AARMS Vol. 17, No. 1 (2018) 87–140. **10.32565/aarms.2018.1.8**

Application of Science–Technology–Society Studies in Information Security Research

Review of Journals for Theory and Advanced Research Design[1]

András NEMESLAKI[2]

The research question and problem statement I posed to answer simply has been: what kind of patterns and specific discourses can be identified around the keywords of "information security" and "social construction" in information systems and its related reference fields such as social sciences, management studies, decision sciences extended to psychology. We may start summarizing the conclusions by stating that "information security" and "social construction" in the SCOPUS domain offers a wide range of literature in the social sciences and related subject areas; the initial search resulted in 406 article hits, whose basic bibliographic parameters with keywords and abstracts were downloaded. I categorized this sample according to the journals H-index, the Scimago Journal & Country Rank (SJR) Q1–Q4 ranking and the individual papers' citations, into five—so-called structural—clusters. Three papers were identified as the highest referenced and most influential, and analysed separately. The other were clustered as follows: 30 papers were classified into CL1, a high impact cluster due to its high citation and H-index, 122 papers were grouped into CL2, a mature cluster, due to their publishing date and medium referencing, 71 papers fell into CL3, a high potential cluster, due to their high H-index and recent appearance and, finally 152 papers were clustered into CL4, the mainstream of the sample due to their medium impact and wide spread of publishing dates. These clusters were further analysed with basic text mining techniques: word counting, key word analysis, textual clusters and N-Gram analysis, and concordance analysis. I found that clusters are different as far as the academic discourse on information security evolves, and each contain unique added value to the social construction of information security amongst users, institutions, technology and public policy. Finally, conclusion and further research opportunities are presented.

Keywords: *information security, social construction, SCOPUS data analysis, text mining, literature review*

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-15-2016-00001 entitled "Public Service Development Establishing Good Governance" in the Ludovika Workshop.

[2] CSc (Ph.D.), Professor of Information Systems, National University of Public Service; e-mail: nemeslaki.andras@uni-nke.hu

Introduction

This contribution is positioned as an integral part of a comprehensive research program executed at the National University of Public Service, which aims to bring together the top down and bottom up dilemmas of information security strategy process. [1] Based on Giddens' structuration and Venkatraman's strategic alignment theories we developed arguments for the application of "social construction" as a metaphor both for gaining understanding of the bottom up agencies and emergencies, and for the top-down trickling of strategies through institutions and policies in information security.

The objective of this paper is to examine how the notion of information security is viewed through the lens of the Science-Technology-Studies program (or sometimes referred as Science-Technology-Society both resulting in the acronym STS). I argue that this proposition is important both for practice and for theory, since the complexity of policies, governance and funding needs guidelines and insight to address the challenges of society in the cyberspace. Information security for individuals, organizations and very importantly to governments is pivotal amongst these challenges, and the reforms and activisms represented by the "broad churches" of STS provide a rich platform to enhance the discourses of scientific and technological knowledge in socio-political contexts. [2]

By taking a grounded theory approach within this framework, I present an exploratory analysis of reviewing the available contemporary scientific research in the field of information systems management and its transdisciplinary subject areas. As a corpus, I chose SCOPUS Scientific Journal Ranking and Journal Search database, mainly due to its broadness and easy access.

The research question and problem statement I posed to answer simply has been: what kind of patterns and specific discourses can be identified around the keywords of "information security" and "social construction" in information systems and its related reference fields such as social sciences, management studies, decision sciences extended to psychology. It is important to note, that I excluded in this paper the review of literature in engineering, computer science and natural sciences—references in these subject areas were only taken into consideration in case the outlets have been cross-listed with social sciences or humanities.

In the next sections, I present the research in the following structure; first a definition and brief review of the search terms are outlined as a conceptual background, then the concept of the research model and research design is shown, including the description of the methods and tools used throughout the study. This is followed by an in-depth discussion of the gathered data and several quantitative and qualitative analyses are displayed. Finally, the findings are summarized, together with the implications taking the limitations and validity into consideration.

Concepts and Definitions

We have three central topics in this review: STS, information security and social construction.

Science Technology Studies – STS

In the course of my proposed research design, they are investigated in the STS framework for three key reasons. Firstly, due to the fact, that STS has an active standpoint; it is often referred to as an "engaged program" assuming actions, creating solutions both conceptual and pragmatic. [3] This approach perfectly fits with the contemporary dilemmas of cyber-security challenges. Secondly, STS is inherently social and treats scientific and technological development as a complex social process, and considers that solutions/products of these developments are not "natural" by themselves. [4] This is especially relevant with information technology and information system applications, since they are all created, programmed, designed by humans where the "sciences of the artificial" apply. [5] And finally, the third reason to embed this work into the STS domain, is the broader context of politics and the role of governance at high and low levels to address the new digital world especially in terms of cyber-threats. Scholars in the STS program have developed clear arguments that not only science and technology forms politics and government, [6] but, and this is probably a more important direction in this case, the political neutrality of science and technology is also questionable [7]—several technological paradigm changes have happened thanks to government interventions or even high level political influences (space programs, the trickling effects of military technology, or even the internet). The STS approach, in conclusion, is broad enough in scope and in breadth to connect theories and practices, institutions and emergencies, not only to theorize information security but also for supporting pragmatic public policy programs, as well.

Information Security – ISec

In the proposed scheme of research design the epistemology of information security is connected to STS. As [8: 838] puts: "a key focus in ISec research is finding ways to motivate end users, employees and consumers to improve protection of their individual and organization information assets". Naturally, ISec is not only a user-oriented terminology, it is generally entailing protection against threats, originating "outside" of institutions, but as it has been investigated recently quite often from "inside" organizations. [9]

While having in mind, that protection of all kinds of data and related processing resources—such as systems and individuals—is a very old concept, and not related to computers or communication technologies at all, in the course of this study I inherently attach ISec to information communication technologies. The main reason for this is the fact, that ICT has become so ubiquitous that it is inseparable from our daily life. [10] ICTs have amplified, transformed and enabled breakthrough innovations to threaten the confidentiality, integrity and availability (the so-called "CIA principle"), that is the assurance of information and IT-security. Technologically these threats take various forms such as viruses, malware, worms, e-mail spam, spyware, Trojan horses, Nigerian-letters—quickly changing variations of malicious codes penetrating into information systems and compromising their functioning. [11] As we showed earlier, the rich social context of ISec has been recognized and intensively investigated, for instance [12] a framework has been developed organizing the challenges into three categories:

- data processing integrity: ensuring that content is correct and reliable,
- system access and protection: data is available, retrievable and properly restricted,
- system structure and usage: how easily information is comprehended and protected.

Furthermore, beyond the classic theories of human and organizational interactions with ICT—such as TAM, [13] UTAUT [14] or sociomateriality [15]—new theories are brought to investigate these extended social challenges such as criminology, [16] general deterrence or protection motivation theories (GDT, PMT) from psychology literature. [8]

Apart from the theoretical compositions of ISec, we have looked at our practical experience in educating information security managers for central and local government institutions. According to the expectations and curriculum requirements, these people have to be in charge of the security of the electronic information systems, and be aware of the legal, administrative, safety and quality management bases of their work. They should be able to perform assessing risks at a high level, be able to control the security of systems, and handle the incidents which occur. Topics they need to acquire in their CISO trainings are:

- *General knowledge areas of management, technology and legislation:*
  - Quality management,
  - Technologies of security,
  - Security policy,
  - Legal and administrative areas,
  - Organization and management.
- *Information Security Systems Management Areas:*
  - Information security standards,
  - Management of information systems,
  - Information security strategy and leadership,
  - Information security organizations.
- *Information Security Process Management Areas:*
  - Information security program,
  - Application of information security technologies,
  - Information security awareness exercise,
  - Security of information systems,
  - Information security of networks,
  - Testing and auditing information security.
- *Incident and Security Risk Management Areas:*
  - Risk assessment and risk management,
  - Practical risk management of intrusion,
  - Incident management and continuity planning,
  - Practical incident management exercise.

Government strategies and institutional legislation for governing information security is expressed and enforced through security policies, decrees, laws and organizational arrangements. In this context, general knowledge and compliance—often addressed as awareness—to these guidelines and directives are imperative elements of ISec. [17] There is a stream of research in this context arguing that both compliance and motivation of users/employees/civil servants can be achieved by raising policy awareness, systematic

enforcement and regular maintenance of technological and human procedures in information security management. [12] [18]

Finally, for conceptualizing on ISec, the "CIA principles" over the last years have been appended with the notion of privacy, authenticity and trustworthiness—which have become integral conditions for all electronic services.

Social Construction of Technology – SCOT

The academic school of SCOT emerged in the discourses about interaction and influence between technology and society. SCOT can be positioned as an alternative to technological determinism, which is a typical engineering world-view, taking technology-related strategies governed by rationality, accurately designed, economically clear and unambiguous investment [4]. In this world-view, quite opposite to SCOT, there is no need for social interpretation of technology solutions, the wider environment is not interesting for how technology evolves, since it is gradually adapting to the effects of technology.

The essence of the SCOT theory is that it does not deal with the highly controversial cause-and-effect relationship between the interaction of society and technology but considers human communities as part of technological innovations. [19] Bijker's book on bicycle, Bakelite and fluorescence flashlight presents details of SCOT through the elaboration of the technical history of these three stories. [19] [4]

Bijker explains the connection between relevant social groups (RSG), the individuals who have similarities in their attitude and behaviour; they share the same technology frame and therefore they have the same interpretive flexibility. The technology frame consists of several elements, all conceptualized by the particular RSGs, like the functionality of the given technology artefact, possible ways it addresses solving the users' problems, the scientific theories underlying its working, the affordances with which it offers intuitions for use, what kind of knowledge it requires to operate, how it was designed, tested and implemented. The essence of interpretive flexibility is that technology frames are different amongst RSGs, the same artefact gets rather different translations about their meaning, use, and value. This leads to the situation that technologies with the same set of functionalities and applications might lead to substantially different problem framing and solutions—or constructions, using STS language.

The interpretation of technology is provided by the shared meaning developed in the given RSGs. Dialogues within the RSGs reinforce the technological frames as the artefacts develop in one way or another. This leads to the situation that isolated RSGs have more and more powerful frames, which in return determine the RSG's impact on the development direction of the artefact. When RSGs are not isolated they dispute with each other, and as long as there is no socially accepted interpretation represented by the most dominant RSG, that technology can be regarded as unstable because its evolution is characterized by many competing variants and experiments. Stabilization or closure is reached when one of the RSG's technology interpretations becomes dominant, and a macro level consensus emerges for the particular artefact. The "flexible" interpretation of technology is thus eliminated and the social meaning of the work becomes stabilized.

According to Bijker's case study on the development of bicycles, the so-called "safety" bicycles have long been awaited, because of the rather diverse relevant social groups in the nineteenth century. For instance, at that time the group of athletic men were the most dominant, and bicycles as artefacts were interpreted according to them as technologies for acrobatic achievements, sport, and masculinity requiring manly skills and competitiveness. Other groups, like women's cyclists, were far less significant, as the early asymmetrical bicycle for them meant high risks, discrimination due to the lack of fitting with acceptable female attire, unreliability and many inconveniences. The safety bicycles got stabilized in their present form, when the artefact allowed more RSGs to realize that the technology frame can be altered, and travel, commuting and leisure can also be part of the interpretive flexibility. [19] Bijker's example of the bike has demonstrated the many experiments, attempts, trials dead-lock directions, often in parallel, but always in accordance with one seemingly dominating interpretation of a particular RSG, and technological framework.

I propose SCOT as a powerful concept to deepen our understanding about the challenges of the cyberspace, since for example, the Internet itself can be easily associated with numerous RSGs and their interpretation of technology. Hackers take it as an environment for solving puzzles and breaking lock pads, armies look at it as new theatres for war, suppliers as new markets for products, administrations as a more and more risky channel to reach citizens, and ordinary users as a jungle of threats and dilemmas regarding their life in the cyber world.

