Health care and cybersecurity: a bibliometric analysis of the literature

Mohammad S. Jalali, Sabina Razak, William Gordon,
Eric Perakslis, and Stuart Madnick

Working Paper CISL# 2018-14

November 2018

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Review Paper

Health care and cybersecurity: a bibliometric analysis of the literature

Mohammad S. Jalali, PhD[1,*], Sabina Razak[1], William Gordon, MD[2], Eric Perakslis, PhD[2], Stuart Madnick, PhD[1]

[1] MIT Sloan School of Management, Cambridge, MA 02142
[2] Harvard Medical School, Boston, MA 02115

*** Corresponding Author:**
Mohammad S. Jalali, PhD
Sloan School of Management
Massachusetts Institute of Technology
245 1st St, E94-1567
Cambridge, MA 02142
United States
Phone: 617-2538596
Email: jalali@mit.edu

Keywords: Cybersecurity, health care, literature analysis, bibliometric review, text mining

Health care and cybersecurity: a bibliometric analysis of the literature

Mohammad S. Jalali, PhD[1,*], Sabina Razak[1], William Gordon, MD[2], Eric Perakslis, PhD[2], Stuart Madnick, PhD[1]

[1] MIT Sloan School of Management, Cambridge, MA 02142
[2] Harvard Medical School, Boston, MA 02115

Abstract:

Background: Over the past decade, clinical care has become globally dependent on information technology. The cybersecurity of healthcare information systems is now an essential component of safe, reliable, and effective healthcare delivery.
Objectives: The objective of this study is to provide an overview of the literature at the intersection of cybersecurity and healthcare delivery.
Methods: A comprehensive search was conducted using PubMed and Web of Science (WoS) for English-language peer-reviewed articles. We carried out chronological analysis, domain clustering analysis, and text analysis of the included articles to generate a high-level concept map composed of specific words and the connections between them.
Results: Our final sample included 472 English-language journal articles. Our review results revealed that the majority of articles are focused on technology: Technology-focused articles made up more than half of all the clusters, while only 32% were managerial. This focus on the technological aspects of cybersecurity suggests that non-technological variables (human-based and organizational aspects, strategy and management) may be understudied. Also, software development security, business continuity, and disaster recovery planning each accounted for 3% of the studied articles. Our results also show that physical security is lacking in research, with only 1% of the literature being categorized as such. Cyber vulnerabilities are not all digital. Many physical threats contribute to breaches, and these threats potentially affect the physical safety of patients.
Conclusions: Our results revealed an overall increase in research in this area, and identified major gaps and opportunities for future work.

Keywords: Cybersecurity, health care, literature analysis, bibliometric review, text mining

INTRODUCTION

Cybersecurity is an increasingly critical aspect of healthcare information technology infrastructure. The rapid digitization of healthcare delivery, from electronic health records and telehealth to mHealth (mobile health) and Internet-of-Things connected medical devices, introduces risks related to cybersecurity vulnerabilities [1]. These vulnerabilities are particularly worrisome because cyberattacks in a healthcare setting can result in the release of highly sensitive personal information or cause disruptions in clinical care [2-5]. The WannaCry and NotPetya ransomware attacks are two recent examples that resulted in impaired healthcare delivery capabilities worldwide [6].

Healthcare organizations are particularly vulnerable to cyber threats. Verizon's 2018 Data Breach Investigation Report, for example, found that health care was the area most affected by data breaches, accounting for 24% of the total investigated breaches across all industries [7]. Additionally, a report by the Ponemon Institute found that almost 90% of respondents in health care had experienced a data breach in the past two years [8]. Another survey revealed that over 75% of healthcare organizations had experienced a recent security incident [9]. The causes are multifactorial, involving both technology and people, with human error and cultural factors playing an increasingly critical role [10, 11]. Despite efforts to teach best-practice security behavior through training programs, recent surveys have revealed that one in five healthcare employees still write down their usernames and passwords on paper [12].

Given the rising importance of cybersecurity for safe, effective, and reliable healthcare delivery, there is a need to provide an overview of the literature at the intersection of cybersecurity and healthcare. Recent systematic reviews synthesized insights from 31 articles about cyber threats in health care [13] and aggregated strategies from 13 articles about responding to cyber incidents in health care organizations [14]. In this paper, we conduct a large bibliometric review of the literature and set out to describe the current state of research on various aspects of cybersecurity in health care in order, not only to understand current trends, but also to identify gaps and guide future research efforts towards improving the security of our healthcare systems.

METHODS

Study Eligibility Criteria

A comprehensive search was conducted using PubMed and Web of Science (WoS) for English-language peer-reviewed articles. We identified search keywords by adopting terminologies in The National Initiative for Cybersecurity Careers and Studies [15] and The British Standards Institution glossaries (see Table S1) [16]. We included articles published from the inception of PubMed (1966) and WoS (1900) to September 2017. Articles were excluded if they did not clearly focus on cybersecurity or health care, or if they were reviews or meta-analyses. Inclusion and exclusion criteria were formulated prior to the preliminary title and abstract screening. The eligibility criteria were intentionally kept nonspecific in order to get a full picture of the research that exists on the topic. To increase our confidence in the inclusion criteria, we conducted an initial pilot screening of 100 articles.

More details about our methodology are available in our supplementary material (Section S1).

