2010

INFORMATION SECURITY AND PRIVACY: RETHINKING GOVERNANCE MODELS

Robert Hodgkinson
ICA EW Chartered Accountants Hall, robert.hodgkinson@icaew.com

Louis Branz
Edward Jones, louis.branz@edwardjones.com

Mary Culnan
Bentley University, MCULNAN@BENTLEY.EDU

Gurpreet Dhillon
Virginia Commonwealth University, gdhillon@vcu.edu

Alastair MacWillson
Accenture, alastair.macwillson@accenture.com

See next page for additional authors

Follow this and additional works at: http://aisel.aisnet.org/icis2010_submissions

Recommended Citation
Hodgkinson, Robert; Branz, Louis; Culnan, Mary; Dhillon, Gurpreet; MacWillson, Alastair; and Ponemon, Larry, "INFORMATION SECURITY AND PRIVACY: RETHINKING GOVERNANCE MODELS" (2010). ICIS 2010 Proceedings. 38.
http://aisel.aisnet.org/icis2010_submissions/38

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Abstract

Concerns about information security and privacy continue to make headlines in the media and rate as serious issues in business and public surveys. Conventional thinking suggests that enhancements to governance models and business practices improve the performance of individual businesses. However, is this enough? Good governance is based on clear rights and responsibilities, and this panel will address the contention that such clarity is lacking in the treatment of personal information. As a result, certain types of business innovation may be constrained and good practices may remain tick box exercises, disconnected from wider business objectives. More radical thinking would go beyond incremental improvements to the status quo and recognize the profound challenges to privacy and information security created by digital technology. This panel will bring together a range of research disciplines and senior business representatives to critique current practice and develop a future research agenda.

Keywords: Privacy/information privacy, data security, ethics/ethical behavior/ethical quandaries, governance, cross disciplinary research, information security/privacy management techniques, risk management, legal environment, trust/online trust
**Introduction**

Failures in information security and concerns about privacy continue to create headlines in the media on a regular basis. Despite years of research and well established principles and processes, there continue to be significant fears about the safety and use of personal information by businesses and governments.

This is a matter of grave concern to everyone. Individual consumers and citizens are put at risk when their personal information is not secured properly, creating a climate of concern about cyber crime. They may feel that their rights have been infringed when information is used or shared in particular ways. This damages trust in individual businesses as well as in the broader digital economy. Furthermore, businesses also suffer direct losses from security and privacy failures, including regulatory fines, remediation costs and reputational damage.

Conventional thinking focuses on steps that individual businesses can take to enhance their performance in these areas. These typically involve improving governance processes and implementing good practices in order to change the way that things are done within organizations and to manage external relationships effectively. However, are incremental improvements to the status quo an appropriate and sufficient approach to continuing failures in information security and concerns about privacy?

In this panel session, ICAEW (Institute of Chartered Accountants in England and Wales) will challenge participants to consider whether there are deeper issues at play. At the heart of many security and privacy issues is a growing confusion and contention over who should have access to personal information and what they should be able to do with it, especially in evolving areas such as social networking and collaboration. This uncertainty undermines the application of good practices and effective governance models and ICAEW is skeptical about the ability of individual businesses to be able resolve many of the issues seen here simply by changing internal practices.

This view is based on ICAEW’s broad experience in corporate governance issues. As a pioneer in corporate governance, ICAEW believes that good governance requires strong foundations and an accepted framework of norms. This argument can be extended across broad areas of business practice. In this panel, ICAEW will contend that more radical thinking on the nature, scope and applicability of privacy is necessary in order to establish firm foundations for governance and other business practices. It will do this by arguing that current uncertainty over access to personal information is at the heart of many business issues surrounding security and privacy:

- hindering business innovation and limiting the value being realized from digital technology;
- undermining governance processes and frequently reducing them to meaningless compliance exercises; and
- reducing organizational commitment to good practices, making it difficult to embed them in individual behavior.

The session will have broad appeal to IS academics. It raises issues which are increasingly important to businesses and individuals both as consumers and citizens and provides an opportunity to understand some of the leading research in the area. It challenges academics and practitioners over whether current approaches are fit for purpose for the future or whether wider engagement and discussion is needed. Furthermore, by bringing together representatives from different disciplines, as well as from the business community, the session aims to foster multidisciplinary debate and develop an agenda for further research which will influence the future direction of IT.

The session will be written up and submitted for publication to the *Communications of the AIS* journal. ICAEW will also publish key points from the session through its communications with the business community. This includes use of the ICAEW online community site IT Counts, which can be used to engage with the business community.