In any case, contribution of SCOT literature might reveal the non-linear pattern of development in security management, and importantly some of the driving forces behind the twist-and-turns of adapting information security compliance.

Research Model and Methodology

This design and methodology were exploratory in nature, and its objective has been to provide a first level insight to a robust text mining research design, based on these results. As part of this work, I tested several open-source text analysis tools, developed in R platform, or using other general application packages. In the course of this paper I cannot discuss the experiences and results, regardless that experimentation has been a valuable effort resulting in creating a toolkit for "easy text-mining". To the conclusions and limitations of this approach I return in the last section of the paper.

Research Model

The research model is summarized in Figure 1. I used keyword search on the terms of information security and social construction. This solution proved to be useful to provide substantial amount of hits, because the inclusion of STS as a key phrase would have limited the search too much.

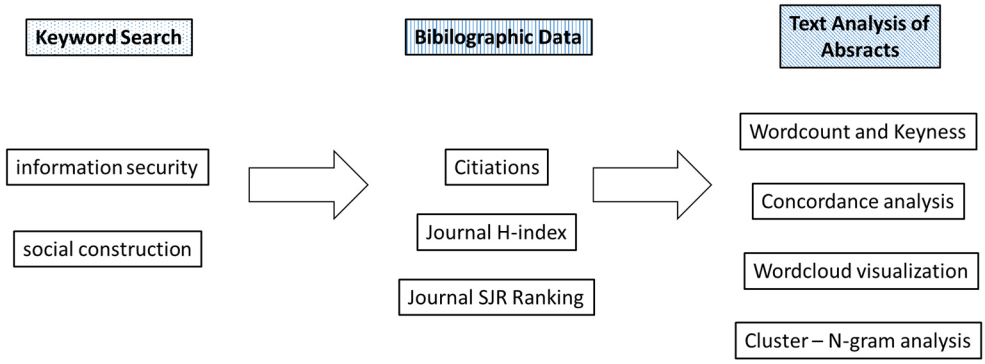

Figure 1. *Research Model.* [Created by the author.]

The second part of the design focused on structural analysis of the bibliographic data—amongst these two are describing the journal (the H-index and the quality ranking) and one particularly the given paper (number of relevant citations).

Finally, in order to get a textual insight to the topics I ran four basic text analysis methods on the corpus of the abstracts of the papers.

Research Methodology

For implementing the design, I used three research methods, a keyword search on the SCOPUS database, a two-step cluster analysis using SPSS, and the text analytics using AntConc,[3] COWO[4] and VOSviewer.[5] In this section I only describe SCOPUS and the sample resulting of the keyword search, the rest of the methods will be introduced in the next, discussion section. The Scopus abstract and citation database is available by Elsevier since 2004 at www.scopus.com. The largest percentage of materials consist of scientific and technical items, and references can be traced back to the 1960s. The database items include books and monographs as well, not only journals, in several languages, but mostly in English. Science Direct, Elsevier's full-text database using SCOPUS is available at www.sciencedirect.com . It provides PDF and other exportable formats of natural, medical, technical journals and books. More than 3,800 journals and 35,000 books can be searched for keywords, author name, title, image, etc.

There are 27 subject areas (e.g. Decisions Sciences, Social Sciences or Computer Science) available for national and periodical ranking, with a total of 313 subject categories (for instance "law" with more than 400 journals is a subject category under the "social sciences" subject area), 8 regions (Africa, Latin America and North America, Western and Central Europe, Pacific region) or country and year (1996-2015). For journal ranking

[3] www.laurenceanthony.net/software/antconc/
[4] http://clementlevallois.net/portfolio.html
[5] www.vosviewer.com/

and targeted search, it is sufficient to provide the journal's title, ISSN number, or the name of the publisher. One can also search for documents by type (journals, book series, or even indexed conference proceedings).

The keyword search on "information security" and "social construction" ran in 8 subject areas and only selecting academic journals (conferences, books were omitted):

- Social Sciences,
- Business, Management and Accounting,
- Arts and Humanities,
- Psychology,
- Decision Sciences,
- Economics and Finance,
- Psychology (Medicine),
- Multidisciplinary.

In order to get an insight to the relevance of the hits, I used three indicators, SCOUPS SJR ranking, the journal H-index and the papers' citations.

Ranking of scientific journals in SCOPUS is assessed by the "SCImago project". The Scimago Journal & Country Rank ranking was developed by researchers in 2009, who are dealing with information analysis, retrieval and presentation of publication data. To determine the index, the number of references should be weighted by the number of references in the referenced journal. SJR journal-based ranking can be divided into groups of high-quality documents—s quartiles (Q) form—on the basis that the document provides specialty prestigious journals which:

- Q1 – "Excellent:" The top 25% of the ranking based on the SJR metrics of the industry.
- Q2 – "Good:" 50 to 75% of the ranking based on the SJR metric.
- Q3 – "Medium:" 25% to 50% of the ranking based on the SJR metric.
- Q4 – "Poor:" The lower 25% of the rankings of the SJR metrics for the industry.

The ranking is publicly available on the official website: www.scimagojr.com. SJR numbers can be sorted and other data can be seen, such as the country in which the publication was made, the H-index, the number of references in the year selected and within 3 years, the number of publications in the year chosen and within 3 years. It is important to note, that journals can be ranked in more subject areas and categories at a time, and the same journal can have different ratings in these areas.

Description of the Sample and the Corpus

The initial search resulted 406 article hits, whose basic bibliographic parameters with keywords and abstracts were downloaded. Yearly distribution can be seen in Figure 2.

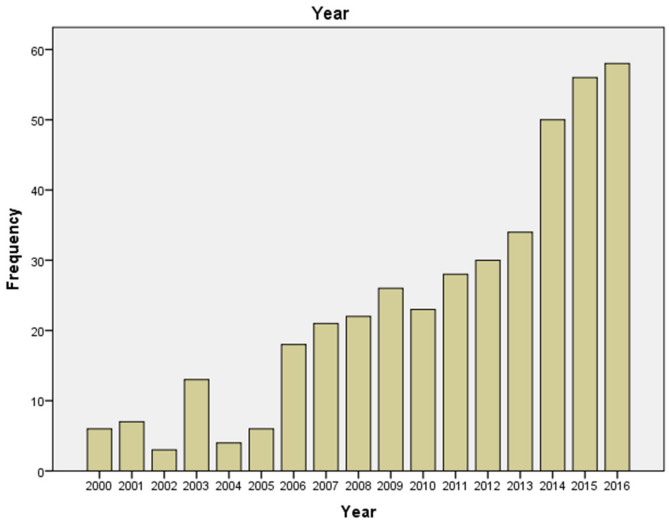

Figure 2. *Papers' yearly distribution between 2000–2016. (Search terms: information security AND social construction.)* [Created by the author.]

It is interesting to notice that publication on this topic started with waves in the early 2000s and until 2013 there was a steady growth in this topic. Then, from 2014 for some reason a boost started and it seems like the social context with information security started to boom.

Distribution between SCOPUS Subject Areas and the journals SJR ranking quality is summarized in Table 1.

Table 1. *Distribution of the corpus by subject areas.* [Created by the author.]

		Subject Areas (SBJA)							
		Business and Management	Social Sciences	Psy-chology	Decision Sciences	Arts	Eco-nomics	Multi-discip	Medi-cal
		Count	Count	Count	Count	Count	Count	Count	Count
SJR	Q1	34	88	20	22	1	9	3	2
	Q2	25	41	7	7	0	3	0	1
	Q3	12	29	3	3	0	0	1	0
	Q4	4	5	2	2	0	0	2	0

As it was accepted, most hits came from Social Sciences and the Management subject areas but the relevant number of publications contains the search words in decision science, and psychology, as well. It is important to note that several journals have more listings—we took the first and the one which harmonizes the journal "title" and genre.

Table 1 also shows that the journals are high quality, the majority of them are Q1 and Q2 SJR ranked. Table 2 lists the most relevant journals of our sample—these are the journals with Hirsch-index higher than 100 at the time of the data collection. As we can see there

are 28 journals amongst the most relevant which all together hold 46 papers of the initial 406. Not surprisingly the ones which included more than one paper with our search word combination are "information system" related (MISQ, Information Sciences, or Journal of MIS) or embedded in decision sciences (DSS, Info Science and Technology, Information and Management). We also find journals from medicine, psychology and social sciences but these are just general indicators without really looking into the content of the papers.

Another important indicator for a paper's relevance is its citation number. This is what we present in Figure 3. Naturally, one has to be careful with judging relevance by citation only, especially in the case of recent papers, since it takes time for a publication to reach readership and climb its citation number. Regardless, a first look at the highest numbers show some interesting insights on what academic readership quotes and refers to a lot. The highest number is a total of 725 references for one article while at the other end we have 41 papers which have 1 SCOPUS citation. All together 311 papers were cited at least once until the time of this essay.

In Table 3 I show the most highly sited papers with our keyword search together with their subject areas. We can see that all papers are Q1 indexed, and from high impact journals (not necessary IF because we use a different database). Six items come from the Decision Science subject area from very high H-indexed journals, two from Business Management and Accounting and one-one from Psychology and Economics.

Table 2. *Journals with a H-index greater than 100 and the papers in the corpus.*
[Created by the author.]

	Journal	**H-index**	**Papers**
1.	*Academy of Management Journal*	252	1
2.	*Journal of Applied Psychology*	218	1
3.	*Quarterly Journal of Economics*	205	1
4.	*Management Science*	198	1
5.	*Social Science and Medicine*	195	2
6.	*Research Policy*	178	1
7.	*MIS Quarterly: Management Information Systems*	177	4
8.	*Ecological Economics*	151	1
9.	*Journal of Organizational Behaviour*	134	1
10.	*World Development*	133	1
11.	*Information Sciences*	131	3
12.	*Tourism Management*	130	1
13.	*Information Systems Research*	128	1
14.	*Information and Management*	128	2
15.	*Global Environmental Change*	120	1
16.	*Journal of Business Ethics*	120	2
17.	*Global Environmental Change*	120	1
18.	*Journal of Management Information Systems*	119	5
19.	*Psycho-Oncology*	113	1
20.	*Journal of the Association for Information Science and Technology*	112	3
21.	*Computers in Human Behaviour*	111	2
22.	*Decision Support Systems*	109	3

	Journal	H-index	Papers
23.	*Journal of Experimental Social Psychology*	108	1
24.	*Accident Analysis and Prevention*	108	2
25.	*Cyber-psychology, Behaviour, and Social Networking*	106	1
26.	*Appetite*	104	1
27.	*Accounting, Organizations and Society*	103	1
28.	*Behaviour Research Methods*	103	1
	Total		46

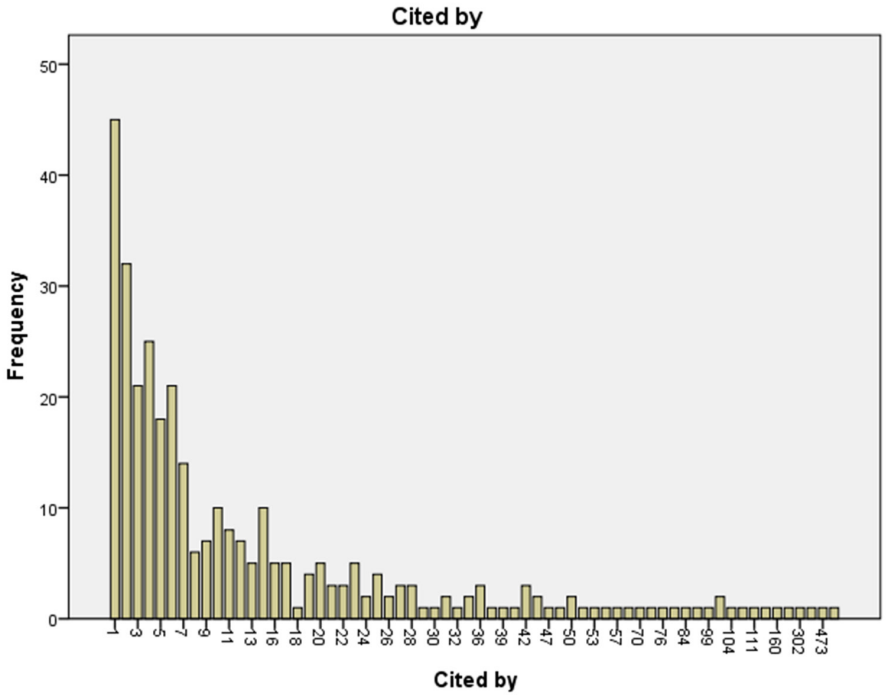

Figure 3. *Number of citations in Scopus.* [Created by the author.]

