2021

Information Security in Business: A Bibliometric Analysis of the 100 Top Cited Articles

Shafiq Ur Rehman Dr.
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia., surehman@iau.edu.sa

Maqsood Mahmud
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia, mMahmud@iau.edu.sa

Atta- ur- Rahman Dr.
Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia, aaurrahman@iau.edu.sa

Ikram Ul Haq
King Saud bin Abdulaziz University for Health Sciences, Riyadh, Saudi Arabia., ikram34439@yahoo.com

Muhammad Safdar Dr.
National University of Sciences and Technology (NUST), Islamabad, Pakistan, safdargr8@gmail.com

Information Security in Business: A Bibliometric Analysis of the 100 Top Cited Articles

Abstract

This study aims a bibliometric analysis of the 100 top-cited articles extracted from the Web of Science database on the topic of information security in the business context. A retrospective method was applied to the dataset extracted from the Web of Science Database. A total of 500 most cited items were downloaded and the authors selected the articles related to information security and business for further analysis. It was found that the top-cited papers were published between the years 1990 and 2018 and had received 3,375 citations. While most of the articles followed the three-author pattern, the single author pattern articles had received the maximum citation impact. Cybersecurity policies were recognized as the most researched topic and the majority of articles had been published in Quartile-1 journals. Furthermore, the majority (67%) of the articles were published in journals having impact factors ranging from 2.3 to 6.95. The Journal of Management Information System was found to top the list of most prolific journals with 13 articles. This study identifies the trends and patterns of research publications on information security in the business. This evaluation is likely to develop awareness in understanding the scope and coverage of information security from a business perspective. The findings of this study have highlighted the various parameters of highly cited articles on information security published during the last three decades. The results might support new researchers' interest in information security in the context of businesses.

Keywords: Information Security, Cybersecurity Policies, Business, Cyber Risks Management, Resilience, Vulnerability Assessments, Digital Forensics.

Introduction

Protection of information has become a leading issue in the current digital age. Organizations have to allocate considerable financial resources to ensure the security of their information. Significant funds have to be set aside for software, hardware, and manpower resources to prevent potential breaches

and threats to data security. Every organization has its own set of unique requirements related to information security. There are also many variations among organizations in terms of the type of information that needs to be secured and the level of desired security. The level of organizational information security also plays a crucial role in the cyber risk assessment of an organization in this digital era and the prevention of potential security breaches to its data (Johnston & Hale, 2009; Solms and Solms, 2005).

In the field of library and information science, bibliometric methods have been widely used. Scientometrics, a subfield of bibliometrics that deals with the study of scientific publications and quotation analysis, is a commonly used bibliometric method (Rousseau, 2014). Bibliometric applications include Thesauri creation and frequency of term measurement as metrics to evaluate scientometrics. Grammatical and syntactical text structures and reader measurements are used for the quantification of the exchanged communication of information on online media (Hovden, 2013). Citation index data can be analyzed to determine whether posts, writers, and publications are popular and impactful. Citation analysis is a commonly used and an important part of the tenure review process to assess the value of an author's work (Hoang, Kaur & Menczer, 2010).

A bibliometric review is a measure of a person, article, or publication's relative value or influence by counting the number of times other works have discussed the author, article, or publication. A study is conducted to identify the influence of certain works, to learn more about a topic or area by recognizing seminal objects in the same field, and to assess the effect of a particular author in his/her discipline (Garfield, 1955; Moed, 2010; Davis, 2011; Haq & Alfouzan, 2019).

There are several citation analyses tools available to researchers, both subscription-based and free. Each has its limitations and strengths, and none can encompass the whole universe of scientific publications. Consequently, it is the wider image of the wisdom of an author or a journal that is more important than the use of a single method. The three main sources of publications for citation analysis are The Web of Science (WoS), Scopus, and Google Scholar (Moed, 2010; Davis, 2011; Haq & Alfouzan, 2019; Alhibshi et al., 2020).

Culnan (1986) suggested that scholars in all academic disciplines contribute to their fields of intellectual growth. As an experiment, it was further narrated that the conceptual evolution of ideas as portrayed by published research in Management Information Systems (MIS) was based on reviews by authors. The resultant mapping acted as a reference point for potential MIS evaluations to track the formation of new research specialists. Goodrum et al. (2001) explored two views of the creation and use of information in computer-related research based on the analysis (citation) of “PDF” and “Postcript” documents using autonomous citation indexing (ACI) and a parallel analysis (citation) of the journal research indexed by the Institute for Scientific Information (ISI). Researchers (Hu, Tai, Liu, & Cai, 2020) stated that the number of citations earned was used as an impact measure for scholarly publications. Authors described that the creation of tools to find documents with high potential had gained much scientific attention in recent times. This study carried out a latent technique to extract subjects and keywords from papers by Dirichlet and showed that the efficiency of the binary classification model could be enhanced with KP (keyword popularity) features. As mentioned, (Cardona, & Sanz, 2015), the Science Edition of the JCR lists about ten thousand articles according to their impact factor and categorizes them into subjects or thematic groups. The impact factor is the "average number of journal articles published over the last 2 years in the current JCR year." Sajid et al. (2021) conducted a study where the citations-based category identification (CBCI) of the computer science research papers was performed. The authors further investigated the references for article classification. Similarly, automatic text and behavior classification methods have also been investigated in serval studies (Rahman et al., 2019; Hiyafi et al., 2019; Rahman and Alhaidari, 2018; Zaman et al., 2021).

Jacso (2006) proposed a study based on Hirsch's (2005) h-Index, a well-known metric, to measure the scientific publication outputs and the effect of a researcher’s work. It is a cumulative metric based on a combination of published papers and the number of citations these papers have received in compliance with WoS and Scopus data and reports. The h-indices were originally intended for the lens of publications to assess researchers' scientific success. The latest analysis of h-index research was carried out by Bornmann and Daniel (2009) and was well-received by renowned scientometricians,

along with the set of guidelines and proposals on derivative indices presented by them (Musleh 2019; Egghe, 2006, Rousseau and Ye, 2008; Schreiber, 2007; Schubert & Glänzel). The index was soon expanded to evaluate the productivity and influence of newspapers, universities, research institutes, and other groups (Braun et al., 2005; Levitt & Thelwall, 2009; Meneghini &Packer, 2006; Prathap, 2006; Van Rann, 2006). Many scientists have supported and used the h index in different fields and countries to rate researchers and research groups (Cronin & Meho, 2006; Meho & Rogers, 2008; Meneghini & Packer, 2006; Oppenheim, 2007). The content and software characteristics of the most used h-index systems and services have also been investigated by scientists (Bar-Ilan, 2008; Jacso, 2008a; Jacso, 2008b). It is also normal to consider using the h-index to determine the country-wide scientific study and publication of scholarships and for this reason, other bibliometric indicators have long been used by researchers (King, 2004; Moravcsik, 1985).

The value of the journals publishing information systems (IS) research was ranked by Clyde et al. (1994). They ranked journals publishing research on business system computation using a technique for citation analysis and compared the uniform classification system to the original classification. The greatest relative change between a pair of journals was 27 when the most significant positive difference is paired with the maximum negative difference. Authors in (Shiau, 2015) reviewed and identified key issues in leading WoS journals collected from its database. Three primary questions have been established with the aid of co-qualified analysts and factor analysts, including (1) technology acceptance; (2) information technology (IT), the efficiency of the company, and the competitive advantage; (3) IT and organizational structure; (4) case study and methods. In the past two decades, the concepts of 'cumulative tradition' and 'reference disciplines' have been an important part of the IS introspective discussions. By using the idea of a 'work point' and 'reference points,' we can place research in the field of IS to find out where an IS paper is written and the degree to which it derives or relates to other disciplines. A quantitative study of more than 72,600 references distributed across 1,406 IS papers from 16 journals published in the period 1990-2003 indicated a distinct tendency towards a cumulative tradition. Secondly, post-hoc content review offers an insight into how other disciplines utilize IS.

