Breaching intellectual capital: critical reflections on Big Data security

Matteo La Torre

Department of Economic Studies, University "G. d'Annunzio" of Chieti-Pescara, Pescara, Italy

John Dumay

Department of Accounting and Corporate Governance, Macquarie University, Ryde, Australia

Michele Antonio Rea

Department of Economic Studies, University "G. d'Annunzio" of Chieti-Pescara, Pescara, Italy

Accepted version

Please cite as:

La Torre, M., Dumay, J. and Rea, M.A. (2018), "Breaching intellectual capital: critical reflections on Big Data security", Meditari Accountancy Research, Vol. 26 No. 3, pp. 463-482. https://doi.org/10.1108/MEDAR-06-2017-0154

Breaching intellectual capital: critical reflections on Big Data security

Abstract

Purpose: Reflecting on Big Data's assumed benefits, this study identifies the risks and challenges of data security underpinning Big Data's socio-economic value and intellectual capital (IC).

Methodology: The study reviews academic literature, professional documents, and public information to provide insights, critique and projections for IC and Big Data research and practice.

Findings: The "voracity" for data represents a further 'V' of Big Data, which results in a continuous hunt for data beyond legal and ethical boundaries. Cybercrimes, data security breaches, and privacy violations reflect voracity, representing the dark side of the Big Data ecosystem. Losing the confidentiality, integrity, or availability of data because of a data security breach poses a threat to IC and value creation. Thus, cyberthreats compromise the social value of Big Data, impacting on stakeholders' and society's interests.

Research implications/limitations: Because of the interpretative nature of this study, other researchers may not draw the same conclusions from the evidence provided. It leaves some open questions for a wide research agenda about the societal, ethical and managerial implications of Big Data.

Originality: This paper introduces the risks of data security and the challenges of Big Data to stimulate new research paths for IC and accounting research.

Keywords:

Intellectual capital; Big Data; data security; data breach; cyberthreats; privacy

Acknowledgments

The authors are grateful to Dr. Aleksandra Pop-Vasileva from Monash University for her precious comments and advice in developing this article.

1. Introduction

Despite its widespread use in practice, the term Big Data has no accepted definition (Gandomi and Haider, 2015), which raises questions about Big Data's ontology. One early and commonly used definition, outlines three main characteristics: data volume, data velocity, and data variety (Laney, 2001). Since 2001, further characteristics have been used to define Big Data, such as data complexity, referring to the complex connections for transforming data from different sources, and veracity, which emphasises the potential value of the information Big Data holds (Gandomi and Haider, 2015). This fourth 'V' underlines that Big Data is an intrinsic source of value.

Undoubtedly, Big Data has opened up a range of opportunities for society. And the applications of Big Data are not limited to business; they involve an extensive number of sectors, such as medical, healthcare, government, and various disciplines, including natural sciences, life sciences, engineering, the arts, and humanities (Wang *et al.*, 2016). Rick Smolan, creator of the documentary "The Human Face of Big Data", acknowledges Big Data as a potential source for "humanity's dashboard" – "an intelligent tool that can help combat poverty, crime and pollution" (Lohr, 2012). Big Data is a powerful tool for addressing various aspects of "societal ills", such as cancer research, terrorism, and climate change (Boyd and Crawford, 2012, pp. 663–664). However, utilising the benefits of Big Data depends on an organisation's ability to leverage this opportunity, and there is an increasing awareness of the barriers facing organisations related to people, technology, and cultural factors (Alharthi *et al.*, 2017; Baumgarten *et al.*, 2013).

The sheer volume of data and its plurality of typologies cause us to question the sources of data and the ways they are gathered and used (Boyd and Crawford, 2012). Today, data is produced by everyone, everywhere through the use of mobile devices, digital services, and the Internet of Things leaving continuous digital traces (Perera *et al.*, 2015; Tien, 2013; Wang *et al.*, 2016). This proliferation of data raises serious concerns about privacy and the use of personal and sensitive user data.

Access to, and the acquisition of, data commonly occurs with the awareness and consent of people, although this is not always the case. Recent research by Arp *et al.* (2017) found serious privacy issues when embedding ultrasonic beacons into audio signals because of the ability to track users using the microphone in mobile devices. Many researchers have addressed privacy and Big Data on the grounds that the proliferation of mobile devices, geo-tagging services, and the wide use of social media gives it increasing relevance (Akoka *et al.*, 2017, p. 111; Smith *et al.*, 2012). Therefore, from the time data is captured to the point where knowledge is extracted, there is a compelling need to protect and enforce a user's privacy (Perera *et al.*, 2015).

While emphasising concerns for privacy, the risk of cyberattacks does not exclusively involve sensitive personal data. It also includes a wider range of data owned and stored by organisations. Most of the cybercrimes against organisations are committed with the intention of industrial espionage (Verizon, 2017). As a Financial Times[i] article points out, hacking or buying stolen sensitive data to gain an advantage over competitors is currently less risky for companies than engaging in the physical theft of files. As a result, "industries such as pharmaceuticals and technology, and defence, have seen products emerge that seem to draw heavily on stolen intellectual property". Chen *et al.* (2012, p. 1172) claim that "security issues are a major concern for most organisations" and the resulting increase in cybersecurity investments means several "security-related disciplines such as computer security, computational criminology, and terrorism informatics" have flourished. Therefore, while privacy is a compelling, yet individual, concern for users, and one that impacts the way organisations process data, the main challenge for companies is protecting their data from cyberthreats and security incidents.

Such social issues are neither merely technical, nor limited to technicians, computer science researchers, and cybersecurity practitioners. Instead, they deserve interest and engagement by various fields from an interdisciplinary perspective (Chen *et al.*, 2012, Chen *et al.*, 2014). Big data is under the spotlight in many research fields and is gaining momentum in IC research as well (Secundo *et al.*, 2017). Secundo *et al.* (2017, p. 242) provide an understanding and a conceptualisation of Big Data and IC by outlining the "socio-economic value of Big Data generated by and about organisational ecosystems". Specifically, as "Big Data and business analytics" can bring "new capabilities to organisational value creation" and support new intangible assets, the authors call for a need to discuss "how they fit within the IC universe" (Secundo *et al.*, 2017, p. 251). Big Data has several advantages for IC and IC management. However, the risks related to Big Data phenomenon have not yet been adequately explored, and very few management and accounting studies have investigated data security, data breaches, and their effects on organisations.

This study is a response to the call to examine Big Data by shifting the focus of IC research from organisations to their wider ecosystems (Secundo *et al.*, 2017). While Big Data continues to promise benefits in practice through utopian projections, this research is motivated by an academic and pragmatic intend to unveil another face of this socio-technical phenomenon, which encloses risks for organisations and society and challenges in creating value from Big Data. By this, it contributes to understanding how Big Data can threaten, rather than benefit, IC practice. Thus, we explore the challenges and risks of data security in the era of Big Data and its implications for IC as a way of introducing this topic to accounting research and to provide avenues for future research. Our intent is not to address any technical specificities, which are the preserve of other fields, but rather to offer new perspectives for Big Data as a managerial paradigm and to consider its critical implications for firms and society.

Accordingly, this study reviews the emerging academic literature, professional research and public information about IC, Big Data and data security issues. Such a review reflects and adopts the three methodological moments of a critical research approach, which are: providing "Insights", "Critique" and developing "Transformative redefinitions" (Alvesson and Deetz, 2000, pp. 17–20; see also Massaro *et al.*, 2016). Therefore, the remainder of this paper proceeds along these steps and is structured as follows. Section 2 provides insights and critiques the research under review, outlining the challenges for IC relating to Big Data and data security. Accordingly, Section 3 provides transformative projections on the implications for IC management and the future research paths in accounting. Last, Section 4 presents our conclusions.

