Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 138 (2018) 401–408

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN/HCist 2018

Information security governance in big data environments: A systematic mapping

Reza Saneei Moghadam[a], Ricardo Colomo-Palacios [a*]

[a]*Østfold University College, B R A Veien 4, Halden 1783, Norway*

Abstract

Information security governance is an important aspects for all organizations. Given the crucial importance of IT systems and the increasing range of threats these systems are facing, there is an increasing interest on the topic. On the other hand, Big Data environments are also beginning to be more pervasive as IT is increasing its importance for organizations worldwide. In order to better know which aspects are the most important for the intersection of Big Data and information security governance, authors present in this paper a systematic mapping on this topic. Authors illustrate challenges and gaps concerning the topic and clarify these challenges by means of a classification of the environments they take place, the security risk spectrums they concern, and the security governance measures they take to mitigate them; by providing solutions as in a framework, model, software or tool, wherever possible. Results are expected to be useful for IT security professionals and information systems practitioners as a whole.

Keywords: information security governance; big data; framework; systematic mapping

[*] Corresponding author. Tel.: + 47 6921 5000; fax: + 47 6921 5002.
E-mail address: ricardo.colomo-palacios@hiof.no

10.1016/j.procs.2018.10.057

1. Introduction

The growing vulnerability of information security has become the major attention in most global information security congregations. As a result of its importance and repercussion, information security has undergone an impressive development in the past decades [1]. Nowadays, security and privacy are some of the cornerstones of information systems as a discipline [2]. Information security goes beyond the security of a computer system to deal with both technical and non-technical information-handling activities [3]. Information Governance is the glue that drives value and mitigates risk. In this scenario, the information security management system must be part of modern organizations that must be managed from a financial and managerial viewpoint [4,5].

On the other hand, Big Data-oriented systems are beginning to be pervasive [6] and the opportunities to use Big Data technologies to gather and process vast amounts of information from a wide panoply of fields is opening a new landscape for computing researchers and practitioners alike [7]. There are several key areas where information governance for big data is critical, such as metadata management, security and privacy, data integration and data quality, and master data management. It is interesting to note that big data innovators recognize the importance of governance to the success of their projects. According to [8], 58% of the organizations who report having active big data efforts included security and governance processes in their efforts. There is, increasingly, the need for an overarching information security framework that can provide context and coherence to compliance activity worldwide. As the intellectual capital value of 'information economy' organizations increases, their commercial viability and profitability – as well as their share price – increasingly depend on the security, confidentiality and integrity of their information and information assets. [9]

There is a lack of research related to information security governance in big data settings, and a growing need for more studies and new proposals related to this matter [10]. Therefore, authors develop a study using the systematic mapping technique on Information Security Governance in Big Data Environments to bridge this gap. This paper is devoted to present the results of the study. The remainder of the paper is structured as follows: mapping process is presented in section 2. Section 3 depicts the main results of the process and finally, conclusions are presented.

2. Systematic Mapping

The systematic mapping study is a technique that provides a global view of a given research field using systematic mapping process steps, with the goal to determine the content and conception of the systematic revision [11].

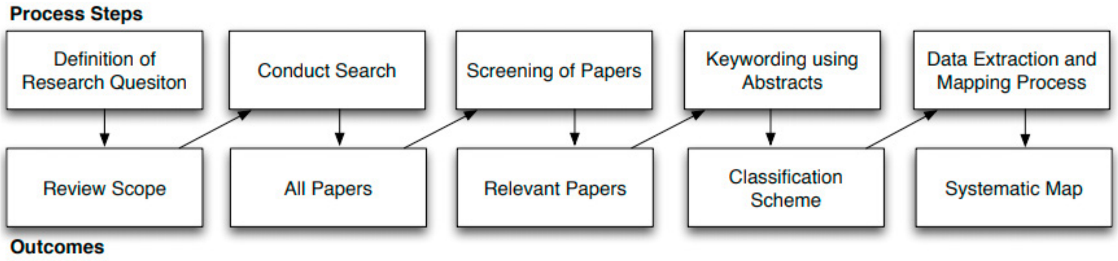

Fig. 1. Systematic Map Diagram

This study was performed using the systematic mapping technique following the steps shown in Figure (1).