Batisticand Kaše (2015) stated that business science and statistics show us the importance of the subject to practitioners and organizational socialization. To explore the field in question, define current research goals, and identify the most relevant papers and authors, the researchers evaluated the data of the past three years using bibliometric methods. They also established thematically linked research clusters and explained how the field of organizational socialization has developed in interconnected but distinct subfields.

There are many benefits that the information age has brought to mankind. Information is widely available and accessible. However, this widespread use of the easily available information, as well as the digital nature of the information, has created many issues related to the protection of information. Information Security is a broad term that incorporates many elements such as computer security, security in communications, and data security, that work together to ensure the security of the information. The United States Defense Department has defined information security as the "protection of information and information systems from unauthorized access or modification in storage, processing, and transit or against service denial to authorized users" (Papp & Alberts, 2002). According to Olijnyk (2015), information security has become a primary societal concern in the last two decades. In the study, Scopus research records from 1995 to 2015, published with effect and productivity measures along with co-word and domain visualization methods, were examined in the bibliometric data taken from 74021 sources. This scientific study offers an analysis of information security from several points of view (e.g., temporal, seminal papers, institutions, sources, authors). Over the decades, many topics of study related to information security have been established, for instance, management and administration of cryptography, information security, intrusion detection, medical data security, steganography, watermarking and wireless security, etc. However, according to Siponen & Oinas-Kukkönen (2007) “scholars from certain disciplines, including computer science, cryptology, computer technology, or IT systems, frequently seem poorly informed of the contributions of researchers from different disciplines.” There is a need for a holistic approach that looks at all aspects of the topic. Vaughn et al. (2004) have also argued that "focus on one area of the security solution (i.e., the operating system) and the absence

of another field (i.e., the policy) will not serve the purpose". Solms (2001) cautioned that there were "real risks" that prevented "a genuinely protected environment if information security is not handled holistically taking all dimensions into account." Scientometrical precautions began the development of robust bibliometric techniques to research a variety of scientific fields effectively (Garfield in 1955; Price 1963 in 1965, 1978; Tabah, 1999; Borgman and Furner, 2002; Morris and Martens, 2008). Such studies mainly examined a specialization in information security itself (such as Botha and Gaaingwe, 2006; Siponen and Oinas-Kukkonen, 2007; Lee, 2008; Dlemini et al., 2009). However, few of these studies employed the new methods to assess the subject composition of information security study literary objects using extremely subjective types of content analysis (e.g., journals, articles).

Studies using a traditional scientometric method tend to be much less popular, except for Lee (2008), who has explicitly focused on emerging developments of the future information security technology. Moreover, no studies were found to use large-scale bibliometric data to quantitatively investigate the structure and dynamics of the information security specialty. The primary aim of this study was to explore and describe information security as a research specialization to create an intellectual profile by uncovering high-impact bibliographic units (e.g., authors, source titles, affiliations, countries) based on quantitative measures and model the evolution of its intellectual structure using a domain visualization tool and technique.

Overview of Information Security Concepts

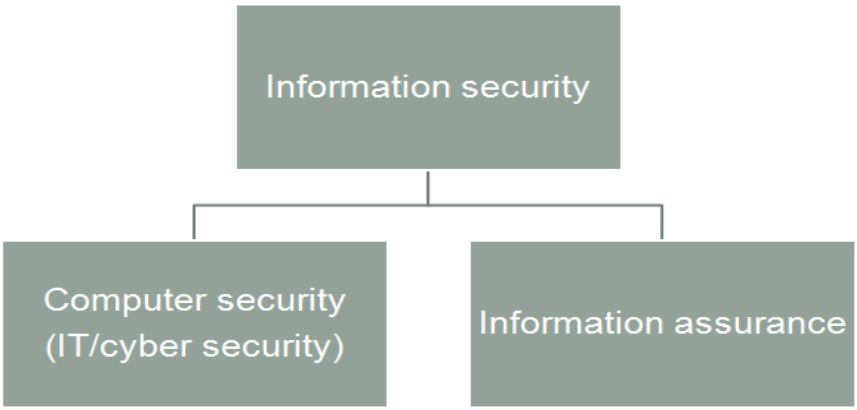
The following section provides a generic overview of the information security concepts related to the business context. Information security is a broad concept that has two crucial offshoots. These include (a) cybersecurity (b) information assurance, as illustrated in Figure 1. These two branches have an in-depth impact on the business community and are an integral part of the business processes. Moreover, information security is a basic concept that is related to computers, information technology, cybersecurity concepts, and information assurance paradigms. Cybersecurity deals with the technical perspective of information security specific to hardware security, software security, or information

technology security-related issues. While information assurance mainly deals with information security policies, planning, and standards like ISO 27001, etc. (Pfleeger & Pfleeger, 2012).

Information security is a combination of various terminologies and concepts. The main concepts of information security are closely related to confidentiality, integrity, availability, accounting, non-repudiation, and authenticity (Figure 2). The confidentiality concept mainly deals with the access policies of computer assets to ensure access by authorized parties only. On the other hand, the integrity concept is mainly focused on the modification aspects of hardware, software, and data.

Figure 1: Basic Classification of Information Security Branches

Source: (Pfleeger & Pfleeger, 2012)



It means that only hardware, software, or data related- information can be changed or altered by authorized persons or authorized methods only. The concept of availability is linked with asset accessibility to legal and authorized persons when needed. So, time is an important factor in the availability of computer assets by legal entities. Accountability is another important aspect of information security in which one's actions need to be traced back uniquely if needed, for normal accountable purposes or even for digital forensics. The concept of non-repudiation is a bit difficult to understand for those who are new to information security. It focuses on the origin of data i.e., source or origin and location of origin, by implementing advanced digital signatures systems. Moreover, it even provides proof of the integrity of the data whether it is spoofed data or un-spoofed data indirectly. Authenticity is also a very crucial concept in information security. It ensures that the data flowing in a

system is original and legitimate whether it is a simple bank transaction, telecommunication data, everyday office work data, or a document, and whether it is in electronic or physical form (Pfleeger & Pfleeger, 2012).

Figure 2: Important Information Security Triangle (CIA) (Pfleeger & Pfleeger, 2012)

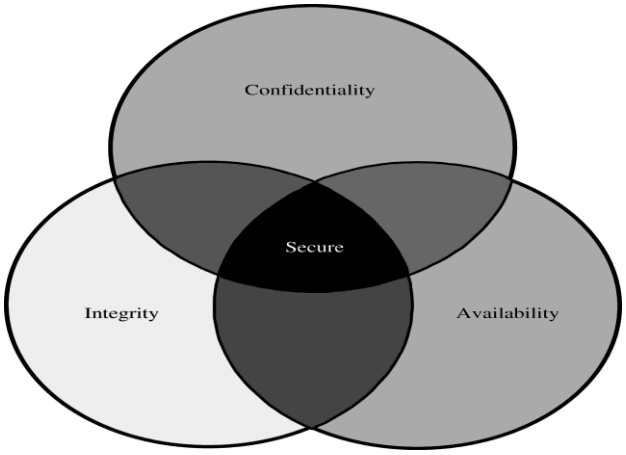


Figure-2 illustrates the secure computing systems which represent the basic paradigms of information security. It shows the three most important constituents which make the basis of information security. These factors are (i) confidentiality (ii) integrity and (iii) availability. We can combine the above concepts in a single sentence that "a threat is blocked by control of a vulnerability to prevent an attack". (Tsochev, Trifonov, Nakov, Manolov & Pavlova, 2020). Tsochev et. al, (2020) focused on the malware aspects of information security like viruses, worms, trojans, adware, etc. Many in Web of Science have also talked about them in-depth. Gozdziak (2021) recently focused on security issues related to human information and opined that it would become an important information security dimension in the future. This dimension of information security needs to be explored further because of its emerging but ubiquitous nature.