They are rather mature papers, the oldest was published in 2003 and the most recent from this list is also six years old. This is again in alignment with the citation cycle, but also indicates the fact that when technology issues get mixed with social impact analysis, more time is needed for assessing results and publish findings of robust research results.

Table 3. *The top cited papers with the search phrases and their subject areas.*
[Created by the author.]

Authors	Title	Year	SJR	H	SBJA	Journal	Cites
Kim D.J., Ferrin D.L., Rao H.R.	A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents	2008	Q1	109	DS	Decision Support Systems	725
Ariely D., Loewenstein G., Prelec D.	"Coherent arbitrariness:" Stable demand curves without stable preferences	2003	Q1	205	ECON	Quarterly Journal of Economics	473
D'Arcy J., Hovav A., Galletta D.	User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach	2009	Q1	128	DS	Information Systems Research	315
Johnston A. C., Warkentin M.	Fear appeals and information security behaviours: An empirical study	2010	Q1	177	DS	MIS Quarterly: Management Information Systems	302
Yousafzai S. Y., Pallister J.G., Foxall G.R.	A proposed model of e-trust for electronic banking	2003	Q1	94	BMA	Technovation	176
Workman M., Bommer W.H., Straub D.	Security lapses and the omission of information security measures: A threat control model and empirical test	2008	Q1	111	PSCHY	Computers in Human Behaviour	160
Li X., Hess T.J., Valacich J.S.	Why do we trust new technology? A study of initial trust formation with organizational information systems	2008	Q1	68	BMA	Journal of Strategic Information Systems	130
Iivari J., Huisman M.	The relationship between organizational culture and the deployment of systems development methodologies	2007	Q1	177	DS	MIS Quarterly: Management Information Systems	111

Authors	Title	Year	SJR	H	SBJA	Journal	Cites
Kim D.J.	Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study	2008	Q1	119	DS	Journal of Management Information Systems	109
Guo K.H., Yuan Y., Archer N.P., Connelly C.E.	Understanding nonmalicious security violations in the workplace: A composite behaviour model	2011	Q1	119	DS	Journal of Management Information Systems	104

In Table 4 I attached the authors' keywords to the papers, so at a quick glance, the topics can be identified in the case of the top cited papers. As a result of this visual check, and verifying by reading the abstract of the missing keywords, I decided to omit this paper from further analysis, since the topic had no connection to information security in the context of information systems or cybersecurity.

Table 4. *There is a significant correlation between journal H-index and citation—even in the dynamic field of info security.* [Created by the author.]

Authors	Paper Title	Author keywords
Kim D.J., Ferrin D.L., Rao H.R. 725	A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents	Antecedents of *trust;* Consumer trust; Electronic commerce; Internet consumer *behaviour*; Perceived risk; Privacy and security; The role of trust; Trusted third-party seal
Ariely D., Loewenstein G., Prelec D. 473	"Coherent arbitrariness": Stable demand curves without stable preferences	No Keywords (After analysing the abstract, the paper is omitted from the analysis)
D'Arcy J., Hovav A., Galletta D. 315	User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach	End-user security; General *deterrence* theory; IS *misuse*; IS security; Security countermeasures; Security management
Johnston A.C., Warkentin M. 302	Fear appeals and information security behaviours: An empirical study	Coping appraisal; Countermeasures; *Fear* appeals; Information assurance; Information security; Persuasive communication; *Protection motivation* theory; *Threat appraisal*
Yousafzai S.Y., Pallister J.G., Foxall G.R. 176	A proposed model of e-trust for electronic banking	Electronic banking; *Perceived risk; Trust*

Authors	Paper Title	Author keywords
Workman M., Bommer W.H., Straub D. 160	Security lapses and the omission of information security measures: A threat control model and empirical test	Information security; *Omissive behaviours; Protection motivation theory; Social cognitive theory; Threat control model*
Li X., Hess T.J., Valacich J.S. 130	Why do we trust new technology? A study of initial trust formation with organizational information systems	e-Government; *Initial trust;* National identity systems; Organizational information systems; *Subjective norm; Technology adoption;* Trusting attitude; Trusting bases; Trusting beliefs; Trusting intention
Iivari J., Huisman M. 111	The relationship between organizational culture and the deployment of systems development methodologies	*Competing values model;* Information systems developers; Information technology managers; *Organizational culture;* Software engineering; Systems development; Systems development methodology
Kim D.J. 109	Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study	*Cross-cultural comparison;* Culture impacts; *Self-perception-based trust;* Transference-based trust; Trust in e-vendor; Type I and Type II cultures
Guo K.H., Yuan Y., Archer N.P., Connelly C.E. 104	Understanding nonmalicious security violations in the workplace: A composite behaviour model	information systems security; *nonlinear construct relationships;* nonmalicious *security violation;* perceived identity match; perceived security risk; relative advantage for job performance; *workgroup norms*
Cao L. 100	In-depth behaviour understanding and use: The behaviour informatics approach	*Behaviour analysis;* Behaviour computing; *Behaviour informatics;* Decision making; Informatics

Discussion of Results: Structural Cluster Analysis of the Papers

Four papers have outstandingly high citations, these were removed from the sample. These four are the following:

Table 5. *The four most cited papers for the keyword combination (information security and social construction).* [Created by the author.]

Authors	Title	Year	Journal	Vol	No	Pages	SJR	H-index	SA
Kim D.J., Ferrin D.L., Rao H.R.	A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents	2008	Decision Support Systems	44	2	544-564	Q1	109	Dec. Sci.

Authors	Title	Year	Journal	Vol	No	Pages	SJR	H-index	SA
Ariely D., Loewenstein G., Prelec D.	"Coherent arbitrariness": Stable demand curves without stable preferences	2003	Quarterly Journal of Economics	118	1	73-105	Q1	205	Econ. Fin.
D'Arcy J., Hovav A., Galletta D.	User awareness of security countermeasures and its impact on informa on systems misuse: A deterrence approach	2009	Information Systems Research	20	1	79-98	Q1	128	Dec. Sci.
Johnston A.C., Warkentin M.	Fear appeals and information security behaviors: An empirical study	2010	MIS Quarterly	34	3. SPEC. ISSUE	549-566	Q1	177	Dec. Sci.

After reading the title and the abstract, based on the content I decided to omit the Ariely paper, because it had no relevance to the ontology of information security in its context of our research. The remaining four, on the other hand, perfectly fit our topic and were kept for further analysis, and treated as seminal papers of the field.

The 382 papers remaining in the sample were further classified by Two-Step Cluster Analysis using three variables: year of publication, citation number and H-index of the journal where the paper appeared. Results indicated in Figure 4 show fair values of silhouette measure of cohesion and separation and showing that the importance of three predictor variables are above 0.77 confirming high predictability. Summary of the mean values and population of each cluster can be seen in Figure 5.

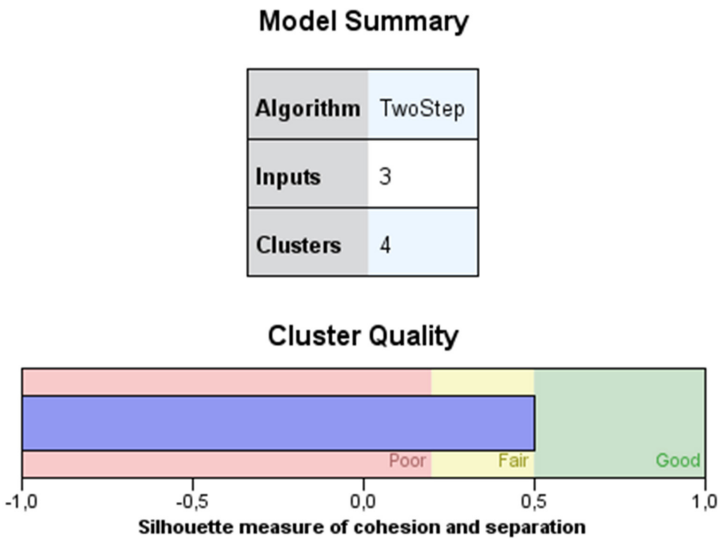

Figure 4. *Model Summary of the Two-Step Cluster Analysis in SPSS.* [Created by the author.]

8% of the papers (30 articles) got clustered into C-1. These papers were published in high H-index outlets, they are mature given the average age of 10 years (2007) and probably these factors contributed to their presently very high citation average (72.53 citation/papers). According to these features these papers were labelled as high-impact papers regarding our topic.

122 papers (32%) were classified into the second cluster—C–2—which I labelled as mature contributions, given the fact that their timing is similar to C–1, but the mean value of citation is almost 6 times lower (12.97 citations/paper) and these contributions have appeared in less highly indexed journals (H = 37.68).

The third cluster, C–3, contains 71 articles (19%) and might be considered as recent contributions, since they are around 3 years in circulation (2014). They were published in high impact journals (H = 86.13), but probably due to the relative freshness their citation number is significantly lower than the first two clusters'. For these reasons I marked these contributions as promising future since dynamically their relevance will grow.

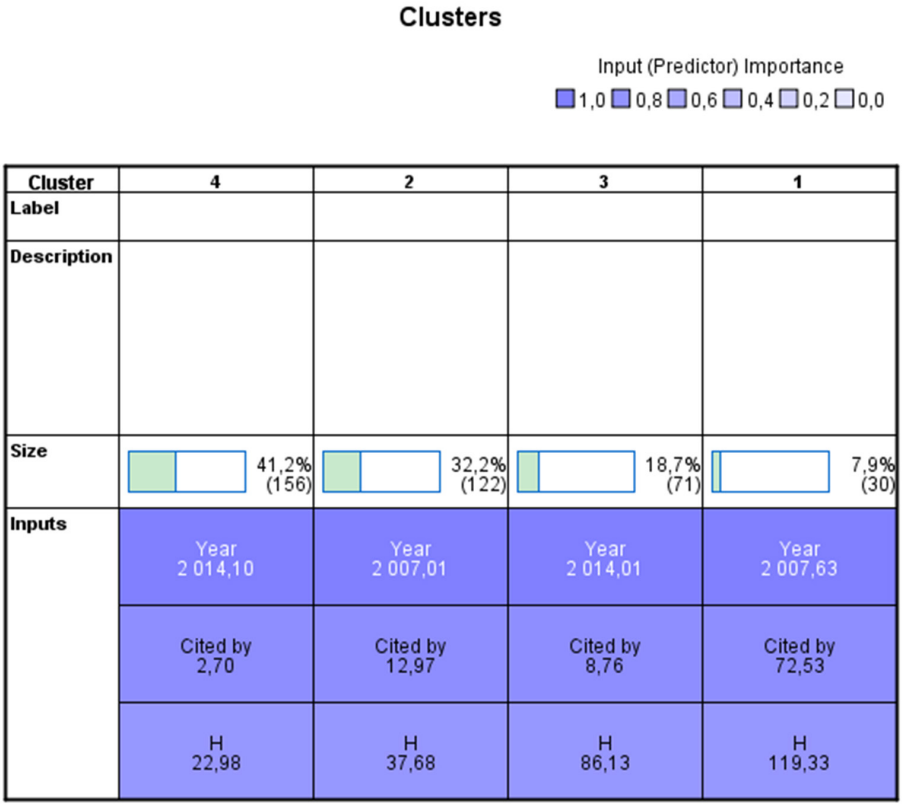

Figure 5. *Description of the four clusters.* [Created by the author.]

