Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The regulatory challenges of Australian information security practice

Mark Burdon [a,*], *Jodie Siganto* [b], *Lizzie Coles-Kemp* [b]

[a] *TC Beirne School of Law, The University of Queensland, Australia*
[b] *Royal Holloway, University of London, UK*

Keywords:
Information security
Data protection
Data breaches
Information security management

A B S T R A C T

Information security is not directly regulated in Australia and is instead subject to a patchwork of different legal and regulatory frameworks. How Australian information security practitioners construct and action information security therefore becomes important to the overall operation of a fragmented regulatory framework. How then do Australian information security practitioners understand information security and make compliance-oriented decisions? Our exploratory interview research examined how nine Australian information security practitioners understood and constructed their role as delegated regulators of organisational information security processes. Participants expressed a number of concerns that reveal a very different world to that traditionally portrayed as the discipline and practice of information security. We examine these concerns and discuss what they mean in the context of the Australian environment.

1. Introduction

Information security, as a discipline, is portrayed as rational and control-oriented. The appropriateness of controls is derived through risk assessment frameworks that consider the contextual realities of the given organisation. In this paradigm, the role of the information security practitioner is to identify security risks that emerge and to design and implement appropriate controls. The practitioner then ensures those controls operate as expected and continue to address identified risks, as part of an iterative process. The implementation of information security therefore regards rational considerations that translate into actions that are accepted as reasonable by organisations. These organisations accept the value of information security as a self-serving good and one that has wider societal benefits from the broader minimisation of risks arising from security failures.[1]

It is therefore not surprising that a developing literature on practitioner perspectives is starting to develop.[2] Such 'human

* *Corresponding author.* TC Beirne School of Law, Forgan Smith Building, St Lucia Campus, The University of Queensland, Brisbane, Queensland 4072, Australia.
E-mail address: m.burdon@law.uq.edu.au (M. Burdon).

[1] See e.g. Roger Clarke, 'The prospects of easier security for small organisations and consumers' (2015) 31(4) *Computer Law & Security Review* 538, 539.

[2] See e.g. Eirik Albrechtsen, 'A qualitative study of users' view on information security' (2007) 26(4) *Computers & Security* 276; Eirik Albrechtsen and Jan Hovden, 'The information security digital divide between information security managers and users' (2009) 28(6) *Computers & Security* 476; Eirik Albrechtsen and Jan Hovden, 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study' (2010) 29(4) *Computers & Security* 432; Debi Ashenden, 'Information Security management: A human challenge?' (2008) 13(4) *Information Security Technical Report* 195; Debi Ashenden and Angela Sasse, 'CISOs and organisational culture: Their own worst enemy?' (2013) 39(11) *Computers & Security* 396; Lizzie Coles-Kemp, 'Information security management: An entangled research challenge' (2009) 14(4) *Information Security Technical Report* 181.

http://dx.doi.org/10.1016/j.clsr.2016.05.004
0267-3649/

factors'[3] or 'human challenges'[4] studies highlight the dissonance between, on the one hand, the theory of information security as a purely control-oriented approach, and on the other, the practice of information security which is negotiated and individually constructed.[5] How practitioners construct and operationalise information security in practice is important to understand in order to assess the effectiveness of legal and regulatory application.

In Australia, understanding the day-to-day lives of practitioners, and their perspectives on information security, and its management, is particularly important because of the legal and regulatory structure employed. Information security is not regulated directly by a governing piece of legislation. Instead, a patchwork of different laws, guidelines and regulations provides a principled range of security obligations for both private and public sector organisations. A broad regulatory framework underpins this patchwork of legal obligation which is predicated on principles-based regulation (PBR).[6] In effect, the regulatory function is partly delegated from the regulator to the regulatee, in this case, the information security practitioner. As such, in a system of delegated regulation,[7] such as in a PBR framework, it is vital to understand practitioner perspectives of information security and how core concepts of information security are being constructed and actioned by delegated regulatory actors.