Terminologies like "Security & Privacy" are sometimes interchangeably used but are two different concepts. They can be broadly categorized based on concepts, implementation, and applicability (Alterman, 2003). Alterman (2003) has investigated the privacy and ethical issues related to biometric identification which is an emergent category and has been the focus of many articles published in the Web of Science. Security and privacy can be considered as two opposing concepts that

are inter-linked. Security is related to the practical aspects of information security such as the processes, practices, and implementations, while privacy is mainly related to the appropriate usage of the existing business or non-business data. Security is important and crucial, but it cannot fulfill the gap of and necessities of privacy and ethics (Bynum & Rogerson, 2004). A business organization or a social media giant like Facebook, Twitter, Instagram, etc. might have perfect processes, practices, strong security protocols regarding data security and access to legitimate users, however, it all becomes moot if they start selling user data for advertising purposes or even political gains. Therefore, companies must have both impenetrable security and ironclad privacy policies. Privacy can be achieved by proposing an appropriate policy measure or lawsuits like General Data Protection Regulation (GDPR-EU). GDPR-EU is a newly implemented privacy law in Europe that mandates that no business company can sell or export a citizen's profile information without their consent. This law is useful for achieving the privacy of citizens and by regularizing their privacy in a business environment. Some of the articles in our study also focused on the privacy aspects of information security and various articles were categorized based on the concept of "privacy" (Voss, 2017). Recently, Floridi (2021) introduced a new concept and terminology of "informational privacy" which is deeply linked with the main concept of "security and privacy". The last important concept that most of the articles in Web of Science categorized is based on the concept of "Adversaries". Adversaries are computer criminals, script kiddies, amateurs, hackers, organized criminals, professional criminals, cyber warriors, or even cyber terrorists that threaten businesses or non-business digital users. It is important to be aware of these entities as they are involved in illegal activities intended to steal data, gain unauthorized access to assets, or perform alteration to secure data. Understanding such adversaries is crucial as it will help us identify and prevent their attacks (Alshammari, et al., 2020).

Information Security in the Business Context

Human civilization has progressed from an agricultural economy to an industrial economy and now a digital economy. Globalization powered by digital businesses, and the advent of the digital economy has brought abrupt changes fueled by new technologies and ongoing innovation worldwide.

Consequently, there has been a growth in the digital presence of businesses and a competitive environment has been created in the business community digitally. Various strategies, policies, and regulations have been proposed and implemented by governments and businesses to secure the digital critical infrastructure. Many businesses and industry sectors operate globally or rely on the interconnectedness of this global digital infrastructure (United States Department of Commerce, 2019). Currently, no such specific taxonomy or common method exists among international businesses related to information security standards, however, various countries are working to develop a specific protocol for information security to avoid the concerns of digital threats. Multiple approaches to deal with the issues have been under consideration because each country has its own specific requirements and demands, to deal with specific situations or threats. One of the available frameworks is the National Institute of Standard and Technology (NIST) framework that points to international viability and acceptability. The NIST contains various standards, guidelines, and practices related to the safe operations of digital businesses and has proved to be successful in dealing with both internal and external threats to information security (United States Department of Commerce, 2019). It was found that the NIST framework has been widely used in various studies in the Web of Science and other related databases, in the context of information security. Smidt and Botzen (2018) discussed the probabilistic approach of the impact of threats on the economic condition of a digital business and risk assessment. The business risk assessment concept has also been widely used by various researchers. Schaik et al., (2017) analyzed IS threats based on the country level and analyzed the internet-related (www) data of British and American students to assess their risk level. They reported that most of the risks were related to identity theft, key logger, cyber-bullying, and social engineering.

Reuters (2013) focused on strategic, operational, tactical, collaborative, and legislative aspects of businesses across a country for mitigating threats level. This approach has been also widely discussed in various databases as it is a soft and strategical approach to handling business-related threats. Siponen & Pahnila (2014) emphasized that most of the security infringements were because of the negligent attitude of employees at the business organization. Adequate training and consultation with employees

would suffice to combat such negligence. Improper policies and unauthorized user access were the other core issues for cybersecurity attacks reported by Kannan, Rees, & Sridhar (2007). Occasionally, it was found that the overly restrictive cybersecurity rules and policies could weaken the performance of an organization (D'Arcy, Herath, & Shoss, 2014; Goel, & Shawky, 2009).

Chen, R. & Wen (2102) proposed a stick and carrot policy for tightening organizational security in which those employees who were more compliant with the security policies would be awarded. Dutta, & McCrohan (2002) and Cavusoglu, Cavusoglu, & Zhang (2008) focused on the fact infrastructures critical to business organization. Ransbotham & Ramsey, (2008) analyzed two (2) years' worth of alert data to investigate the vulnerabilities of digital businesses. Hoy & Foley (2015) focused on the soft aspect of information security i.e., audit-based security via ISO 9001, ISO 27001, and other audits. The concept of such audit concepts has also been widely discussed in scholarly literature. Moody, Siponen, & Pahnila, (2018) also worked on the soft aspect of information security and were convinced that policy designing and modeling would fulfill the holistic view of information security.

The current study has been designed to analyze the 100 most cited articles on information security in the context of business. The purpose of the study was to categorize the research trends, authorship patterns, and other relevant factors with a focus on highly cited authors, countries, institutions, journals, and articles. Moreover, the subject dispersion and research methodology of highly cited articles were also explored to provide a holistic view of the information security based on the bibliography.

Research Questions

1. What is the publication trend of the articles?
2. What authorship patterns exist in selected articles?
3. What are the important features of journals used in most cited articles (title, frequency, IF, quartile, country, and citation impact)?
4. Who are the highly cited authors, institutes, and papers?
5. What is the subject dispersion of highly cited articles?

Methodology

Data for this article was downloaded from the Core collection of Clarivate Analytics - Web of Science database in the first week of May 2019. The keywords "Information Security" has been typed in the main search box and the option of “Topic” was selected in the subsequent box. To further refine the retrieved dataset, firstly, the data was organized by citations instead of by publishing date, and secondly, in the index of document type the option of ‘Articles’ was selected. All the other types of documents were excluded. The complete bibliographical records of the top 500 most cited articles were downloaded for the selection of the most relevant articles.

A Microsoft Excel spreadsheet was prepared to highlight the distribution of articles by their year of publication. The total number of authors was counted for every publication to identify the authorship patterns. The impact and quartile factors of journals and publication country were written down by using the Journal Citation Report 2017. The affiliated country and university of every author were noted to assess the most productive country and institution in the top-cited articles. The most productive authors were also investigated. The articles were also segregated by their subject matter to discover the most popular areas of research. A list of 100 top-cited articles with their number of citations has been added to the paper as Appendix.

The scope of the study has been limited to information security issues in a business context. Information, other than this, was considered to be out of the scope of our research work. This work categorizes only those information security issues that have a direct relation with business studies/implications.

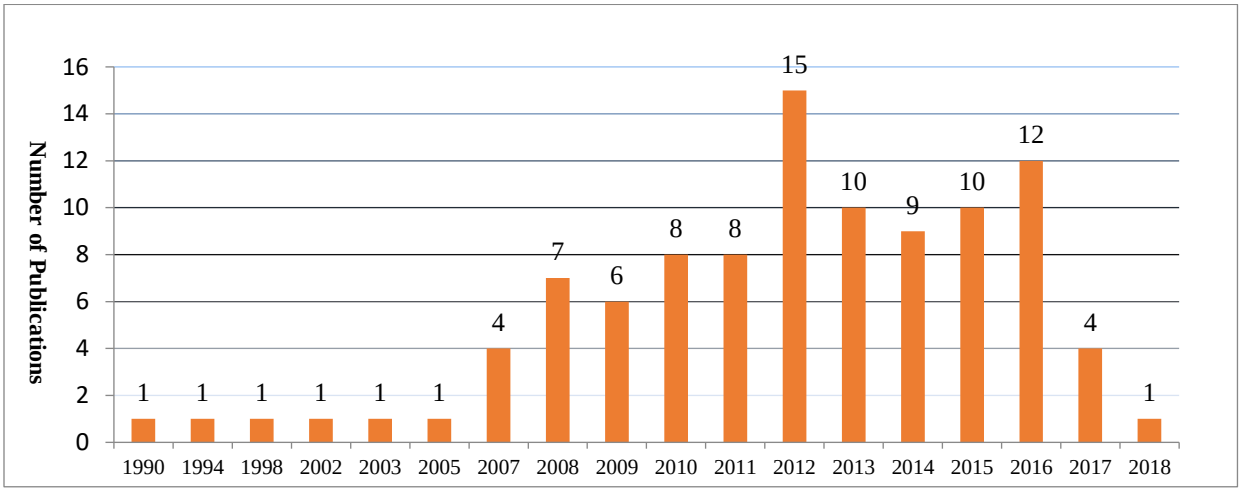
Results

Distribution of Publications by Year

Figure-3 highlights the top-cited papers on information security published from 1990 to 2018. Most of the papers (n=15) were published during the year 2012, followed by the year 2016 with 12 publications, and ten each during 2013 and 2015. Only 6 of the top-cited papers were published in the first 17 years (1990 to 2006) of the period under study, while 94 papers were published during the last

12 years (2007 to 2018) of the period. The overall average of papers published during the span of 29 years was 3.44.% per year.