2. Big Data challenges and risks for intellectual capital

In this section, we review and critique the challenges of Big Data phenomenon, so as to remark its impact and risks for IC. The first subsection focuses on the relations between Big Data and IC, by discussing how Big Data brings organisations to transform their IC. The second one introduces the challenge of data security arising from Big Data. The third subsection examines the risks of data breaches for IC, by developing a framework that explains how cyberthreats effect IC.

2.1. Re-shaping intellectual capital

2.1.1. Big Data and intellectual capital

IC is a well-established and flourishing research topic, yet it is continually evolving (Guthrie et al., 2012). As outlined by Dumay and Garanina (2013, p. 169), IC has been defined in several ways and has undergone a continuous evolution over the transformational stages of IC research. Dumay (2016) recently adapted a seminal definition of IC to highlight its role in creating value. He defines IC as "the sum of everything everybody in a company knows that gives it a competitive edge. Intellectual capital is intellectual material, knowledge, experience, intellectual property, information that can be put to use to create value" (Dumay, 2016, p. 169). As value creation is embedded in the fourth stage of IC research, investigations into IC management need to shift attention from the organisation to its wider ecosystem where knowledge and value are created (Dumay, 2013; Dumay and Garanina, 2013, p. 21). The interaction between an organisation and its ecosystem is bidirectional, encompassing how value is created for, and by means of, the entire ecosystem in addition to its external impacts.

Within this ecosystem, Big Data currently represents a megatrend for organisations. In examining the nexus between Big Data and IC, Secundo *et al.* (2017) argue that "a Big Data perspective validates the need to shift IC's research focus from organisations onto ecosystems, and to view intangible asset creation and management", because "Big Data can originate from either inside organisations or from wider ecosystems" (Secundo *et al.*, 2017, p. 238). The root of Big Data is neither internal to a single organisation nor restricted to one or a narrow group of companies.

Volume, velocity, and variety are external factors characterising the current data management scenario. Big Data is the result of a wide set of components of the Big Data ecosystem (Demchenko *et al.*, 2014), and the amount of available data is the result of the current social, economic, and technological environment. This data not only includes social media data, the data derived from the Internet of Things, mobile data, and sensor data, etc. but also the technological infrastructure that stores and processes it, such as cloud computing and high performing architectures (Yaqoob *et al.*, 2016, p. 1234). Big Data is the result of the systemic interaction of factors that form organisational ecosystems, and which they, in turn, contribute to shaping.

Using Big Data also affects organisations and their internal processes. Research from the McKinsey Global Institute (2011, p. 2) suggests that Big Data is as a driver of "innovation, productivity and growth", and "new modes of competition and value capture". Big Data's tangible advantages include more access to data, better experimentation and segmentation for customised actions, support for human decisions through automated algorithms, and the discovery and innovation of new business models (McKinsey Global Institute, 2011, p. 5). According to this view, argue that Big Data can improve IC management regarding the IC (Petty and Guthrie, 2000, p. 166):

- human capital, by improving know-how and innovativeness for example;
- relational capital, resulting from better relations with customers; and
- structural capital, concerning changes in management processes.

Secundo *et al.* (2017, p. 247) state that Big Data "creates new value and new opportunities for IC management", which provide value for organisations and their wider ecosystems. In their framework, the authors conclude that the value gained from Big Data is coherent with the IC strategic objectives "to move beyond IC's monetary value and find organisational wealth in more general terms", by promoting a more equal and inclusive society, organisational transparency, continuous innovation, and better decision making" (p. 249). However, Big Data's potential impact is neither immediate nor easy to achieve. Data has no intrinsic value alone, and neither the volume nor velocity of data can create a competitive edge, since "the potential value of Big Data is unlocked only when it is leveraged to drive decision making" (Secundo *et al.*, 2017, p. 249; 251). Hence, although Big Data has several implications and potential impacts in different contexts, its source of competitive advantage needs to be analysed by reducing Big Data's use to its narrowest purpose.

The basic aim of Big Data applications is to support decision-making. Wang *et al.* (2016, p. 751) assert that while "decision science supports decisions in the procedures of analysis of data … the overarching purpose and reason of Big Data are about decision making" which "can result in intelligent decisions based on raw data". Figure 1 shows Tien's (2013, p. 131) framework for decision-making. It explains how raw data is transformed into valued insights for facilitating and developing knowledge. Wang *et al.* (2016, pp. 750–751) argue that "decisions are made by deriving information from data, obtaining knowledge from information and then achieving wisdom from knowledge" to finally gain competitive advantage. As more decisions become strategic and systemic in this process (for example in transforming insights into organisation knowledge), so too is the human factor becoming more crucial in providing valuable insights from that data to create knowledge.

Insert Figure 1 here

2.1.2. The challenge of transforming IC and human capital

The human factor represents a significant non-technical challenge for Big Data. Alharthi *et al.* (2017) argue that, in addition to the technological challenges, there are important organisational and human barriers for Big Data initiatives. These include the lack of a proper organisational culture and, on the human side, the need to develop Big Data skills. The main challenge of Big Data is "to support human analysts and managers to make quicker decisions" based on reliable and valued information, and this entails the need to develop technologies that can enhance the interaction between data and users (Wang *et al.*, 2016, p. 760). Accordingly, this highlights the need to improve the interface between analytics and human cognition by addressing the challenge of "visualisation", i.e., the ability to represent knowledge and facilitate human understanding (Assunção *et al.*, 2015, p. 10; Yaqoob *et al.*, 2016, p. 1244). Thus, despite its technological roots, Big Data highlights the importance of the human dimension, which may also be its doom if not properly addressed.

Academic research recognises Big Data and analytics as a means of enabling knowledge management and creating knowledge for strategic decision-making (Intezari and Gressel, 2017; Uden and He, 2017). Thus, it takes advantage of an organisation's intangible assets (Rothberg and Erickson, 2017). Such pools of knowledge extend benefits to machine learning and artificial intelligence applications that provide pattern analysis and predictions to assist timely, data-driven decisions (Tian, 2017). Wang *et al.* (2016, p. 757) point out that, in using social media data,

> *"researchers and managers can derive knowledge from the customers' opinions to realize the market transformation and improve their business strategies; Agencies can identify the features and the patterns of crimes and criminals from environmental and situational factors to support law enforcement; Service providers could visualize social media data to enable better user experience and service".*

Big Data is opening up new ways of discovering and creating knowledge with impacts on the activity, business, and competitiveness for all kinds of enterprises. However, these benefits mostly depend upon an organisation's ability to leverage the knowledge with that data, and this is a privilege of human intelligence.

Big Data analytics, whether predictive, descriptive, or prescriptive (Chen *et al.*, 2012, p. 1182) and however produced (Wang *et al.*, 2016, p. 756), are designed for human intelligence – people have to use and apply the results. Accordingly, IC gains significance in such a process. In their study on IC, Petty and Guthrie (2000, p. 157,159) observe that IC "is implicated in the process of leveraging and developing organisational knowledge" and knowledge management exists in the act of managing the IC controlled by a company. Secundo *et al.* (2017, p. 251) argue that Big Data can bring new capabilities to organisational value creation, but there is a need to unlock the value of Big Data. IC management is a way of unlocking Big Data's value, but it depends on certain IC assets. In particular, organisations must be able to create knowledge from that data and then convert it into value.

McAfee and Brynjolfsson (2012) state that before seeing a beneficial impact from Big Data on management and performance, companies must first revolutionise the culture surrounding their organisational decision-making processes. In the context of Big Data, it is human capital that provides valuable insights and knowledge from data. Organisations need to face the challenge of re-shaping their human, relational, and structural capitals to allow IC management to capture Big Data's value. This means changing people's skills, approaches to innovation and change, the organisational culture, internal procedures, information systems, and decision-making processes. Therefore, while we agree that Big Data is a valuable source of IC for organisations, our concerns rest with the challenges organisations still need to address to increase the value of their intangible assets.

