DEVELOPING ICT-ENABLED INFORMATION PROCESSING CAPABILITIES FOR COMBATTING E-COMMERCE IDENTITY FRAUD: A CASE STUDY OF TRUSTEV'S SOCIAL FINGERPRINTING SOLUTION

Daniel Cheng, School of Information Systems, Technology and Management, UNSW Business School, UNSW Australia, daniel.cheng@unswalumni.com

Felix Tan, School of Information Systems, Technology and Management, UNSW Business School, UNSW Australia, f.tan@unsw.edu.au

Zixiu Guo, School of Information Systems, Technology and Management, UNSW Business School, UNSW Australia, z.guo@unsw.edu.au

Michael Cahalane, School of Information Systems, Technology and Management, UNSW Business School, UNSW Australia, m.cahalane@unsw.edu.au

Abstract

Given the importance of information processing capabilities in improving business performance, organisations are seeking solutions for leveraging the use of big data and analytics. An emerging application is to inform organisations of potential fraudulent behaviour, which results in reducing online fraud and its associated costs. This paper introduces a case study in which social fingerprinting is used as a big data profile-based fraud detection technique for e-commerce transactions. Through an analysis of semi-structured interviews, this research in progress identifies three information processing capabilities based on social fingerprinting that a business must develop to eliminate fraud. Further interviews and analysis are proposed in order to have a better understanding of how social fingerprinting can be used in e-commerce. By uncovering interrelationships of social fingerprinting as online fraud detection solution, this study will provide significant contribution to information processing and analytic theory and practice.

Keywords: E-commerce, Information Processing Capabilities, Online Fraud Detection, Social Fingerprinting.

1 INTRODUCTION

E-commerce has become more popular as society moves deeper towards a digital economy, simultaneously provoking a growth of transaction fraudulent activities. Often, the security infrastructure of organisations is inadequate and introduces significant risks of becoming a target for fraud (Roberts et al. 2013). As a result, online fraudulent activities and fraud prevention have led to significant financial costs. In 2012, a total of $20 billion has been lost to fraud, growing at a rate twice as fast online commerce (CyberSource 2012). Additionally, the Association of Certified Fraud Examiners projected a potential global fraud loss of more than $3.5 trillion on Gross World Product (ACFE 2012). Therefore, organisations are now seeking to make significant inroads into commensurate security among their e-commerce initiatives to reduce the impact of fraud (Jamieson et al. 2012; Roberts et al. 2013). Simultaneously, e-commerce growth has led to an explosion of digital footprint, the emergence of big data, and business analytics. Since 2009, big data and analytics have remained in the top 5 technology priorities in Gartner's annual survey of CIOs (Gartner 2013). With expected growth to reach $32.4 billion in 2017 (Corporation 2013), the hype about big data and business intelligence continues to be prominent amongst the technology industry. As a result practitioners are determined to build business analytic capabilities. However, the application of business analytics to prevent e-commerce fraud is rarely reported and remains under-researched.

This study uses information processing (Galbraith 1977; Tushman & Nadler 1978) as a preliminary guiding lens to examine the role of ICT-enabled information processing capabilities in an e-commerce context. The objective is to investigate its effect on alleviating costs of identity fraud. The implications of using information processing as a theoretical lens can inform businesses that are coping with information asymmetries and fraudulent transactions. In operationalising our research objective, our study aims at answering the following research question: *How does ICT-enabled information processing disrupt identity fraud?* To address this question, we present an exploratory case study of an emerging technology organisation specialising in real-time online identity verification. The organisation's solution aims at eliminating fraud from e-commerce transactions using social fingerprinting. This study presents social fingerprinting as an application of big data and business analytics to fight online fraud and make e-commerce safer. Social fingerprinting is a dynamic verification technique where behavioural, social, transactional, and historical data are combined to formulate a measure of fraud. The complex use of data and analytic techniques coupled with authentication technologies aid the organisation in identifying potential fraudsters.