Screening and Selection

Screening of titles and abstracts was conducted with the software package Abstrackr [17]. Full texts of the 'maybe' articles were independently reviewed by two trained individuals to assess study eligibility. Disagreements about study inclusion were discussed until consensus was reached.

Chronological, Clustering, and Trend Analysis

We carried out chronological analysis of the number of articles published per year and the number of authors per article. We topically clustered articles using ten security domains created by the International Information Systems Security Certification Consortium to categorize each article—see Table S2 in the Appendix for the list and definitions of the ten clusters. Each clustered article was further categorized into technological, managerial, legal, and/or interdisciplinary if it fell into more than three categories (see Table S3 in the Appendix). Features of the included articles, such as publishing journal and the number of citations, were recorded.

Text Analysis

We created word clouds to visualize the word frequencies in titles and abstracts over time. We then assessed text titles and abstracts to generate a high-level concept map composed of specific words and the connections between them. We used the software package Leximancer text analytics (version 4.5), which starts with an unsupervised machine learning approach (underpinned by Bayesian theory) to extract a network of meaning from the data, and develops a heat map that visually illustrates the end results [18, 19]. Heat maps consists of "themes," represented by bubbles, and "concepts," represented by grey dots.

RESULTS

Search Results

The primary search on PubMed containing terms pertaining to "cyber" yielded 1,480 articles, while the search on WoS yielded 810 articles. After removing 310 duplicates, the titles and abstracts of 1,980 articles were then screened, a process facilitated by Abstrackr software [20]. Based on the inclusion criteria, 1,262 articles were excluded in the first screening, narrowing the results down to 718 articles for full-text review. Eventually, a further scan removed additional articles to narrow the final selection to 472 articles. Figure 1 presents the search method and results.

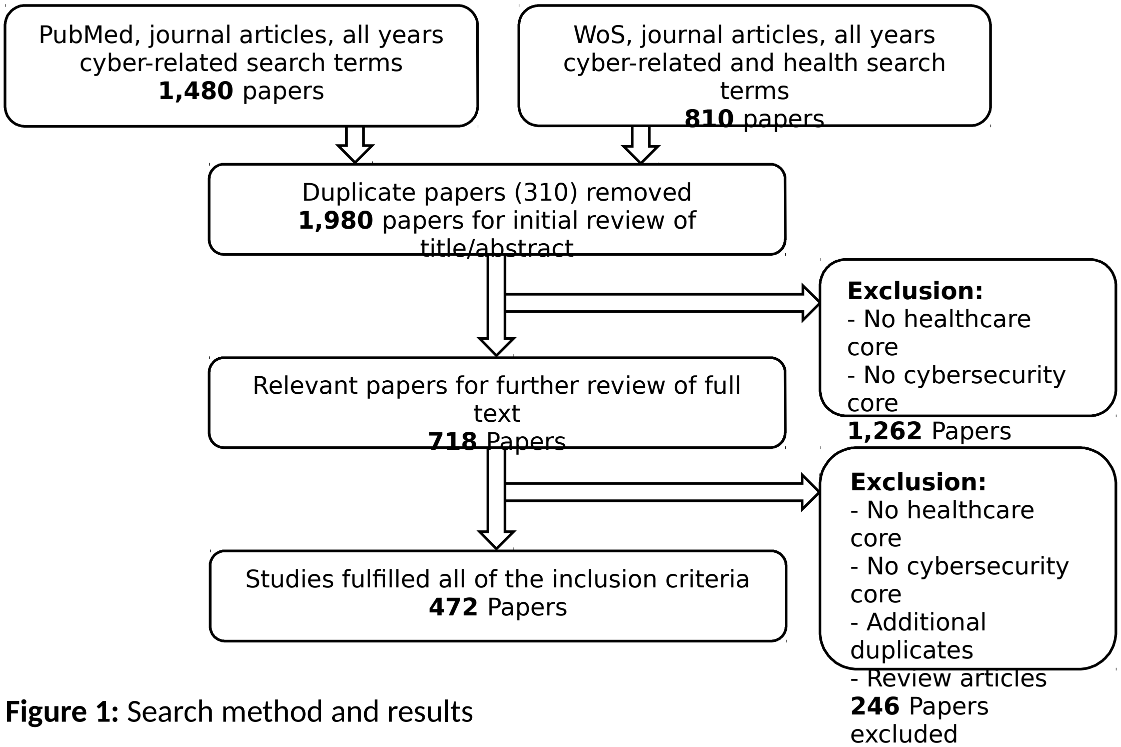

PubMed, journal articles, all years
cyber-related search terms
1,480 papers
WoS, journal articles, all years
cyber-related and health search terms
810 papers
Duplicate papers (310) removed
1,980 papers for initial review of title/abstract
Exclusion:
- No healthcare core
- No cybersecurity core
1,262 Papers
Relevant papers for further review of full text
718 Papers
Exclusion:
- No healthcare core
- No cybersecurity core
- Additional duplicates
- Review articles
246 Papers excluded
Studies fulfilled all of the inclusion criteria
472 Papers

Figure 1: Search method and results

Chronological, Clustering, and Trend Analysis

Figure 2 presents the overall trend of all publications over time, from 1985 to September 2017; the first included article was published in 1979 but was excluded from the figure for better visualization. Figure 2 shows a steady increase in the number of articles published on cybersecurity in health care (see Figure S1 in the online Appendix for the analysis of the number of co-authors).