**Controversial Issues and Panelists’ Positions**

*Statement 1 – Uncertainty Over Information Privacy is Hindering Business Innovation*

The chair, Robert Hodgkinson, will firstly challenge panelists with the assertion that current uncertainties around personal information are creating significant issues for businesses which are trying to innovate in this area. IT is a particularly powerful technology because it radically changes the economics of information (ICAEW 2008). It shifts the supply and demand curves of information by reducing its costs and increasing the benefits that can be gained
through it. This creates a vast new space of economically efficient information, making new activities viable and profoundly changing the way that businesses create and deliver value to customers.

However, these radical changes also lead to heightened contests over the control of valuable information and create confusion as new activities become possible. This makes it harder to articulate who has rights over what information in what circumstances. It therefore presents businesses with tremendous new dilemmas on how to use information in innovative ways which are also socially acceptable and respect the rights of individuals where relevant. What can seem like a fantastic innovation to one person can seem like a violation of privacy to others, for example Google’s Street View. This is likely to become an even bigger challenge in future years given the amount of information that businesses are collecting about individuals, from RFID tags to smart electricity meters. Without greater clarity on the limits of using personal information, businesses will find it increasingly hard to innovate successfully.

In response, it could be argued that many businesses are innovating successfully, despite this uncertainty. While there may be occasional controversy and debate, there is no evidence that businesses are being constrained in any way. Indeed, innovation is an iterative process involving trial and error. It is only possible to resolve tensions when they arise in a specific context and therefore the key for businesses is to manage expectations, respond to issues and change direction where needed. Furthermore, it could be argued that uncertainty provides an opportunity for businesses to differentiate themselves and create competitive advantage where they can understand the needs and expectations of their customers. The business environment is inherently unpredictable and good businesses are able to manage and respond to a wide range of uncertainty and change.

**Statement 2 – A Lack of Firm Foundations is Reducing Governance Processes in Information Security and Privacy to Meanless Compliance**

Robert Hodgkinson will secondly challenge panelists with the assertion that effective governance practices are predicated on clear rights that a business can align to, such as the rights of shareholders in corporate governance. Without that clarity, governance processes, including decision rights and accountability, the development of corporate policies, verification activities such as audits and risk processes, have little meaning for a business. Instead, they are seen as compliance measures or tick-box exercises which are a burden and without value. This is a serious challenge for many information security and privacy processes in businesses today.

As a result, increment improvements to governance practices will only have limited effectiveness in improving business performance. Instead, governance practices in information security need to be linked more explicitly to rights to control access to personal information to provide the necessary foundations. And while there continues to be uncertainty over the limits and application of rights in this area, businesses will continue to struggle to implement effective governance processes.

In response, it could be argued that it is perfectly possible to separate these issues. There are many businesses that have effective governance practices, despite uncertainty over the exact rights which different parties may have. While there may be some uncertainty at the leading edge, there is still sufficient clarity in most cases. Furthermore, governance practices around privacy and information security are in early stages of maturity and as businesses gain more experience with them, implementation will improve. Therefore, an incremental approach is appropriate and will ultimately result in improved business performance.

**Statement 3 – A Failure to Link Good Security and Privacy Practices to Business Objectives is Making Them Difficult to Embed**

Robert Hodgkinson will thirdly challenge panelists with the assertion that although many businesses have invested substantially in information security and privacy practices in recent years, in many cases, good practices have not become embedded in the way that people do things. Most failures still stem from human error, carelessness or malevolence. Unless businesses can fundamentally change the way that employees approach security and privacy, and make it a higher priority for them, failures are likely to continue.

This can be traced to a more general failure to link good security and privacy practices to broader business objectives. Many practices seem to be implemented simply because they are ‘good practices’ and without any particular consideration for the costs and benefits of measures. As a result, employees may circumvent them or not apply them particularly consistently. An analogy is often made by information security specialists with health and
safety practices, comparing the way that these practices have become embedded into organizations. However, there is a clear business objective with health and safety and the benefits are obvious. This is often not the case with information security and privacy practices, where the benefits of applying practices may not be at all clear.

In response, it could be argued that there are many reasons for difficulties in embedding practices. Security continues to be seen by many as primarily a technology problem. Responsibility sits in the IT function and is disconnected from wider business concerns, with little senior management commitment. This technology-based approach also takes little account of human behavior or wider organizational factors, which are fundamental to improving performance. As a result, by recognizing these softer factors, a business can take practical steps that will help to embed good practices into the organization and do not require radical new thinking.

Panelists’ Positions

The panelists will respond to these challenges through very distinct perspectives, including:

- US and European perspectives;
- research and practice perspectives; and
- IS, legal and technical perspectives.

Mary Culnan will bring out the wider theoretical issues relating to privacy and the security of personal information. She will highlight what leading research tells us about the adoption of good governance and wider business practices, and she will be broadly in favor of the need for wider engagement and resolution of the deeper issues.

Gurpreet Dhillon will focus on the socio-organizational aspects of security and privacy, highlighting what leading research tells us about the organizational factors stopping the adoption of effective governance and the embedding of good practices throughout the business.