In this article, we report on findings from our exploratory interview research which examined how nine Australian information security practitioners understood and constructed their role as delegated regulators of organisational information security processes. Our findings reveal a very different world to that traditionally portrayed as the theory, discipline and practice of information security. Participants in our study had irregular working days and the 'average day' for all of our participants focused mostly on processes of interaction and negotiation. Definitions of information security also varied significantly which revealed a number of different understandings about the core constructs of information security, such as risk and risk assessment. Most importantly, compliance considerations also varied and it was clear that participants considered the application of law and regulation from different sources and in different ways. Our research therefore reveals a world and practice of information security that is not as ordered and structured as the control-oriented tradition of information security would have us believe.

[3] Human factors in this sense often refers to insider actors as threats. See Carl Colwill, 'Human factors in information security: The insider threat – Who can you trust these days?' (2009) 14(4) *Information Security Technical Report* 186.

[4] Ashenden more broadly refers to human challenges in relation to the complex actions of information security actors. See Debi Ashenden, 'Information Security management: A human challenge?' (2008) 13(4) *Information Security Technical Report* 195.

[5] Gurpreet Dhillon and James Backhouse, 'Current directions in IS security research: towards socio-organizational perspectives' (2001) 11(2) *Information Systems Journal* 127.

[6] See for an overview of PBR Julia Black, Martyn Hopper and Christa Band, 'Making a Success of Principles-Based Regulation' (2007) 1(4) *Law and Financial Markets Review* 191.

[7] See more broadly Cary Coglianese and David Lazer, 'Management-Based Regulation: Prescribing Private Management to Achieve Public Goals' (2003) 37(4) *Law & Society Review* 691.

Section 2 briefly outlines the legal and regulatory framework for information security in Australia. Section 3 details the research methodology employed in the study and Section 4 covers some key research findings. Section 5 provides some discussion in relation to what our study means for the legal and regulatory framework currently adopted in Australia and Section 6 concludes our article in relation to future directions.

2. Regulating information security in Australia

Information security in Australia is not directly regulated by a specific and governing piece of legislation that covers all public and private sectors. Government agencies are regulated by a range of both Commonwealth and state laws and guidelines. As a consequence, both federal and state governments have developed approaches to secure the information held in government-controlled systems.

Australian federal government agencies are covered by a specially designed framework comprising the Protective Security Policy Framework (PSPF)[8] and the Information Security Manual (ISM).[9] The ISM is based on a series of high-level principles which are supported by a detailed controls manual. The first principle is information security risk management, which supports agencies making informed, risk-based decisions specific to their unique environments, circumstances and risk appetite (subject to the implementation of a number of controls which are stated to be mandatory). In addition, there is a range of more technology-specific principles dealing with topics including product security, media security, software security, email security, network security and cryptography.[10]

The Victorian Government in 2012 adopted the Commonwealth Government's PSPF and ISM.[11] Other state governments in Australia have adopted different approaches to ensuring the

[8] The Commonwealth Attorney-General sets the Australian Government's protective security policy and has released the Protective Security Policy Framework, in pursuance of that responsibility. Attorney-General's Department, 'Government Response to the House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime ' (Commonwealth of Australia, 2010). See also Sharon Oded, *Corporate Compliance New Approaches to Regulatory Enforcement* ('Edward Elgar, 2013).

[9] The ISM is published by the Australian Signals Directorate pursuant to the *Intelligence Services Act 2001* (Cth). It is made up of a number of different publications. See Intelligence and Security Department of Defence, *Australian Government Information Security Manual – Principles* (2015); Intelligence and Security Department of Defence, 'Australian Government Information Security Manual – Controls' (2015) <http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf>.

[10] Intelligence and Security Department of Defence, 'Australian Government Information Security Manual – Controls' (2015) <http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf>, 37 – 60.

[11] Victorian Government standards include Victorian Government CIO Council, 'Information Security Management Framework' (2014) <http://www.enterprisesolutions.vic.gov.au//wp-content/uploads/2014/07/SEC-STD-01-Information-Security-Management-Framework.pdf>.