Figure 3: Distribution of top-cited publications by year



Authorship Pattern

It was found that a total of 272 authors had produced the 100 most cited papers, with an average of 2.72 authors per paper. The majority of the papers (n=92) were written collaboratively by authors and only eight papers were written by single authors. The three-author pattern was found in 38 papers, followed by a two-author pattern in 35 papers, and a five-author pattern in four papers. The top-cited 100 papers had received 3374 citations with an average of 33.74 citations per paper. The highest citation impact (38.37) was found in the single author pattern followed by the three-author pattern with 35.73 citations per paper.

Table-1: Authorship Pattern

Number of Authors	Publications	Citations	Citation Impact
Single author pattern	8	307	38.37
Two-authors pattern	35	1276	36.4
Three-author pattern	38	1358	35.73

Four-author pattern	15	367	24.74
Five-author pattern	4	66	16.5
	100	3374	33.74

Distribution of Publications by Subject

Table-2 describes the distribution of articles by the subject matter. The majority of the papers (n=40) were written on the IS sub-category of Cybersecurity policies, followed by Cybersecurity Resilience (n=23) and Cybersecurity Risk Management (n=21). Some articles had also reported on the Vulnerability Assessment (n=8), Cybersecurity Procedures (n=7), and Digital Forensics (n=1). Furthermore, the paper on Digital Forensics received the highest citation impact (52.00), followed by Cybersecurity Policies (42.95) and Cybersecurity Risks Management (41.09). The articles on Cybersecurity Procedures received the lowest citation impact with 4.28 citations per paper.

Table 2: Distribution of Publications by Subject

S. No.	Subject	Publications	Citations	Citation impact
1	Cybersecurity Policies	40	1718	42.95
2	Cybersecurity Resilience	23	634	27.56
3	Cybersecurity Risks Management	21	863	41.09
4	Vulnerability Assessment	8	77	9.26
5	Cybersecurity Procedures	7	30	4.28
6	Digital Forensics	1	52	52.00

Distribution of Journals by Quartile Factor

Table-3 highlights that the journals having the quartile factor Q1 received the highest citation impact of 54.92, and the lowest quartile factor journals received a comparatively smaller number of citations.

Table 3: Quartile of Journals with Publications, Citations, and Citation Impact

Quartile	Publications	Citations	Citation Impact
Q1	41	2252	54.92
Q2	27	818	30.29
Q3	15	235	15.66
Q4	8	40	5.00
Conference Paper	6	21	3.5
Without Quartile	3	8	2.66

Distribution of Journals by Impact Factor

Table-4 shows the relationship of the frequency of publications with the journal's impact factor. Most of the publications (n=30) were published in journals having 2.3 to 2.91 impact factors, followed by 21 articles in 3.13-3.89 impact factor journals. Slightly more than half of the articles (n=51) had been published in journals having impact factors between 2 and 3.9, and only 16 articles were published in journals having an impact factor of more than 4. Articles published in high-impact factor journals received a high ratio of citations.

Table 4: Distribution of journals by Impact Factor

Impact factor	**Publications**	**Citations**	**Citation Impact**
0.48-0.96	8	61	7.62
1.03-1.86	16	224	14.00
2.3-2.91	30	925	30.83
3.13-3.89	21	799	38.04
4.31	4	132	33.00
5.43	11	1181	107.36
6.95	1	23	23.00
Without Impact factor	9	29	3.22

Distribution of Journals by Impact, Quartile and Publishing Country

Table-5 reveals that 94 papers had been published in 34 journals and 6 were conference papers published as part of conference proceedings. The maximum number (n=13) of papers had been published in the Journal of Management Information Systems, followed by 11 papers each in Information & Management and MIS Quarterly. Only three journals had more than 10 papers each, while 18 journals had only one article each. Thirteen journals published in the United States of America had published 40 papers, followed by seven journals from the Netherlands with 26 papers, and ten journals from England with 24 papers. Table- 5 also shows that the majority of the papers (n=90) had been published in 30 journals from three countries i.e., the United States of America, Netherlands, and England.

Table 5: Journal with Impact factor, Quartile , Publishing Countries with Number of Publications (NP) and Number of Citations (NC) and Citation Impact (CI)

Name of Journal	Impact factor	Quartile	Publishing Country	NP	NC	CI
Journal of Management Information Systems	2.74	Q2	England	13	312	24.00
MIS Quarterly	5.43	Q1	USA	11	1214	110.35
Information & Management	3.89	Q1	Netherlands	11	555	50.45
Information Systems Research	2.3	Q2	USA	9	408	45.33
The Journal of Strategic Information Systems	4.31	Q1	Netherlands	4	132	33.00
Information Technology and Management,	1.63	Q3	USA	3	16	5.33
International Journal of Electronic Commerce	2.51	Q1	USA	3	112	37.33

Management science	3.54	Q1	USA	3	114	38.00
European Journal of Operational Research	3.42	Q1	Netherlands	3	35	11.66
International Journal of Accounting Information Systems	0.96	Q3	Netherlands	3	28	9.33
Journal of Business Ethics	2.91	Q2	Netherlands	3	54	18.00
California Management Review	3.3	Q1	USA	2	79	39.50
Decision Sciences	1.64	Q3	USA	2	113	56.50
Journal of Organizational and End User Computing	0.74	Q4	USA	2	10	5.00
Disaster Prevention and Management: An International Journal	1.06	Q4	England	2	5	2.50
Total Quality Management & Business Excellence	1.52	Q3	England	2	13	6.50
Decision Analysis,	1.06	Q4	USA	1	8	8.00
Journal of Electronic Commerce Research	1.66	Q3	USA	1	10	10.00
MIS Quarterly Executive	1.86	Q3	USA	1	33	33.00

System Dynamics Review: The Journal of the System Dynamics Society	0.85	Q4	USA	1	9	9.00
Technological Forecasting and Social Change	3.13	Q1	USA	1	14	14.00
IJISPM-International Journal of Information Systems And Project Management	0	0	Portugal	1	3	3.00
African Journal of Business Management,	1.1	Q3	Nigeria	1	18	18.00
Human Resource Management Review	3.27	Q1	Netherlands	1	8	8.00
Marketing Letters,	1.35	Q3	Netherlands	1	2	2.00
Electronic Markets,	3.81	Q1	Germany	1	4	4.00
Information Systems and e-Business Management	1.03	Q4	Germany	1	4	4.00
Engineering Management Journal	0.48	Q4	England	1	4	4.00
International Journal of Contemporary Hospitality Management	2.87	Q2	England	1	36	36.00
Journal of Enterprise Information Management,	2.48	Q2	England	1	3	3.00

Journal of Global Operations and Strategic Sourcing,			England	1	2	2.00
Journal of Information Technology	6.95	Q1	England	1	23	23.00
Journal of Science & Technology Policy Management			England	1	3	3.00
Technology Analysis & Strategic Management	1.49	Q3	England	1	2	2.00

Distribution of Publications by Affiliated Country of the Authors

The 272 researchers who have published the top-cited articles belonged to 29 countries, as shown in Table-6. A total of 153 researchers (including multiple counts) from 63 organizations of the United States of America had contributed 72 papers, including 63 with the first author. Twenty authors belonging to 13 universities in China have published 6 papers. Fourteen English authors associated with eight organizations have published eight, nine German authors have published six, and five Australian authors have published four articles. Fourteen (14) countries have contributed one paper each in the 100 top-cited papers list.

