed to provide the secure and trusted environment believed necessary for high security on-line services to flourish.

Research Questions and Methodology

A critical methodological point to note with the research reported in this paper is that the data was collected directly from *the setting* and allowed *the respondents* to delineate what was important to them. The researcher did not predefine what was important by developing *a priori* theoretical constructs or models. Essentially this research has been conducted using *post-positive* methodological assumptions (ontological (Berger & Luckman 1967, Walsham 1995), epistemological, and axiological (Lincoln & Guba 1985)) as the authors believe these are more appropriate to the aims and setting under investigation (ibid.; Gummesson 1998). With little known about government IdM in the (non-technical) IS literature, this research has been necessarily 'exploratory'.

The interview data has been collected, transcribed and then coded with the aid of qualitative data analysis software (NVIVO) so that dominant themes can be identified (Glaser & Strauss 1968). The respondents in this research have been senior government officials responsible for e-Government development and/or strategy. They included government policy-makers, 'application owners', and 'data and infrastructure owners'.

Due to the open-ended nature of this research, unstructured interviews (King 1994) were conducted. In accordance with the methodological assumptions adopted, it is not appropriate for the researcher to develop an interview schedule or protocol (as this would constrain the data collection). Instead, the researcher used simple opening statements to get the unstructured interviews started. In this respect the researcher explained to respondents the area of interest. The data has been anonymised due to the fact that the government respondents

have indicated that the subject matter is sensitive for them and is frequently subject to government confidentiality controls.

Research Data & Analysis

Four major themes emerged from the data collected in this research. The themes can be considered as representing current challenges and issues facing US State and Federal government in attempting to develop, implement and maintain electronic identity management systems. The results are presented in order of prominence in the data (i.e. frequency of occurrence and proportion of data).

1. From e-Commerce to Security

One senior ranking government official stated: "We now need to secure our data against cyber-warfare". This reflects a marked shift in the dominant driver of the US Federal government rationale for investing in IdM. The e-Authentication initiative was guided by principles of citizen and business convenience and quality of service (e-Authentication, GSA, 2006) and there has now been a shift to focus on security of government data. One respondent crystallized this by saying, "It started out as an e-Commerce initiative and now it's a security initiative". The US Government's extensive use of 'contractors' is fuelling this emphasis on security. This is because a large number of on-line government applications are operated and accessed by governments' contractors. A senior government technology strategist explained that the contractors "need at least level 3, in some cases level 4 assurance, credentials, to get in". The 'assurance levels' are governments' degree of certainty that the user has presented an identity credential that refers to his or her identity, and that the government can be 'assured' of 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued (Bolten, 2003).

2. State government implementation of strong online security

At a State level, there are increasing demands for 'high end' IdM policies and technology. An increasing range of State services driving this requirement are the "first responder programme, transit workers programme, homeland security partnerships, State troopers, police, fire and State healthcare providers". As noted by one respondent, their challenge is to implement "high assurance digital certificate technology for logical access to systems, using [identity] providers [that are] cross-certified with the Federal Bridge... all these state entities ... need these high assurance credentials".

3. Core dominant reference model derived from standards and Federal 'guidance'

The information management decisions in State and Federal government in relation to IdM policy and technology are based on a minimal (core) set of government standards, a Presidential mandate and Office of Management and Budget guidance. These are explained in the following.

A 'risk management framework' was described in Memorandum M-04-04 from the Executive Office of the President, Office of Management and Budget to the Heads of all Departments and Agencies (Bolten 2003). This memorandum sought to implement "section 203 of the E-Government Act, 44 U.S.C. ch. 36". However, building effective IdM systems around this risk management framework has been challenging for parts of the US government. Several respondents stated that it was important that "common definitions" existed in government but that different parts of government interpreted the memorandum in different ways – leading to inconsistent outcomes.

The core NIST (National Institute of Standards and Technology) document describing 'IT security requirements' for electronic authentication is NIST SP800-63 (Burr et.al. 2006). The NIST standards have been dominant in government's efforts to produce 'high assurance' IdM policies and systems. The standard sets out minimum technical requirements for each of four levels of assurance (those outlined in Bolten, 2003) in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.

In 2004, a Homeland Security Presidential Directive (HSPD12) sought to establish a "Policy for a Common Identification Standard for Federal Employees and Contractors" with a strict timeline for implementation (6 months) that was unrealistic and subsequently not achieved. The multiple efforts of the Federal government to agree on IdM standards and policies have left some State governments confused and averse to taking any action toward implementing secure systems.

