Cybersecurity: Current State of Governance Literature

Emergent Research Forum (ERF)

Aurelia Mandani
University of Colorado Denver
Aurelia.Mandani@ucdenver.edu

Ronald Ramirez, PhD
University of Colorado Denver
Ronald.Ramirez@ucdenver.edu

Abstract

With the growing use of integrated, web-based technology, there is need for an in-depth understanding of cybersecurity for risk mitigation and how to govern private information held within firms. The researchers explore the current state of literature that focuses on digital governance and cybersecurity. Using a bibliometric analysis (publication analysis) of extant literature, the researchers analyzed a dataset of 2,202 articles published on digital governance and cybersecurity from 1999-2018. An analysis identifies key areas and themes within the existing research and highlights fruitful directions for future research.

Keywords

IT Governance, Digital Governance, Cybersecurity, IS Research, Text Analysis.

Introduction

Based on current data from the Privacy Rights Clearinghouse, there have been over 11,582,808,013 records that have been breached since 2005, with over 8,681 reported breaches in the United States (Privacy Rights Clearinghouse, 2018). Cybersecurity has become a growing problem for businesses as technologies and applications continue to become implemented within business processes (de Carvalho et al., 2017; Gashami et al. 2016; Moody et al. 2018). The need for more research and understanding of cybersecurity is apparent, especially as businesses begin to move their services on the cloud (Gashami et al. 2016).

The International Data Group (IDG) conducted a survey on cloud computing and found that 73% of respondents had "at least one cloud application or a portion of their computing structure already in the cloud" and that the remaining "17% plan to do so within the next 12 months" (IDG 2018). As firms start to move towards the cloud, they have started to replace in-house software's with SaaS (systems as a software) applications. Additionally, the International Data Corporation (IDC) has predicted that cybersecurity spending will reach $91.4 billion in 2018, growing to $120.7 billion in 2021; indicating that cybersecurity and related issues will continue to be problem (IDC 2018). IS research is just now starting to examine and develop an understanding of the impacts of cybersecurity (de Carvalho et al., 2017; Gashami et al. 2016; Moody et al. 2018). To develop an understanding of the literature to guide future research, the researchers pose the question: *what topics have been published in cybersecurity and digital (IT) governance?*

This article is as follows: in section one, the researchers will explore existing research on IT governance and cybersecurity governance; in section two, the methods are discussed; in section three, a preliminary bibliometric analysis of the existing research on IT governance and cybersecurity is conducted.

IT Governance

IT governance is defined as a framework that helps firms in their decision making, evaluation, and implementation processes of IT use (Weill 2004). Research on IT governance has spanned topics such as information value, business value, firm capabilities, outsourcing, and computing security (Tallon et al. 2013; Sambamurthy & Zmud 1999; Peterson 2004; Wilkin & Chenhall 2010; Ali & Green 2012; Rebollo et al. 2015). Earlier research on IT governance focused on the theory of multiple contingencies and IT

governance found that the theory of multiple contingencies plays a role in IT governance through amplifying, dampening, and overriding IT governance within a firm (Sambamurthy & Zmud 1999). Research on IT governance and information value focused on how information governance can boost firm performance (Tallon et al. 2013). Business value and IT governance research found that big data and data governance can contribute to firm performance. Research has found that an effective implementation of IT Governance architecture involves the following: structural, process, and relational capabilities (Tallon 2013). Within an industry, the COBIT 5 model is often implemented to help firms address governance from the five aspects of firms: a firm's internal audit process, the control processes, management within the firm, the IT governance of a firm, and finally, the governance of enterprise IT systems (ISACA, 2018).