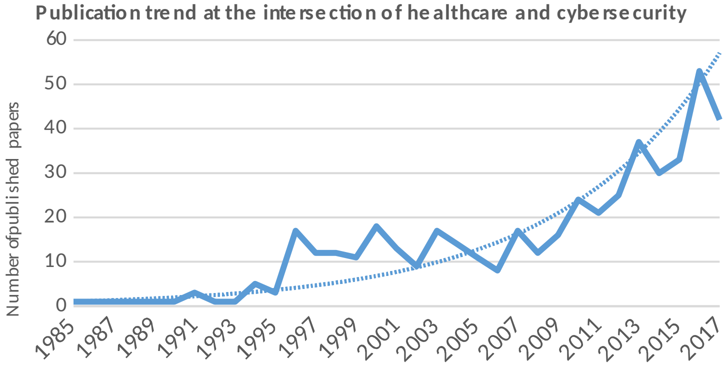


Figure 2: The annual number of published papers at the intersection of health care and cybersecurity

Figure 3 presents the distribution of articles in the ten clusters (clusters were identified by two researchers; see identified cluster/clusters for each article in Table S3 in the Appendix). Figure 3 shows that (a) Information Security, Governance, and Risk Management, and (b) Security Architecture and Design were the most commonly used clusters, each accounting for more than

20% of all articles. There was much less focus on Software Development Security, Business Continuity and Disaster Recovery Planning, and Physical (Environmental) Security.

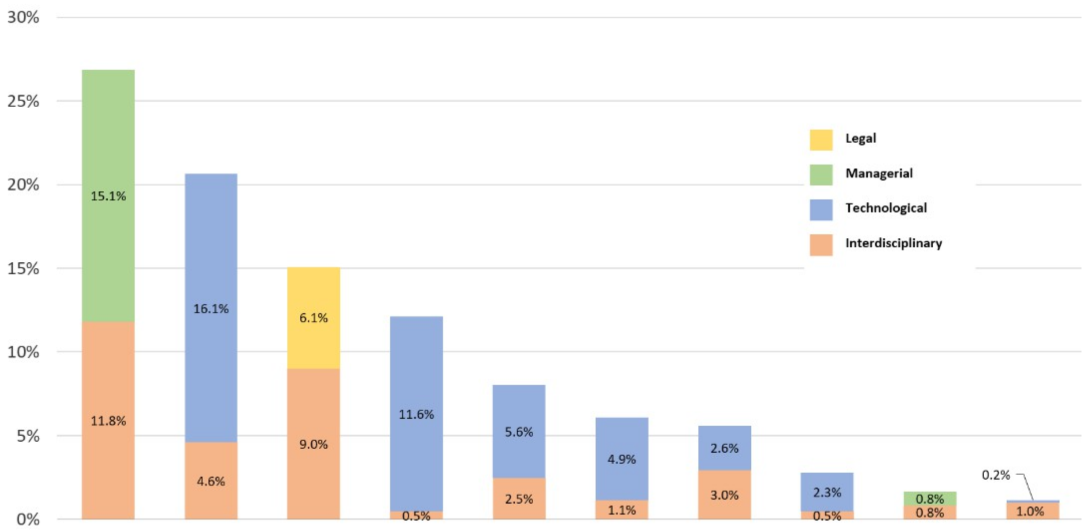


Figure 3: Cluster distributions

Figure 3 also shows the distribution within the three high-level categories: technological, managerial, and legal (see Table S3 in the Appendix for the clusters in each). The seven technological clusters made up more than half of the overall clusters, the two managerial clusters represent 32%, and the legal cluster, 18%.

The orange-shaded portion within each cluster represents interdisciplinary articles (those that spanned multiple high-level categories). While Physical Security has the lowest number of publications, it was the most interdisciplinary cluster (six out of the seven articles; 6/7=85.7% identified as interdisciplinary). Legal, Regulations, Investigations and Compliance was the second most interdisciplinary cluster (59.8% of the articles in this category were interdisciplinary), followed by Operations Security (52.9%), Business Continuity and Disaster Recovery Planning (50%), Information Security Governance and Risk Management (43.9%), and Access Control (30.6%). While Security Architecture and Design is the second-most-frequent cluster overall, only 22.2% of the articles were found to be interdisciplinary. Amongst the less interdisciplinary categories were Telecommunications and Network Security (18.9%), Software Development Security (17.6%), and Cryptography (4%) (see Figure S2 in the Appendix for the distribution of the interdisciplinary clusters).

We then looked at publication trends over time in the ten clusters. All clusters have increased in frequency, with some, including Security Architecture and Design, Information Security

Governance and Risk Management, and Cryptography, demonstrating particularly steep increases.