Finally, we can see 41%—the highest number—of papers in C–4, the fourth cluster. In terms of age these papers are almost identical to C–3, but they are significantly different as far as the lower impact (Citation = 2.7/paper—one fourth of C–3) and lower ranking of

journals is concerned (H = 22.98). These papers are structurally contemporary, but both in their prestige and impact bear the features of mainstream contributions—on average showing less potential than C–3, but reaching a wide group of readership regardless.

In order to get deeper insights to the four clusters, two evaluation fields were introduced, the variable of journal SJR classification (Q1–Q4) and the subject areas of the papers. These values were not used in determining the clusters, but their distribution helps us structuring the corpus better.

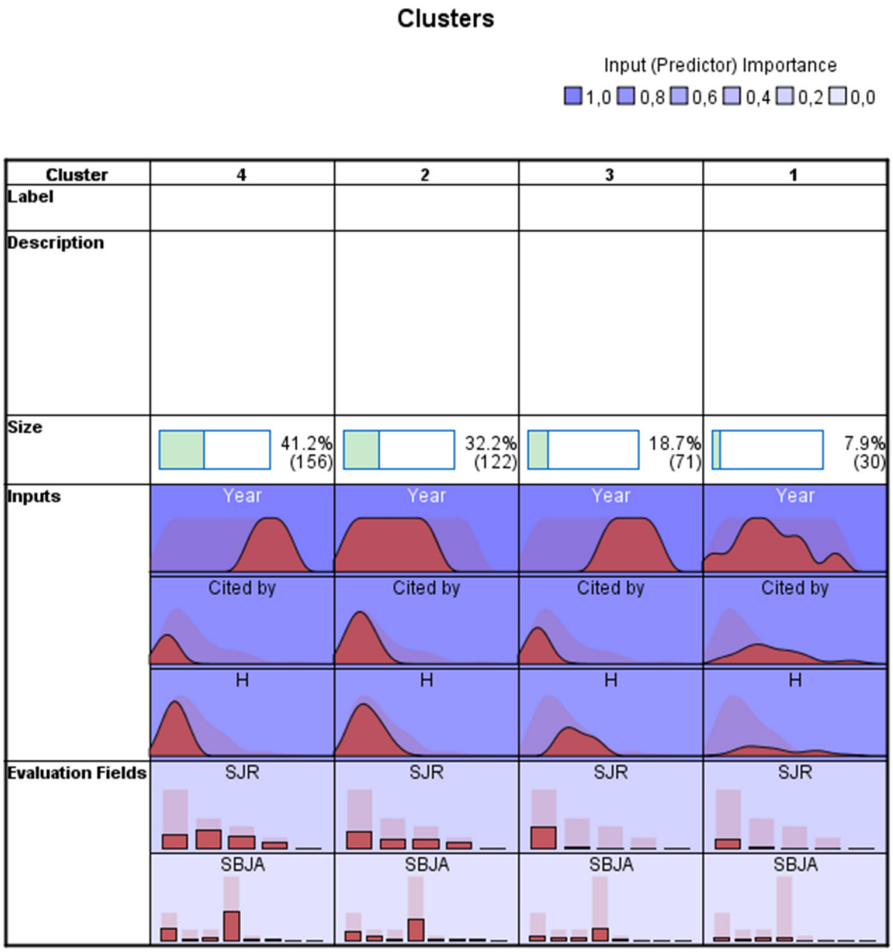

Figure 6. *Visualization of the clusters by including two evaluation fields and value distributions.* [Created by the author.]

In Figure 6 similarities and differences are visualized of the four clusters both for input and evaluation variables. Given the fact, that the evaluation fields are categorical variables "shape of distribution" is more narrative than the SPSS outputs of means. I would like to draw the attention of the reader to the interesting visual fact regarding the subject areas, that the C4, the mainstream cluster, holds significantly more submissions in

business-management-accounting and decision sciences (the first and fourth column), and the modus of the SJR ranking is Q2 journals, while in the other clusters topically decision science dominates and the journals are Q1 level mostly.
Cluster differences can also be studied by comparing the block-box diagrams in Figure 7 and Figure 8.

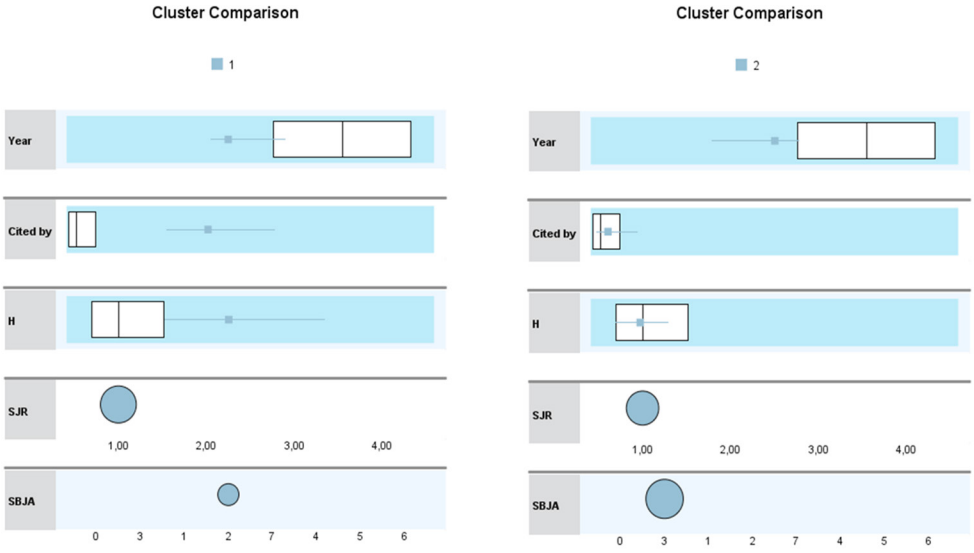

Figure 7. *Comparison of cluster variables for C1 and C2.* [Created by the author.]

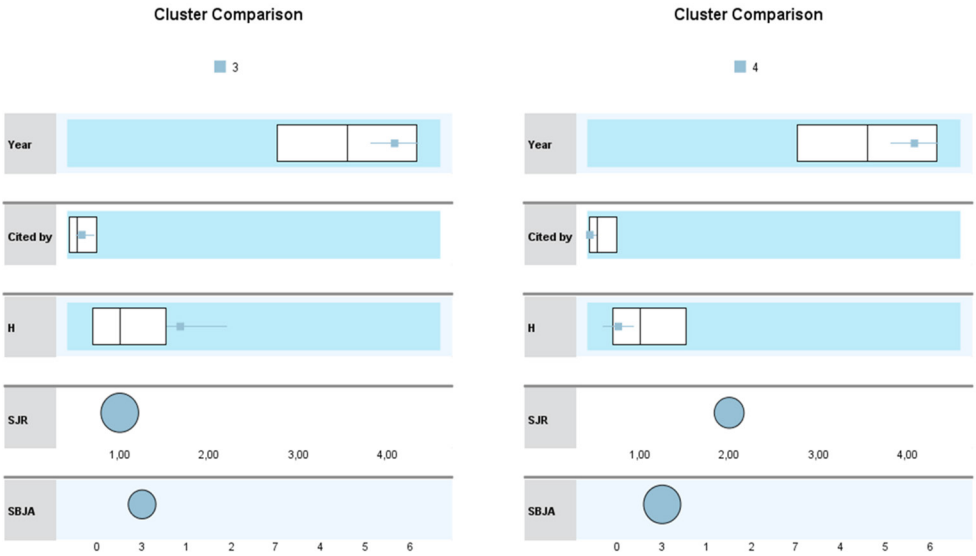

Figure 8. *Comparison of cluster variable for C3 and C4.* [Created by the author.]

The scatter-plot diagrams of the clusters provide several additional observations and implications for further analysis of our corpus. (Figure 9)

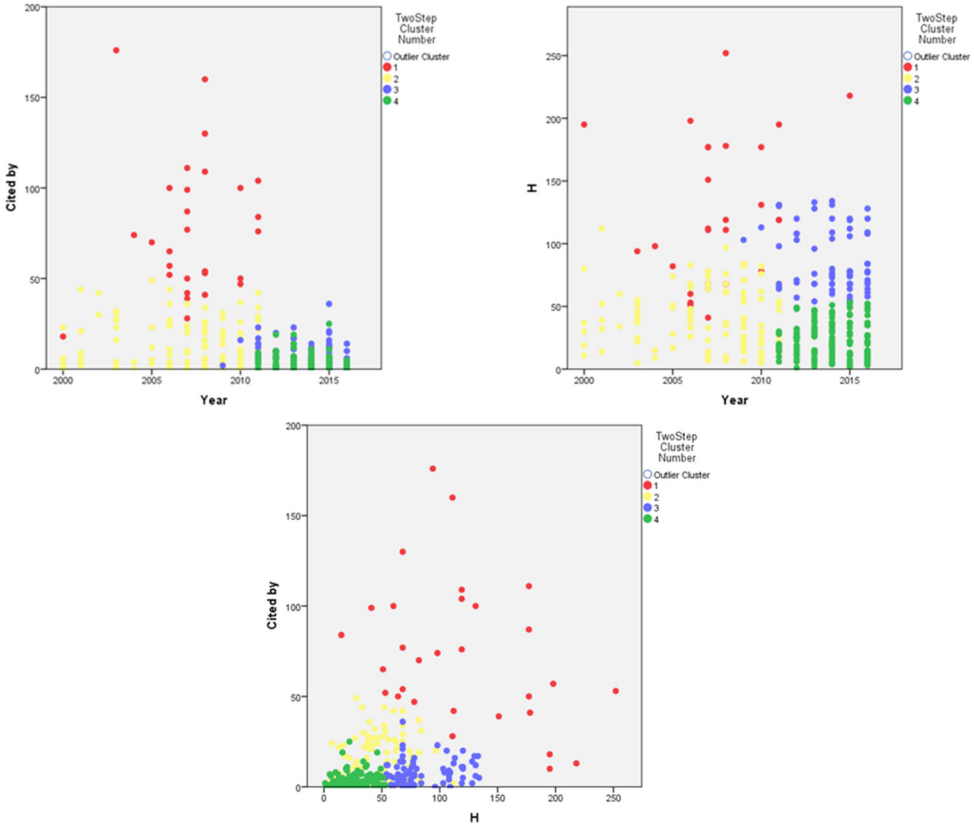

Figure 9. *Scatter plot diagrams of the abstract "points"—according to publication years, citationand journal H-index.* [Created by the author.]

For instance, the first scatter-plot in Figure 9 nicely demonstrates the high impact C1 is populated in the centre of our publication period of 2000-2016 and how much the cluster is elevated in terms of the citations above the others. This is then further emphasized in the second and, especially the third plots. This last one nicely shows the visual difference between C3 and C4 which are similar in terms of citations, and position on the year axis, but different in terms of journal impact. In the second plot this is indicated basically by C3 "sitting on" C4 demonstrating its higher potential for future impact. We can also see, how the mainstream cluster C2, spreads through the years and gives space from around the early 2010s to the green and blue clusters of C3 and C4, yet taking the main bulk of present citations between the high impact C1 and most recent C3 and C4.