Cybersecurity Governance

Cybersecurity governance is an important body of research within IS as firms will continue to implement technologies to assist with core processes and strategies in general and as systems become more interconnected and digitized specifically The researchers adopt Muller's definition of cybersecurity governance; "the aggregate of all attempts by organizations and individuals to institutionalize rules, standards and practices that manage and minimize risk associated with engagement in cyberspace" (2017). Extant research on cybersecurity governance has focused on: the NIST cybersecurity framework and the COBIT 5 framework, implications of implementation of security frameworks, and the identity of cybersecurity governance (NIST 2018; ISACA 2012). As one of the widely used cybersecurity frameworks, the NIST (National Institute of Standards and Technology) cybersecurity framework addresses governance and processes internal to a firm or organization (NIST 2018). This framework addresses the steps that firms and organizations need to make when there is a cybersecurity threat, and how to regain control of the IS systems under threat (NIST 2018). Additionally, within an industry, the NIST cybersecurity framework has started to be coupled with COBIT 5 to help firms address internal security concerns and practices to enable full cybersecurity governance (Thomas 2018; ISACA 2012). Rebollo et al. found that if firms implement cloud cybersecurity frameworks, they have the potential to have better security outcomes, which in turn, gives a firm a higher amount of cybersecurity governance (2015). Meanwhile, research on the history and identity of cybersecurity governance has found that there is a discourse of how cybersecurity governance research and views are often segmented into two categories: 1) governmental policy, and 2) through a "transnational community that is primarily civilian in outlook" (Mueller 2017; Cavelty 2007; Weber 2010). Given the nascency of research on IT governance and cybersecurity, coupled with the growth in cybersecurity events and subsequent growth in risk, more research on IT governance and cybersecurity could greatly benefit firms.

Methodology

Previous research has shown that information systems governance has the potential to explain and understand different aspects of technology within the firm (Wilkin & Chenhall 2010). In order to develop an understanding of current digital governance and cybersecurity literature in the IS field, the researchers conduct a Bibliometric systematic literature review. Bibliometrics have been used in the information science field to help researchers and librarians understand publication trends, thematic analyses, and collaborative research data (Clarivate Analytics 2008).

Bibliometrics offers IS academic researchers the opportunity to develop a deeper understanding of extant literature published within the field to better analyze an identify gaps in existing research (Clarivate Analytics 2008). The methods for this research are as follows: the researchers used the Web of Science (WoS) Core Collection database that provides data about publications, citation amounts, and other helpful data points about published articles. The researchers searched the following query into WOS to see what articles were published on cybersecurity and governance:

> *TOPIC:(Cybersecurity) OR TOPIC: (CyberSecurity) AND TOPIC: (Governance)OR TOPIC: (Digital Governance) Refined by: DOCUMENT TYPES: (PROCEEDINGS PAPER OR ARTICLE) Timespan: All years. Indexes: SCI-EXPANDED, CPCI-S, BKCI-S.*

The results from the query produced 2,202 results. All 2,202 abstracts were then analyzed for publication trends by year, word occurrence, and average year of word occurrence though statistical software and

VOSviewer (a bibliometric network analysis tool), further explained in the next section (van Eck & Waltman 2019).

Preliminary Results

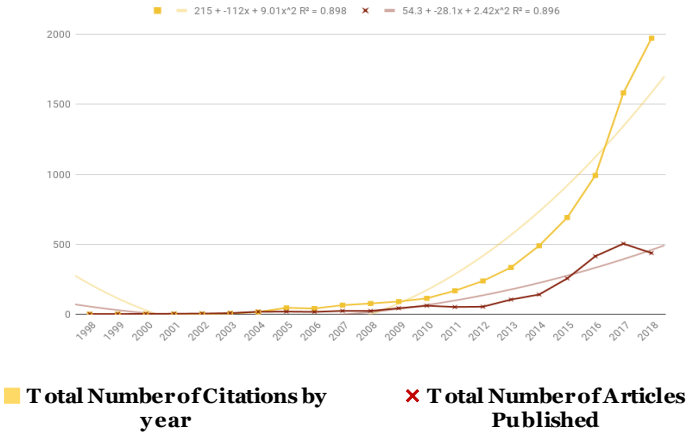

Figure 1. Trend Analysis of Publication and Citation Counts From 1998-2018

In order to understand the publication stratification, a preliminary bibliometric analysis included: a trend analysis, word occurrence analysis, and average year of word occurrence. The trend analysis in Figure 1 illustrates the number of articles published along with the number of citations per year on digital governance and cybersecurity. Based on the findings, the first article on digital governance and cybersecurity, was published in 1998. As Figure 1 illustrates, both the citation counts, and publication numbers did not start to take off until around 2013, where there were 104 publications, and 165 citations on articles. The trend analysis graph also illustrates that by 2016, the number of citations and articles grew at an even higher rate. In 2016, there were 414 total publications with 489 articles cited, and in 2017, there were 504 publications, with over 1583 citations made on digital governance titles. Based on the dataset from Web of Science of articles published from 1998-2019, the curve fitting the trend graph had an R^2 of 0.626, and an R^2 of 0.572 for the total number of citations by year. Looking at the trends, it is seen that the field of digital governance and cybersecurity is becoming a popular topic within research, and that there is a possibility of extending current research that has been done within academia.