2.2. The challenge of Big Data security

Given the benefits from Big Data do not depend solely on technical factors, there is a compelling call to address the non-technical barriers that prevent value creation from Big Data (Assunção *et al.*, 2015). One of those challenges is privacy preservation and data security. The National Academy of Engineering identifies securing cyberspace as one of 14 "grand challenges" coming from Big Data and classifies the need for "enhancing privacy and security" among the challenges with the highest impact (Tien, 2013, p. 140). The Global Risks Report 2017 unveils "rising cyber dependency", due to "increasing digital interconnection of people, things, and organisations", as one of five global trends and sources of risk (World Economic Forum, 2017, p. 11,63). In an age where digital data is generated by everyone, everywhere using mobile devices, digital services, and web applications, societal, financial, and geopolitical cyberrisk is at the forefront of concern.

Baumgarten *et al.* (2013, p. 6) assert that "data generated from everything … will continue to create new sources of value and insight". However, it also raises concerns that are bringing individual privacy issues to the fore. As Michael and Miller (2013, p. 23) explain, we constantly "leave behind digital footprints that, when combined, could denote unique aspects about ourselves that would otherwise go unnoticed, akin to digital DNA". So, despite the claim that volume and variety are the main advantages of Big Data, they are also the main source of concern regarding privacy and significant constraint for organisations in acquiring and processing personal data.

Privacy issues are not the only concern in data security. In addition to privacy, Big Data brings further security challenges (Chen *et al.*, 2014, p. 204). Big Data security concerns three qualities of data: confidentiality, integrity, and the availability of data (Akoka *et al.*, 2017). According to ISO/IEC 27001 the main aims of an "information security management system" are to preserve the "confidentiality, integrity and availability of information by applying a risk management process and give confidence to interested parties that risks are adequately managed" (ISO, 2013, p. V). The potential loss of any of these three characteristics will have an impact on the value of Big Data.

Big data security is a major component of the whole Big Data ecosystem (Demchenko *et al.*, 2014), and it is gaining momentum in Big Data research (Akoka *et al.*, 2017, p. 111; Chen *et al.*, 2014). Protecting information, even when paper-based, is an ancient human imperative, but the socio-economic context has changed. Digitalisation, the modern knowledge-based economy, and advances in technology all increase the risks to security and the threat of privacy violations and data breaches[ii], amplifying the need for increased data security. They also stem from the same driving forces as Big Data – the high volume, high velocity, and high variety of data. Thus, data protection is the flip-side of the Big Data coin.

Protecting data is not merely an altruistic act by corporations for the sake of user privacy or regulatory constraints, it is also driven by self-serving interests. Regarding data security, Lee (2017, p. 301) argues that "weak security creates user resistance to the adoption of Big Data", as "it also leads to financial loss and damage to a firm's reputation" because without "proper security mechanisms, confidential information could be transmitted inadvertently to unintended parties". Thus, the risk of a security breach not only impacts individual privacy but may have a serious effect on the organisations because that data may hold significant value. If using Big Data can increase a firm's competitiveness, then data is a source of value for organisations with many corresponding economic rationales to protect that value from external threats.

The paradigm "data as value" affects the competitive dynamics among firms. According to Verizon's (2017, p. 6) annual survey on data breaches, most breaches are motivated by financial reasons or cyberespionage. In the current business environment, stealing or buying hacked digital data to gain a competitive advantage is easier than in the past. These trends are creating a real marketplace for data on the dark web, an encrypted network where hackers buy and sell hacked and stolen data. For example, Yahoo Inc. has recently experienced a massive data breach of its user data. Users received a message from the company, shown in Figure 2[iii]. The stolen data was subsequently sold on the dark web for $300,000 per unit, and some are still for sale[iv]. This represents the emergence of a "hidden data economy", where stolen data, such as identities, financial data, credit card information, and access information, finds a market on the dark web (Mcfarland *et al.*, 2015). Data-driven competition pushes organisations to compete in a race to acquire as much data as possible. This voracity for data is detrimental with implications for the wider ecosystem in terms of the risks to organisational value creation.

Insert Figure 2 here

2.3. Threats to intellectual capital: a framework for the cyberthreats to intellectual capital

The risks of data breaches and cyberthreats are results of the voracity for data, which, in turn, affects IC. Snyder and Crescenzi (2009) point out that IC's great value in creating wealth is offset by its increasing vulnerability to cybercrime, and has created a new environment that puts IC at risk of financial crime. It is difficult to find a unique definition of cybercrime, mainly due to the wide taxonomies of crimes and the different perspectives that can be employed to classify them (Gordon and Ford, 2006). Yet, to distinguish cybercrime from financial crime, Gordon and Ford (2006, p. 16) argue that "the user whose machine is penetrated but suffers no financial loss has not really participated in the cybercrime – the crime is purely technological in nature". In the Big Data context, we would add that this risk for IC extends to many other cybercrimes because, even without a direct financial loss, a cyberattack may cause indirect costs or an intangible loss of value.

A data breach can involve several costs for an organisation. The average total cost of a data breach is $4 million ($158 per lost or stolen record), and this is mostly due to the loss of customers (Ponemon Institute, 2016, p. 2). The rapid "digitisation of consumers' lives" will increase the cost of data breaches to $2.1 trillion globally by 2019 (almost four times the estimated cost of breaches in 2015)[v]. Although there are differences among countries and industries, about half of this cost is due to indirect costs, including a loss of goodwill and customer churn (Ponemon Institute, 2016, p. 20). These indirect costs reflect just some of the financial threats arising from a security breach.

Security breaches can threaten several aspects of IC value and its role in creating value from data. The effects on IC's intangible assets can be framed using the three data security criteria – confidentiality, integrity, and availability. Table 1 summarises the effects on IC by outlining the threats and risks for the three groups of IC's intangible assets – relational capital, human capital, and structural capital (Petty and Guthrie, 2000, p. 166). Accordingly, these threats are discussed in detail in the following sub-sections to provide a framework for explaining the impacts of cyberthreats and data breaches on IC. Thus, our framework contributes to understanding the risks for IC by framing the relations between data security breach, cyberthreats and intangible assets.

Insert Table 1 here.

2.3.1. Threats from a confidentiality theft or leak

Loss of confidentiality can occur when data is stolen, or even disclosed, by unauthorised parties. When a data breach involves personal or sensitive data about customers or employees, its confidentiality is lost causing serious reputational risks for organisations. Reputational damage is the biggest impact of a data breach for firms, as it affected brand image and decreased economic value.

The most devastating breaches to an organisation's reputation and brand image come from stealing or losing confidential customer data and business information (Ponemon Institute, 2011). Consequently, customers tend to lose trust in both the company and its efforts to protect their data, undermining the value of its relational capital.

The risks from customer loyalty damage may be higher for web companies, like social networks or email service providers, whose market value mostly depends upon a large number of users. In these scenarios, a serious data breach may bring a viral drop in user numbers with a significant impact on the business. For example, after the public disclosure of the massive Yahoo data breach in 2016, Verizon Communications Inc. sliced $350 million off its acquisition offer for Yahoo, dropping its offer down from $4.83 billion to $4.48 billion[vi]. The Yahoo case, among many others, like the massive breach involving eBay's customer data in 2014[vii], demonstrates the impact of security breaches on businesses.

Reputational risk is also demonstrated by the need to publicly disclose security breaches. Many states have recognised the public interest in disclosing certain data breaches and have enacted security breach laws that require organisations to notify consumers of breaches to their personal data. For example, the recent General Data Protection Regulation (EU Regulation 2016/679), enacted by the EU, requires a mandatory breach notification to customers within 72 hours of an organisation becoming aware of an incident that will likely "result in a risk to the rights and freedoms of natural persons". However, as the Yahoo case demonstrates, data breaches may be discovered and publicly revealed years after the incident, and this delay may weaken customer reactions.