The paper proceeds as follows. The next section summarises the literature review. We discuss the prevalence of identity fraud in e-commerce as well as the application of ICT-enabled information processing capabilities. Next, we present our research method. Then, we introduce the case organisation in more depth and present our preliminary findings. Finally, we discuss potential contributions and future work.

2 LITERATURE REVIEW

In this section, we discuss two bodies of literature relevant to our study: online identity fraud and organisational information processing capabilities. The literature review seeks to encapsulate the current business analytic landscape from an organisational capability perspective focusing its application and role on fraud detection. It also aims to build an argument of why it is necessary to study the applications of an information processing capability in reducing fraud.

2.1 Online Identity Fraud

Identity fraud involves the use of a fabricated identity for financial gain or other benefits (Jamieson et al. 2012). In fact, identity fraud includes the adoption of another person's personal information to

commit fraudulently activity (identity theft) or intentionally misrepresenting identification for unlawful purposes (identity deception). The most basic form of fraudulent business activity involves manipulating corporate identities and their associated parties in order to increase wealth in profits and/or assets (Roberts et al. 2013). With the introduction of e-commerce, identity fraud has evolved to occur in the digital environment. The consequences of identity crime and identity related crimes not only have a financial impact in the billons (ACFE 2012), but also compromise consumer confidence and trust in service providers (Turner et al. 2005).

Currently, there is a lack of enterprise-wide IT architecture for supporting identity management to combat fraud. Yang et al. (2010) note that a key element of the architecture for an identity management system is the data set. With big data and analytics, the sourcing of several data points, or items from various sources to determine the unique identity of an individual or organisation, is achievable. Therefore, in order to detect fraud, it is necessary to develop a data set of identification attributes that can uniquely describe individuals or potential fraudsters. This data set also needs the ability to check for inconsistencies and internally 'triangulated' for uncertainties, errors, and in particular, fraud (Yang et al. 2010).

2.2 ICT-enabled Information Processing Capabilities

Information processing includes the identification of information processing needs and capabilities and the fit between the two to obtain the desired outcomes (Premkumar et al. 2003). The theoretical notion builds on the basis that organisations are open social systems environment, such that groups and individuals need quality information, and the ability to gather, interpret, synthesise and disseminate that information properly, in order to cope with uncertainties and to improve decision-making (Tushman & Nadler 1978).

One aspect of information processing focuses on developing dynamic network-based structures which operate as a coordination mechanism (Kwon et al. 2007). This builds the foundation for a data-orientated culture, necessary to conduct business analytics, which in turn reduces the effect of uncertainty. Continual exposure to a specific type of structure will propel individuals toward proficiency in processing information. It will also enhance their ability and confidence to solve problems, through ongoing learning, in a manner consistent with this structure (Turner & Makhija 2012). Avgerou et al. (2011) claim that the organisational structures constitute the institutional setting for networks of e-commerce entrepreneurs. Implementing such structural mechanisms requires information processing capabilities in order to enhance the information flow. Hence, developing information processing control on top of networks is central to developing information processing capabilities, according to Huang et al. (2014). A sense of control guides individuals and groups during the change process, and can be provided both formally by business (Scheyvens 1999; Taibi 1994) that provide access to productive resources in an area, and informally by social actors in a group maintaining and/or enhancing a group's equilibrium (Scheyvens 1999).

Joshi et al. (2010) and Kim et al. (2011) confirm the importance of IT in creating a strong foundation for data acquisition necessary to build organisational capability. Accordingly, the emergence of business analytics and ICT-enabled information processing are inadvertently linked. In support of this view, a number of recent studies describe the growing value of using business analytics and big data on value creation or firm performance (Gillon et al. 2014; Seddon et al. 2012; Shanks et al. 2010; Wixom et al. 2013) and citing a lot of room for further empirical research. Business analytics is an "extensive use of data, statistical and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions." (Davenport & Harris 2007). Business analytics has been identified to contribute to firm performance and create competitive advantage (Davenport & Harris 2007). Profitability rates are 5-6% higher for firms with analytic capabilities than those without (Barton 2012; McAfee & Brynjolfsson 2012). High performing businesses have implemented data and analytics into their core business functions allowing for repeatable and accurate decision-making processes to maximise the potential of their data (Mulani 2013). We consider that

developing a business analytics capability is an ICT-enabled capability of information processing. However, to date, there is little research on the components and interrelationships between business analytics capabilities and information processing. Addressing this research gap can posit how business analytical capabilities lead to resource exploitation (Cosic et al. 2012), offering an integrated view of the relationships between IT capability and business value (Kim et al. 2011).