Concluding the cluster analysis, we can safely say that the articles show a structured pattern based on their three cluster inputs and also regarding their two evaluation variables. We found five different groups analysing these parameters; the first being a small

set of "outliers" in terms of their citation number consisting of three papers in the topic of information security and social construction. Then, the second highest impact is a set of 30 papers in C1 with high citation numbers and impact, the only dilemma with them being the relative timeliness issue regarding information security given that these are around 10-year-old contributions. The third most relevant group is the next 71 papers in C3 which are relatively contemporary—3 years on average—and appeared in high impact journals. Our assumption is that these contributions have topics, methodologies and issues discussed which will be the next high impact cluster in some years. Finally, C2 and C4 are papers in similar quality journals, where C4 cluster members are more recent—probably covering different topics—and therefore also less cited. My assumptions are that C4 is potentially the next mainstream just like presently C2 covering both topically and methodologically ordinary craftsmanship of our profession—decent but breakthrough research in the field of information security.

In order to find out how the clusters differentiate, and weather the assumption based on the cluster variables hold, in the next chapter I present the result of the text analysis of the abstracts.

Discussion of Results: Text Analysis of the Abstracts

Based on the results of the two-step cluster analysis, I created five separate text files containing the 386 abstracts, and consider these as the main corpus for simple text mining and contextualizing the accumulated knowledge.

Table 6. *Text mining corpus merged from the abstract files.* [Created by the author.]

	File name	Cluster	Number of abstracts
1.	abstract_big_three.txt	Outlier three paper	3
2.	abstract_cluster_1.txt	CL1	30
3.	abstract_cluster_2.txt	CL2	122
4.	abstract_cluster_3.txt	CL3	71
5.	abstract_cluster_4.txt	CL4	156

Given the fact, that this amount of information does not have the depth of the full texts only the basic, simplest text processing methods were applied using AntConc 3.4.4., a freely available but robust multiplatform tool for carrying out corpus linguistics research and data-driven learning, developed by Anthony Laurence at the Faculty of Science and Engineering at Waseda University in Japan.

Word Counting

The first, and simplest way to look into the textual information of the corpus is to run word counts and compare word frequencies across the different clusters. For this I designed the following method.

Figure 10 shows the user interface, how the wordlist was created on the five files composing the abstract corpus. As a result, 82,700-word tokens were created using 7,920 different word types. This list then was used as the keyword list range, or as a corpus reference, compared to which I calculated the so-called keyness variable for each cluster file.

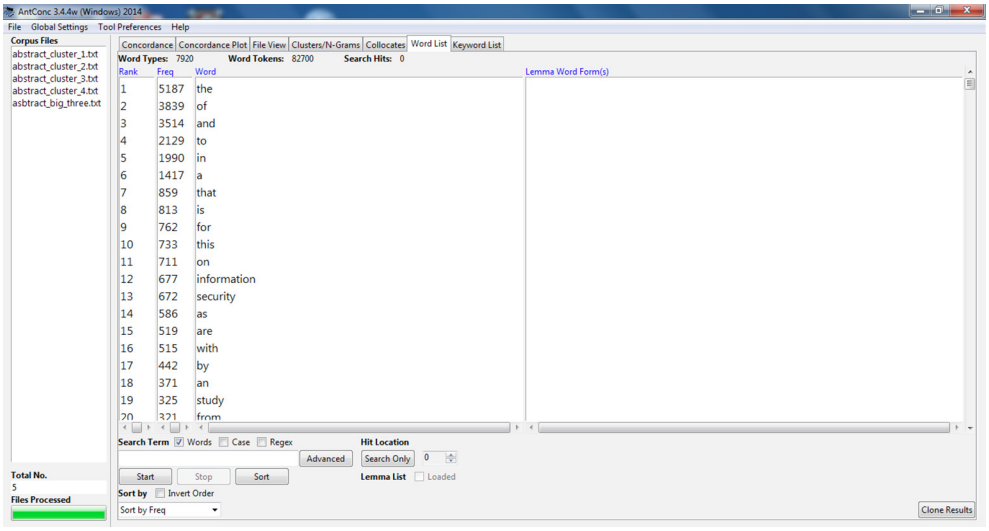

Figure 10. *Wordlist creation with AntConc on the Corpus.* [Created by the author.]

The analysis goes beyond a simple word count, since it shows which words are unusually frequent (or infrequent) in comparison with the words in a reference corpus. This allows us to identify characteristic words—hopefully unique to the individual clusters—as part of a genre.

Keyness is calculated using the Log Likelihood method. [20] When using either Log Likelihood or Chi-squared as the statistical measure, the following significance values apply:

- 95^{th} percentile; 5% level; $p < 0.05$; critical value = 3.84;
- 99^{th} percentile; 1% level; $p < 0.01$; critical value = 6.63;
- 99.9^{th} percentile; 0.1% level; $p < 0.001$; critical value = 10.83;
- 99.99^{th} percentile; 0.01% level; $p < 0.0001$; critical value = 15.13.

Taking this into consideration, I chose the 99% level of significance, using 7.00 as a critical keyness value. Accordingly, a word was considered a keyword—compared to the reference corpus—in case its keyness value was greater than 7.00. Results of the five different clusters are the following:

Three Top Cited Paper (Outlier Cluster)

Table 7. *Keyword keyness of the three most cited papers in the sample.* [Created by the author.]

	Freq.	**Keyness**	**Keyword**	**Verification with concordance analysis KeyWord in Context (KWIC)**
1.	8	51.608	misuse	IS misuse, misuse of information systems
2.	6	29.815	fear	fear appeals
3.	4	25.345	purchasing	purchasing decision, purchasing behaviour
4.	5	21.907	end	end user
5.	3	21.475	appeals	fear appeals
6.	8	21.291	trust	trust, reputation, privacy concerns,
7.	5	18.534	computer	computer users, computer monitoring, the context of computer security and information assurance, computer security actions, human-computer interaction,
8.	6	17.782	users	end user, IT user, computer user
9.	3	17.632	severity	severity of social influence, severity of sanctions severity of sanctions, certainty of sanctions,
10.	3	15.846	sanctions	
11.	2	14.317	certainty	
12.	2	14.317	efficacy	
13.	2	14.317	mitigation	
14.	4	13.786	consumer	consumer behaviour, consumer disposition to trust, consumer decision
15.	4	12.593	consumers	
16.	4	12.288	suggest	
17.	4	12.288	threat	threat to organizations, threat to punishment
18.	2	12.252	deterrence	
19.	3	11.962	actions	
20.	4	11.855	internet	Internet consumer
21.	6	11.081	model	deterrence theory model, conceptual model
22.	3	10.433	awareness	
23.	15	10.158	is	IS misuse, IS security
24.	2	9.938	reputation	
25.	2	9.938	website	
26.	3	9.726	user	
27.	4	9.248	perceived	perceived risk, perceived threat, perceived certainty and severity, perceived severity of sanctions
28.	2	8.520	incidents	

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
29.	4	8.308	impact	impact is not uniform, impact the actions of end users, impact of sanction perceptions
30.	3	7.827	perceptions	
31.	1	7.158	describing	
32.	1	7.158	infusion	
33.	1	7.158	originate	
34.	1	7.158	posture	
35.	1	7.158	sanction	
36.	1	7.158	SETA	security education training awareness

In order to get a contextual understanding of the keywords, I copied results of the concordance analysis for those words, where the frequency of occurrences was greater than 4.

High Impact (C1) cluster

In Table 8 given the large number of significant keywords, I only went through the concordance analysis where the frequency of occurrence is higher than 10.

Table 8. *Keyword keyness of the High Impact Cluster (C1) in the sample.* [Created by the author.]

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
1.	27	37.78	behaviour	behaviour analysis, modelling, informatics (BI), patterns
2.	14	34.95	SaaS	Software as a Service solutions, adoption, literature
3.	26	29.34	people	people requiring institutional care, technology supporting people, people become victims
4.	10	27.42	IFAC	IFAC Swiss registered non-governmental organization
5.	10	27.42	Obama	Obama campaign 2008
6.	16	25.71	culture	culture of secure behaviour, organizational culture, cross-culture, rational culture, Type I, II.
7.	22	25.70	perceived	perceived security, perceived privacy, perceived importance
8.	8	20.75	trusting	
9.	7	19.20	ISS	
10.	8	18.68	campaign	
11.	25	18.44	systems	information systems, information system development, information system field
12.	25	18.20	trust	trust determinants, trust formations, trust in people, trust in technology

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
13.	7	18.02	rivals	
14.	7	16.96	retirement	
15.	6	16.46	dementia	
16.	6	15.29	bi	
17.	8	14.70	everyday	
18.	5	13.71	accreditation	
19.	6	13.32	methodologies	
20.	10	12.56	ability	perceived work ability
21.	8	12.31	behavioural	
22.	7	12.21	initial	
23.	5	11.56	aids	
24.	8	11.30	internal	
25.	9	11.26	type	
26.	4	10.97	contravention	
27.	4	10.97	telecare	
28.	5	10.68	banking	
29.	5	10.68	rational	
30.	10	10.65	housing	“Construction” context
31.	9	10.46	external	
32.	4	9.84	homes	
33.	8	9.56	complex	
34.	7	9.54	patterns	
35.	6	9.23	deployment	
36.	5	9.19	codes	
37.	5	9.19	solutions	
38.	4	8.88	his	
39.	6	8.72	outside	
40.	9	8.72	job	
41.	34	8.68	research	*Methodologically Related*
42.	5	8.55	relative	
43.	12	8.53	organizations	virtual organization, individuals and organizations
44.	8	8.45	identity	
45.	13	8.30	organizational	organizational systems, organizational change, organizational culture
46.	3	8.23	arena	
47.	3	8.23	Beijing	
48.	3	8.23	dwelling	
49.	3	8.23	neighbourhood	
50.	3	8.23	normative	
51.	3	8.23	outlaw	
52.	3	8.23	qual	

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
53.	3	8.23	workgroup	
54.	5	7.97	attitudes	
55.	5	7.97	virtual	
56.	10	7.93	processes	processes of abstraction, social process, governance process, decision-making process
57.	6	7.79	intentions	
58.	7	7.52	identification	
59.	7	7.52	outcomes	
60.	8	7.47	user	
61.	5	7.43	standard	
62.	4	7.35	shaping	
63.	4	7.35	vendors	
64.	3	7.13	bases	
65.	3	7.13	hospitals	
66.	3	7.13	prompt	
67.	3	7.13	punishment	

Mature cluster (C2)

The mature cluster has only 12 significant keywords, in alignment with the assumption that this cluster characteristically is "mainstream" that is not different from the corpus averages.

Table 9. *Keyword keyness of the Mature Cluster (C2) in the sample.* [Created by the author.]

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
1.	57	22.545	health	health care and social security
2.	34	17.074	attachment	children attachment, attachment to the house
3.	28	12.809	disclosure	information disclosure and non-disclosure, property disclosure, ISIS
4.	25	12.446	home	working from home, home-based work
5.	16	9.809	family	family in the social setting (not related)
6.	44	9.577	different	different colleagues, different environments, different IT, different disciplines, different mechanisms
7.	117	9.291	IT	IT as a security problem, IT-based signals, IT features, cooperation with IT vendors, IT professionals
8.	10	7.646	drug	Medical terms, *Not Related*
9.	10	7.646	mother	Social terms, not related.
10.	23	7.457	ICT	ICT use, ICT innovation, ICT adoption, ICT operations
11.	17	7.379	children	children safety and security

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
12.	21	7.077	communities	different IS communities, communities of practice, diverse communities, on-line communities

There are two interesting general features however, the first one is the non-related health and social security topics, which naturally need to be omitted from information security context analysis, but apart from this we can also find more "classic" IS topics such as the IT and ICT terms, the questions of use and adoption along with the diversity issues of technology, people and communities ("different").