Table 6: Distribution of publications with authors' country affiliation and number of publications

S. No.	Country	Publications	Organizations	Authors
1.	United States	72	63	153
2.	England	8	8	14
3.	China	6	13	20
4.	Germany	6	6	9

5.	Canada	5	9	13
6.	Australia	4	4	5
7.	South Africa	3	3	4
8.	Sweden	3	3	4
9.	Taiwan	3	3	4
10.	Finland	2	7	9
11.	India	2	2	3
12.	Italy	2	2	2
13.	Singapore	2	2	3
14.	Slovenia	2	2	2
15.	South Korea	2	5	5
16.	Austria	1	1	3
17.	Denmark	1	1	1
18.	Greece	1	1	1
19.	Iran	1	1	2
20.	Mauritius	1	1	2
21.	Netherland	1	1	2
22.	Norway	1	1	2
23.	Pakistan	1	1	1
24.	Portugal	1	1	1
25.	Saudi Arabia	1	1	3
26.	Scotland	1	1	2
27.	Spain	1	1	1

28.	Tunisia	1	1	1
29.	Turkey	1	1	1

Detail of Productive Authors

A total of 252 authors (272 authors as multiple counts) produced these 100 top-cited papers. Amongst the most productive authors, 18 authors belonged to 14 organizations of the United States of America: 4 were from the University of Texas, 2 from the State University of Florida, and one each from the other 12 American universities. There were 3 authors from two Canadian universities, 3 from two Chinese universities, 2 from two universities of Finland, and one from South Korea who were also included in the most productive author list. Cavuoglu, H. of the University of Texas, USA, and Lowry, P. B. of the City University of Hong Kong, China, shared the top position with six articles each. Three authors, Posey, C. of the University of Alabama System, USA; Roberts, T. L. of Louisiana Technical University, USA; and Siponen, M. of University of Jyvaskyla of Finland produced four papers each and were ranked second on the list of most productive authors. Other authors mentioned in the table-7 produced three and two papers, respectively.

Table 7: Productive Authors (n=27), their affiliated organization, country and number of publications (NP)

Rank	Author	Affiliated Organization	Country	NP
1	Cavusoglu, H.	University of Texas	United States	6
1	Lowry, P. B.	City University of Hong Kong	China	6
2	Posey, C.	University of Alabama System	United States	4
2	Roberts, T. L.	Louisiana Technical University	United States	4
2	Siponen, M.	University of Jyvaskyla	Finland	4
3	D'Arcy, J.	University of Notre Dame	United States	3
3	Hu, Q.	Iowa State University	United States	3

3	Kannan, K.	Purdue University	United States	3
3	Pahnila, S.	University of Oulu	Finland	3
3	Straub, D. W.	Georgia State University	United States	3
3	Vance, A.	Brigham Young University	United States	3
4	Benbasat, I.	University of British Columbia	Canada	2
4	Bennett, R. J.	University of Louisiana System	United States	2
4	Cavusoglu, H.	University of British Columbia	Canada	2
4	Cooke, D.	State University System of Florida	United States	2
4	Dutta, A.	George Mason University	United States	2
4	Gao, X.	Southeast University	China	2
4	Goel, S.	State University of New York	United States	2
4	Hart, P.	State University System of Florida	United States	2
4	Herath, T. C.	Brock University	Canada	2
4	Kim, B. C.	Korea University	South Korea	2
4	Mookerjee, V.	University of Texas	United States	2
4	Raghunathan, S.	University of Texas	United States	2
4	Ransbotham, S.	Boston College	United States	2
4	Zhang, J.	University of Texas	United States	2
4	Zhao, X.	University of North Carolina	United States	2
4	Zhong, W.	Southeast University	China	2

Discussion

The study results have highlighted interesting patterns and trends in publications on the topic of Information Security in the context of Business. They show an increasing trend of publishing on the topic. Interestingly, the maximum number of articles (15) were published in the year 2012. This highlights the growing interest in information security at the organizational level in the context of business. Chen, Ramamurthy, & Wen (2012) have reported a focus on organizational information security policy compliance in their article published in the Journal of Management Information Systems. After analysis of the journal of the said author, it is conceived that researchers worked more on the topic of information security at the organizational level or in the business context. The researcher started work on the said topic in 1990 and published only one article in the top 100 highly cited indexed articles list. The results of the study highlight the need for research on the topic of Cybersecurity risks as it is an emerging area in the business context. Organizations are continuously fighting off cyber-attacks to keep their data secure and cyber malware attacks such as Shamoon-I, Shamoon-II, Ransom WanaCry attacks, etc., have become common place in recent times (Damjanovic, 2017).

The analysis of authorship patterns and author productivity help highlight key persons in a particular research area. Cavusoglu and Lowry were found to top the list of the most productive authors on the topic of information security in the context of business. They had both published six (6) articles each in the top-ranked category of the top 100 highly cited list. Other researchers also had publication frequency of 4, 3, and 2, respectively. Cavusoglu belonged to the University of Texas, USA, while Lowry belonged to the City University of Hong Kong, China.

Important features of journals used in most cited articles give a clue about the different important patterns that can be used for various purposes by seasoned and naïve researchers. The frequency of articles being published depicts the quality and quantity of a journal's articles. Sometimes low frequency may determine the quality of the journals. The impact factor (IF) of a journal is one of the criteria for judging the quality of the journal in any area of research. Table 5 shows the quartile, country, age, and citation impact of the top 100 articles. The journal with the most publications was the Journal of

Management Information Systems (MIS). It had published 13 articles, followed by MIS Quarterly with 11 articles. The Journal of MIS is ranked Q2 and MIS quarterly is ranked Q1. The Journal of Information Technology along with other journals in Table 4 had all published only one article in the top 100 categories. Although the journal claimed the highest impact factor of 6.95, still it had only one publication in the top 100 categories.

The highly cited institutes and articles are other interesting parameters that could be of interest to many researchers wanting to collaborate with certain institutes and to study high quality articles relevant to their areas of interest. According to Table 7, the most cited authors were from the University of Texas and City University of Hong Kong China. Researchers working on information security in a business context may collaborate with these top universities to strengthen their research profiles. The University of Alabama System was also ranked second to the City University of Hong Kong China and the University of Texas in this field of study.

Generally, researchers are most interested in the subject dispersion of highly cited articles in the relevant literature. Dutta and McCrohan (2002) discussed the management's role in information security in a cyber-economy and stressed the importance of information security for businesses. Table 1 shows a clear subject dispersion of highly cited articles in the field of information security in a business context. A sub-area of information security, Cybersecurity policies, had the most highly cited articles and appeared to be a popular area among researchers. Articles related to the topic had 1718 citations, much higher than any of the other sub-areas of information security like Cybersecurity resilience, Cyber Risk Management, Vulnerability assessment, Cybersecurity procedures, and digital forensics. On the other hand, Digital forensics, as a topic, had the lowest number of cited articles. It had been cited 52 times in the top 100 high cited Web of Science (WOS) categories. However, it should be noted that Cybersecurity policies' sub-area citation impact was 42.95, which was lower than the one for the sub-area of digital forensics, which had a citation impact of 52.0.

Knowledge about the most productive countries in the field of information security in a business context publishing would also be valuable to other researchers. Table 6 shows that the United States of

America was the most productive country in the field of information security with regards to highly cited publications, followed by England, China, Germany, and Canada respectively. Developing countries like Iran, Saudi Arabia, Pakistan, Mauritius, Tunisia, and Turkey only had one article each. Furthermore, researchers working in the field of information security in the context of business preferred to visit these highly productive countries to enhance their knowledge area and skills. Table 3 presents the quartile factors of Journals. Q1 journals in the top 100 highly cited categories produced 41 articles with 2252 citations and a citation impact of 52.92. Table 3 also highlights some interesting trends regarding Q2, Q3, Q4 journals along with conference papers and articles not in the range of quartiles. Table 1 shows extra information for the researchers working in the field. The results presented in the table show that some researchers preferred to work solo. Single authors had published a total of 8 articles on the topic and received 307 citations with a citation impact of 38.37. On the other hand, the maximum number of authors to collaborate on an article was five. It is hoped that the analysis and results presented in the article would provide valuable insights to other researchers regarding the topic and its publishing trends. There is an appendix at the end of this paper, which provides a complete list of all articles analyzed in the current study so that readers could benefit from research already conducted and discover future avenues for further research.