3 RESEARCH METHOD

A two-phase research approach is adopted (see Table 1) to identify (social fingerprinting as) an ICT-enabled information processing capability, and to develop a framework for the components and interrelationships of social fingerprinting. The first phase uses a case study methodology (Walsham 1995; Walsham 2006) to explore a technology start-up that applies a big data approach for fraud detection. We present a case study of Trustev, an organisation using social fingerprinting as a business analytic capability coupled with profile-based digital identity management to combat fraud. This method is necessary due to the absence of empirical research that specifically pertains to applications of business analytics capabilities and its direct impact towards specific business problems.

Stage	Step	Technique	Output
1. Identify components for social fingerprinting as an information processing approach	1) Interview participants	Semi structured interview	Data from eight interviews
	2) Analyse interview data	Content analysis	List of components of social fingerprinting
2. Develop a framework for interrelationships of social fingerprinting	3) Identify direct and indirect relationships among components 4) Develop a framework	Interpretive structural modelling	Generate a framework for social fingerprinting

Table 1. Research Approach

3.1 Data Collection and Analysis

Table 1 illustrates the empirical investigation that begins with semi-structured interviews, allowing us to perform probing when necessary. Following the interviews, content analysis can be used to interpret the data and identify components of social fingerprinting described in the interview. Then, in phase two, the interpretive structural modelling (ISM) technique (Warfield 1973) will be applied to allow us to find the interrelationships among the components of social fingerprinting. The intended output is a structured framework based on the interrelated components from the interview data.

No.	Title	Role/ Topics discussed
1	Chief Marketing Officer	History of company, Marketing strategies, key elements of social finger printing
2	Director of Fraud and data strategy	Social fingerprinting technologies, analytics, Trustev score.
3	Project Manager	Technical flow of social fingerprinting, Project methodology
4	Chief Technology Officer	The market for company, challenges of current mechanisms, logic behind systems, analytic technologies
5	Chief Executive Officer	Company's mission, corporate identity, vision, progress
6	Fraud and data specialist	Aims of company solutions, value of big data, capabilities built
7-8	Website User 1 and 2	Attraction of the company solution, how it can help the business

Table 2. List of Interviewees

The selection of interviewees was appointed by the organisation's Chief Marketing Officer (CMO) allocating those who had the greatest potential to address the research question. An accompanying interview guide creates opportunities to collect multiple sources of evidence. The use of open-ended

questions allows the interviewees to freely respond to the question without being directed or pressured into a particular response. Concurrently, a combination of temporal bracketing, narrative, and visual mapping strategies were applied to the empirical data to capture relevant themes (Langley 1999). In this paper, we present the results of the first phase of our research with a list of social fingerprinting components. For phase two, future work is to be conducted in order to develop a framework for the interrelationships among the components of social fingerprinting.

4 CASE DESCRIPTION AND PRELIMINARY FINDINGS

Named one of Forbes Magazine's Hottest Global Startups in 2013, Trustev is addressing the challenge of online fraud by using real-time, online identity verification to prevent fraud in e-commerce transactions. Since launching at TechCrunch Disrupt in New York City, Trustev has grown from three employees to 23 and raising US$3million by 2013 in one of Europe's largest seed funding rounds. With a focus on validating individuals making transactions, not just the payment method they are using, Trustev is using data analytics to reduce fraud and the cost of fraud. Trustev's social fingerprinting solution has proven to be successful since inception, as their big data initiatives have proven to turn insights into outcomes. Trustev tackles the problem using multiple, dynamic data sources — behavioural, transactional and social — instead of restrictive rules-based decision-making and profiling. This enables Trustev to gain maximum insights and therefore maximum trust into the actual identities of online merchant's customers through social media account information.