2.1. *Research Questions*

The authors of this study stated the following research questions:

RQ1: Which aspects of information security governance in big data have been covered by literature?
RQ2: Which information security risk spectrums are being addressed by literature?

RQ3: Which solutions are identified to information security governance issues?
RQ4: What types of models, frameworks and tools have been identified in these solutions?

2.2. *Search strategy*

As academic databases authors used: IEEExplore, ACM Digital Library, Springer Link, Science Direct, and, in order to raise grey literature, Google Scholar was also considered as a meta-database.

Authors used a general query completed with associated terms from a thesaurus and rewritten according to the expression rules of advanced queries in each database. This general query is based on three relevant topics in our research on information security governance, namely "Information Security Governance", "Big Data" and "Framework" and their counterparts. General query is as follows:
("Information Security Governance" OR "ISG" OR "Data Security") AND ("Framework*" OR "Model*" "Tool*") AND "Big Data")

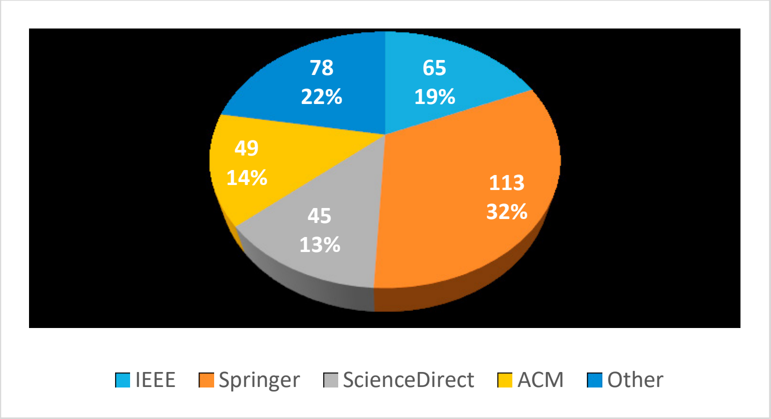

Fig. 2. Selected databases and retrieved papers

This query resulted in 350 results as the initial set. This set was later filtered as depicted in what follows.

2.3. *Study Selection*

The selection criteria, including exclusion and inclusion criteria, is as follows:

- Ensuring the paper is written in English, ensuring the paper is peer-reviewed, and published after 2013.
- Eliminating any paper that are clearly irrelevant to the topic.

After applying the inclusion and exclusion criteria, authors obtained 224 papers, in the second phase. 96 relevant articles remained after the filtering based on the paper titles and abstracts analysis. Among these 96 publications, only 31 papers targeted an aspect of information security governance in big data environments. Authors carefully chose these papers to ensure that they cover at least one of the security governance measures. Table 1 illustrates the details of the search results.

Table 1. Study selection reading detail

Phase	# of studies
Search	350
Title	224
Abstract	96
Full-text	31

2.4. Study classification

After analysing the titles and the abstracts of the selected papers in the mapping study, authors obtained three groups of categories corresponding to aspects such as Environment, Security and Security Governance. The rest of the mapping is based on this classification and categories:

1. Environment: This group characterizes the environments the paper describes. Articles could be related to general environment or could describe a security risk in particular environments like Clouds, Smart cities, Health Sector…
2. Security: According to NIST Big Data Security Taxonomies [12], a taxonomy for Big Data security and privacy should encompass the aims of existing useful taxonomies. Authors used a taxonomy that best entails the Risk spectrums concerning big data, as demonstrated in [13]. Hence, authors derived 6 categories: Data Quality, Privacy, Security, Usage, Data Architecture, Data Management and Governance Risk spectrum. This classification completely maps with NIST [12], ENISA [14] and CSA [15] taxonomies. For the details of this Risk-based classification and what factors it includes refer to [13].
3. Security Governance: For the purpose of this paper, authors categorized security governance in terms of the information security governance outcomes it targets. As described in the European Union Agency for Network and Information Security Practice Guide [14], these outcomes are:
   - Strategic Alignment
   - Risk Management
   - Resource Management
   - Performance Measurement
   - Value Delivery

Authors mapped these categories into a more concise ones, in terms of governance processes including Risk Mitigation Process Management, Business Process/Security Process Management and Regulatory Compliance Management According to [13].

2.5. Data extraction and synthesis of results

Most of the final resources were conference papers (17), followed by journal papers (12) and book chapters (2). Classifications and extracted data are shown in figures 3-6 and detailed in the next section.

3. Analysis and Reporting

In what follows, authors discuss the results obtained by conducting the study according to the steps described in the previous section in order to find answers to the research questions of this study.

RQ1: Which aspects of information security governance in big data have been covered by literature?

According to Figure 3, most of the studies refer to the information security governance of big data in a general way. These general environments include governments and national security, in USA [16], Russia [17], Taiwan [18] and China [19]. An inter-organizational market case [20] have been published and there is also a case of Swedish municipalities' [21]. Finally, a paper presents a case of two governments sharing data [22]. The next major focus of articles refer to the Health Sector, then the cloud (cloud software), and smart cities. There was a case specific to IoT which was discussed in [23].