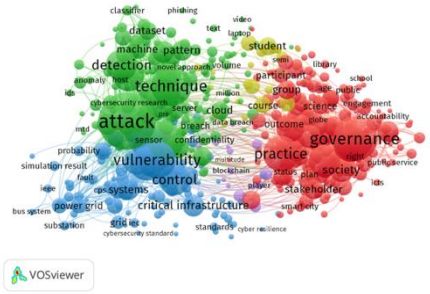

Figure 2. Network Analysis of Word Occurrences

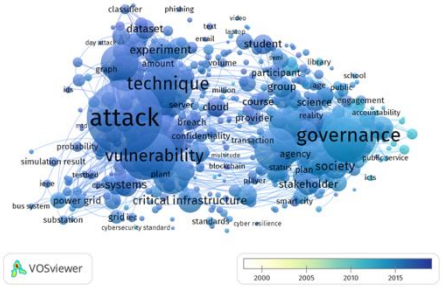

Figure 3. Network Analysis of Word Occurrences Based on Year

Figures 2 and 3 show the word occurrence network based on year of occurrence based on the 2,202 articles. The larger the bubble, the higher the occurrence (van Eck & Waltman 2019). The lines connecting the bubbles indicate word co-occurrence frequencies. Figure 2 shows the five cluster areas, words that are clustered with one another are the same color. Based on the findings, governance, attack, and technique co-

occurred in the key terms of the published articles more frequently. Figure 3 shows the word occurrence network based on average year of occurrence. It was found that word co-occurrence happened more frequently between 2015-onward, which aligns with the growth of number of articles published by year and indicate that with the growth of publications on this topic, common themes such as: governance, attack, vulnerability, and technique were all topics that were highly published about in IT governance and cybersecurity research.

Keyword	# of Occurrences	Year of Occurrence	Number of Links
attack	439	2016	524
governance	303	2013	470
technique	259	2015	516
vulnerability	231	2015	496
device	222	2016	491
government	221	2013	467
practice	216	2014	483
cyber attack	199	2015	470
architecture	193	2015	462
policy	184	2014	450

Table 1. Top 10 Occurring Words in Cybersecurity and Digital Governance Articles

Keyword	# of Occurrences	Year of Occurrence	Number of Links
iot	76	2017	328
neural network	33	2017	179
iot device	22	2017	153
blockchain	19	2017	133
previous work	19	2017	148

Table 2. Top 5 Occurring Words in Cybersecurity and Digital Governance Articles in 2017

Table 1 and 2 show the top 10 keywords based on the number of occurrences along with the average year of occurrence. Out of the top 10 keywords, 2015 held four of the top 10 occurring words of *technique, vulnerability, cyber attack,* and *architecture* (shown in Table 1). Meanwhile, the top occurring words were *attack* and *device*. The number of links indicates the number of co-authorships occur between articles with the listed keywords (van Eck & Ludo Waltman 2019). Within the number of links across articles in cybersecurity and digital governance, *attack* had 524 links to other articles, *technique* linked to 516 other articles, and *vulnerability* linked to 496 other articles. Table 2 illustrates the top 5 keywords based on occurrence in 2017, which were: *iot, neural network, iot device, blockchain,* and *previous work*. The information shown in Table 2 shows that the newer publications on digital governance and cybersecurity are starting to move towards newer topics. The keyword occurrence, number of links and year of occurrence can illustrate the top topics that articles in digital governance and cybersecurity have focused on.

Conclusion

This research contributes three things to the body of IS research: 1) understanding what extant literature on cybersecurity governance currently addresses, 2) proposes bibliometrics as a supplementary analysis for literature reviews, and 3) analyzes the areas of research on cybersecurity governance that the IS field is moving to. Through this preliminary analysis, the researchers have found that much of the existing research is based on a classical view of cybersecurity and digital governance, however, these topics have started to shift and move towards looking at topics like IOT and blockchain. As cybersecurity continues to become a growing problem for firms, solutions for understanding the depth and complexity of cybersecurity governance and its relation to newer technologies (ex., cloud services) are needed. Based on the initial findings, research is moving towards cybersecurity governance topics. Future work on this project will involve a similar analysis of newswire cybersecurity events to examine if existing practitioner cyber events is aligned with the current state of research.