Loss of confidentiality also impacts on the value of intangible assets belonging to human and structural capital. A data breach may result in the theft of intellectual property and organisational knowledge that are sources of competitive advantage. Clarke (2016, p. 12) asserts that, in addition to personal and sensitive data leaks, other "valuable information, such as intellectual property, are under threat from cyber-espionage, insider threats and inadvertent exposure". Companies attempt to obtain "information related to trade secrets and intellectual property that can bring financial payoffs, market leadership, and economic growth", by breaching secret knowledge about designs, formulas, manufacturing processes, research and future plans. Firms use competitive intelligence to shape their strategic planning, but sometimes they may cross ethical and legal boundaries (Sinha, 2012, p. 37). In other cases, gaining market share and increasing profits are justifications for such behaviour, and corporate spying is "a deliberate strategy to undermine competitors or even an entire industry" (Bressler and Bressler, 2014, p. 1). Hence, cyberespionage is a compelling concern for knowledge-intensive firms and for some entire industries.

Industrial espionage is the "dark side of the digital era" (Nodoushani and Nodoushani, 2002), and the current scenario of increasing cybercrime is extending the shadow. Warren (2015, p. 5) asserts that an "intellectual property breach can be catastrophic for employees too", because "financial losses from cyber-theft could cause as many as 150,000 Europeans to lose their jobs". Accordingly, "cyber-security has become a priority for company boards across virtually all business sectors". Cyberespionage is a risk for IC because the theft of intellectual property and leaks of valuable trade knowledge undermines a firm's innovativeness and competitiveness, and may mean serious consequences for its long-term prospects and competitive advantage.

2.3.2. Threats from compromising integrity and availability

Integrity and the availability of data are further characteristics of data security, which, in turn, affect the quality of data. When unauthorised third parties steal, modify, or delete data, data security is violated, and the quality of the data may be compromised. Along with confidentiality and privacy, integrity and availability must be ensured (Subashini and Kavitha, 2011, p. 5) because interruptions to the available data supply can raise serious problems. SQL injection, for example, is a common malicious attack used to manipulate, cancel, or retrieve data from databases. Although this is a very old and well-known attack, it remains a pervasive threat (Ponemon Institute, 2014). Malicious users can gain unauthorised access to sensitive enterprise data, causing financial loss and lack of reliability, which affects the value of the information and the knowledge resulting from the data.

A data breach that compromises the integrity or availability of data has implications for both structural and human capital since it can affect information systems, IT systems, data systems, management processes, operating processes, and employee knowledge. However, while these are the most immediate and tangible impacts, the most drastic effects are embedded in the process of knowledge creation and management. A study by Gemalto (2017, p. 14) underlines the current importance of "integrity cyber-attacks", stating that, "organizations base their decisions on the data they have access to and often rely heavily on its validity … if hackers or governments can modify the integrity of the data, major business decisions can be manipulated, resulting in significant yet still unknown consequences". When data is altered or destroyed, it loses the ability to provide useful knowledge for decision making. In fact, the resulting lack of data integrity could even drive users to make wrong decisions.

Data integrity is currently being undermined by the emerging phenomenon of "data sabotage". A recent report from Stroz Friedberg (2017) found that data sabotage is the next imminent cyberthreat and will become a reality in 2017. "Criminals will seek to sow confusion and doubt over the accuracy and reliability of information, impairing decision-making across the private and public sector" (p. 12). Compared to data destruction, data sabotage is a more devious and malicious attack, as it remains a hidden but persistent menace to knowledge and internal processes until its detection and leads to unreliable information and dysfunctional decisions.

The impact of data sabotage can have catastrophic effects because of the increasing connections between people, things, and technology. Due to the rising adoption of machine learning and automation, data sabotage is a big concern for the Internet of Things because the effects of those devices extend into people's daily lives. When the integrity and availability of data are compromised, many aspects of knowledge management are threatened, and the detrimental effects extend throughout the entire IC ecosystem where decisions find their societal impacts.

3. Projections and implications for research and practice

This section presents transformative projections resulting from our review. By this, we deal with the third and last step of our research. By synthetising our research findings, Table 2 summarises the insights and critique of our review and the related research and practical implications discussed in the subsections below.

Insert Table 2 here.

3.1. Implications for IC management: a call for a human-oriented movement

Although research attention has predominantly focused on the technological aspects of Big Data, over time, Big Data is revealing the importance of its human and social implications. As argued, Big Data reshapes an organisations' IC. This implies the need to connect and align Big Data technologies with human capital, by arguing that the compelling need to make organisations ready for the Big Data era is pushing them to revise and reshape their human capital (Baumgarten et al., 2013). While the technological architecture of Big Data is needed to manipulate, process and analyse data, the human factor is crucial to transform data into knowledge and then develop organisational wisdom. Therefore, in creating new knowledge, Big Data's value depends upon the organisations' human capital.

To realise Big Data's knowledge creation benefits highlights the need to develop employees' talents, skills and develop a data-centric culture. Similarly, Wang *et al.* (2016, p. 760) assert that "human expertise still plays an important role in decision making and cannot be easily replaced by Big Data analysis in business and management models", while also arguing that, "technologies for Big Data should enhance their functions of interacting with users". Organisations are becoming, or should become, data-centric when producing data-driven knowledge, but the Big Data movement and technologies need to be human-oriented.

Big Data-driven decisions can be improved if organisations can combine technological advances in Big Data with their internal processes and resources. Gaining benefits from Big Data requires a "new culture of decision making", which rises to the challenges of building a suitable leadership team, a new company culture, and new rules, talents, and skills (McAfee and Brynjolfsson, 2012, pp. 65–67). These challenges also require reflection on the changes to teleoaffective structures – the transformations in human and structural capital.

Schatzki (2005, pp. 471–472) defines teleoaffective structures as "an array of ends, projects, uses (of things), and even emotions that are acceptable or prescribed for participants in the practice". He offers an ontological approach to social practices, called "site ontology", which assumes that "social life is tied to a context (site) of which it is inherently a part … the site of social life is composed of a nexus of human practices and material arrangements" (Schatzki, 2005, p. 465). Ahrens and Chapman (2007, p. 8) observe that an understanding of the "rules and the engagements of teleoaffective structures organise chains of actions", which provide an understating of dynamics that make up practices. Action research on IC could fruitfully embrace such an ontological perspective to better understand Big Data practice within organisations and the resulting changes in teleoaffective structures to enable value creation from data.

Changes in teleoaffective structures must establish internal mechanisms for data protection and security. In response to cyberthreats and the risk of security breaches, IC management needs to revise human and structural capital by establishing procedures, processes, knowledge, and skills to enact proper security management systems. In this process, human capital has a critical role since the greatest organisational vulnerability lies in human and behavioural factors.

Alharthi *et al.* (2017) argue that "although technology glitches may lead to privacy or security breaches, it is the behavioural side of privacy and security that is often most problematic". They specify that "it does not matter how strong or advanced the technical dimension of security is as long as humans are in charge of the data" (p. 291). Similarly, a lack of proper skills among employees may increase data entry or data management errors causing the loss of valuable information or limiting the value gained from the data (Alharthi *et al.*, 2017, p. 288). Therefore, behind any cyberattack, security breach, or incident, there is a human responsibility, which reflects the vulnerabilities resulting from a lack of proper skills, knowledge, and awareness.