Alastair MacWillson will highlight the importance of linking security with the contribution that valuable information makes to achieving business goals. He will also consider how academic research can help move business thinking forward in these areas.

Larry Ponemon will reflect on how businesses are successfully adopting effective governance models and good business practices, based on his research with businesses in this area. He will highlight some of the good practices of leading businesses and suggest opportunities for further incremental improvements.

Louis Branz will contribute a distinctly legal approach, assessing the extent to which security and privacy are becoming a demanding compliance and oversight challenge and how the legal framework fits with broader business objectives. He will also consider whether there are broader lessons that can be learned from the legal approach.

Panel Structure

The panel will be based around a discussion between panelists and questions from the audience and there will be no formal PowerPoint presentations. Robert Hodgkinson will chair the debate. He will take a proactive and provocative role in the panel and challenge panelists with ICAEW thinking in each of the three areas to be debated.

The panel will be divided into three sections, with a short introduction at the beginning and an opportunity for panelists to reflect on the session and present some conclusions at the end. Each section will last 25 minutes. The statement will be presented by Robert Hodgkinson (2-4 minutes) and each panelist will have 1-2 minutes to state briefly whether or not they agree with it and why. The discussion will then be opened to the audience for questions and comments (approximately 15 minutes).

Participation Statement

All the panelists have committed to attend the conference and sit on the panel if the submission is accepted.
Biographies

Robert Hodgkinson

Robert Hodgkinson is the Executive Director, Technical at ICAEW, a world leading professional body which represents 135,000 members, over half of whom work in business. The ICAEW IT Faculty published a report on IT value in 2008, entitled *Measuring IT Returns*, of which Robert was co-author with Kirstin Gillon. He also moderated the panel *Returns on IT Investments: Could We Do Better?* at ICIS 2009 and is a co-author of the panel write up, which was published in the *Communications of the AIS* in 2010. He is a Chartered Accountant and a Board member of the International Federation of Accountants. He graduated in Philosophy, Politics & Economics from Corpus Christi College, Oxford University.

Louis Branz

Louis Branz has been with Edward Jones in the position of Associate General Counsel since 1984. He is the firm's Chief Privacy Officer. He was in private practice with the firm of Schuchat, Cook & Werner of St. Louis, Missouri, from 1982 to 1984. He served as the Chairman of the Securities Industry Association Committee on Brokered Deposits from 1995 to 2003. Mr. Branz received his Bachelor of Arts degree from Southern Illinois University in 1978, and received his Juris Doctor degree from Washington University School of Law, St. Louis, in 1982.

Mary Culnan

Professor Mary Culnan is Slade Professor of Management and Information Technology at Bentley University. Her current research interests include information privacy and social media. Her publications include papers in the published Journal of Public Policy and Marketing, Journal of Interactive Marketing, Journal of Social Issues, The Information Society, MIS Quarterly, Management Science and Organization Science. She serves on the editorial board of The Information Society. She served as a Commissioner on the President's Commission on Critical Infrastructure Protection and the FTC Advisory Committee on Access and Security.

Gurpreet Dhillon

Professor Gurpreet Dhillon is a faculty in the School of Business at Virginia Commonwealth University, USA. Professor Dhillon is a graduate of the London School of Economics and Political Science, UK where he studied organizations and information. His research led him to explore aspects of information security, identity and assurance. He has authored over 100 research articles that have been published in various journals. Professor Dhillon is also an author of six books, including *Principles of Information Systems Security: Text and Cases* (Wiley, 2007). He is the Editor-in-Chief of the Journal of Information System Security, besides serving on the board of several flagship journals.

Alastair MacWillson

Dr. Alastair MacWillson is the Global Managing Partner of Accenture’s global security practice, which comprises over 2,500 security professionals, and works with business and government leaders around the world on critical issues relating to technology strategy and risk, operational performance and management, cyber and information security, and critical infrastructure protection. Based in London, he also serves on the leadership council of Accenture’s global technology consulting business. Prior to joining Accenture in 2002, Dr. MacWillson was the global leader of the technology consulting practice in PricewaterhouseCoopers. Dr. MacWillson has a B.Sc. in Theoretical Physics, postgraduate diplomas in Computer Science and Digital Imaging, and a Ph.D. in Cryptography.

Larry Ponemon

Dr. Larry Ponemon is the Chairman and Founder of the Ponemon Institute, a research think tank dedicated to advancing privacy and data protection practices. Dr. Ponemon consults with leading multinational organizations on global privacy management programs. He has extensive knowledge of regulatory frameworks for managing privacy and data security including financial services, health care, pharmaceutical and Internet. In addition to Institute activities, Dr. Ponemon is an adjunct professor for ethics and privacy at Carnegie Mellon University’s CIO Institute.

References