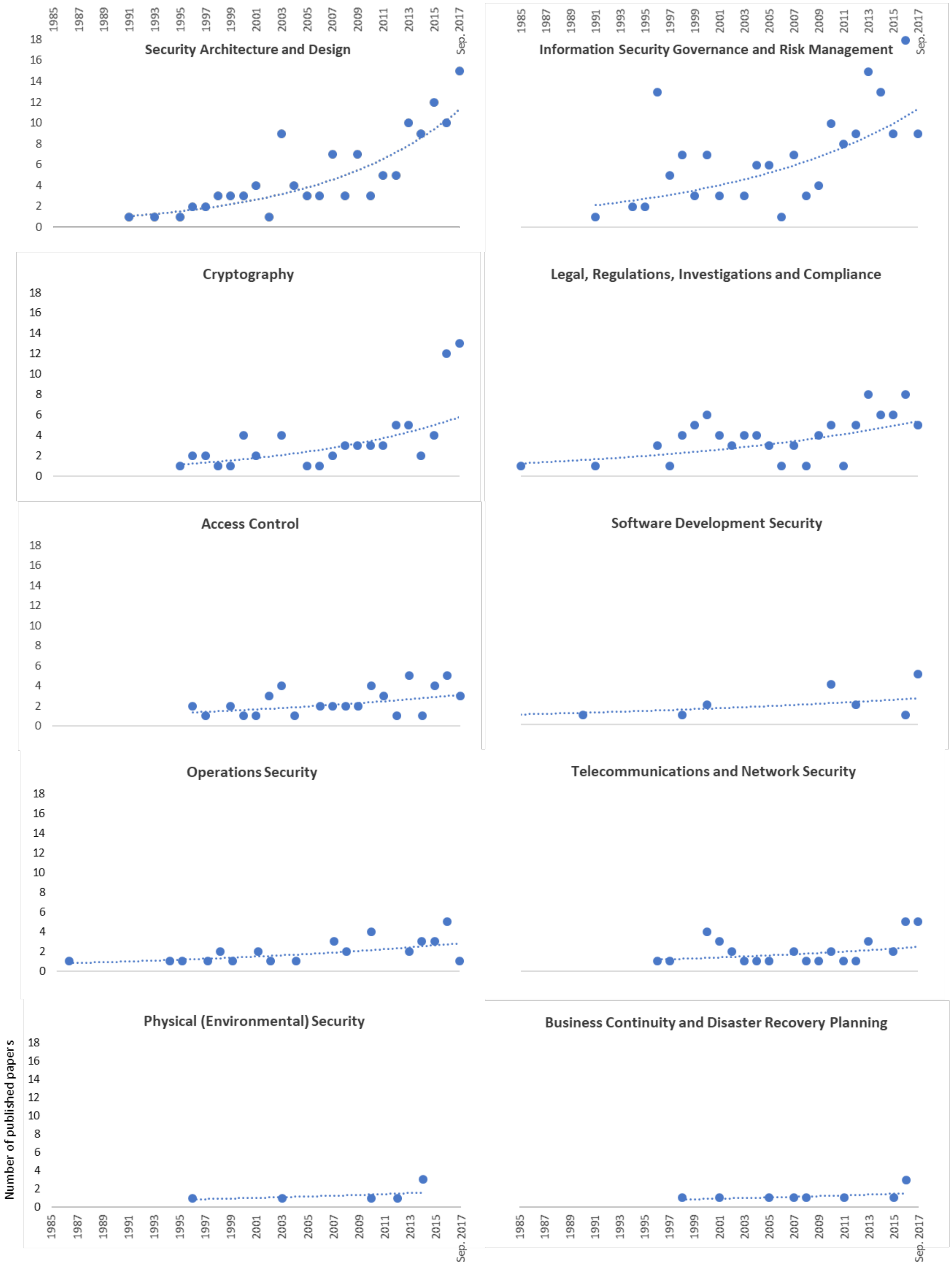


Figure 4: Trend of 10 clusters over time

Journal Characteristics

Overall, the 472 included articles were published in 239 unique journals. We sorted the journals according to the number of published articles and ranked the ones with more than three articles, which resulted in the list of 17 journals presented in Table 1. According to the corresponding Incites Journal Citation Reports (JCR) categories [21], the top journals tended to focus on computer science, information systems, and medical informatics. The most popular JCR category, accounting for seven out of the ten journals listed on JCR, was medical informatics. Six journals had a computer science categorization, specifically within information systems, interdisciplinary applications, and/or theory and methods. Five journals came from a healthcare sciences and services journal. Only one of the top fifteen journals was categorized as a biomedical engineering journal, one as a math and computational biology journal, and one as a radiology, nuclear medicine, and medical imaging journal.

Additionally, about 73% of the 239 journals had only published one article in this area. The high number and diversity of the journals included, along with the low publication rate, suggest that there is currently no major niche for medical practice readership at the intersection of cybersecurity and health care, due to the cross-disciplinary nature of the field.

Table 1: Journals with the most articles

Number of published papers	Journal	Indexed categories (according to Journal Citation Reports)
47	Studies in Health Technology and Informatics	Not indexed
24	International Journal of Medical Informatics	Computer Science, Information Systems; Health Care Sciences & Services; Medical Informatics
17	Journal of Medical Systems	Health Care Sciences & Services; Medical Informatics
9	Journal of Diabetes Science and Technology	Not indexed
8	Healthcare Financial Management	Not indexed
8	Medical Informatics	Computer Science, Information Systems; Computer Science, Interdisciplinary Applications; Medical Informatics
8	International Journal of Bio-Medical Computing	Computer Science, Interdisciplinary Applications; Computer Science, Theory & Methods; Engineering, Biomedical; Medical Informatics
7	Computers & Security	Computer Science, Information Systems
7	Journal of the American Medical Informatics Association	Computer Science, Information Systems; Computer Science, Interdisciplinary Applications; Health Care Sciences & Services; Medical Informatics
7	Journal of Healthcare Protection Management	Not indexed
5	Telemedicine Journal and E-Health	Health Care Sciences & Services
4	IEEE Journal of Biomedical and Health Informatics	Computer Science, Information Systems; Computer Science, Interdisciplinary Applications; Mathematical & Computational Biology; Medical Informatics
4	Journal of the American Health Information Management Association	Not indexed
4	Journal of Digital Imaging	Radiology, Nuclear Medicine & Medical Imaging
4	Journal of Healthcare Information Management	Not indexed
4	Journal of Medical Internet Research	Health Care Sciences & Services; Medical Informatics
4	Journal of Medical Practice Management	Not indexed