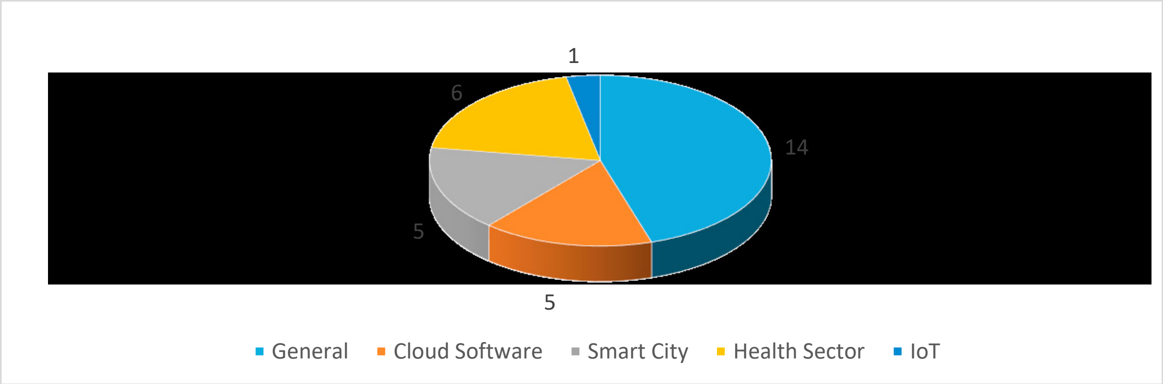

Fig. 3. Big Data Environments

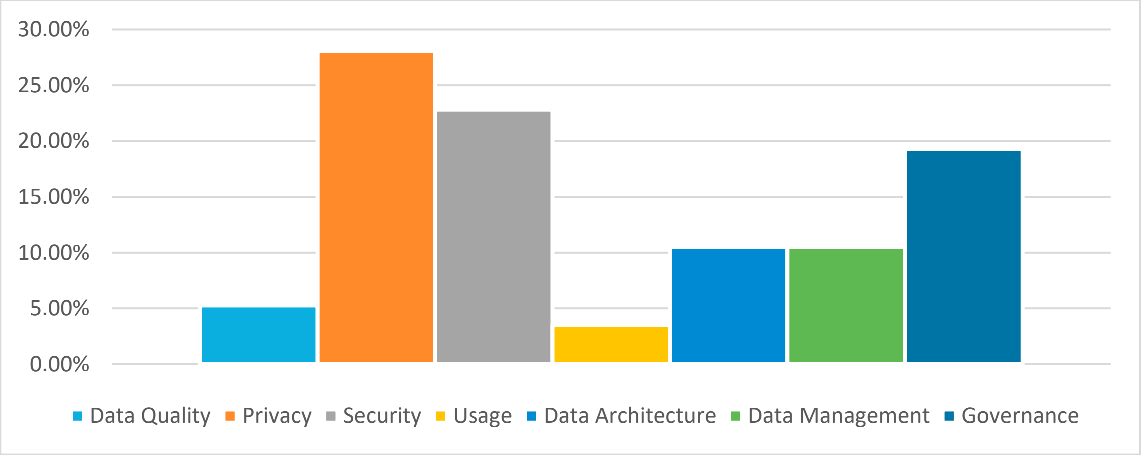

Fig. 4. Studies that cover the information security Risk Spectrums

RQ2: Which information security risk spectrums are being addressed by literature?

According to the classification of information security risk factors (Figure 4) Privacy and Security aspects are the ones more covered in the literature, followed by Governance. However, we need to take into account that some of the studies fall into more than one category and this happens in 26 cases, reaching a total of 57 aspects in 31 studies.

Health sector is one of the most important exponents of privacy and security Risks. In [24] ethical concerns and privacy issues in combining big data with ‘small data’ is mentioned. A major issue in health sector is the privacy violation by bringing together multiple sources of each individual patient data. In [25] a problem of data governance, distribution, and accessibility is analysed. Data Quality Risk mentioned is mentioned in [13], [26]; authors propose frameworks in a general environment and a smart city [27].

RQ3: Which solutions are identified to information security governance issues?

Most of the solutions cover the risk mitigation and then business and security processes aspect of governance in big data as presented in figure 5. In [18], [27], [22] and [28] some changes or proposals for regulations have been mentioned and they mostly cover the Privacy Risk of the big data security. In [24], the use of accredited ‘safe-havens’ (restricted environments for the secure analysis of data), supported by robust protection and governance is proposed. In [29], a sustainability management approach is proposed. In [30] both a risk mitigation process and security measuring process have been proposed to control the risk of an IT-disposed asset. In [26] a security management measure was taken to build a model to mitigate security risks in clouds.

