Computer Standards & Interfaces 37 (2015) 1–8

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Cyber security readiness in the South Australian Government

Brenton Borgman [a,b], Sameera Mubarak [a], Kim-Kwang Raymond Choo [a,*]

[a] Information Assurance Research Group, University of South Australia, GPO Box 2471, Adelaide, SA 5001, Australia
[b] Auditor-General's Department, South Australian Government, Adelaide 5000, Australia

ARTICLE INFO

Article history:
Received 13 November 2013
Received in revised form 29 May 2014
Accepted 4 June 2014
Available online 2 August 2014

Keywords:
Cyber security
Information security management framework (ISMF)
Information security management system (ISMS)
South Australian Government
Whole of government approach

ABSTRACT

In this paper, we conducted a series of face-to-face interviews with 17 participants from 11 SA government entities, with the aim of validating whether existing processes and strategic direction were sufficient to satisfactorily achieve the implementation of an ISMS and classification of data for the respective SA government entities. Based on our interviews and review of ISMS associated reviews conducted within other Australian State and Territory jurisdictions, we identify key areas that the SA Government may need to consider as part of the progressive roll-out of the other phases of ISMF version 3 implementation up and to June 2017.

Contents

1. Introduction: cyber security

Cyber security is one of the highest-priority items on the global policy and national security agendas, and an increasingly challenging policy area for governments. The 2008 report of the Centre for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency reported: 'We began with one central finding: The United States must treat cybersecurity as one of most important national security challenges it faces' [9]. Three years later in 2011, cyber security remains one of the greatest threats identified in cyber space — '[t]he findings of our first report still stand: cybersecurity is now a major national security problem for the United States .... and adopting a comprehensive national security strategy that embraces both the domestic

[*] Corresponding author. Tel.: +61 8 8302 5876(office).
E-mail address: Raymond.choo@unisa.edu.au (K.-K.R. Choo).

http://dx.doi.org/10.1016/j.csi.2014.06.002
0920-5489/© 2014 Elsevier B.V. All rights reserved.

and international aspects of cybersecurity will make us more secure' [10]. Cyber security was also identified as one of the four highest priority/tier one national security risks by UK's National Security Council in 2010 [23], and one of Australia's top tier national security priorities in the country's first National Security Strategy launched in January 2013 [7].

In order to meet future cyber security challenges, entities need to ensure that effective security controls underpin information systems and its sensitive data [41]. The review of the Australian (Federal) Government's use of information and communication technology as reported in the Sir Peter Gershon's report of 2008 recommended that agencies needed to strengthen their governance mechanisms and move closer to standardisation within specific IT architecture [18]. The security of information systems (IS) and its data is also an on-going research area and various theories have been used in IS and information security research. Within the area of behavioural IS security literature, studies have focused on the relationship and lessons learnt between IS security and the behaviour of employees (i.e. insiders) (see [37]). As explained by Choo [11] and Levi [25] using the routine activity and rational choice theory [13,17], individuals tend to maximise their utility given the situational opportunities that confront them. In an IS context, effective information security measures within the organisations limit malicious cyber activities [22,24], and both extrinsic motivators (i.e. increased severity of penalties, increased certainty of detection, and social pressures—normative beliefs) and intrinsic motivators (i.e. perceived effectiveness) can encourage compliance with organisational information security policies [20,21] through the recognition of lesson learnt, and the strengthening of governance mechanisms and the locating of specific controls as close to the data as possible (which may assist in improving efficiency and effectiveness of compliance measures). Stronger controls around the classifications of information data will also reduce the potential for information to be compromised.

Various Australian government jurisdictions have gradually been strengthening their information security controls through the implementation of their own versions of an information security management system (ISMS) as a means to safeguard information. This will eventually establish a consolidated common security control position across Australia based upon the standard 'AS/NZS ISO/IEC 27001:2006 Information technology — Security techniques — Information security management systems — Requirements' (will be referred to AS 27001 in the remainder of this paper) [29].