High Potential Cluster (C3)

Keyness in the high potential cluster indicates the major difference of these abstracts firstly around the phrases of teaching, instruction and scripts. By running the concordance analysis of these terms, we can see however, that some of these contributions are strictly related to education. The cluster is more relevant in terms of the contributions of Social Media or Social Networking Cites, which is a rather important stream of research in information security. Closely coupled with this the term of information sharing and social capital.

Similarly, safety in a very broad context seems to be a relevant term, followed by the topics of privacy which has not gained keyness in other clusters.

Similarly, to the terms of teaching, food security—although a very relevant area of security management—needs to be omitted from further analysis due to its distance from information security.

Table 10. *Keyword keyness of the High Potential Cluster (C3) in the sample.* [Created by the author.]

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
1.	28	36.921	teachers	teachers reactions to scripts
2.	105	31.851	we	
3.	16	19.686	scripts	scripts in education
4.	14	17.955	instruction	instruction in the educational context
5.	13	17.627	SNS	Social Networking Sites, sharing behaviour, SNS users, ethical challenges, norms of using SNS, self-presentation
6.	12	16.271	scripted	scripted instruction method
7.	23	16.079	sharing	information sharing, sharing behaviour, knowledge sharing, process of social sharing
8.	9	12.204	millennials	
9.	26	12.147	network	social capital, SNS, social network analysis, network monitoring, management protocol, network operators, network structure, learning network, emerging network

	Freq.	Keyness	Keyword	Verification with concordance analysis KeyWord in Context (KWIC)
10.	31	11.68	safety	safety management, safety leadership, safety outcomes, safety participation, safety information
11.	10	11.615	illegal	illegal immigrants
12.	8	10.848	ca	
13.	8	10.848	eco	
14.	8	10.848	froebelian	
15	8	10.848	montessori	
16.	8	10.848	projection	
17.	8	10.848	snapchat	
18.	10	10.762	insecure	insecure information flow, insecure group conditions
19.	18	10.001	method	Related to research methodology
20.	22	9.711	energy	future energy systems, long term energy security, energy industries
21.	7	9.492	deduplication	
22.	7	9.492	humanitarian	
23.	7	9.492	ISDB	
24.	7	9.492	kindergarten	
25.	7	9.492	procedural	
26.	7	9.492	wri	
27.	9	9.444	abuse	
28.	9	9.444	scenario	
29.	27	9.081	food	food security—*Not Related*
30.	26	8.52	perceived	perceived usefulness of SNS, perceived privacy risk, perceived control and barriers
31.	28	8.512	privacy	privacy SNS users, privacy concerns, privacy vs publicity
32.	7	8.495	born	
33.	7	8.495	dissatisfaction	
34.	7	8.495	fisheries	
35.	6	8.136	congress	
36.	6	8.136	healthy	
37.	6	8.136	intergroup	
38.	6	8.136	neutralization	
39.	26	7.962	users	users are concerned, potential users, users permissions
40.	7	7.616	investigations	
41.	8	7.4	Facebook	
42.	6	7.149	clustering	
43.	6	7.149	conservation	

Recent mainstream cluster (C4)

In Table 11 from the 4th row the keyness log likelihood is only significant on the 1% level, so I did not execute concordance analysis, the key differences of this cluster are clearly seen from the keyword list. Discussion and research is focusing on all kinds of managerial issues, business and entrepreneurship and organizations.

Table 11. *Keyword keyness of the Mainstream Cluster (C4) in the sample.* [Created by the author.]

	Freq.	**Keyness**	**Keyword**	**Verification with concordance analysis KeyWord in Context (KWIC)**
1.	58	11.133	cloud	cloud services adaption, cloud storage, cloud service providers, benefits and risks of cloud computing
2	138	7.995	management	information security management, knowledge management, management of…, disaster management, environmental management
3.	2578	7.333	the	Grammatically interesting.
4.	23	6.566	entrepreneurs	
5.	23	6.566	malls	
6.	25	6.535	shopping	
7.	76	6.52	construction	understand the problem of social construction, discursive construction of security, construction of regulatory institutions
8.	63	6.285	business	
9.	28	5.773	supply	
10.	28	5.294	computing	
11.	18	5.139	cilicia	historical research—*Not Related.*
12.	17	4.853	rough	historical research—*Not Related.*
13.	34	4.773	organisations	
14.	89	4.716	factors	
15.	35	4.649	media	
16.	22	4.606	border	historical research—*Not Related.*
17.	15	4.282	indexes	
18.	15	4.282	smart	
19.	17	4.26	schemes	

As we identified in the cluster analysis, most papers appear in the business and management subject area listing, so this result is according to expectations. Apart from management, the cloud topic appears in this cluster in the context of service, storage and management adoption. It is interesting to note, that a special form of cloud computing—the SaaS topic—shows with very high frequency in C1, the high impact cluster.

Visualization of Clusters

In Figure 11 the visualization of the full corpus of the abstracts can be seen, followed by a zoom to the centre in Figure 12.

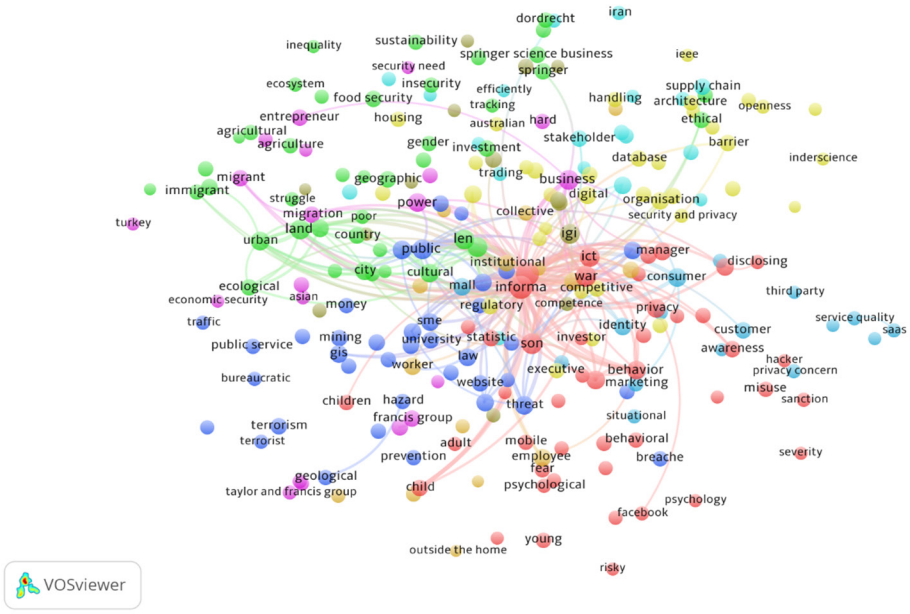

Figure 11. *Visualization of the full corpus (C1–C4 and top three cited papers).*
[Created by the author.]

The centre of the cluster-network shows terms such as information security, ICT, awareness, privacy; and other areas also appear such as national security, law, cyber or identity. In Figure 13, Figure 14, Figure 15 and Figure 16 the four main clusters are visualized—the outlier three-element cluster did not contain enough words in the abstracts to run the analysis. These series of figures provide a more structured insight to the discourses on information security.

The high impact CL1 cluster indicates discourses on three main word clusters, a core security topic, a managerial/organizational topic and a cultural/environmental topic.

CL2, the mature paper cluster holds much more abstracts and Figure 14 is a richer word cloud network. The major differentiators which we can see are the discussion on social securities in family setting (child, mother etc.), a broader set of topics on technology (architecture, ICT, technology) and business. What is also important in this cluster is the appearance of public administration, bureaucracy and criminal justice.

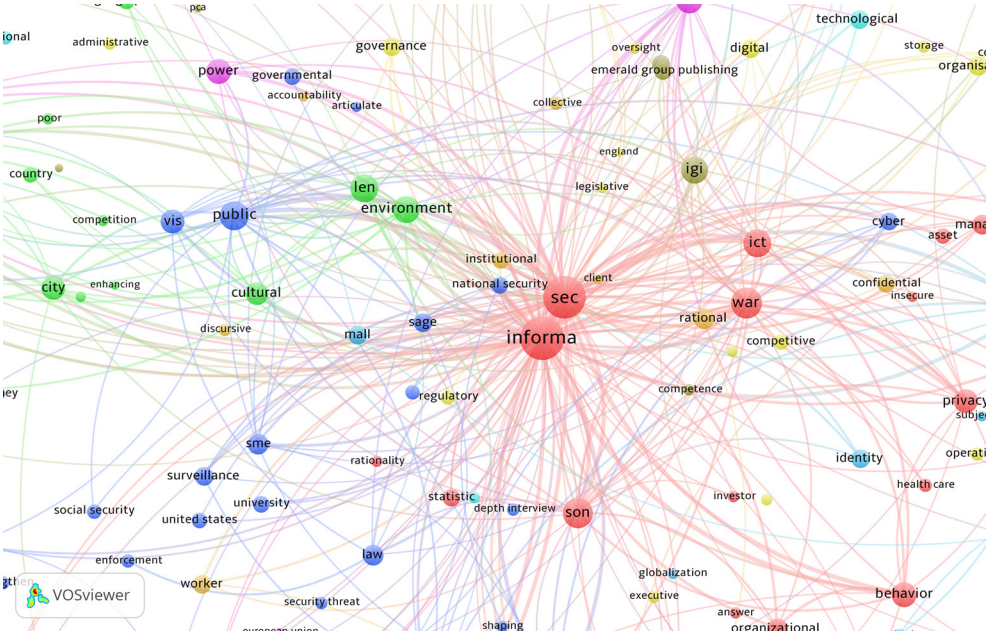

Figure 12. *Centre of the corpus network (information security).* [Created by the author.]

In CL3, what we called high potential cluster, Figure 15 shows also some new terms such as surveillance, security and privacy, employee and ethical. CL2 and CL3 both indicated topics of urban development and "city;" juxtaposing these terms with the keyness analysis we see that the smart city discourses appear in these clusters.

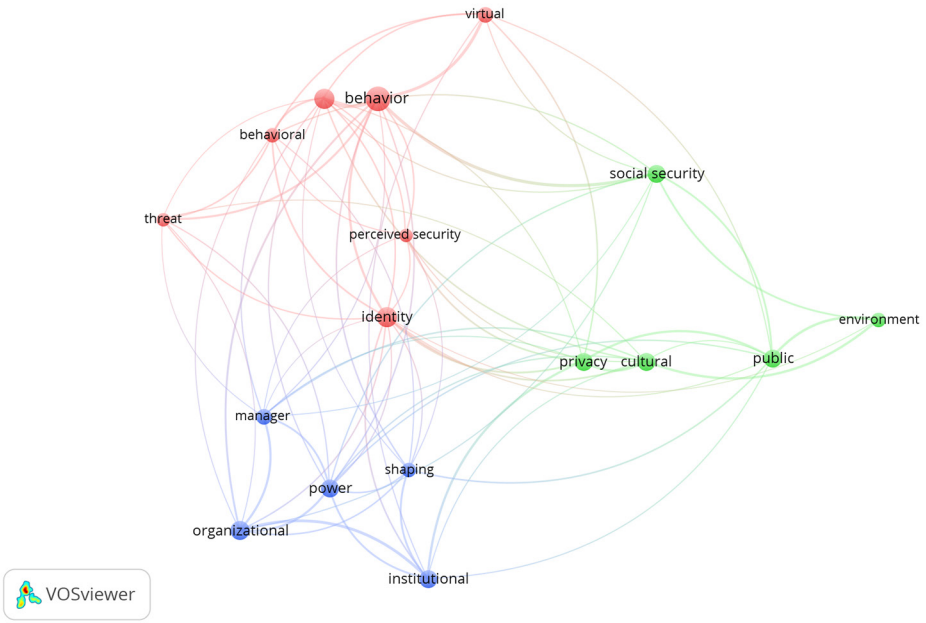

Figure 13. *VOS viewer visualization of CL1 text—high impact cluster.* [Created by the author.]