4.1 Trustev's Social Fingerprinting Solution

Applying state of the art big data techniques to the traditional definition of fingerprinting, Trustev's ICT-enabled fraud prevention solution posits that the impact of skin friction ridges could be used to match personal identity and be applied to the social side of businesses. Based on this, Trustev's strategy is to combine the elements of a digital identity with dynamic verification technology to formulate a score for fraud. This formula is known as a *Trustev score* (out of 100) and is presented to the merchant or customer. This process resembles a pyramid structure where all scores are grouped in categories. With the algorithm and machine learning, it will eventually go to the top of the pyramid and become a single Trustev score. Each one of Trustev's customers receives a bespoke configuration uniquely designed to promote positive and safe e-commerce growth. Trustev's customers have the choice of three thresholds when using the total score, which are to automatically reject, accept, or review the order. There are four key categories of information that assist in the scoring process – social data, behavioural data, transactional data and historical data. For example, in the "social data" category, if the investigated account is determined to be fake, the social score is basically weighed down to 0. This will have a significant impact on the overall Trustev score as it will indicate that the account is either compromised or illegitimate. During a transaction scenario, the user or requestor for the transaction will be rejected. However, it has been recognised that it is not essential for the customer to have social data - *"but our logic doesn't require customer or social input because not everybody has social and not every site has social. So our decision logic is actually dynamic. It recognises social data and reweights all the other inputs"* (Director of Fraud and Data Strategy, Trustev).

The implementation of the Trustev social fingerprinting scores consists of four steps. The first step involves adapting machine learning and algorithms to consumer behaviour on their customer's website. The second step is for the customer to integrate Trustev's solution. According to our investigation, this integration is supported by advanced analytics that provide big data visualisations to Trustev's customers in a fast and effective way. The third step is implementing Trustev's real-time decision engine which calculates the Trustev score. Eight supporting technologies enable this: (1) Machine Learning, (2) Algorithms, (3) Static profiler, (4) Activity Profiler, (5) Interaction Profiler, (6) Contact Profiler, (7) Location Profiler, (8) Transaction Profiler. Each of these technologies draw from various data sources in order to calculate a score, then those scores are weighted and eventually a full Trustev

score out of 100 is presented. In the final step and when the full Trustev score is presented to the merchant or customer, Trustev's customers can use this information to verify the consumer. A Trustev score below a defined threshold indicates that there is fraudulent activity and the transaction should be rejected. The end result enables merchants to increase the number of transactions that are trusted which increases revenue while at the same time decreasing fraud.

4.2 Developing Information Processing Capabilities for Combatting E-commerce Fraud

By applying the information processing notion, we identify an initial set of three ICT-enabled information processing capabilities that organizations must develop −based on the business analytic solution that is social fingerprinting− for combatting identity fraud. The capabilities are interrelated and work together, and cannot be viewed in isolation. Tables 3-5 show the development of information processing capabilities and the role of ICT.

Developing Identity Profiling posits the role of an authenticating reference which provides information regarding the user. This process of identifying and assessing the user is an ongoing relationship management activity that occurs behind the technology, i.e. the verification of the user's information is done before the user enters the website and especially before any transaction. The identity profile of the user is a strong indicator of whether the user is conducting fraudulent activities. As a result, the user's identity profile will be used to verify for specific business decisions, and in this case transactions on websites and any potential fraudulent activity on e-commerce platforms. With increasing digital identity fraud, creating a robust profile identity management system will make significant inroads towards reducing fraud and its associated costs. To generate the identity profile in social fingerprinting, three categorical sources of data are used: social content, interactivity and location. Social Content determines the authenticity of the user. The context of a user's Facebook profile, analysis on their friends and uploaded content online are captured, specifically, the volume of friends, the age groups of friends and other public information linking the user and their friends. Additionally, the age of the user's profile, from creation date and historical updates from the user where available can be used to generate an identity profile and be calibrated to produce a social score. It is noteworthy that the content of a user's social profile is not limited to Facebook, as users have different preferences for social media platforms. Data is captured through user's browser ultimately leading to their frequency of use – the second component of social fingerprinting, interactivity.