The driving assumption of NIST and the Federal government in developing IdM standards is that whilst 'compliance' with the standards can be measured, this will lead to 'effective' security. Clearly real world experience in managing identity would suggest that some caution with this assumption is needed. For example, the US border control implemented a fingerprinting system which started with one finger, moved to two, and now several. Presumably one finger was 'compliant' with the relevant standard at the time, but practice proved that this was insufficient (i.e. ineffective security).

4. Government retracting from IdM operations

Government officials expressed that they were finding it challenging to run both IdM policy definition *and* operations. One respondent said "...the government wants to be out of the business of *assessing* credential providers and be in the business of *defining* – in the policy business". To this end government has been working with a group of vendors and other organizations (known as the Liberty Alliance, see Liberty Alliance, 2008) to create an identity assurance framework – the Liberty IAF (LIAF) (see Cutler, 2008). It is "designed to embody the principles of 800-63, embrace the conceptual model of the levels of assurance (LOA) *matched* to degrees of risk". The LIAF is being designed for private assessors/accreditors to be able to audit identity credential providers and provide them with accreditation vis-a-vis compliance with the LIAF. If this is closely aligned with 800-63 and the government's LOAs, then government will no longer need to perform this function, and can retract from IdM *operations*.

Figure 1 summarizes the four major and current IdM challenges faced by State and Federal government. The State 'requirements' shown to the left of the figure are relatively new and further and more detailed research should be conducted to create a more complete picture. This research has included the views of senior officials in only two States, and the results can not be used to generalize.

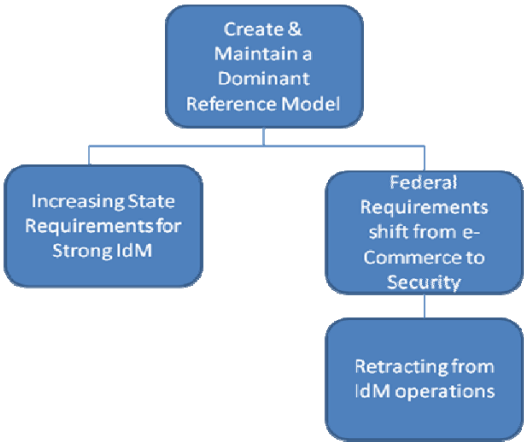

Figure 1: Current IdM Challenges in US State and Federal Government

Conclusions & Further Research

US State and Federal government have struggled with the security of on-line government transactions for some time. The need to electronically (often remotely) identify citizens, business and other government agencies on-line

has posed significant challenges for governments around the world. This research sought to identify the current challenges faced by different levels of the US government and through qualitative data analysis has found four dominant themes. Whilst exploratory research of this nature is not intended for generalization, the small sample size of ‘State’ data needs caution. The ‘Federal’ data has been drawn from key stakeholders and may be ’accepted’ with less reservation. The results indicate that the IdM space is dynamic and presents significant information and policy challenges for all parts of government. Longitudinal research would be most appropriate in studying the impact of IdM on government IS operations, policy and management over time. It is hoped that this small study will inspire other researchers to conduct further work on this topic.

References

Athens authentication (2008) "How Athens Works", [online] available at, http://www.athensams.net/how_athens_works, [accessed 14 May 2008].

Berger, P. L. & Luckman, T. (1967) *The social construction of reality: A treatise in the sociology of knowledge*, Allen Lane, London.

Bolten J.B., (2003), Memorandum to the heads of all departments and agencies, "E-Authentication Guidance for Federal Agencies", Executive Office of the President , Office of Management and Budget , Washington, D.C. December 16 (M-04-04).

Carter, L., & Bélanger, F. (2005) The utilization of e-government services: citizen trust, innovation and acceptance factors, *Information Systems Journal*, Vol. 15, No. 1. pp. 5-25.

Cutler, R. 2008, (Ed.), Liberty Identity Assurance Framework, Version: 1.1, *Liberty Alliance*, [online] available at, http://www.projectliberty.org/strategic_initiatives/identity_assurance, [accessed 16 February 2009].

Dearstyne, B. W. (2001) The view from the fast lane: The future of information management from the perspectives of Fortune's fastest growing companies, *Information Management Journal*, Vol 35, No. 2. pp. 4-12.

eAuthentication, (2006, 2008) *E-Authentication Solution and the US E-Authentication Identity Federation*, [online] available at, http://www.cio.gov/eauthentication/, [accessed 14 May 2008].