The emerging "social engineering" techniques for cyberattacks reflect such human vulnerability by taking advantage of human cognitive biases. Social engineering refers to psychological tactics (e.g., phishing) that manipulate people into performing actions within a complex fraud scheme. By these means, hackers leverage people's emotions – curiosity, empathy, fear, greed, excitement, and so on (Abraham and Chengalur-Smith, 2010, p. 187). Accordingly, human resources and organisational cultures are the main centres of focus for effective security management systems (Chang and Lin, 2007). However, in practice, the human factor is "generally considered the weakest link in an information security program" (Abraham and Chengalur-Smith, 2010, p. 183). It has been demonstrated that auditing human behaviour is difficult and that informal approaches aimed at changing internal cultures are often more effective for preventing cybercrimes (Vroom and von Solms, 2004). Practitioners need to be aware of the importance of the human factor in protecting their data. In establishing data security systems, policies, and procedures, managers have to control their IC in a way that aligns human and structural capital to mitigate cyber threats. For example, security awareness training can create and promote proper organisational knowledge and people skills for data security.

The challenges of Big Data are not merely technological. Big Data use is a social practice with managerial and human implications. Cybercrime, the threat of data breaches, and the need for data security are just some of the challenges for Big Data. They shape current organisational ecosystems and threaten IC and the value of data. And, since there is little knowledge and empirical evidence in IC research on this topic, we advocate that future empirical studies need to investigate the effects of cyberthreats on IC and value creation, including its ethical and social implications, thus shifting the focus to the wider IC ecosystem.

3.2. Social and ethical implications of Big Data: the emergence of a new corporate accountability

The digital age is changing modern society, and Big Data presents new societal and ethical challenges. Privacy issues are one of the challenges that involve people and their life in society. Privacy is an ancient issue with little agreement as to its definition (Moore, 2013). Yet, there is widespread consensus on the privacy concerns arising from Big Data.

Boyd and Crawford (2012, p. 662) offer a critical examination of the "cultural, technological, and scholarly phenomenon" that is Big Data. The authors claim that with the rise of Big Data as a "socio-technical phenomenon", there is a need to critically interrogate its assumptions and biases. Despite admitting that very little is understood about the ethical implications of Big Data, they question whether Big Data will "usher in a new wave of privacy incursions and invasive marketing" (Boyd and Crawford, 2012, p. 662). Claims that the use of publicly available data is ethical are also dubious. Using data requires a sense of accountability that crosses the boundaries of privacy (Boyd and Crawford, 2012), and while Big Data has increased concerns over people's privacy, it implies reflection on the accountability of organisations and researchers in using data, even when it is publicly available.

Such accountability should recognise and limit the end use of Big Data, and consider the implications of that use on people's life and society. Michael and Miller (2013) observe that "corporations are using Big Data to learn more about their workforce, increase productivity, and introduce revolutionary business processes". Yet, these benefits may be derived at the cost of continuously tracking employees' actions and measuring their performance in a way that builds "a level of oversight that can quash the human spirit" (Michael and Miller, 2013, p. 23). Thus, the ethical challenges that Big Data presents are embedded in the way this new phenomenon is changing human life and its detrimental effects on society. The current ecosystem, where the voracity for data creates a data hunt resulting in data breaches and theft, demonstrates these detrimental effects. When user data stored by a company is stolen, an individual's personal privacy is the victim. Therefore, corporations have a responsibility and an ethical duty to protect personal data, and data security becomes a collective interest for stakeholders and society.

People and corporations have unequal interests and power in controlling and using data. Boyd and Crawford (2012, p. 673) point out that "new digital divides" emerge from Big Data ecosystem because, in practice, large amounts of data are not available to everyone. Access to data is usually limited to a few groups of companies and individuals. This creates societal inequalities between those who create data by leaving digital traces – the largest part of society – and those who can collect and analyse it – the smallest and most privileged part. This latter group represents those with the power to "determine the rules about how Big Data will be used" (Boyd and Crawford, 2012, pp. 674–675). Power is concentrated around a small group of large, well-known companies who can access, collect, and use the large volume of data people create. Such power is reflected in the language companies use on their websites to acquire consents for collecting data from users (Pollach, 2005). In this context, Big Data implies the emergence of a new corporate accountability to an organisation's stakeholders resulting from the threats to user privacy when storing and using personal data, and the power these corporations wield within Big Data ecosystem.

3.3. Implications for accounting research agenda

Stemming from its traditional purpose of producing, analysing, and using data for internal and external purposes, the accounting discipline has close ties with Big Data. As such, accounting is entering a potential new dimension of complexity with respect to sustaining competitive advantage and managing various stakeholder interests. While the notion of Big Data is gaining momentum in accounting research (with a dedicated special issue of Accounting Horizons, 2015, Vol. 29 as one example), very little is known about data security in management and accounting. Some aspects of Big Data usage, analytics, storage, costs, and form have been considered potential challenges for the audit profession, and rightfully so (Alles, 2015; Cao *et al.*, 2015; Krahel and Titera, 2015; Yoon *et al.*, 2015). The accounting profession and the emerging behavioural issues regarding audit judgement and decision making have also been explored (Vasarhelyi *et al.*, 2015; Warren *et al.*, 2015).

However, further exploration of Big Data's broader implications for stakeholders has thus far been overlooked. Furthermore, as Big Data shapes the future of accounting and corporate reporting, data security and cyberthreats can be fruitfully explored as significant factors in investor decision making.

Big data is expanding the ecosystem of corporate data usage (Vasarhelyi *et al.*, 2015), along with the risks for organisations and their stakeholders. Adding to the complex organisational milieu linked to Big Data is the issue of data security and the threat of data breaches, which exposes organisations to further vulnerability. These include threats to innovation, looming detrimental effects in research and development, loss of competitive edge, reputation, brand image damage, impaired relationships with customers, and long term adverse effects on future profitability. A data breach involving customer data may be detrimental to the relationships between companies and stakeholders and implies accountability for companies. Consequently, organisations prefer to keep their security incidents secret and are not often willing to unveil data breaches, to avoid trouble arising from adverse stakeholder reactions. Moreover, as the nature of the relationships between corporations and their customers is not purely transactional, the weight of a data breach resulting from approaches to managing customer information can carry well beyond market share to impact societal, ethical, and cultural domains.

Notwithstanding the rhetoric on the public interest of accounting information, the rise of cybercrime poses the question of how such risks will impact accounting information and the extent to which acts of cybercrime turn into a public risk. Cyberrisks, like data fraud or theft, cyberattacks and the adverse consequence of technological advances, now represent a large share of the major global risks and are strongly connected to financial, societal, and geopolitical issues (World Economic Forum, 2017).Therefore, considering the widespread claims about accounting for the public interest (Sawabe, 2005), the lack of interest from academics and practitioners in accounting regarding cyberthreats would seem to be logically unjustified. Consequently, broader considerations of corporate accountability with respect to data security management and the exercise of power over the use and misuse of Big Data serves as an area worthy of further research exploration and attention by policy makers in accounting.

4. Conclusion

This study examines Big Data, by critically exploring the effects of data security and cyberthreats on IC. While Big Data helps create IC value, it also threatens an organisation's IC and its impact on the wider ecosystem. The Big Data ecosystem suffers from security threats that undermine IC and organisational value creation. The paradigm "data-as-value" creates a data-driven competition in which organisations compete to gather as much data as possible. However, the higher risk of data security breaches, along with the threat of privacy violations, emanate from the same forces that characterise Big Data ecosystems – high volume, high velocity, and high variety. Cybercrimes and data breaches represent the other, detrimental, side of Big Data that is seldom discussed in the Big Data debate. We advocate that the "voracity" for data represents another 'V' which characterises Big Data, and one that emphasises the detrimental effects of cyberthreats and data security issues that are part of Big Data.