Constructs	Quote [sub-construct]
Social content and Role of ICT	"online, you see all these sources of data that is available, creating a social graph… dynamic information that is literally kept up to date by the user, every minute, every day is being added to" **[Uploaded content]** (Chief Marketing Officer, Trustev) "their friends, the volume of friends [couple hundred friends]… the age profile… And that's what ties in with the profile. All that kind of stuff, is part of what builds up the social score" **[Friends]** (Director of fraud and data strategy, Trustev)

Table 3. Developing Identity Profile

Developing Colocation Advice: Developing information combining of both physical and digital locations is crucial to determining fraudulent behaviour. *"location is one of the strongest indicator of fraud as it is very hard to replicate location in terms of a fake account"* (Director of fraud and data strategy, Trustev). To capture physical location, mobile cell site verification is used. In brief, mobile triangulation data can be captured as a mobile phone is transmitting information between cellular towers for Internet and phone reception. This data enables the service provider to pinpoint metres within your physical location with the mobile device. Additionally, now smartphones have a geolocation-tagging feature on social media platforms. Relating back to the social content provided by the user, status updates, and even conversation logs have a location attached to them. Geolocation is an important feature captured by applications such as Facebook. However, in our case, location is more closely related to digital location, as social fingerprinting looks at where the data is coming from

and where the user is "checking-in" on social media. Furthermore, the logic of social fingerprinting looks at the various types of interaction, the frequency of activity usage on social, and web browsing history. The behaviour of a user in the digital environment provides significant information about the user in regards to being a fraudster or the use of a compromised device. Furthermore, analysis of browsing patterns and website visits presents a more holistic view of the user.

Constructs	Quote [sub-construct]
Location Profile	"Derived information such as IP address and spoofing with location" **[Network location]** (Project Manager, Trustev) "their check-in location or some status updates have a location attached to them. That's all recorded via Facebook's API. So, that's an important feature... from a fraud prevention point of view. Again, location is probably one of the strongest indicator of fraud" **[Check-in digital location]** (Director of fraud and data strategy, Trustev)
Role of ICT	"dynamic decisioning based on user activity, their online movements, looking for signs of automated behaviour" **[Online activity]** (Chief Marketing Officer, Trustev) "So we have built into our logic a lot of that from Facebook, whereby if you look into frequency and every element of the account and ensure that this is, a human account and it is a used account by a real person" **[Frequency of use]** (Director of fraud and data strategy, Trustev) "If I'm using all the different features in Facebook with the frequent updates, frequent picture updates… you can consider a pretty good profile in general" **[Usage of different functionality]** (Director of fraud and data strategy, Trustev)

Table 4. Developing Colocation Profile

Developing Socio-Technical Expertise: Developing and applying socio-technical information processing techniques to ICT tools are essential. In support of this notion, Davenport and Harris (2007) note that analytics capabilities are driven by two supporting factors: i) enabling technologies and ii) analytics people. Similarly, Kiron and Shockley (2011) note that a data-oriented culture enables an organisation to drive insights from data and foster analytical people. In light of social fingerprinting, the people behind the technology are essential as they are able to produce the results. The Project Manager at Trustev attributed the success of social fingerprinting to the people who are using the tools in the team, who can effectively use it, and who can draw meaningful information from data.