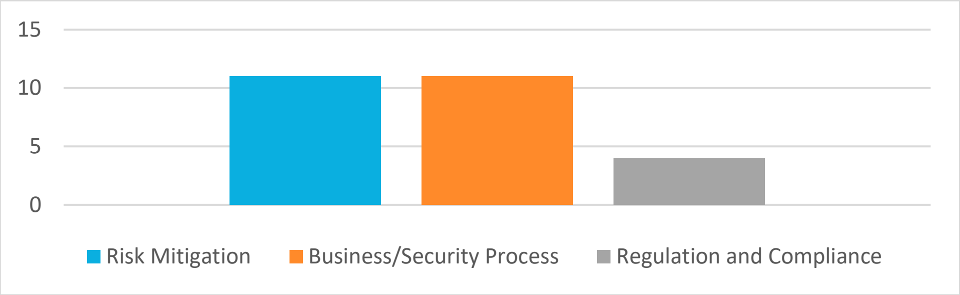

Fig. 5. Security Governance Aspect of the studies

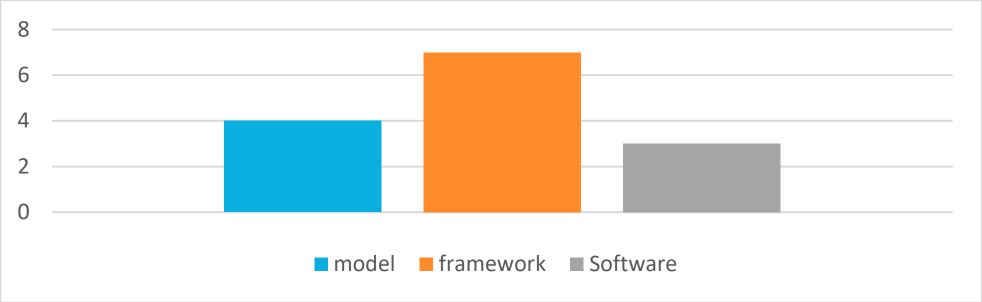

Fig. 6. Classification Solutions Proposed

RQ4: What types of models, frameworks and tools have been identified in these solutions?

Figure 6 presents the distribution of frameworks, models and tools are proposed in literature. In [13], a governance framework is proposed based on Analytic hierarchy process and Delphi Method. This framework implements a method of risk prioritization and ranking. In [18], a case of smart cities in Taiwan, a digital continuity model for managing big data is proposed. This model covers data provenance, data stakeholders, data processing, and data risk management risks and several big data governance problems are tackled including data assurance, data loss, data trustiness, data security and data reusability in the development of smart cities. In [22], a case of international cooperation and sharing of big data between Japan and EU is reported. In the paper, a privacy protection model is proposed and cross border data distribution and data protection issues are detailed. The governance framework is named DPEC and the project is called iKaaS (intelligent Knowledge-as-a-Service). In [28], a best-practice framework based on critical success factors is proposed. This framework is based on ISO/IEC 27014 and COBIT including security governance management aspects. A framework for identity management in the cloud is presented in [31] based on the fact that cloud services suffer from access control and authentication. In [32] in an IoT setting, a risk management framework is proposed. The framework covers security and privacy concerns of big data in that setting. A model for behaviour prediction of employees is proposed in [33]. It implements self-assessment of security within the organization, and a decentralized IT governance. A cloud-based model is proposed for health sector that mitigates confidentiality and privacy risks in [34]. In [35] a methodology is proposed that identifies the threats and attacks and proposes solution based on guides from NIST [12] and CSA [15] for cloud environments. In [36], [37] two IBM solutions are introduced. In [38] the privacy issue of data integration in health sector is addressed, and a privacy-preserving policy model is proposed. The model enhances eXtensible Access Control Markup Language (XACML) or other existing security policy specification languages.

4. Limitations and Conclusions

The main limitation of the study is coming from the decision to include recent papers, conference papers and book chapters that are peer-reviewed and target at least one aspect of information security governance as a solution for information security risks classified. Many resources have been omitted, due to ambiguity to mention information security governance aspects in a big data setting or solely proposed solution in the more conceptual and technical information security aspects. Also, due to having several taxonomies in big data security society and lack of a solid universal framework and guidelines in big data security aspects [12], some aspects of information security in big data might have not been deeply scrutinized.

In this paper, authors provide an overview of the information security governance in big data environments by means of a systematic approach. Information security governance necessitates a constant control associated with using governance techniques like risk management, business process management and security process management to ensure business value. The analysis of the elaborated charts as well as answers to the research questions shows a lack of research and work in regulation and compliance aspects of information security governance in big data settings. Authors also would like to underline the absence of comprehensive and specific models and frameworks in this area. Future works are aimed to be devoted to the development of a specific framework for information security governance in big data settings.

References

[1] Georg L. Information security governance: pending legal responsibilities of non-executive boards. J Manag Gov 2017;21:793–814. doi:10.1007/s10997-016-9358-0.

[2] Lowry PB, Dinev T, Willison R. Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda. Eur J Inf Syst 2017;26:546–63. doi:10.1057/s41303-017-0066-x.

[3] Kolkowska E, Karlsson F, Hedström K. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. J Strateg Inf Syst 2017;26:39–57. doi:10.1016/j.jsis.2016.08.005.