The South Australian Government (SA Government) has also acknowledged that mounting evidence within Australia (as provided by the Australian Government Defence Signals Directorate) and from overseas jurisdictions suggests that the government is being targeted from various threat vectors and that these risks are on the rise. The SA Government has subsequently implemented an initiative for all their agencies, commissions, corporations and other regulatory bodies (collectively referred to as SA government entities or entities) to develop an ISMS and classify information data.

In this paper, we interviewed 17 participants across 11 SA government entities to assess how the SA Government and its entities have approached the implementation of an ISMS and classified data based upon assessed sensitivity (including in accordance with SA whole of government mandated strategic direction). The study has also compared the published compliance reviews from other Australian jurisdiction Auditor-Generals. This sought to leverage from these reports and discuss the benefits, consequences and challenges that the SA Government would need to address in order to ensure that the data is adequately protected from internal and external vulnerabilities. Our study examines the adequacy of the proposed SA Government process through its guidance and implementation by entities of government, and whether a standardised approach which centred upon AS 27001 has been consistently conveyed and applied by respective government entities. Our findings will assist the SA community to determine if their information data is adequately safeguarded and the implementation of the ISMS and classification of data are progressed in an effective and efficient manner.

The rest of this paper is organised as follows: Section 2 describes the research methodology and participant demographics. Section 3 discusses the findings from our interviews. Section 4 presents the collective observations from ISMS associated reviews conducted within other Australian State and Territory jurisdictions. The last section concludes the paper.

2. Research methodology and participant demographics

Within the SA Government, there are numerous agencies, commissions, corporations and other regulatory bodies established in accordance with the Public Sector and other enabling legislations. These government entities vary in complexity based upon their operational size, uniqueness of business, nature and coverage. From an ICT perspective, the entities vary from having simple to complex computer systems. Whilst the simple ICT systems support singular environments, the complex entities comprise varying departmental portfolio and complex relational functions which have a direct reference to the critical informational data held that are seen as critical to both SA Government and the respective individual entities.

At a whole of government strategic directional level, it was identified that 40 key entities exist that potentially retain critical/important informational data. Our research has sought to incorporate a cross section of government entities. Hence, we approached 14 SA government entities to participate, but 3 entities either declined the invitation or were unavailable due to the narrow timeframe in which the study was conducted. Of the 11 entities that participated in the research, nine contained elements that were unique to that entity alone and included complex functionality such as treasury, transportation, water, agricultural/horticulture, education and legal considerations. A total of 17 participants — four agency security executives (ASE), 11 information technology security advisors (ITSA) and two whole of government strategic advisors — from these 11 entities, participated in a series of interviews. The roles of ASE, ITSA and the whole-of-government strategic advisor, in accordance with the SA Government ISMF Guideline 13 [33] are as follows:

- The role of the ASE is a position of trust assigned to overview security performance outcomes and operations and support stated executive outcomes and performance requirements specific to the ISMS through their involvement in security management commitments, Agency Security Plan, Consolidation of control documentation and overall ISO certification assessment for each respective SA government entity.
- The ITSA is involved at most stages of the ISMS development in an advisory capacity and is to review and provide commentary and advice on risk assessments that are undertaken by various parts of the business.
- The whole of government strategic direction analysts have prepared a suite of high level guidelines for entity use which strive to make reference to South Australian legislative and the SA Government's ISMF, International Standards, and best practices. Also these analysts seek to relate with entities on areas of general uncertainty of an IT nature. It is intended that entities will use this information to develop measures that will assist in mitigating identified risk(s).

In May 2012, as a pre-curser to the interviews with participants, we obtained a listing of entity nominated ASE and the ITSAs from the SA Government. This listing identified that a number of positions had been vacant for an extended period of time (ranging from six to 12 months). In some instances, the SA Government's recent restructure/reshuffle which occurred in late 2011 had contributed to the movement of certain government staff that had yet to be replaced. Failure to initiate replacements for the ISMS project based upon specifically assigned staff may restrict the development of an ISMS for that entity in accordance with set June 2013 milestone.