Gil-García, J.R., Chengalur-Smith, I. & Duchessi, P. (2007) Collaborative e-Government: impediments and benefits of information-sharing projects in the public sector, *European Journal of Information Systems*, Vol. 16, No. 2, pp. 121-133.

Glaser, B.G. & Strauss, A.L. (1968) *The discovery of grounded theory: Strategies for qualitative research*, Weidenfeld and Nicholson, London.

Gummesson, E. (1988),Qualitative Methods in Management Research, Chartwell-Bratt Ltd., Bickley, Bromley.

Holden, S.H. & Millett L.I. (2005) Authentication, privacy, and the federal E-Government, *Information Society*, Vol. 21, No. 5, pp. 367-377.

Hui, K.L., Teo, H.H. & Lee, S. (2007) The Value of Privacy Assurance: An Exploratory Field Experiment, *MIS Quarterly*, Vol. 31 No. 1. pp. 19-33.

King, N (1994) The qualitative research interview, in Cassell C. and Simon G. (eds.) *Qualitative Methods in Organizational Research*, Sage Publications, London, pp. 14-36.

Layne, K. & Lee J. W. (2001) Developing fully functional E-government: A four stage model, *Government Information Quarterly*, Vol. 18, No. 2, pp.122-136.

Liberty Alliance (2008) Liberty Alliance History, [online] available at, http://www.projectliberty.org/liberty/about/history, [accessed 14 May 2008].

Lincoln, Y.S. & Guba, E.G. (1985) *Naturalistic Inquiry*, Sage Publications, London.

Mahmood, M.K, Siponen, M., Straub, D., & Rao, H.R., (2008) MIS Quarterly Call for papers *Information Systems Security in a Digital Economy* [online] available at, http://www.misq.org/BulletinBoard/ISSecurity.pdf, [accessed 10 May 2008].

Miyata T., Koga Y., Madsen P., Adachi S., Tsuchiya Y., Sakamoto Y. & Takahashi K. (2006) A survey on identity management protocols and standards, *IEICE Transactions on Information and Systems*, Vol. E89D, No. 1, pp. 112-123.

Moon J. M. & Norris, D. F. (2005) Does managerial orientation matter? The adoption of reinventing government and e-government at the municipal level, *Information Systems Journal*, Vol. 15, No. 1. pp. 43-60.

Burr, W.E., Dodson D.F., Polk , W.T., *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, (2006), [online] available at, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf, [accessed, 24 February 2009].

Otjacques, B., Hitzelberger, P. & Feltz, F. (2008) Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing, *Journal of Management Information Systems*, Vol. 23 No. 4, pp. 29-51.

Pavlou, P., Huigang, L. & Yajiong ,X. (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective, *MIS Quarterly*, Vol. 31, Issue 1, pp. 105-136.

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

Walsham, G., (1995), The emergence of interpretivism in IS research, *Information Systems Research*, Vol. 6, pp. 376–394.

The University of Sydney Business School is committed to continuous quality improvement and achieving and maintaining international accreditations and engagements. It is currently the only business school in Australia accredited by AACSB International – The Association to Advance Collegiate Schools of business – for both business and accounting programs. AACSB is the United States based global accrediting body for business schools.

The University of Sydney Business School also has EQUIS accreditation conferred by the European Foundation for Management Development (EFMD). EQUIS accreditation indicates that a business school is judged to be of international standing.

In 2008, the University of Sydney Business School was admitted to CEMS – The Global Alliance in Management Education, as their Australian member business school. In each country, only one institution is chosen to be part of the CEMS alliance.

Accredited by:

EARNED EXCELLENCE

AACSB ACCREDITED EST. 1916

THE BEST BUSINESS SCHOOLS IN THE WORLD

EFMD EQUIS ACCREDITED

International member of:

CEMS

THE GLOBAL ALLIANCE IN MANAGEMENT EDUCATION

BUSINESS SCHOOL

THE UNIVERSITY OF SYDNEY

FOR MORE INFORMATION CONTACT

The Discipline of Business Information Systems
The University of Sydney Business School
University of Sydney NSW 2006
T +61 2 9036 9432
F +61 2 9351 7294
E business.biswps@sydney.edu.au
sydney.edu.au/business/information_systems

ABN 15 211 513 464
CRICOS 00026A