[4] Haufe K, Dzombeta S, Brandis K, Stantchev V, Colomo-Palacios R. Improving Transparency and Efficiency in IT Security Management Resourcing. IT Prof 2018;20:53–62. doi:10.1109/MITP.2018.011291353.

[5] Dzombeta S, Stantchev V, Colomo-Palacios R, Brandis K, Haufe K. Governance of Cloud Computing Services for the Life Sciences. IT Prof 2014;16:30–7. doi:10.1109/MITP.2014.52.

[6] Vera-Baquero A, Colomo-Palacios R, Stantchev V, Molloy O. Leveraging big-data for business process analytics. Learn Organ 2015;22:215–28. doi:10.1108/TLO-05-2014-0023.

[7] Vera-Baquero A, Colomo-Palacios R, Molloy O. Real-time business activity monitoring and analysis of process performance on big-data domains. Telemat Inform 2016;33:793–807. doi:10.1016/j.tele.2015.12.005.

[8] Ballard C, Compert C, Jesionowski T, Milman I, Plants B, Rosen B, et al. Information Governance Principles and Practices for a Big Data Landscape. IBM Redbooks; 2014.

[9] Calder A, Watkins S. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Kogan Page; 2015.

[10] Fazlida MR, Said J. Information Security: Risk, Governance and Implementation Setback. Procedia Econ Finance 2015;28:243–8. doi:10.1016/S2212-5671(15)01106-5.

[11] Petersen K, Feldt R, Mujtaba S, Mattsson M. Systematic Mapping Studies in Software Engineering. Proc. 12th Int. Conf. Eval. Assess. Softw. Eng., Swindon, UK: BCS Learning & Development Ltd.; 2008, p. 68–77.

[12] NIST Big Data Public Working Group Security and Privacy Subgroup. NIST Big Data Interoperability Framework: Volume 4, Security and Privacy. National Institute of Standards and Technology; 2015.

[13] Bharathi SV. Prioritizing and Ranking the Big Data Information Security Risk Spectrum. Glob J Flex Syst Manag 2017;18:183–201. doi:10.1007/s40171-017-0157-5.

[14] Big Data Security — ENISA 2018. https://www.enisa.europa.eu/publications/big-data-security (accessed April 23, 2018).

[15] Top Ten Big Data Security and Privacy Challenges. Cloud Secur Alliance 2018. https://cloudsecurityalliance.org/download/top-ten-big-data-security-and-privacy-challenges/ (accessed April 23, 2018).

[16] Crampton JW. Collect it all: national security, Big Data and governance. GeoJournal 2015;80:519–31. doi:10.1007/s10708-014-9598-y.

[17] Arkhipov V, Naumov V. The legal definition of personal data in the regulatory environment of the Russian Federation: Between formal certainty and technological development. Comput Law Secur Rev 2016;32:868–87. doi:http://dx.doi.org/10.1016/j.clsr.2016.07.009.

[18] Exploring privacy and trust for employee monitoring | Industrial Management & Data Systems | Vol 115, No 1 2018. https://www.emeraldinsight.com/doi/abs/10.1108/IMDS-07-2014-0197 (accessed April 23, 2018).

[19] Li J. Network Information Security Challenges and Relevant Strategic Thinking as Highlighted by “PRISM.” Cloud Comput. Secur., Springer, Cham; 2015, p. 147–56. doi:10.1007/978-3-319-27051-7_13.

[20] Langley D., Wijn R, Epskamp S, van Bork R. Should I get that jab? Exploring influence to encourage vaccination via online social media. AIS Electronic Library (AISeL); 2015.

[21] Svärd P. Public Information Directive (PSI) implementation in two Swedish municipalities. Rec Manag J 2018;28:2–17. doi:10.1108/RMJ-04-2016-0012.