Conclusion

This paper presents the results of an extended bibliometric study and analysis of the top 100 cited papers in the field of "information security in business". The purpose of this study was to provide a deeper insight into the significance of the research area to other researchers and stakeholders. Information security in general, and its applications in business in particular, has been a hot area of research in recent years. The researchers choose the Web of Science database for data collection purposes and the results of the study truly reflect the amount and type of efforts being made in this area of research, especially with regards to the research's country-wise distribution and authors' impact on the said area. Overall, the 100 most-cited articles gained an average of 33.74 citations per article. The single-author articles received the highest citation impact as compared to other authorship patterns. The

category of cybersecurity had the bulk of the articles which had the maximum number of citations. More than one-third (n=35) of the top-cited articles had been published in only three journals, the Journal of Information Management System, MIS Quarterly, and Information and Management. An analysis of the authors' affiliation showed that authors who belonging to 29 countries contributed to the top-cited articles, and the American authors topped the list with the maximum number of contributions with 72 articles. Cavusoglu and Lowry shared the title of the most productive authors with six articles each. The results of this study provide insights into the research trends and patterns of publications on Information Security in the context of business. They also provide understanding about the topic to other researchers, academicians, organizations, industry leaders, and governments.

References

Alshammari, A., Rawat, D., Garuba, M., Kamhoua, C. & Njilla, L. (2020). Deception for cyber adversaries: status, challenges, and perspectives. *Modeling and Design of Secure Internet of Things*, 141-160.

Alhibshi, A. H., Alamoudi, W. A., Haq, I. U., Rehman, S. U., Farooq, R. K., & Al Shamrani, F. J. (2020). Bibliometric analysis of Neurosciences research productivity in Saudi Arabia from 2013-2018. *Neurosciences*, *25*(2), 134-143.

Alhiya¯, J, A Rahman, F Alhaidari and A Alghamdi (2019). Automatic text categorization using fuzzy semantic network. In Proc. 1st Int. Conf. Smart Innovation, Ergonomics and Applied Human Factors (SEAHF), pp. 24-34, Madrid, Spain.

Alterman, A. (2003). A piece of yourself: Ethical issues in biometric identification. *Ethics and Information Technology*, *5*(3), 139–150.

Bar-Ilan, J. (2008). Which h-index? A comparison of WoS, Scopus, and Google Scholar. *Scientometrics*,*74*(2), 257-71.

Baskaran, C. (2013). Scientometric analysis of cryptography research output. *SRELS Journal of Information Management*, *50*(4), 413-421.

Batistic, S. & Kaše, R. (2015). The organizational socialization field fragmentation: A bibliometric review. *Scientometrics*, *104* (1), 121-146.

Borgman, C. L., & Furner, J. (2002). Scholarly communication and bibliometrics. *Annual Review of Information Science and Technology*, *36*(1), 2-72.

Bornmann, L., Daniel, H. D. (2007). What do we know about the h index?. *Journal of the American Society for Information Science and Technology*, *58*(1), 1381-5.

Botha, R. A., & Gaaingwe, T. G. (2006). Reflecting on 20 SEC conferences. *Computers and Security*, *25*(4), 247–256.

Braun, T., Glänzel, W., & Schubert, A. (2005). A Hirsch-type index for journals. *The Scientist*,*19*(22), 1-6.

Bynum, T. W., & Rogerson, S. (2004). *Computer ethics and professional responsibility*. Oxford: Blackwell.

Cardona, G., &Sanz, J. P. (2015). Publication analysis of the contact lens field: what are the current topics of interest?. *Journal of Optometry, 8*(1), 33-39.

Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security patch management: Share the burden or share the damage?. *Management Science, 54*(4), 657-670. 2008.

Chen, Y., R., K., & Wen, K. W. (2102) Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems, 29*(3), 157-188.

Clyde W. H., Linda E, J., Herman M. & John T. (1994). Business computing research journals: A normalized citation analysis. *Journal of Management Information Systems, 11*(1), 131-140,

Cronin, B., & Meho, L. (2006). Using the h-index to rank influential information scientists. *Journal of the American Society for Information Science and Technology, 57*(9), 1275-8.

Damjanović, D. Z. (2017). Types of information warfare and examples of malicious programs of information warfare. *Vojnotehnički Glasnik, 65*(4), 1044-1059.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31*(2), 285-318.

Davis, P. M. (2011). Open access, readership, citations: a randomized controlled trial of scientific journal publishing. *The FASEB Journal, 25*(7), 2129-2134.

Dlamini, M., Eloff, M., &Eloff, J. (2009). Information security: The moving target. *Computers & Security, 28*(3-4), 189-198.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber-economy. California Management Review, 45(1), 67-87.

Egghe, L. (2006). Theory and practise of the g-index. *Scientometrics, 69*(1), 131-52.

Floridi, L. (2021). *The ontological interpretation of informational privacy*. 10.1007/978-3-030-54522-2_4.

Fuchs, L., Pernul, G., &Sandhu, R. (2011). Roles in information security-A survey and classification of the research area. *Computers & Security, 30*(8), 748-769.

Garfield, E. (1955). Citation indexes for science: A new dimension in documentation through association of ideas. *Science, 122*(3159), 108-111.

Gozdziak, E. (2021). *Human trafficking as a security threat*. 10.1007/978-3-030-62873-4_3.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404-410.

Goodrum, A, A., McCain, K, W., Lawrence, S., & Giles C. L. (2001), Scholarly publishing in the Internet age: a citation analysis of computer science literature. *Information Processing & Management, 37*(5), 661-675

Grover, V., Gokhale, R., Lim, J., Coffey, J., & Ayyagari, R. (2006). A citation analysis of the evolution and state of information systems within a constellation of reference disciplines. *Journal of the Association for Information Systems, 7*(5), 270-325.

Haq, I. U., & Al Fouzan, K. (2019). Research in dentistry at Saudi Arabia: Analysis of citation impact. *Library Philosophy and Practice (e-journal)*, 2765.

Hirsch, J.E. (2005). An index to quantify an individual's scientific research output. *Proceedings of the National Academy of Sciences of the United States of America, 102*(46), 16569-72.

Hoang, D., Kaur, J.,&Menczer, F. (2010). *Crowdsourcing scholarly data, Proceedings of the WebSci10: Extending the Frontiers of Society On-Line,* April 26-27th, 2010, Raleigh, NC: US.

Hovden, R. (2013). Bibliometrics for internet media: Applying the h-index to YouTube. *Journal of the American Society for Information Science and Technology, 64*(11): 2326–2331

Hoy, Z., & Foley, A. (2015). A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits. *Total Quality Management & Business Excellence, 26*(5-6), 690-702.

Hu, H, Y., Tai, T, C., Liu, E, K., & Cai, F, C. (2020). Identification of highly-cited papers using topic-model-based and bibliometric features: the consideration of keyword popularity. *Journal of Informetrics, 14*(1), 101004.

Jacso, P. (2008a). The pros and cons of computing the h-index using Web of Science. *Online Information Review, 32*(5), 673-88.

Jacso, P. (2008b). The pros and cons of computing the h-index using Scopus. *Online Information Review, 32*(4), 524-35.

Jacso, P. (2009). The h-index for countries in Web of Science and Scopus. *Online Information Review, 33*(4), 831-837.

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM, 52*(1), 126-129.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69-91.

King, D. (2004). The scientific impact of nations. *Nature, 430*(6697), 311-6.

Lee, W. H. (2008). How to identify emerging research fields using scientometrics: An example in the field of information security. *Scientometrics, 76*(3), 503-525.

Levitt, J. M., & Thelwall, M. (2009). The most highly cited library and information science articles: interdisciplinarity, first authors and citation patterns. *Scientometrics, 78*(1), 45-67.

Meho, L.I., & Rogers, Y. (2008). Citation counting, citation ranking, and h-index of human-computer interaction researchers: a comparison of Scopus and Web of Science. *Journal of the American Society for Information Science and Technology, 59*(11), 1711-26.