Characteristics of the Most-Cited Articles

Table 2 shows the most influential publications in the field of cybersecurity in health care, ranked by the number of citations as of September 2017. Six out of the top 15 cited articles were published in five journals of the Institute of Electrical and Electronics Engineers (IEEE). The clusters show that there is a mix of article domains, across the legal, managerial, and technological domains. The author-denoted keywords support this as well.

Looking at the total clusters of the top 15 articles, 38% were Security Architecture and Design. Cryptography was the next most popular at 17%, followed by Legal, Regulations, Investigations and Compliance and Access Control at 13% each. Overall, 79% of the clusters were technological, 13% legal, and 8% managerial. Additionally, 20% of the papers were interdisciplinary with multiple clusters of distinct high-level categories. It should be noted that the list of most-cited articles does not reflect the most recent research as there is often a significant delay for articles to receive citations.

Table 2: Top 15 most cited article

Rank	Citations	Title	Author	Year	Journal	Clusters	Author Denoted Keywords
1	443	Data security and privacy in wireless body area networks	Li, M., W. J. Lou and K. Ren	2010	IEEE Wireless Communications	Telecommunications and Network Security	Data security; Data privacy; Body sensor networks; Biomedical monitoring; Wireless sensor networks; Wearable sensors; Wireless communication; Medical services; Application software; Patient monitoring
2	304	Analyzing regulatory rules for privacy and security requirements	Breaux, T. D. and A. I. Anton	2008	IEEE Transactions on Software Engineering	Legal, Regulations, Investigations and Compliance	Data security and privacy; Laws and regulations; Compliance; Accountability; Requirements engineering
3	173	Medical image security in a HIPAA mandated PACS environment	Cao, F., H. K. Huang and X. Q. Zhou	2003	Computerized Medical Imaging and Graphics	Legal, Regulations, Investigations and Compliance; Security Architecture and Design	Data encryption; Picture archiving and communication system security; Image integrity; Digital imaging and communication in medicine; Compliance; Health insurance portability and accountability act
4	168	SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency	Lu, R. X., X. D. Lin and X. M. Shen	2013	IEEE Transactions on Parallel and Distributed Systems	Access Control; Security Architecture and Design	Mobile-healthcare emergency; Opportunistic computing; User-centric privacy access control; PPSPC
5	158	Authenticity and integrity of digital mammography images	Zhou, X. Q., H. K. Huang and S. L. Lou	2001	IEEE Transactions on Medical Imaging	Cryptography; Telecommunications and Network Security	Data embedding and cryptography; Digital mammography; Image authenticity and integrity; Telemammography
6	131	Security in health-care information systems--current trends	Smith, E. a. J. H. E.	1999	International Journal of Medical Informatics	Access Control; Information Security Governance and Risk Management	Health-care information systems security; Risk-analysis in health-care information systems; Access control for computerized health-care; Electronic patient record; International Medical Informatics Association; managed health-care
7	112	How to ensure data security of an epidemiological follow-up: quality assessment of an anonymous record linkage procedure	Quantin, C., H. Bouzelat, F. A. Allaert, A. M. Benhamiche, J. Faivre and L. Dusserre	1998	International Journal of Medical Informatics	Cryptography; Security Architecture and Design	Data security; Computerized record; Linkage procedure
8	103	IBE-Lite: a lightweight identity-based cryptography for body sensor networks	Tan, C. C., H. D. Wang, S. Zhong and Q. Li	2009	IEEE Transactions on Information Technology in Biomedicine	Security Architecture and Design; Cryptography	Body sensor network; Identity-based encryption; Privacy; Security
9	89	A security architecture for interconnecting health information systems	Gritzalis, D. and C. Lambrinoudakis	2004	International Journal of Medical Informatics	Access Control; Security Architecture and Design	Information systems security; Computer security; Medical data security; Medical Data Protection; Electronic healthcare records; Role-based access control
10	85	Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling	Bui, F. M. and D. Hatzinakos	2008	Eurasip Journal on Advances in Signal Processing	Security Architecture and Design; Cryptography	N/A
11	84	Mhealth data security: the need for HIPAA-compliant standardization	Luxton, D. D., R. A. Kayl and M. C. Mishkind	2012	Telemedicine Journal and E-Health	Software Development Security; Legal, Regulations, Investigations and Compliance	Security; HIPAA; Encryption; Telehealth; Mobile health
12	82	Analysis of the security and privacy requirements of cloud-based electronic health records systems	Rodrigues, J. J., I. de la Torre, G. Fernandez and M. Lopez-Coronado	2013	Journal of Medical Internet Research	Security Architecture and Design	Cloud-computing; eHealth; Electronic health records (EHRs); Privacy; Security
13	82	Health care management and information systems security: awareness, training or education?	Katsikas, S. K.	2000	International Journal of Medical Informatics	Information Security Governance and Risk Management	Health information systems; Information systems security; Health care management; Education; Training; Awareness
14	82	Securing m-healthcare social networks: challenges, countermeasures and future directions	Zhou, J., Z. F. Cao, X. L. Dong, X. D. Lin and A. V. Vasilakos	2013	IEEE Wireless Communications	Security Architecture and Design	Mobile communication; Social network services; Medical services; Mobile computing; Personal digital assistants; Privacy; Network security; Electronic medical records