[22] Kato N, Takasaki H, Murakami Y. Proposal of a New Privacy Protection Scheme for the Data Subject on the International Cooperation Information Sharing Platform. EHealth 360°, Springer, Cham; 2017, p. 23–8.

[23] Dittakavi S, Bhamidipati G, Neelam VSK. Big Data Analytics via IoT with Cloud Service. Big Data Anal., Springer, Singapore; 2018, p. 319–28.

[24] Docherty AB, Lone NI. Exploiting big data for critical care research: Curr Opin Crit Care 2015;21:467–72. doi:10.1097/MCC.0000000000000228.

[25] Newman D, Herrera CN, Parente ST. Overcoming barriers to a research-ready national commercial claims database. Am J Manag Care 2014;20:eSP25–30.

[26] Hassan S, Pernul G. Efficiently Managing the Security and Costs of Big Data Storage Using Visual Analytics. Proc. 16th Int. Conf. Inf. Integr. Web-Based Appl. Serv., New York, NY, USA: ACM; 2014, p. 180–4. doi:10.1145/2684200.2684333.

[27] An X, Sun S, Bai W, Deng H. Data integration in the development of smart cities in China: Towards a digital continuity model, Academic Conferences and Publishing International; 2016, p. 13–20.

[28] Gashgari G, Walters R, Wills G. A Proposed Best-practice Framework for Information Security Governance:, SCITEPRESS - Science and Technology Publications; 2017, p. 295–301. doi:10.5220/0006303102950301.

[29] Seele P. Predictive Sustainability Control: A review assessing the potential to transfer big data driven “predictive policing” to corporate sustainability management. J Clean Prod 2017;Complete:673–86. doi:10.1016/j.jclepro.2016.10.175.

[30] Williams PAH. Information security governance: a risk assessment approach to health information systems protection. Stud Health Technol Inform 2013;193:186–206.

[31] Lonea AM, Tianfield H, Popescu DE. Identity Management for Cloud Computing. New Concepts Appl. Soft Comput., Springer, Berlin, Heidelberg; 2013, p. 175–99.

[32] Irshad M. A Systematic Review of Information Security Frameworks in the Internet of Things (IoT). 2016 IEEE 18th Int. Conf. High Perform. Comput. Commun. IEEE 14th Int. Conf. Smart City IEEE 2nd Int. Conf. Data Sci. Syst. HPCCSmartCityDSS, 2016, p. 1270–5. doi:10.1109/HPCC-SmartCity-DSS.2016.0180.

[33] Lin C, Wittmer JLS. Proactive information security behavior and individual creativity: Effects of group culture and decentralized IT governance. 2017 IEEE Int. Conf. Intell. Secur. Inform. ISI, 2017, p. 1–6. doi:10.1109/ISI.2017.8004865.

[34] Chandra S, Ray S, Goswami RT. Big Data Security in Healthcare: Survey on Frameworks and Algorithms. 2017 IEEE 7th Int. Adv. Comput. Conf. IACC, 2017, p. 89–94. doi:10.1109/IACC.2017.0033.

[35] Ayala IDCL, Vega M, Vargas-Lombardo M. Emerging Threats, Risk and Attacks in Distributed Systems: Cloud Computing. Innov. Adv. Comput. Inf. Syst. Sci. Eng., Springer, New York, NY; 2013, p. 37–51.

[36] Keeping Information Governance Agile. IBM Big Data Anal Hub 2018. http://www.ibmbigdatahub.com/blog/keeping-information-governance-agile (accessed April 23, 2018).

[37] Bolstering Big Data Protection for Confident Decisions. IBM Big Data Anal Hub 2018. http://www.ibmbigdatahub.com/blog/bolstering-big-data-protection-confident-decisions (accessed April 23, 2018).

[38] Lu Y, Sinnott RO. Semantic-Based Privacy Protection of Electronic Health Records for Collaborative Research. 2016 IEEE Trust., 2016, p. 519–26. doi:10.1109/TrustCom.2016.0105.