Constructs	Quote [sub-construct]
Role of ICT	"we are a shared platform for fraud prevention. The data we use, and the information we have is actually shared on the platform for others to benefit from. It's the network effect" **[scalability and reliability]** (Director of fraud and data strategy, Trustev) "We have everything from JS data, which is device fingerprinting proxy, IP, proxy piercing technology, mobile verification, which is coming online soon. And dynamic blacklisting which is somewhat intelligent - matching logic itself, to other profiles." **[security and analytics]** (Director of fraud and data strategy, Trustev) "simple to integrate with straight forward implementation, code change is minimal, integration is done in a clean interface that can be customised" **[scalability]** (Project Manager, Trustev) "So we have metrics on things like, fingerprints, session hijacking, proxy usage volumes and that's all live" **[security]** (Director of fraud and data strategy, Trustev)
Socio-technical expertise	"So the key to data analytics is the people behind it, the people look at it, the people who present it… it is and always be the people who design, people who build and the people who review are the key to successful analytics." **[expertise]** (Director of fraud and data strategy, Trustev) "Having the fraud expertise to look at the data and to improve the algothirms." **[expertise]** (Project Manager, Trustev) "And the analyst function is to cross reference that with all the other data points to bring that down to a meaningful level and that's where, the fraud comes in. They have the fraud background but they also have some exposure to data. So they know exactly what they're looking for before they are going in." **[analyst]** (Director of fraud and data strategy, Trustev)

Table 5. Developing Socio-Technical Expertise

The socio-technical profile has implications on the scalability, security, reliability, and analytics of Trustev's solution. For scalability, the modular architecture of the solution enables "up and down" scaling, while remaining adaptive to different e-commerce environments. In terms of security, using techniques such as IP Detection, proxy piercing and real-time mobile lookup provides a continued service for preventing fraud and potential breaches. Additional techniques such as identification of browser ID, device ID, and site velocity contribute to network effects for vendors of the Trustev platform. Together with scalability and security, reliability is ensured through real-time decision-making, proactive detection using the machine learning models as well as having payment industries compliance and security standard specifications.

5 FUTURE WORK AND CONCLUSION

To achieve the goals of identifying the components of social fingerprinting and their interrelationships, further analysis will be continued after all interviews are completed. Based on the key components elicited during the interviews, a hierarchical framework will be generated to illustrate the interrelationship among the components. To do so, Interpretive Structural Modeling (ISM) technique, a well-established methodology for identifying and developing relationships within a system of related elements (Sage 1977; Warfield 1974), will be adopted. The objective of this methodology is "to expedite the process of creating a digraph, which can be converted to a structural model, and then inspected and revised to capture the user's best perceptions of the situation" (Malone 1975). ISM has been extensively applied by a number of researchers to develop a better understanding of the complex systems under considerations such as evaluating IS effectiveness (Kanungo et al. 1999), IT enablers and barriers for knowledge management systems (Anantatmula 2008; Bhattacharya & Momaya 2009) and student technology use motivations (Guo et al. 2012; Guo et al. 2011). Building an ISM of social fingerprinting will involve a number of steps specified in Table 6.

Step	**Description**
Step 1	Defining a set of components of social fingerprinting (preliminary results were presented above)
Step 2	Establishing a contextual relationship among all components (will be identified via a follow-up focused group discussion)
Step 3	Developing a structural self-interaction matrix (SSIM) to reflect pair-wise relationships of components identified during the interviews
Step 4	Developing a reachability matrix from the SSIM, and checking the matrix for transitivity
Step 5	Partitioning the reachability matrix into different levels
Step 6	Forming a canonical form of the matrix
Step 7	Drawing a directed graph (DIGRAPH) and removing the transitive links
Step 8	Converting the resultant digraph into an ISM by replacing component nodes with statements.

Table 6. Steps to Build an ISM of Social Fingerprinting

Social fingerprinting is introduced in this paper as an ICT-enabled information processing capability to combat online fraud and reduce cost. With business analytics promising in combating online fraud, organisations need to develop such ICT-enabled information capabilities which includes identity profiling, colocation advice, and socio-technical expertise. To demonstrate that social fingerprinting is a pathway for online businesses in combating online fraud, the key components of social fingerprinting will be further identified, and the hierarchical framework will be depicted to illustrate the interrelationships among them. Such an understanding of relationship among these social fingerprinting components is important as it will identify the "strength" of a component, thereby aids in understanding the relative position and influence of these components on each other (Hasan et al. 2007). Armed with this information, organisations will be better able to assess the relative importance of the influencing social fingerprinting components and their direct and indirect hierarchical relationships. Furthermore, the identification of the components that are at the root of other components (called driving components) and those which are most influenced by the others (called

dependent components) will allow organisations to prioritize their resources efficiently by focusing attention on the most significant capability, which is especially important when resources are scarce.