Meneghini, R., &Packer, A.L. (2006), "Articles with authors affiliated to Brazilian institutions published from 1994 to 2003 with 100 or more citations: II - identification of thematic nuclei of excellence in Brazilian science. *Anais Da Academia Brasileira De Ciencias, 78*(4), 855-83.

Moed, H. F. (2010). Measuring contextual citation impact of scientific journals. *Journal of informetrics, 4*(3), 265-277.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-311

Moravcsik, M. J. (1985). Applied scientometrics: an assessment methodology for developing countries. *Scientometrics, 7*(3), 165-76.

Morris, S. A., & Martens, B. (2008). Mapping research specialties. *Annual Review of the American Society for Information Science and Technology, 42*(1), 213-295.

Olijnyk, N. (2015). A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. *Scientometrics, 105*(2), 883-904.

Oppenheim, C. (2007). Using the h-index to rank influential British researchers in information science and librarianship, *Journal of the American Society for Information Science and Technology, 58*(2), 297-301.

Papp, D. S., & Alberts, D. (2002). *The information age: An anthology on its impact and consequences*. Retrieved from: https://www.hsdl.org/?view&did=439809

Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analyzing computer security: A threat / vulnerability / countermeasure approach*. Prentice Hall Professional.

Prathap, G. (2006). Hirsch-type indices for ranking institutions' scientific research output. *Current Science, 91*(11), 1439.

Price, D. J. S. (1963). *Little science, big science.* New York, NY: Columbia University Press.

Price, D. J. S. (1965). Networks of scientific papers. *Science, 149*(3683), 510-515.

Price, D. J. S. (1978). Toward a model for scientific indicators. In: E. Yehuda, J. Lederberg, R. K. Merton, A. Thackray, & H. Zuckerman (Eds.), *Toward a metric of science: The advent of scientific indicators* (pp. 69-96). New York, NY: Wiley.

Rahman, A., Alhaidari, F.A. (2018). The digital library and the archiving system for educational institutes. *Pakistan Journal of Information Management and Libraries (PJIM&L)*, 20(1), 94-117.

Rahman, A., Dash, S., Luhach, A.K. et al. (2019) A Neuro-fuzzy approach for user behaviour classification and prediction. J Cloud Comp 8, 17. https://doi.org/10.1186/s13677-019-0144-9.

Ransbotham, S., M., S., & Ramsey, J. (2008). Are markets for vulnerabilities effective?. *ICIS 2008 Proceedings*, 24.

Reuters. (2013, May 17). *Saudi Arabia says hackers sabotage government websites*. Retrieved from: https://www.reuters.com/article/us-saudi-cyber-idUSBRE94G0LY20130517. [Accessed: 03-Apr- 2019].

Rousseau, R. (2014). Library Science: Forgotten founder of bibliometrics. Nature, 510: 218

Rousseau, R., &Ye, F.Y. (2008). A proposal for a dynamic h-type index. *Journal of the American Society for Information Science and Technology, 59*(11), 1853-5.

Sajid, N.A., Ahmad, M., Afzal, M.T., Rahman, A. (2021). Exploiting papers' reference's section for multi-label computer science research papers' classification. *Journal of Information & Knowledge Management*, *20*(2), 1-21. DOI. 10.1142/S0219649221500040.

Schaik, P. V., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kuse, P. (2017). Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior, 75*, 547e559

Schreiber, M. (2007). Self-citation corrections for the Hirsch-index. *Europhysics Letters, 78*(3), 30002.

Schubert, A., & Glänzel, W. (2007). A systematic analysis of Hirsch-type indices for journals. *Journal of Informetrics, 1*(3), 179-84.

Shiau, W. L., Chen, S. Y., & Tsai, Y. C. (2015). Management information systems issues: co-citation analysis of journal articles. *International Journal of Electronic Commerce Studies, 6*(1), 145-162.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38*(1), 60-80.

Siponen, M., M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Smidt, G. D. & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers, 43,* 239-274.

Solms, B. (2001). Information security-A multidimensional discipline. *Computers & Security, 20*(6), 504-508.

Tabah, A. N. (1999). Literature dynamics: Studies on growth, diffusion, and epidemics. *Annual Review of Information Science and Technology, 34,* 249-286.

Tsochev, G., Trifonov, R., Nakov, O., Manolov, S. & Pavlova, G. (2020). *Cyber security: Threats and challenges*. 1-6. 10.1109/ICAI50593.2020.9311369.

United States Department of Commerce, National Institute of Standards and Technology. (2019). *NIST roadmap for improving critical infrastructure cybersecurity version* 1.1. Retrieved from https://www.nist.gov/sites/default/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf

Van Rann, A.F.J. (2006), Statistical properties of bibliomteric indicators: research group indicator distributions and correlations. *Journal of the American Society for Information Science and Technology, 57*(3), 408-30.

Vaughn, R. B., Dampier, D. A., & Warkentin, M. B. (2004). *Building an information education program.* In Proceedings of the first annual conference on information security curriculum development (pp. 41-45). New York: ACM.

Von Solms, B., & Von Solms, R. (2005). From information security to business security?. *Computers & Security, 24*(4), 271-273.

Voss, W. (2017). European Union data privacy law reform: General data protection regulation, privacy shield, and the right to Delisting. *Business Lawyer, The*. 72. 221.

Zaman, G., Mahdin, H., Hussain, K., Rahman, A. (2021). Information extraction from semi and unstructured data sources: a systematic literature review. *ICIC Express Letters*, 14(6), 593-603.

Appendix

List of 100 most-cited papers on the topic of '*Information Security'*

S. No.	Article	Citations
1.	Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, *22*(4), 441-469.	373
2.	Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.	368
3.	Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.	247
4.	Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.	146
5.	Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*(4), 757-778.	114
6.	Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.	109
7.	Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 503-522.	105

8.	Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224.	98
9.	Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270.	81
10.	Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99-110.	63
11.	Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. *The Journal of Strategic Information Systems*, *16*(2), 153-172.	58
12.	D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285-318.	57
13.	Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, *12*(1), 69-91.	55
14.	Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404-410.	53

15.	Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? Think again. *Management Science*, *51*(5), 726-740.	52
16.	Grazioli, S., & Jarvenpaa, S. L. (2003). Consumer and business deception on the Internet: Content analysis of documentary evidence. *International Journal of Electronic Commerce*, *7*(4), 93-118.	52
17.	Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*(4), 1189-1210.	52
18.	Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.	48
19.	Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber-economy. *California Management Review*, *45*(1), 67-87.	48
20.	Vance, A., Lowry, P. B., & Eggett, D. L. (2015). Increasing accountability through the user interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345-366.	47
21.	Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security patch management: Share the burden or share the damage?. *Management Science*, *54*(4), 657-670.	45
22.	Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567-594.	43

23.	Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373-384.	36
24.	Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991-1010.	36
25.	Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, *25*(2), 241-280.	35
26.	Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly executive*, *9*(3), 2012-52.	33
27.	Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research*, *23*(3-part-2), 918-939.	33
28.	Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems. *Information Systems Research*, *20*(2), 198-217.	32
29.	Shi, Y. (2007). Today's solution and tomorrow's problem: the business process outsourcing risk management puzzle. *California Management Review*, *49*(3), 27-44.	31

30.	Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282-300.	31
31.	Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information &Management*, *51*(1), 138-151.	30
32.	Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179-214.	30
33.	Ransbotham, S., Mitra, S., & Ramsey, J. (2008). Are markets for vulnerabilities effective?. *ICIS 2008 Proceedings*, 24.	29
34.	Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information &Management*, *51*(5), 551-567.	27
35.	Yue, W. T., & Cakanyildirim, M. (2007). Intrusion prevention in information systems: Reactive and proactive responses. *Journal of Management Information Systems*, *24*(1), 329-353.	27
36.	Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123-134.	27
37.	Chen, P. Y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, *35*(2), 397-422.	26