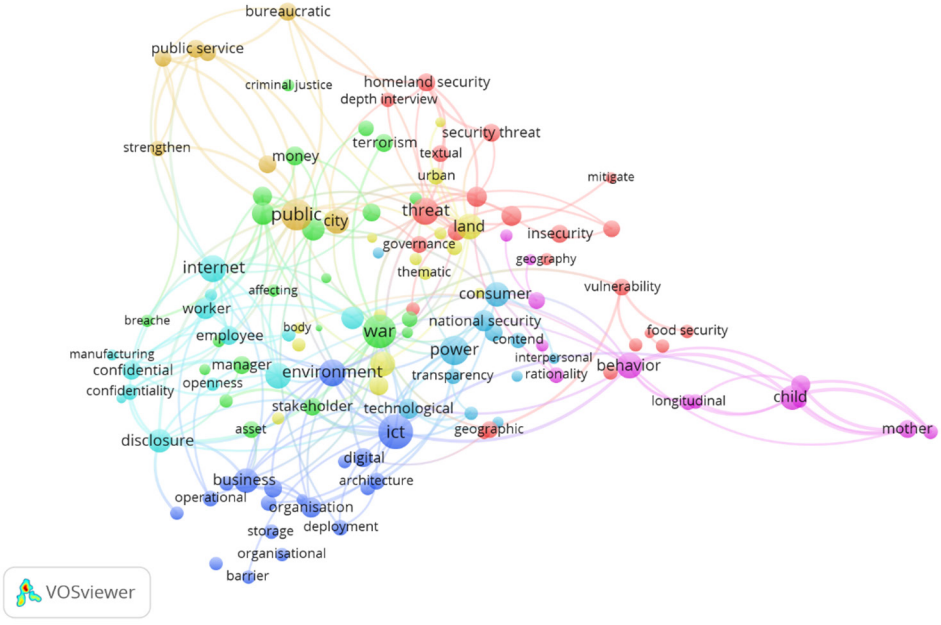

Figure 14. *Visualization of CL2 text Mature Cluster.* [Created by the author.]

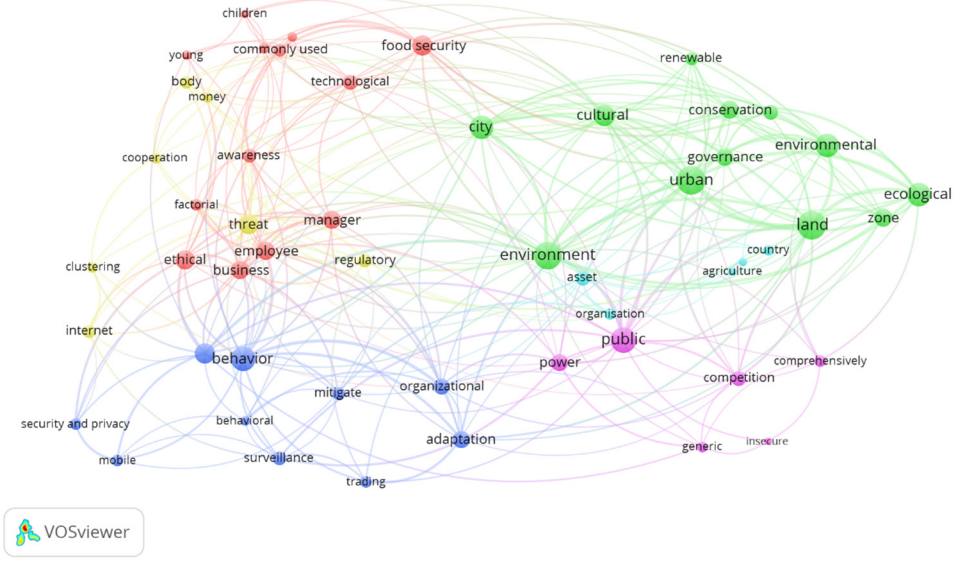

Figure 15. *Visualization of C3 text—High Potential Cluster.* [Created by the author.]

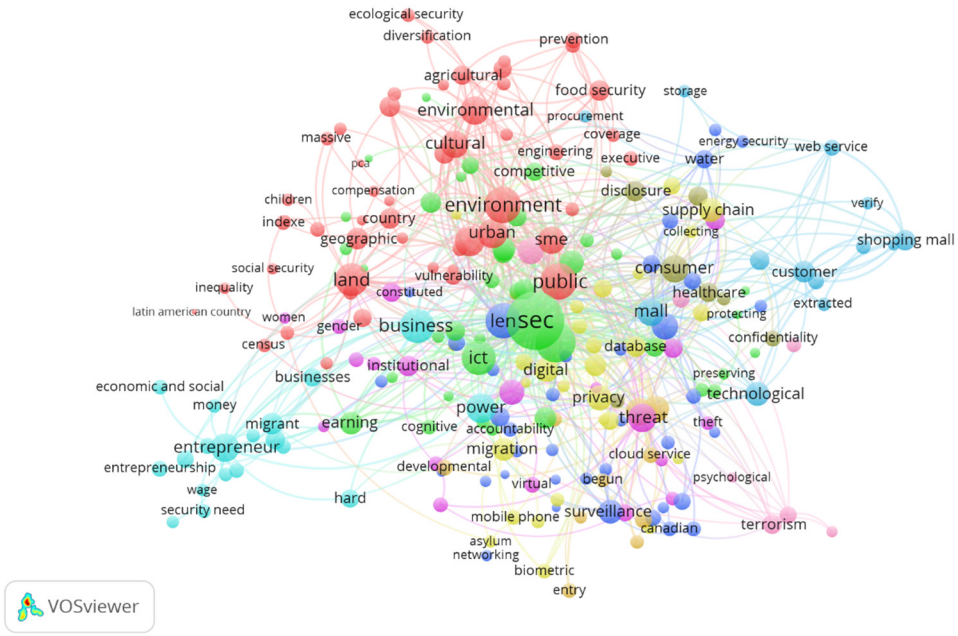

Figure 16. *Visualization of C4 text—Mainstream Cluster.* [Created by the author.]

Figure 16 visualizes the most populated mainstream cluster; discussion which appear in the relatively low H-index papers and probably have achieved the maturity of citation level. This figure is the most similar to the entire corpus: however, issues of healthcare and the family security topics are missing—therefore this cluster can be considered more relevant to the notion of "information security", epistemology related to its cyberspace and ICT context.

Results of Word Clustering and N-Gram Analysis

In order to further contextualize the corpus, I ran a simple word clustering analysis using AntConc clustering and N-gram applications. Then, based on these results which are presented in Table 12, Table 13, Table 14, Table 15, Table 16 I checked the highest frequency clusters in their concordance and for the purpose of further research I summarized them in the Appendix. These outputs, I hope, serve as useful inputs for a more specific literature analysis in the areas of how information security gets socially constructed.

The technique of cluster analysis in AntConc takes a search word, set by the analyst, and lists all the word cluster containing this word according to the defined minimum and maximum cluster element. As it is indicated in the Appendix, I chose minimum 2 and maximum 4 words in a cluster. N-gram analysis, contrary to cluster, does not require a search word—this algorithm basically lists all the clusters with minimum 2 and maximum 4 members in our case. As the Appendix shows, in our corpus there has been 2,378 such cluster types and 27,813 different so-called N-Gram tokens, that are separate two, three, four-word phrases. For handling this huge amount of data, I applied an initial filtering of those clusters which do not appear more than 5 times in the whole corpus.

When the N-gram result was received, I ran a word search on the keywords of my interest: information in Table 12, security in Table 13, social in Table 14, construction in Table 15, and technology in Table 16. These tables contain the frequency of the clusters, the range which is showing in how many text files of the entire corpus can the cluster expression be found, and probability indicates the likelihood that the second word in the cluster follows the first. In the Appendix the concordance tables indicate the corpus files, which are useful for checking which specific papers, in which of our five structural clusters have been dealing with the particular issue. These concordance analyses were only run for the high-frequency word clusters—in most cases where the frequency was higher than 10.

Given the self-explanatory nature of the textual result, I do not present comments to the following tables, the reader is invited to go through the terms, and counter position it with the more detailed concordance analysis in the Appendix. I draw the main conclusions in the next, last section of the paper.

Table 12. *N-Gram Results: Information.* [Created by the author.]

	Freq.	**Range**	**Prob**	**N-Gram Result:** Information
911	20	4	0.01	information about
912	7	4	0.003	information about the
913	43	4	0.021	information and

	Freq.	Range	Prob	N-Gram Result: Information
914	16	4	0.008	information and communication
915	9	4	0.004	information and communication technologies
916	5	4	0.002	information and communication technology
917	5	4	0.002	information assets
918	5	3	0.002	information disclosure
919	6	3	0.003	information exchange
920	7	2	0.003	information for
921	14	3	0.007	information in
922	15	4	0.007	information is
923	6	3	0.003	information management
924	25	4	0.012	information on
925	5	2	0.002	information on the
926	5	3	0.002	information personal
927	7	3	0.003	information processing
928	5	2	0.002	information provided
929	6	3	0.003	information provision
930	7	3	0.003	information quality
931	98	4	0.048	information security
932	6	3	0.003	information security and
933	6	3	0.003	information security is
934	15	3	0.007	information security management
935	5	2	0.002	information security policies
936	8	3	0.004	information security policy
937	17	3	0.008	information sharing
938	5	2	0.002	information sharing and
939	8	2	0.004	information society
940	6	3	0.003	information sources
941	19	4	0.009	information system
942	43	5	0.021	information systems
943	5	3	0.002	information systems is
944	5	3	0.002	information systems security
945	32	5	0.016	information technology
946	9	3	0.004	information technology it
947	5	3	0.002	information that
948	6	3	0.003	information the
949	7	3	0.003	information to
950	5	4	0.002	information was

Table 13. *N-Gram results: Security.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: Security
1546	103	5	0.051	security and
1547	9	4	0.004	security and privacy

	Freq.	Range	Prob	N-Gram Result: Security
1548	6	2	0.003	security and the
1549	7	4	0.003	security are
1550	6	3	0.003	security as
1551	5	2	0.002	security at
1552	5	2	0.002	security at the
1553	5	4	0.002	security but
1554	5	4	0.002	security has
1555	22	4	0.011	security in
1556	7	2	0.003	security in the
1557	5	2	0.002	security information
1558	12	4	0.006	security is
1559	15	4	0.007	security issues
1560	21	4	0.01	security management
1561	6	3	0.003	security measures
1562	6	2	0.003	security needs
1563	31	4	0.015	security of
1564	7	3	0.003	security of the
1565	11	5	0.005	security policies
1566	5	3	0.002	security policies and
1567	13	4	0.006	security policy
1568	6	2	0.003	security practices
1569	13	3	0.006	security requirements
1570	5	4	0.002	security research
1571	5	2	0.002	security risk
1572	5	2	0.002	security risks
1573	14	4	0.007	security the
1574	6	2	0.003	security threats
1575	7	3	0.003	security to

Table 14. *N-Gram results: Social.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: SOCIAL
1604	24	4	0.028	social and
1605	5	3	0.006	social and environmental
1606	10	2	0.012	social capital
1607	6	3	0.007	social information
1608	5	2	0.006	social learning
1609	7	3	0.008	social media
1610	7	3	0.008	social network
1611	8	3	0.009	social policy
1612	12	3	0.014	social representations
1613	6	2	0.007	social representations of
1614	20	4	0.024	social security

	Freq.	Range	Prob	N-Gram Result: SOCIAL
1615	9	3	0.011	social support
1616	5	2	0.035	society the
1617	10	2	0.128	socio economic
1618	11	3	0.141	socio technical

Table 15. *N-Gram Results: Construction.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: Construction
456	6	3	0.018	construction and
457	7	2	0.021	construction industry
458	35	3	0.105	construction of
459	9	3	0.027	construction of a
460	11	3	0.033	construction of the

Table 16. *N-Gram Results: Technology.* [Created by the author.]