Cybercrimes and data security breaches shape the current IC ecosystem, undermining IC and value creation. The loss of confidentiality, integrity, and availability of data resulting from data theft, data leaks, cyberespionage, and data sabotage threaten relational, structural, and human capital. Thus, reputational risk, damage to brand image, a lack of competitiveness and innovation, losing the value of knowledge for decision-making, and damage to infrastructure assets are all risks to IC's value that stem from data security concerns.

The transformative projections we previously discussed lay out a new research agenda underlining the business and societal challenges that undermine Big Data's benefits. Big data can benefit IC but organisations also have to face challenges, and data security is one (Assunção *et al.*, 2015; Wang *et al.*, 2016). Organisations have societal, ethical and managerial facets, and these reveal Big Data's important human dimension, which could become its doom if not properly addressed. Data is fuel for complex Big Data ecosystems (Demchenko *et al.*, 2014), and organisations need to enact internal changes to use it across their entire value creation process.

First, organisations need to reshape their IC by changing their relational, structural, and human capitals to capture value from data. In managing IC, human capital needs to change to unlock value from Big Data (Baumgarten et al., 2013) since it is human capital that provides the valuable insights and knowledge extracted from data. Similarly, data security challenges also reveal the importance of the human factor in protecting data and establishing effective security management systems. Accordingly, IC management needs to develop human and structural capital to face cyberthreats and reduce vulnerabilities in data security. Therefore, despite the call for data-centric organisations to produce data-driven knowledge, the Big Data movement needs to be human-oriented and face its social, ethical, and human responsibilities related to cybercrimes and data security issues.

Second, the power stemming from Big Data and the social inequalities in accessing and using data are implications highlighting the accountability between who has the privilege of storing and using data, and people, who actually preserve concerns about their privacy. This leads us to reflect on the inadequacy of accounting information and the public interest of security breach disclosure, thus advocating the need to improve information to stakeholders about cyberthreats and data security management. Such managerial, societal, and ethical redefinitions of Big Data demonstrate that analysing this phenomenon cannot be limited to its original technological domain. Before Big Data was a managerial practice, it was an engaging social practice. It can affect any aspect of society or an organisation. Therefore, interdisciplinary research can fruitfully examine Big Data's social impacts. Thus, research on Big Data needs to expand beyond the boundaries of its technological roots and explore the benefits and risks to society.

Academics and practitioners need to consider the hidden implications and challenges of Big Data, to avoid the pitfalls and risks of becoming a myth founded on unexamined beliefs (Alvesson, 1993). This implies reflecting on data security risk as well. Boyd and Crawford (2012, p. 663) argue that "like other socio-technical phenomena, Big Data triggers both utopian and dystopian rhetoric". Their claim rests on a "widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy". This highlights the need for more awareness about the actual consequences and changes from Big Data.

Similarly, academics and practitioners need to be aware of the epistemological revolution behind Big Data (Boyd and Crawford, 2012). Many scholars claim the data-driven advantages of Big Data, and this is curious because a data-driven approach is exactly the opposite of many mainstream scientific epistemological approaches. Boyd and Crawford (2012, p. 665) highlight that "Big Data reframes key questions about the constitution of knowledge, the processes of research, how we should engage with information, and the nature and the categorization of reality". McAbee *et al.* (2017) argue that Big Data analytics can support the spread of the inductive reasoning underpinning the logic of data-driven knowledge. They underline that inductive reasoning is in contrast to the deductive approaches of the dominant research model that use hypothetic-deductive strategy to inspire testing theories for empirical adequacy (McAbee *et al.*, 2017). Thus, due to the increasing call for data-driven knowledge, one question may be worth asking: Will the Big Data movement be at the forefront of a new empiricism?

The study has two limitations. First, because our study is interpretative, other researchers may not draw the same conclusions from the literature and the evidence as us. Second, while we do not present empirical research, and even though we use publicly available evidence, it leaves open questions for future empirical research to demonstrate the effects of Big Data and cyberthreats. These questions are part of a wider research agenda for IC and accounting that calls for embracing an interdisciplinary research agenda of the Big Data ecosystem. Our projections about the need for a human-oriented movement, the societal power behind Big Data and the emergence of new corporate accountability stemming from cyberthreats, outline a research agenda for unveiling the multifaceted and detrimental implications of Big Data for business and society. Thus, drawing on our conclusions, our question is whether Big Data can promote an equal society, transparency, and a better decision making? Or does it promote the opposite?

To conclude, while we agree that Big Data is a wide revolutionary socio-technical phenomenon, we believe its positive revolutionary changes cannot occur until its risks and challenges are acknowledged in research and practice. Academics and practitioners have a significant responsibility in researching, sustaining and participating in the revolution. Thus, to enable transformative redefinition of Big Data, they need to address the hidden effects and threats of Big Data by embracing a more holistic view of it. Academics and practitioners have to go beyond Big Data's technological aspects, and acknowledge its managerial, sociological and ethical implications, along with engaging with their moral judgement when using Big Data.

5. References

Abraham, S. and Chengalur-Smith, I. (2010), "An overview of social engineering malware: Trends, tactics, and implications", *Technology in Society*, Vol. 32 No. 3, pp. 183–196.

Ahrens, T. and Chapman, C. S. (2007), "Management accounting as practice", *Accounting, Organizations and Society*, Vol. 32 No. 1–2, pp. 1–27.

Akoka, J., Comyn-Wattiau, I. and Laoufi, N. (2017), "Research on Big Data – A systematic mapping study", *Computer Standards & Interfaces*, Vol. 54 No. January, pp. 105–115.

Alharthi, A., Krotov, V. and Bowman, M. (2017), "Addressing barriers to big data", *Business Horizons*, "Kelley School of Business, Indiana University", Vol. 60 No. 3, pp. 285–292.

Alles, M. G. (2015), "Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession", *Accounting Horizons*, Vol. 29 No. 2, pp. 439–449.

Alvesson, M. (1993), "Organizations as rhetoric: Knowledge-intensive firms and the struggle with ambiguity", *Journal of Management Studies*, Vol. 30 No. 6, pp. 997–1015.

Alvesson, M. and Deetz, S. (2000), *Doing Critical Management Research*, SAGE Publications.

Arp, D., Quiring, E., Wressnegger, C. and Rieck, K. (2017), "Privacy Threats through Ultrasonic Side Channels on Mobile Devices", *Proc. of IEEE European Symposium on Security and Privacy (EuroS&P)*, available at: https://www.sec.cs.tu-bs.de/pubs/2017a-eurosp.pdf.

Assunção, M. D., Calheiros, R. N., Bianchi, S., Netto, M.A. S. and Buyya, R. (2015), "Big Data computing and clouds: Trends and future directions", *Journal of Parallel and Distributed Computing*, Vol. 79–80, pp. 3–15.

Baumgarten, J., Dickstein, M. and Rizk, N. (2013), *Beyond the Hype. Building a Big Data-Enabled Organization*.

Boyd, D. and Crawford, K. (2012), "Critical questions for Big Data", *Information, Communication & Society*, Vol. 15 No. 5, pp. 662–679.

Bressler, M. S. and Bressler, L. (2014), "Protecting your company's intellectual property assets from cyber-espionage", *Journal of legal, ethical and regulatory issues*, Vol. 17 No. 2, pp. 1–16.

Cao, M., Chychyla, R. and Stewart, T. (2015), "Big data analytics in financial statement audits", *Accounting Horizons*, Vol. 29 No. 2, pp. 423–429.

Chang, S. E. and Lin, C. (2007), "Exploring organizational culture for information security management", *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438–458.

Chen, H., Chiang, R. H. L. and Storey, V. C. (2012), "Business Intelligence and Analytics: From Big Data to Big Impact", *MIS Quarterly*, Vol. 36 No. 4, pp. 1165–1188.