15	80	Privacy and data security in E-health: requirements from the user's perspective	Wilkowska, W. and M. Ziefle	2012	Health Informatics Journal	Security Architecture and Design	E-health; Gender; Medical assistive technologies; Privacy; Security

Text Analysis

The text mining analysis identified more specific trends in the article texts. The map produced from all titles and abstracts is shown in Figure 5. The thematic bubbles are ranked by relevance based on a heat-map color scheme: Hot colors indicate more important themes, and cool colors indicate less important themes. The relative positions of the bubbles show the relationship between aggregated ideas, reflecting how closely they are related to each other. The sizes of the bubbles are only set to be inclusive of their grey dots, but the size of each grey dot (a common word within the theme) indicates its relative frequency. The lines between these dots signifies connectivity and association of concepts.

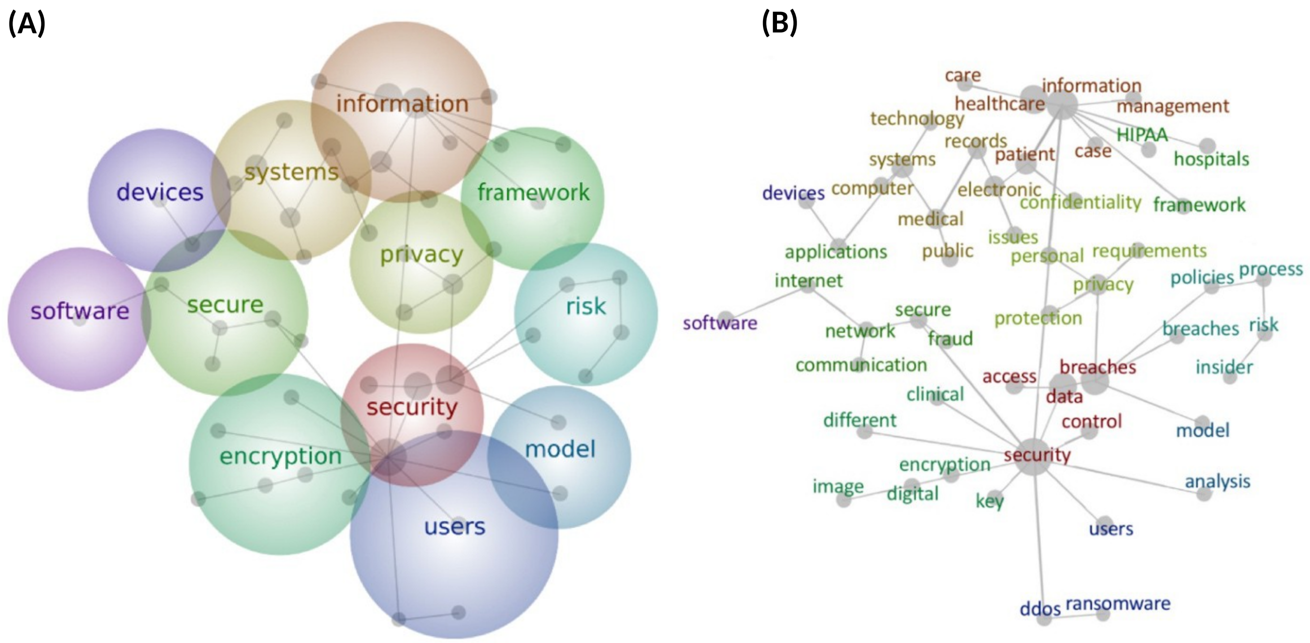


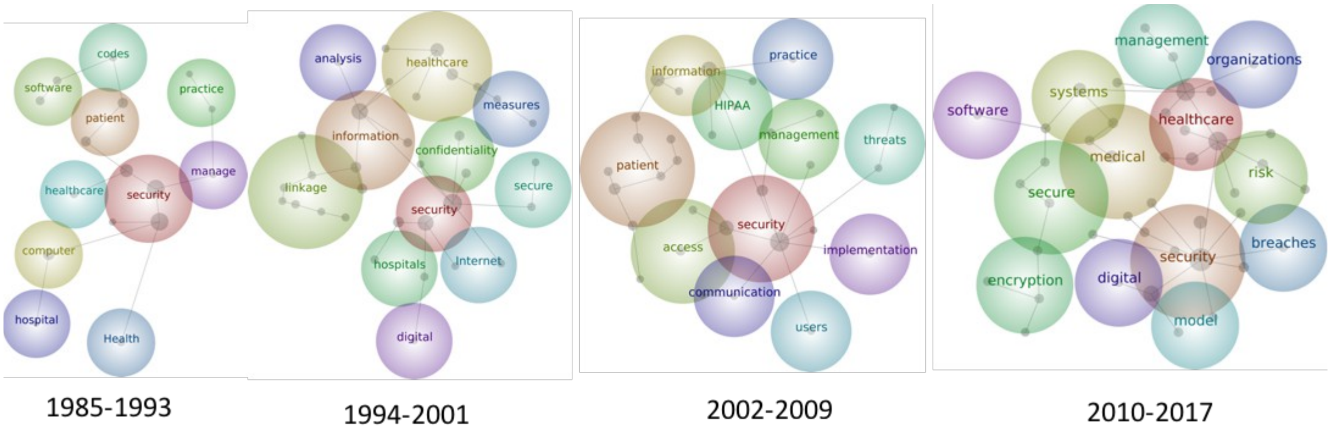
Figure 5: Thematic map of all titles and abstracts (A) and concept cloud of all titles and abstracts (B)