38.	Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, *133*(1), 111-123.	26
39.	Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, *19*(4), 281-295.	25
40.	Mookerjee, V., Mookerjee, R., Bensoussan, A., & Yue, W. T. (2011). When hackers talk: Managing information security under variable attack rates and knowledge dissemination. *Information Systems Research*, *22*(3), 606-623.	24
41.	Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60-77.	23
42.	Herath, H. S., & Herath, T. C. (2008). Investments in information security: A real options perspective with Bayesian postaudit. *Journal of Management Information Systems*, *25*(3), 337-375.	23
43.	Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics*, *121*(3), 385-401.	23
44.	Png, I. P., Wang, C. Y., & Wang, Q. H. (2008). The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems*, *25*(2), 125-144.	22

45.	Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314-341.	22
46.	Cremonini, M., & Nizovtsev, D. (2009). Risks and benefits of signaling information system characteristics to strategic attackers. *Journal of Management Information Systems*, *26*(3), 241-274.	20
47.	Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201-218.	19
48.	Khansa, L., & Liginlal, D. (2009). Valuing the flexibility of investing in security process innovations. *European Journal of Operational Research*, *192*(1), 216-235.	18
49.	Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862-10868.	18
50.	Cezar, A., Cavusoglu, H., & Raghunathan, S. (2013). Outsourcing information security: Contracting issues and security implications. *Management Science*, *60*(3), 638-657.	17
51.	Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91-112.	16
52.	Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services,	14

	and risk pooling arrangements. *Journal of Management Information Systems*, *30*(1), 123-152.	
53.	Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330.	14
54.	Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), 385-400.	14
55.	Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, *13*(3), 228-243.	14
56.	Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, *22*(2), 175-186.	13
57.	Tang, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179-186.	12
58.	Ioannidis, C., Pym, D., & Williams, J. (2012). Information security trade-offs and optimal patching policies. *European Journal of Operational Research*, *216*(2), 434-444.	11
59.	von Solms, R., Van Der Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. *Information & Management*, *26*(3), 143-153.	10

60.	Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research*, *26*(3), 565-584.	10
61.	Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting Information Systems*, *13*(4), 357-381.	10
62.	Durowoju, O. A., Chan, H. K., & Wang, X. (2011). The impact of security and scalability of cloud service on supply chain performance. *Journal of Electronic Commerce Research*, *12*(4), 243-256.	10
63.	Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review: The Journal of the System Dynamics Society*, *24*(3), 349-375.	9
64.	Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More harm than good? How messages that interrupt can make us vulnerable. *Information Systems Research*, *27*(4), 880-896.	9
65.	Gao, X., Zhong, W., & Mei, S. (2013). Information security investment when hackers disseminate knowledge. *Decision Analysis*, *10*(4), 352-368.	8
66.	Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. *Human Resource Management Review*, *23*(1), 105-113.	8
67.	Fenz, S., Pruckner, T., & Manutscheri, A. (2009, April). Ontological mapping of information security best-practice guidelines. In *International Conference on Business Information Systems* (pp. 49-60). Springer, Berlin, Heidelberg.	8

68.	Aurigemma, S., & Panko, R. (2012, January). A composite framework for behavioral compliance with information security policies. In *2012 45th Hawaii International Conference on System Sciences* (pp. 3248-3257). IEEE.	8
69.	Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-A-22.	8
70.	Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems*, *33*(2), 597-620.	8
71.	Hoy, Z., & Foley, A. (2015). A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits. *Total Quality Management & Business Excellence*, *26*(5-6), 690-702.	7
72.	Schilling, A., & Werners, B. (2016). Optimal selection of IT security safeguards from an existing knowledge base. *European Journal of Operational Research*, *248*(1), 318-327.	6
73.	Martin, C., Bulkan, A., & Klempt, P. (2011). Security excellence from a total quality management approach. *Total Quality Management*, *22*(3), 345-371.	6
74.	Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, *54*(4), 452-464.	6

75.	Wang, J. A., Guo, M., Wang, H., & Zhou, L. (2012). Measuring and ranking attacks based on vulnerability analysis. *Information systems and e-business management*, *10*(4), 455-490.	5
76.	Matwyshyn, A. M. (2009). CSR and the corporate cyborg: Ethical corporate information security practices. *Journal of Business Ethics*, *88*(4), 579-594.	5
77.	Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626.	4
78.	Otero, A. R. (2015). An information security control assessment methodology for organizations' financial information. *International Journal of Accounting Information Systems*, *18*, 26-45.	4
79.	Bojanc, R., & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal*, *25*(2), 25-37.	4
80.	Vaidyanathan, G., Devaraj, S., & D'Arcy, J. (2012). Does Security Impact E-procurement Performance? Testing a Model of Direct and Moderated Effects. *Decision Sciences*, *43*(3), 437-458.	4
81.	Williams, S. P., Hardy, C. A., & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, *23*(4), 341-354.	4
82.	Aissa, A. B., Abercrombie, R. K., Sheldon, F. T., & Mili, A. (2012). Defining and computing a value based cyber-security	4

	measure. *Information Systems and e-Business Management*, *10*(4), 433-453.	
83.	Ji, Y., Kumar, S., & Mookerjee, V. (2016). When being hot is not cool: Monitoring hot lists for information security. *Information Systems Research*, *27*(4), 897-918.	3
84.	Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). A process framework for information security management.*International Journal of Information System and Project Management*, *4*(4), 27-47.	3
85.	Ahmed, G., Ragsdell, G., & Olphert, W. (2014). Knowledge sharing and information security: a paradox?. Academic Conferences and Publishing International Limited.	3
86.	Sun, W., Kong, X., He, D., & You, X. (2008, August). Information security problem research based on game theory. In *2008 International Symposium on Electronic Commerce and Security* (pp. 554-557). IEEE.	3
87.	Ramtohul, A., & Soyjaudah, K. M. S. (2016). Information security governance for e-services in southern African developing countries e-Government projects. *Journal of Science & Technology Policy Management*, *7*(1), 26-42.	3
88.	Sharma, S., & Routroy, S. (2016). Modeling information risk in supply chain using Bayesian networks. *Journal of Enterprise Information Management*, *29*(2), 238-254.	3
89.	Yusop, Z. M., & Abawajy, J. (2014). Analysis of insiders attack mitigation strategies. *Procedia-Social and Behavioral Sciences*, *129*, 581-591.	3

90.	Guster, D. C., Lee, O. F., & McCann, B. P. (2012). Outsourcing and replication considerations in disaster recovery planning. *Disaster Prevention and Management: An International Journal*, *21*(2), 172-183.	3
91.	Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information security control theory: achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems*, *34*(4), 1082-1112.	2
92.	Hanafizadeh, P., & Zare Ravasan, A. (2017). An investigation into the factors influencing the outsourcing decision of e-banking services: a multi-perspective framework. *Journal of Global Operations and Strategic Sourcing*, *10*(1), 67-89.	2
93.	Gao, X., & Zhong, W. (2016). Economic incentives in security information sharing: the effects of market structures. *Information Technology and Management*, *17*(4), 361-377.	2
94.	Park, Y. W., Herr, P. M., & Kim, B. C. (2016). The effect of disfluency on consumer perceptions of information security. *Marketing Letters*, *27*(3), 525-535.	2
95.	Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining users' security behaviors with the security belief model. *Journal of Organizational and End User Computing (JOEUC)*, *26*(3), 23-46.	2
96.	Da Veiga, A., & Martins, N. (2014, September). Information security culture: a comparative analysis of four assessments. In *Proceedings of the 8th European Conference on IS Management and Evaluation* (Vol. 8, No. 2014, pp. 49-57).	2

97.	Kim, B. C., & Jung, S. (2013). Effective immunization of online networks: a self-similar selection approach. *Information Technology and Management*, *14*(3), 257-268.	2
98.	Lindström, J. (2012). A model to explain a business contingency process. *Disaster Prevention and Management: An International Journal*, *21*(2), 269-281.	2
99.	Tsiakis, T. (2012). Consumers' issues and concerns of perceived risk of information security in online framework. The marketing strategies. *Procedia-Social and Behavioral Sciences*, *62*, 1265-1270.	2
100.	Van Wessel, R., Yang, X., & de Vries, H. J. (2011). Implementing international standards for information security management in China and Europe: A comparative multi-case study. *Technology Analysis & Strategic Management*, *23*(8), 865-879.	2