Chen, M., Mao, S. and Liu, Y. (2014), "Big Data: A survey", *Mobile Networks and Applications*, Vol. 19 No. 2, pp. 171–209.

Clarke, S. (2016), "Reducing the impact of cyberthreats with robust data governance", *Computer Fraud & Security*, Vol. 2016 No. 7, pp. 12–15.

Demchenko, Y., de Laat, C. and Membrey, P. (2014), "Defining architecture components of the Big Data Ecosystem", *2014 International Conference on Collaboration Technologies and Systems (CTS)*, IEEE, pp. 104–112.

Dumay, J. (2013), “The third stage of IC: towards a new IC future and beyond”, *Journal of Intellectual Capital*, Vol. 14 No. 1, pp. 5–9.

Dumay, J. (2016), “A critical reflection on the future of Intellectual Capital: From reporting to disclosure”, *Journal of Intellectual Capital*, Vol. 17 No. 1, pp. 168–184.

Dumay, J. and Garanina, T. (2013), “Intellectual capital research: a critical examination of the third stage”, *Journal of Intellectual Capital*, Vol. 14 No. 1, pp. 10–25.

Gandomi, A. and Haider, M. (2015), “Beyond the hype: Big data concepts, methods, and analytics”, *International Journal of Information Management*, Vol. 35 No. 2, pp. 137–144.

Gemalto. (2017), *Mining for Database Gold. Findings from the 2016 Breach Level Index*, available at: http://www.breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf.

Gordon, S. and Ford, R. (2006), “On the definition and classification of cybercrime”, *Journal in Computer Virology*, Vol. 2 No. 1, pp. 13–20.

Guthrie, J., Ricceri, F. and Dumay, J. (2012), “Reflections and projections: A decade of Intellectual Capital Accounting Research”, *The British Accounting Review*, Vol. 44 No. 2, pp. 68–82.

Intezari, A. and Gressel, S. (2017), “Information and reformation in KM systems: big data and strategic decision-making”, *Journal of Knowledge Management*, Vol. 21 No. 1, pp. 71–91.

ISO. (2013), *ISO/IEC 27001 - Information Technology, Security Techniques, Information Security Management Systems, Requirements*, Geneve.

Krahel, J. P. and Titera, W. R. (2015), “Consequences of big data and formalization on accounting and auditing standards”, *Accounting Horizons*, Vol. 29 No. 2, pp. 409–422.

Laney, D. (2001), *3D Data Management: Controlling Data Volume, Velocity, and Variety,* Meta Group Inc.

Lee, I. (2017), “Big data: Dimensions, evolution, impacts, and challenges”, *Business Horizons*, “Kelley School of Business, Indiana University”, Vol. 60 No. 3, pp. 293–303.

Lohr, S. (2012), “The Age of Big Data”, *New York Times*, available at: http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html.

Massaro, M., Dumay, J. and Guthrie, J. (2016), “On the shoulders of giants: Undertaking a structured literature review in accounting”, *Accounting, Auditing & Accountability Journal*, Vol. 29 No. 5, pp. 767–801.

McAbee, S. T., Landis, R. S. and Burke, M. I. (2017), “Inductive reasoning: The promise of big data”, *Human Resource Management Review*, Vol. 27 No. 2, pp. 277–290.

McAfee, A. and Brynjolfsson, E. (2012), “Big Data. The management revolution”, *Harvard Buiness Review*, Vol. 90 No. 10, pp. 61–68.

Mcfarland, C., Paget, F. and Samani, R. (2015), *The Hidden Data Economy. The Marketplace for Stolen Digital Information*, Santa Clara, CA, available at: https://www.mcafee.com/it/security-awareness/articles/hidden-data-economy.aspx.

McKinsey Global Institute. (2011), *Big data: The next frontier for innovation, competition, and productivity*, *McKinsey Global Institute*.

Michael, K. and Miller, K. (2013), “Big data: New opportunities and new challenges”, *Computer*, Vol. 46 No. 6, pp. 22–24.

Moore, A. D. (2013), "Privacy", *International Encyclopedia of Ethics*, Blackwell Publishing Ltd, Oxford, UK.

Nodoushani, O. and Nodoushani, P. A. (2002), "Industrial espionage: The dark side of the 'digital age'", *Competitiveness Review*, Vol. 12 No. 2, pp. 96–101.

Perera, C., Ranjan, R., Wang, L., Khan, S. U. and Zomaya, A. Y. (2015), "Big Data Privacy in the Internet of Things Era", *IT Professional*, Vol. 17 No. 3, pp. 32–39.

Petty, R. and Guthrie, J. (2000), "Intellectual capital literature review", *Journal of Intellectual Capital*, Vol. 1 No. 2, pp. 155–176.

Pollach, I. (2005), "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent", *Journal of Business Ethics*, Vol. 62 No. 3, pp. 221–235.

Ponemon Institute. (2011), *Reputation Impact of a Data Breach*, Traverse City, Michigan, available at: https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf.

Ponemon Institute. (2014), *The SQL Injection Threat Study*, Traverse City, Michigan, available at: http://www.dbnetworks.com/pdf/ponemon-the-SQL-injection-threat-study.pdf.

Ponemon Institute. (2016), *2016 Cost of Data Breach Study: Global Analysis*, *Ponemon Institute Research Report*, Traverse City, Michigan, available at: https://www.ibm.com/security/data-breach/.

Rothberg, H. N. and Erickson, G. S. (2017), "Big data systems: knowledge transfer or intelligence insights?", *Journal of Knowledge Management*, Vol. 21 No. 1, pp. 92–112.

Sawabe, N. (2005), "Accounting for the public interest: a Japanese perspective", *Accounting, Auditing & Accountability Journal*, Vol. 18 No. 5, pp. 631–647.

Schatzki, T. R. (2005), "Peripheral Vision: The Sites of Organizations", *Organization Studies*, Vol. 26 No. 3, pp. 465–484.

Secundo, G., Del Vecchio, P., Dumay, J. and Passiante, G. (2017), "Intellectual capital in the age of Big Data: establishing a research agenda", *Journal of Intellectual Capital*, Vol. 18 No. 2, pp. 242–261.

Sinha, S. (2012), "Understanding Industrial Espionage for Greater Technological and Economic Security", *IEEE Potentials*, Vol. 31 No. 3, pp. 37–41.

Smith, M., Szongott, C., Henne, B. and von Voigt, G. (2012), "Big data privacy issues in public social media", *2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, IEEE, pp. 1–6.

Snyder, H. and Crescenzi, A. (2009), "Intellectual capital and economic espionage: new crimes and new protections", *Journal of Financial Crime*, Vol. 16 No. 3, pp. 245–254.

Stroz Friedberg. (2017), *2017 Cybersecurity Predictions*, available at: https://content.strozfriedberg.com/2017-stroz-friedberg-cybersecurity-predictions-report.

Subashini, S. and Kavitha, V. (2011), "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, Vol. 34 No. 1, pp. 1–11.

Tian, X. (2017), "Big data and knowledge management: a case of déjà vu or back to the future?", *Journal of Knowledge Management*, Vol. 21 No. 1, pp. 113–131.

Tien, J. M. (2013), "Big Data: Unleashing information", *Journal of Systems Science and Systems*

Engineering, Vol. 22 No. 2, pp. 127–151.

Uden, L. and He, W. (2017), "How the Internet of Things can help knowledge management: a case study from the automotive domain", *Journal of Knowledge Management*, Vol. 21 No. 1, pp. 57–70.

Vasarhelyi, M. A., Kogan, A. and Tuttle, B. M. (2015), "Big data in accounting: An overview", *Accounting Horizons*, Vol. 29 No. 2, pp. 381–396.