The overlay of grey-dot concepts onto thematic bubbles allows for more specific analysis of terms. Technological terms emerge as the main theme in Figure 5(A), including words like “encryption” and “software.” Concept words within these themes highlight common elements of an organization’s IT structure related to cybersecurity: “Internet,” “network,” “applications,” “records,” “breaches,” “key,” and “electronic.” Managerial and legal terms are also found as concepts in Figure 5(B). “Management” is a concept within the “information” theme. “Policies” and “process” as concepts in the risk theme suggests the influence of risk analysis on the cybersecurity policies and procedures of organizations. “HIPAA” is a concept that stems from the “information” concept in the “important” theme.

The two central themes “security” and “information” include multiple large grey-dot concepts that branch out into other thematic areas. There is an overlap between “security” and “encryption,” suggesting that encoding material is fundamental to security. An overlap between “security” and “users” could imply that user control is imperative to security.

For further analysis of word frequencies, the articles from 1985 to 2017 were split into four time periods, with the first period being nine years and each of the next three, eight years: 1985–1993, 1994–2001, 2002–2009, 2010–September 2017. Figure S3 in the Appendix shows the word clouds within the four time periods. The size of the word represents its occurrence frequency. The term “privacy” increased in size in the last three time periods. “Internet” appears in 1994–2001, around the time of the dot-com bubble. “Legal” is mentioned in 1985–1993, and “legislation” is found in 1994–2001. “HIPAA” appears in 2002-2009 and again, though smaller, in 2010-2017.

Maps of the four time periods were also created to identify the trends over time, shown in Figure 6. “Security” remained the most popular concept from 1985 to 2009, only to be overtaken by “health care” from 2010 to 2017 (the most popular concept is always indicated by the red bubble). The time period maps in Figure S4-7 in the Appendix provide further details.



1985-1993 1994-2001 2002-2009 2010-2017

Figure 6: Thematic maps of titles and abstracts of articles in four time periods

DISCUSSION

This article provides an analysis of the literature at the intersection of cybersecurity and health care. We found that in general, research in this area has been increasing over the past 20 years. This research is continually being represented in a wide, distributed array of academic journals, reflecting the importance of this topic. With rising cybersecurity attacks against hospitals, and healthcare delivery increasingly being dependent on technology, we expect cybersecurity to continue to have a central role in healthcare delivery.

Despite the increase in research and attention to cybersecurity, shortcomings in research remain. For example, our research suggests that the majority of articles on cybersecurity are focused on technology. In our domain clustering analysis, technology-focused articles made up more than half of all the clusters, while only 32% were managerial. Similarly, in our journal analysis, 58 of the articles included in the 15 most published journals were from computer science journals, 12 articles were from health-focused journals, and 79% of the top 15 most cited paper clusters were technological. This focus on the technological aspects of cybersecurity suggests that non-technological variables (human-based and organizational aspects, strategy and management) may be understudied. Investment in technological tools should be the output of a robust cybersecurity strategy, rather than the foundation [22]. The overwhelming majority of cybersecurity incidents are caused or propagated by people [23], and technological solutions can only go so far in mitigating this risk.

We also found discordance between the topics of the highly cited articles and the topical breakdown of our cluster analysis (these articles were published more than five years ago, implying that emergent threats are poorly captured). This suggests that articles on topics such as cryptography have significant traction even though they are not widely present in the literature. On the other hand, few information security governance and compliance articles were frequently cited even though they make up a large portion of the literature.

Cybersecurity is most often examined with respect to privacy and compliance. Our results show that physical security is lacking in research, with only 1% of the literature being categorized as such. Cyber vulnerabilities are not all digital. Many physical threats contribute to breaches, and these threats potentially affect the physical safety of patients. Software development security, business continuity, and disaster recovery planning each accounted for 3% of the studied articles. Further examination is needed on these topics, and our study suggests that incident recovery (critical to the success of recovery from incidents) is not a significant focus within the research community. Legal-focused articles were the least represented. Moreover, federal cybersecurity guidance, such as the publications of the National Institute of Standards and Technology (NIST), is seldom observed in our text analysis. Also, massive increases in cybersecurity spending [24] is not driving proportional growth in the literature.

Furthermore, our lexical analysis highlighted a separation of security processes and software terminology, with longer word distances between these themes. Additionally, the time period maps for 2002-2009 and 2010-2017 show no overlap between the management and technological themes. More interdisciplinary research is needed to avoid the gaps that come from only looking at managerial and technological security issues.

It should be noted that unlike medical research, which is set up to be open to benefit human lives [25], cybersecurity is based on the premise of an active adversary. The presence of this adversary may, unfortunately, drive a school of thought that knowledge, especially specific strategies and tactics, should not be shared openly, which impedes the growth and utility of the research.