Acknowledgements

The authors would like to sincerely thank Dr Jan Ondrus for his kind advice and invaluable comments on the previous drafts of this paper. The authors would also like to thank Pat, Donal and the Trustev team for their time on this project.

References

ACFE. (2012). Report to the Nations on Occupational Fraud and Abuse. 2012 Global Fraud Study Retrieved 19 July 2014. from http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

Anantatmula, V. S. (2008). The Role of Technology in the Project Manager Performance Model. Project Management Journal, 39 (1), 34-48.

Avgerou, C., Li, B., and Poulymenakou, A. (2011). Exploring the Socio-Economic Structures of Internet-Enabled Development: A Study of Grassroots Netrepreneurs in China. The Electronic Journal of Information Systems in Developing Countries, 49.

Barton, D. C., David. (2012). Making Advanced Analytics Work for You. Harvard business review, 90 (10), 78-83, 128.

Bhattacharya, S., and Momaya, K. (2009). Interpretive Structural Modeling of Growth Enablers in Construction Companies. Singapore Management Review, 31 (1), 73-97.

Corporation, I. D. (2013). New Idc Worldwide Big Data Technology and Services Forecast Shows Market Expected to Grow to $32.4 Billion in 2017. Retrieved 16 April 2014. from http://www.idc.com/getdoc.jsp?containerId=prUS24542113

Cosic, R., Shanks, G., and Maynard, S. (2012). Towards a Business Analytics Capability Maturity Model. In Proceedings of ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012, p. 1-11, ACIS.

CyberSource. (2012). Uk Online Fraud Report 2012. Retrieved 25/07/14, 2014. from http://www.cybersource.com/en-ANZ/company/news/view.php?page_id=2172

Davenport, T. H., and Harris, J. G. (2007). Competing on Analytics: The New Science of Winning. Harvard Business Press.

Galbraith, J. R. (1977). Organization Design: An Information Processing View. Organizational Effectiveness Center and School, 21.

Gartner. (2013). Cio Agenda Insights 2013. Retrieved 15 April 2014. from http://www.gartner.com/imagesrv/cio/pdf/cio_agenda_insights2013.pdf

Gillon, K., Aral, S., Lin, C.-Y., Mithas, S., and Zozulia, M. (2014). Business Analytics: Radical Shift or Incremental Change? Communications of the Association for Information Systems, 34 (1), 13.

Guo, Z., Li, Y., and Stevens, K. J. (2012). Analyzing Students' Technology Use Motivations: An Interpretive Structural Modeling Approach. Communications of the Association for Information Systems, 30.

Guo, Z., Lu, X., Li, Y., and Li, Y. (2011). A Framework of Students' Reasons for Using Cmc Media in Learning Contexts: A Structural Approach. Journal of the American Society for Information Science and Technology, 62 (11), 2182-2200.

Hasan, M. A., Shankar, R., and Sarkis, J. (2007). A Study of Barriers to Agile Manufacturing. International Journal of Agile Systems and Management, 2 (1), 1-22.

Huang, P.-Y., Pan, S. L., and Ouyang, T. H. (2014). Developing Information Processing Capability for Operational Agility: Implications from a Chinese Manufacturer. European Journal of Information Systems, 23 (4), 462-480.