Verizon. (2017), *2017 Data Breach Investigations Report*, available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

Vroom, C. and von Solms, R. (2004), "Towards information security behavioural compliance", *Computers & Security*, Vol. 23 No. 3, pp. 191–198.

Wang, H., Xu, Z., Fujita, H. and Liu, S. (2016), "Towards felicitous decision making: An overview on challenges and trends of Big Data", *Information Sciences*, Vol. 367–368, pp. 747–765.

Warren, J. D., Moffitt, K. C. and Byrnes, P. (2015), "How big data will change accounting", *Accounting Horizons*, Vol. 29 No. 2, pp. 397–407.

Warren, M. (2015), "Modern IP theft and the insider threat", *Computer Fraud & Security*, Vol. 2015 No. 6, pp. 5–10.

World Economic Forum. (2017), *The Global Risks Report 2017. 12th Edition*, Geneva, available at: https://www.weforum.org/reports/the-global-risks-report-2017.

Yaqoob, I., Hashem, I. A. T., Gani, A., Mokhtar, S., Ahmed, E., Anuar, N. B. and Vasilakos, A. V. (2016), "Big data: From beginning to future", *International Journal of Information Management*, Vol. 36 No. 6, pp. 1231–1247.

Yoon, K., Hoogduin, L. and Zhang, L. (2015), "Big data as complementary audit evidence", *Accounting Horizons*, Vol. 29 No. 2, pp. 431–438.

---

[i] Source: Financial Times (https://www.ft.com/content/01714ea4-262e-11e5-bd83-71cb60e8f08c)

[ii] In this paper, we refer to the definition of data breach adopted by the ISO/IEC 27040: a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed".

[iii] Source of the Yahoo message: https://yahoo.tumblr.com/post/150781911849/an%ADimportant%ADmessage%ADabout%ADyahoo%ADuser%ADsecurity1/3

[iv] Source: CNN (http://money.cnn.com/2016/12/16/technology/yahoo-for-sale-data-dark-web/)

[v] Source: Juniper Research (https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion)

[vi] Source: Yahoo's investor press release, Feb. 21, 2017 (https://investor.yahoo.net/releasedetail.cfm?ReleaseID=1012633)

[vii] The disclosure of the massive breach involving eBay's customer data in 2014 caused a loss of user trust and an immediate and dramatic impact on their sales volume (Financial Times: https://www.ft.com/content/66cef02c-0d29-11e4-bcb2-00144feabdc0)

Figure 1. Tien's (2013) framework for Big Data decision-making

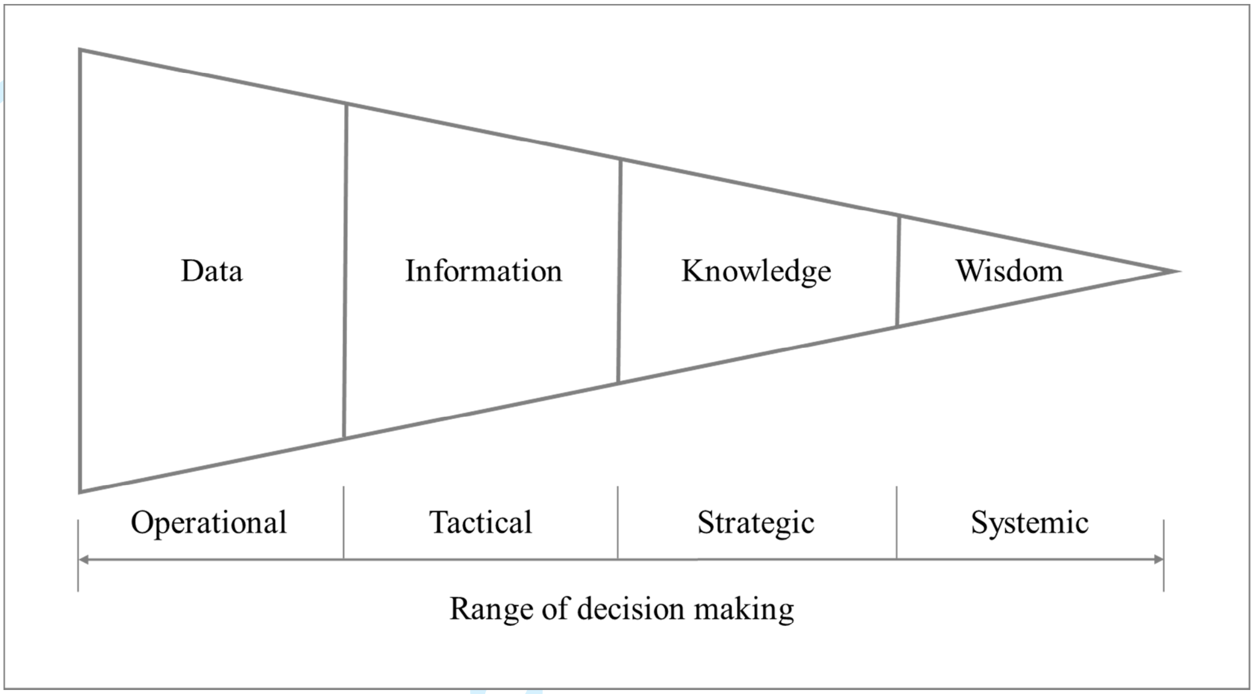

Figure 2. Message regarding the data breach sent to Yahoo users

An Important Message About Yahoo User Security

By Bob Lord, CISO

A recent investigation by Yahoo has confirmed that a copy of certain user account information was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected. Based on the ongoing investigation, Yahoo believes that information associated with at least 500 million user accounts was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network. Yahoo is working closely with law enforcement on this matter.

Table 1. Data breach risks for intellectual capital

Effects of data breach	***Cyberthreats***	***Risks***	***Impact on intellectual capital***
Loss of confidentiality	Stealing or disclosing users' data	*Reputational risk* *Brand image damage*	Relational capital
	Theft of intellectual property	*Lack of competitiveness or innovativeness*	Structural capital
	Theft of other organisational knowledge	*Lack of competitiveness or innovativeness*	Structural capital / Human capital
Loss of integrity	Data sabotage (data alteration)	*Unreliable information and dysfunctional decisions (losing value of knowledge, mistakes in decision-making)*	Structural capital / Human capital
Loss of availability	Data sabotage (data destruction)	*Loss of data* *Ineffective decision-making*	Structural capital / Human capital
		Damage to infrastructure assets (stoppage of information systems and operating processes)	Structural capital

Table 2. Insights and transformative projections for future research

Insights and critique	***Transformative projections and implications***
Human capital is a crucial factor to enable the value of Big Data in creating knowledge and supporting decision-making Privacy preservation and data security are main challenges in the current organisations' digital eco-system: - Big data security as a component of the Big Data ecosystem - Security breaches can threaten IC and value creation from data (see the framework in Table 1) - The paradigm "data as value" is a driving force of the "hidden data economy", data-driven competition and cyberthreats (i.e. cyber espionage, theft or leak of data, data sabotage)	**Implications for IC management - the need for a human-oriented movement:** - Addressing the challenge of reshaping organisations' IC and human capital - Changes in teleoaffective structures - Establishing internal mechanisms for data protection and security - Reducing human vulnerabilities to protect data and reduce the risks of security breaches
"Voracity" for data is a further characteristic of the Big Data phenomenon Big Data has increased societal concerns over people's privacy Cyberthreats and security risks have detrimental effects for organisations and society	**Social and ethical implications of Big Data:** - Data as power**:** People and corporations have unequal interests and power in controlling and using data - Need for accountability**:** The emergence of a new corporate accountability resulting from the threats to user privacy when storing and using data **Implications for accounting:** - Public interest of cyberthreats and security breaches - New accounting information for investors and other stakeholders - Changes to accounting information and corporate reporting, by reflecting the corporate accountability in data security management