Limitations and Suggestions for Future Research

Our review was limited to journal articles indexed in PubMed and WoS, and did not look at non-English articles or documents other than journal articles (e.g., conference articles, white papers, or reports by governments or other organizations). A more comprehensive search could consider these sources. Information retrieval was limited to articles that included the terms of the search strategy in their titles or abstracts—any articles that used different terminology was not retrieved. Also, we only included articles that had cybersecurity in the core of the study.

Future reviews could focus on individual clusters that we reviewed to provide a more in-depth analysis of the cluster. For instance, they could look specifically at business continuity and disaster recovery planning, or software development security. Such a detailed focus can help synthesize research findings and provide best practices. They could also analyze the gap in managerial research and the implications of a narrow technological focus. Moreover, they could focus on different settings in health care, such as inpatient and outpatient care, translational research, health and wellness environments, integration of mobile devices and networked systems, among others.

Comparison of our analyses of texts and trends of research with those of non-peer reviewed articles (published in media outlets and weblogs) would be also informative. Such articles provide more timely information about the advanced, persistent threats of today, and are often published by authors who do not necessarily publish in scientific journals.

Acknowledgements

Financial support for this study was provided by Cybersecurity at MIT Sloan; also known as MIT (IC)^3—the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity.

Conflicts of Interest

None declared.

References:

1. Jalali, M.S. and J.P. Kaiser, *Cybersecurity in Hospitals: A Systematic, Organizational Perspective.* J Med Internet Res, 2018. 20(5): p. e10059.
2. Gordon, W.J., A. Fairhall, and A. Landman, *Threats to Information Security — Public Health Implications.* New England Journal of Medicine, 2017. 377(8): p. 707-709.
3. Perakslis, E.D., *Cybersecurity in Health Care.* New England Journal of Medicine, 2014. 371(5): p. 395-397.
4. Jarrett, M.P., *Cybersecurity—a serious patient care concern.* JAMA, 2017. 318(14): p. 1319-1320.
5. Kramer, D.B. and K. Fu, *Cybersecurity concerns and medical devices: Lessons from a pacemaker advisory.* JAMA, 2017. 318(21): p. 2077-2078.
6. Furnell, S. and D. Emm, *The ABC of ransomware protection.* Computer Fraud & Security, 2017. 2017(10): p. 5-11.
7. Verizon, *Verizon 2018 Data Breach Investigations Report* 2018.
8. Institute, P., *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. 2016.

9. Healthcare Information and Management Systems Society. *2018 HIMSS Cybersecurity Survey*. 2018 July 10, 2018]; Available from: http://www.webcitation.org/70oQtDbCw.
10. Madnick, S., et al. *Measuring Stakeholders' Perceptions of Cybersecurity for Renewable Energy Systems*. 2017. Cham: Springer International Publishing.
11. Jalali, M.S., M. Siegel, and S. Madnick, *Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment*. The Journal of Strategic Information Systems, 2018.
12. Accenture, *Healthcare Workforce Survey on Cybersecurity*. 2018.
13. Kruse, C.S., et al., *Cybersecurity in healthcare: A systematic review of modern threats and trends*. Technology and Health Care, 2017. 25(1): p. 1-10.
14. Jalali, M., et al., *EARS to Cyber Incidents in Health Care*. SSRN, 2018.
15. National Initiative for Cybersecurity Careers and Studies. *Glossary of Common Cybersecurity Terminology*. 2017 November 27, 2017; Available from: https://niccs.us-cert.gov/glossary.
16. BSI, *Glossary of cyber security terms*. 2018.
17. Wallace, B.C., et al., *Deploying an interactive machine learning system in an evidence-based practice center: abstrackr*, in *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*. 2012, ACM: Miami, Florida, USA. p. 819-824.
18. Smith, A.E. and M.S. Humphreys, *Evaluation of unsupervised semantic mapping of natural language with Leximancer concept mapping*. Behavior Research Methods, 2006. 38(2): p. 262-279.
19. Cheng, M. and D. Edwards, *A comparative automated content analysis approach on the review of the sharing economy discourse in tourism and hospitality.* Current Issues in Tourism, 2017: p. 1-15.
20. Byron C. Wallace, K.S., Carla E. Brodley, Joseph Lau and Thomas A. Trikalinos, *Deploying an interactive machine learning system in an evidence-based practice center: abstrackr.* Proc. of the ACM International Health Informatics Symposium (IHI), 2012: p. 819-824.
21. Clarivate Analytics. *InCites Journal citation Reports*. 2018; Available from: http://www.webcitation.org/73XTpO9jx.
22. Health Care Industry Cybersecurity Task Force. *Report on improving cybersecurity in the health care industry*. Department of Health and Human Services: Public Health Emergency 2017; Available from: http://www.webcitation.org/70oQxvqIp.
23. van Zadelhoff, M., *The biggest cybersecurity threats are inside your company.* Digital article-Harvard Business Review, 2016.
24. *Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017*. 2018; Available from: http://www.webcitation.org/73XT5gFp1.
25. Ioannidis, J.P.A., et al., *Increasing value and reducing waste in research design, conduct, and analysis.* The Lancet, 2014. 383(9912): p. 166-175.

Abbreviations

NIST: the National Institute of Standards and Technology
WoS: Web of Science