Jamieson, R., Wee Land, L. P., Winchester, D., Stephens, G., Steel, A., Maurushat, A., and Sarre, R. (2012). Addressing Identity Crime in Crime Management Information Systems: Definitions, Classification, and Empirics. Computer Law & Security Review, 28 (4), 381-395.
Joshi, K., Chi, L., Datta, A., and Han, S. (2010). Changing the Competitive Landscape: Continuous Innovation through It-Enabled Knowledge Capabilities. Information Systems Research, 21 (3), 472-495.
Kanungo, S., Duda, S., and Srinivas, Y. (1999). A Structured Model for Evaluating Information Systems Effectiveness. Systems Research and Behavioral Science, 16 (6), 495-518.
Kim, G., Shin, B., Kim, K. K., and Lee, H. G. (2011). It Capabilities, Process-Oriented Dynamic Capabilities, and Firm Financial Performance. Journal of the Association for Information Systems, 12 (7).
Kiron, D., and Shockley, R. (2011). Creating Business Value with Analytics. MIT Sloan Management Review, 53 (1), 56-63.
Kwon, D., Oh, W., and Jeon, S. (2007). Broken Ties: The Impact of Organizational Restructuring on the Stability of Information-Processing Networks. Journal of Management Information Systems, 24 (1), 201-231.
Langley, A. (1999). Strategies for Theorizing from Process Data. Academy of Management review, 24 (4), 691-710.
Malone, D. W. (1975). An Introduction to the Application of Interpretive Structural Modeling. Proceedings of the IEEE, 63 (3), 397-404.
McAfee, A., and Brynjolfsson, E. (2012). Big Data: The Management Revolution. Harvard business review, 90 (10), 60-68.
Mulani, N. (2013). The Million Dollar Opportunity: Reaping Returns from Analytics. Information Management.
Premkumar, G., Ramamurthy, K., and Saunders, C. S. (2003). Information Processing View of Organizations: An Exploratory Examination of Fit in the Context of Interorganizational Relationships. Journal of Management Information Systems, 22 (1), 257-294.
Roberts, L. D., Indermaur, D., and Spiranovic, C. (2013). Fear of Cyber-Identity Theft and Related Fraudulent Activity. Psychiatry, Psychology and Law, 20 (3), 315-328.
Sage, A. P. (1977). Methodology for Large-Scale Systems.
Scheyvens, R. (1999). Ecotourism and the Empowerment of Local Communities. Tourism management, 20 (2), 245-249.
Seddon, P. B., Constantinidis, D., and Dod, H. (2012). How Does Business Analytics Contribute to Business Value?
Shanks, G., Sharma, R., Seddon, P., and Reynolds, P. (2010). The Impact of Strategy and Maturity on Business Analytics and Firm Performance: A Review and Research Agenda. ACIS 2010 Proceedings.
Taibi, A. D. (1994). Banking, Finance, and Community Economic Empowerment: Structural Economic Theory, Procedural Civil Rights, and Substantive Racial Justice. Harvard Law Review, 1463-1545.
Turner, K. L., and Makhija, M. V. (2012). The Role of Individuals in the Information Processing Perspective. Strategic Management Journal, 33 (6), 661-680.
Turner, T., Schwager, A., and Guo, Z. (2005). Verifying E-Government Market Segments. In Proceedings of Proceedings of the International Conference on e-Government (ICEG 2005), p. 441, Academic Conferences Limited.
Tushman, M. L., and Nadler, D. A. (1978). Information Processing as an Integrating Concept in Organizational Design. Academy of management review, 3 (3), 613-624.
Walsham, G. (1995). Interpretive Case Studies in Is Research: Nature and Method. European Journal of information systems, 4 (2), 74-81.
Walsham, G. (2006). Doing Interpretive Research. European journal of information systems, 15 (3), 320-330.
Warfield, J. N. (1973). On Arranging Elements of a Hierarchy in Graphic Form. Systems, Man and Cybernetics, IEEE Transactions on, (2), 121-132.

Warfield, J. N. (1974). Toward Interpretation of Complex Structural Models. Systems, Man and Cybernetics, IEEE Transactions on, (5), 405-417.
Wixom, B. H., Yen, B., and Relich, M. (2013). Maximizing Value from Business Analytics. MIS Quarterly Executive, 12 (2).
Yang, Y., Lewis, E., and Newmarch, J. (2010). Profile-Based Digital Identity Management—a Better Way to Combat Fraud. In Proceedings of Technology and Society (ISTAS), 2010 IEEE International Symposium on, p. 260-267, IEEE.