Future work in the field should start to address the components of governance that are applied within firms and cybersecurity. As firms continue to incorporate internet-based technologies, firms need to address how to effectively understand and incorporate effective cybersecurity governance to secure their intellectual properties (Thomas 2018; ISACA 2012). The dataset that was pulled from WoS can give a great overview of

what existing literature says, however, further text analysis using a combination of citation datasets including resources like Google Scholar will be an ongoing project for the researchers to understand how cybersecurity governance has been shaped throughout the years. In addition, future research should also start to look in depth at cybersecurity research that have arisen directly through firms via industry-related reports, which can illustrate the industry trends of cybersecurity governance. Overall, this research is part of an ongoing project to delve into the state of cybersecurity governance research and other in-depth analyses identify what cybersecurity research needs exist within today's firms.

REFERENCES

Ali, S., and Green, P. 2012. "Effective Information Technology (IT) Governance Mechanisms: An IT Outsourcing Perspective," *Information Systems Frontiers* (14:2), pp. 179-193.

Cavelty, M. D. 2007. *Cyber-Security and Threat Politics: Us Efforts to Secure the Information Age*. Routledge.

Clarivate Analytics. 2008. "Using Bibliometrics: A Guide to Evaluating Research Performance with Citation Data." From http://ips.clarivate.com/m/pdfs/325133_thomson.pdf

de Carvalho, C. A. B., Andrade, R. M. D., de Castro, M. F., Coutinho, E. F., and Agoulmine, N. 2017. "State of the Art and Challenges of Security Sla for Cloud Computing," *Computers & Electrical Engineering* (59), pp. 141-152.

Gashami, J. P. G., Chang, Y., Rho, J. J., and Park, M. C. 2016. "Privacy Concerns and Benefits in SaaS Adoption by Individual Users: A Trade-Off Approach," Information Development (32:4), pp. 837-852.

IDC. 2018. "Worldwide Spending on Security Solutions Forecast to Reach $91 Billion in 2018, According to a New IDC Spending Guide." From https://www.idc.com/getdoc.jsp?containerId=prUS43691018

IDG. 2018. "2018 Cloud Computing Survey." From https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/

ISACA. 2012. "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT". From http://www.isaca.org/COBIT/Pages/COBIT-2019-Publications-Resources.aspx

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1).

Mueller, M. 2017. "Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings," *Digital Policy, Regulation and Governance* (19:6), pp. 415-428.

NIST. 2018. "Cybersecurity Framework Version 1.1." from https://www.nist.gov/cyberframework/framework

Peterson, R. 2004. "Crafting Information Technology Governance," *Information Systems Management* (21:4), pp. 7-22.

Privacy Rights Clearinghouse. 2018. Data Breaches Dataset. Retrieved from https://www.privacyrights.org/data-breaches

Rebollo, O., Mellado, D., Fernández-Medina, E., and Mouratidis, H. 2015. "Empirical Evaluation of a Cloud Computing Information Security Governance Framework," *Information and Software Technology* (58), pp. 44-57.

Sambamurthy, V., and Zmud, R. W. 1999. "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies," *MIS Quarterly*, pp. 261-290.

Tallon, P. P. 2013. "Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost," *Computer* (46:6), pp. 32-38.

Tallon, P. P., Ramirez, R. V., and Short, J. E. 2013. "The Information Artifact in IT Governance: Toward a Theory of Information Governance," *Journal of Management Information Systems* (30:3), pp. 141-178.

Thomas, M. 2018. "Cobit 5 and the NIST Cybersecurity Framework – a Simplified Framework Solution." From https://www.isaca.org/Knowledge-Center/Blog/Lists/ Posts/Post.aspx?ID=808

Van Eck, N.J., & Waltman, L. (2019). VOSviewer Manual. From http://www.vosviewer.com/getting-started

Weber, R. H. 2010. "Internet of Things–New Security and Privacy Challenges," *Computer law & security review* (26:1), pp. 23-30.

Weill, P., and Ross, J. W. 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Press.

Wilkin, C. L., and Chenhall, R. H. 2010. "A Review of IT Governance: A Taxonomy to Inform Accounting Information Systems," *Journal of Information Systems* (24:2), pp. 107-146.