	Freq.	Range	Prob	N-Gram Result: Technology
1697	6	3	0.035	technologies and
1698	6	2	0.035	technologies of
1699	16	4	0.045	technology and
1700	9	3	0.025	technology in
1701	7	2	0.02	technology is
1702	9	3	0.025	technology it

Conclusions, Implications and Limitations

We may start summarizing the conclusions by stating that "information security" and "social construction" in the SCOPUS domain offers a wide range of literature in the social sciences and related subject areas, even if the technical areas are excluded from the search.

By categorizing the academically classified journal submissions according to the journals H-index, SJR Q1–Q4 ranking and the individual papers' citations, we classified our sample to five—so-called structural—clusters. First, I identified the top four highest cited papers, amongst which one was omitted due its lack of relevance. The remaining three were published in Decision Support Systems, Information Systems Research and MIS Quarterly. Two of them deal effectively with ISec and explore the concept of deterrence and fear; and one deals with trust especially in the context of e-commerce.

After running a two-step cluster analysis on the remaining papers, I received four other clusters; one containing highly citied and high H-index articles (CL1 – High Impact Cluster), second populating relatively older papers with high references (CL2 – Mature Cluster), a third with relatively recent papers published in high H-index outlets (CL3 – High Potential Cluster) and finally a fourth published in mainstream journals and achieving a saturation with their citation (CL4 – Maturity Cluster). The textual analysis of the abstracts in these

structural cluster reveals a pattern of ISec discourses characterized by key words and textual clusters.

Running N-Gram analysis with AntConc in the range of 2–4 words has resulted in 2,378 N-Gram types and 27,813 N-Gram tokens, while creating textual clusters with the help of CoWo and VosViewer produced 245 nouns organized into 9 clusters with 9,680 connections of co-occurrence.

In the top three papers cluster topics revolve around misuse of information systems, the concept of fear and trust. These papers take a strongly end user viewpoint to ISec through the lens of the term computer. Keyness in this group is also determined by the use of sanctions and their severity regarding social influences.

Papers in the high impact cluster (CL1) demonstrate keyness in terms of deeper discussions in behavioural analysis and patterns. People are also centred, especially in the context of technology relationship and becoming victims of security breaches. I found also high keyness key words as culture, trust and the general concept of perception in connection with several terms such as privacy, importance, and security. This cluster is unique by focusing on organizations and processes in general and in the context of virtual organizations and individual accounts, as well. An interesting stream of research got assigned to this structural cluster, and that is the documentation of the 2008 Obama campaign, exploiting social media the first time in the history of political elections.

The mature cluster (CL2) is adding value in terms of information disclosure and non-disclosure topics, and more frequent use of the terms IT and ICT in many contexts. These are the papers which deal mostly with the exposure of communities, especially in the context of their differences and diversities. Differentiation of this cluster was also stemming from a non-related stream of research which is using information security in a different context: these are the papers in healthcare and social-security issues of families. These papers need to be omitted from further analysis.

High potential cluster (CL3) is different in the focusing on discourses related to social networking and social media, which is also closely intertwined with information sharing and networks. Users' trust, privacy and perception are also high level of keyness in this cluster. We found non-related differentiators as well; the topics of teaching, scripts and education—in non-security related cases—have to be left out from further analysis. The situation is similar, although less obvious, in the cases of energy and food security, which are more connected to general security problems in our modern social environment, but they are also distant from ISec in its ICT context.

The last and most populated cluster—the mainstream cluster (CL4)—logically has the least number of key words with high keyness value, being close to the word list of the corpus. However, the terms management and construction appear mostly in this cluster in connection with security, regulatory institutions and social construction. There are some historical papers—discussing security of states in ancient Roman times—which need to be left out, due to their lack of topical relevance.

Textual clusters reveal two other important discourses in ISec, which can be seen from Figure 11 to Figure 16. The first of these textual clusters is connecting the topics of national security, governments, homeland security, public administration, law enforcement and terrorism. The second embraces the areas of urban, cities, smartness, environment and ecosystems.

As a conclusion I hope researches find the clusters and the organized topics relevant to anchor their research to them, or to find ways to more easily identify where the research adds value to the already existing body of knowledge in the ISec domain. Naturally, these endeavours might only be valid within the limitations of this study, which at the same time gives place to implications for further improvement of research.

Amongst these limitations I have to mention the need to extend the analysis to full papers not only texts and get a deeper insight by running a co-citation analysis to find more connections between the topics, authors and journal styles. Secondly, keywords need to be refined—cybersecurity for instance is also an important phrase which might reveal other types of contributions in the area. Finally, the range of publication outlets might also be extended, indexed books, conference proceedings also contain threads of relevant discussions and worthy for analysis.

Despite these limitations the analysis is convincing that social construction of technology framework reveals new domains of discussion about information security and a large body of literature is available to create programmable actions addressing the complex challenges of information security.

Appendix. Results of N-Gram cluster analysis.

Minimum words: 2. Maximum words: 4. Minimum Range: 2. Minimum frequency: 5. N-Gram types: 2,378, N-Gram Tokens: 27,813.

	Concordance Analysis Results: information and communication	**Range**
1	… to empower managers, IS engineers, and information and communication technology users wit	abstract_cluster_1.txt
2	…actices surrounding hospitals' new investments in information and communication technologies tend to	abstract_cluster_1.txt
3	…networks. For the Internet and other information and communication technologies to sup…	abstract_cluster_2.txt
4	…of surveillance countermeasures. In this context, information and communication technologies have be	abstract_cluster_2.txt
5	…is possible to create multiple identities. Information and communication technologies were se	abstract_cluster_2.txt
6	…and influenced by the degree that information and communication technology are part	abstract_cluster_2.txt
7	…manipulation of sensible information. These new information and communication technologies (ICT)	abstract_cluster_2.txt
8	…fossil fuel peak. The effects of information and communication technologies and tec	abstract_cluster_3.txt
9	…critical understanding of the role of information and communication technology (ICT) in	abstract_cluster_3.txt
10	Advances in information and communication technologies have le …	abstract_cluster_4.txt

11	…licies. Through the proposed approach, education, information and communication are seen as keys	abstract_cluster_4.txt
12	…, which is a multidimensional model. Information and communication technologies (ICTs)	abstract_cluster_4.txt
13	…reluctant to support proper freedom of information and communication. In short, they have	abstract_cluster_4.txt
14	…effort to address issues related to information and communication technology. Technol	abstract_cluster_4.txt
15	…factors that influence the adoption of Information and Communication Technologies (ICT) b	abstract_cluster_4.txt
16	…and the latter's use of information and communication technology (ICT) in	abstract_cluster_4.txt

	Concordance Analysis Results: information technology	**Range**
1	company initiatives, especially those involving information technology. The interweaving of top-do	abstract_cluster_1.txt
2	ICT diffusion dynamics within three large information technology (IT) literate Australian co	abstract_cluster_2.txt
3	in their OC by implementing different information technology (IT) features that should s	abstract_cluster_2.txt
4	studies pay any serious attention to information-technology-related security issues. Th	abstract_cluster_2.txt
5	Dyson, M. Hendriks, S. Grant (Eds.) Information technology and indigenous people, Idea	abstract_cluster_2.txt
6	service, and health workers. Innovations in information technology in the past decade or	abstract_cluster_2.txt
7	ompetitive advantage for organisations worldwide, information technology professionals, consumers an	abstract_cluster_2.txt
8	service, and health workers. Innovations in information technology in the past decade or	abstract_cluster_2.txt
9	become known as India's premier information technology (IT) hub and a magnet	abstract_cluster_2.txt
10	roles of two different criminal justice information technology (IT) security systems-that	abstract_cluster_2.txt
11	systems are discussed. Past research on information technology (IT) security training and	abstract_cluster_3.txt
12	the use value of domain ontology. Information technology has dramatically increased	abstract_cluster_3.txt
13	costs and expand markets by deploying information technology through new and existing bu	abstract_cluster_3.txt
14	findings to decrease CA occurrences. Unethical information technology (IT) use, related to activi	abstract_cluster_3.txt
15	and makes extensive use of spatial information technology and can be widely applied	abstract_cluster_3.txt
16	to the CAI. Economic growth and information technology development has stimulated	abstract_cluster_4.txt

	Concordance Analysis Results: information technology	Range
17	agencies to adopt innovative forms of information technology in order to survive and	abstract_cluster_4.txt
18	electronic commerce (B2C e-commerce) information technology applications in order to ob	abstract_cluster_4.txt
19	with which to interpret cloud-based information technology outsourcing. Purpose – Emp	abstract_cluster_4.txt
20	support and reinforce the contributions of information technology to the development process.	abstract_cluster_4.txt
21	turn to (b) key imperatives of information technology-development linkages and th	abstract_cluster_4.txt
22	knowledge society through the provision of information technology (IT) green services. Furthe	abstract_cluster_4.txt
23	factors are presented. These factors are information technology (IT) tools, information sys	abstract_cluster_4.txt
24	of cyberspace. Failure to engage with information technology, and globally mediated sex,	abstract_cluster_4.txt
25	organizational flexibility. This study presents information technology executive's perspective and	abstract_cluster_4.txt
26	and management, namely, law, economics, sociology, information technology and information resources m	abstract_cluster_4.txt
27	that, for example, advanced equipment and information technology can be harnessed to handle	abstract_cluster_4.txt
28	which are (electronic trust, financial resources, information technology infrastructure, perceived r	abstract_cluster_4.txt
29	Computing opens a new chapter in Information Technology. It has its roots in	abstract_cluster_4.txt
30	advantages in certain effects of globalization, information technology, scientific and technical p	abstract_cluster_4.txt
31	such as airports, special economic zones, information technology parks, real estate ventures	abstract_cluster_4.txt
32	practice of IS security are discussed. Information technology executives strive to align	asbtract_big_three.txt

	Concordance Analysis Results: ICT in, ICT and	Range
1	new ICT unless effective use of ICT and performing operations electronically (eBus	abstract_cluster_2.txt
2	awareness, often combined with mistrust regarding ICT and ICT service providers, costs, lack	abstract_cluster_2.txt
3	service providers, costs, lack of internal ICT and management knowledge, Network infrastructu	abstract_cluster_2.txt
4	particular, to engage more fully with ICT and develop sustainable business practices: 1)	abstract_cluster_2.txt
5	in Colombia regarding the adoption of ICT and independent variables identified in the	abstract_cluster_4.txt
1	new information and communication technologies (ICT), in continuous development, have expanded als	abstract_cluster_2.txt

	Concordance Analysis Results: ICT in, ICT and	Range
2	role of information and communication technology (ICT) in humanitarian action, this article explores	abstract_cluster_3.txt
3	prism through which the role of ICT in humanitarian action is explored is	abstract_cluster_3.txt
4	policies that foster the implementation of ICT in SMEs based on an analysis	abstract_cluster_4.txt
5	use of information and communication technology (ICT) in business processes. Also, the characterist	abstract_cluster_4.txt

	Concordance Analysis Results: technologies of, technology in	Range
1	over time, have long been governmental technologies of control. I further argue that	abstract_cluster_2.txt
2	assesses the threat assessments produced through technologies of risk management and the development	abstract_cluster_2.txt
3	management and the development of new technologies of surveillance. Third it describes t	abstract_cluster_2.txt
4	article explores how biometrics function as technologies of embodiment that both redefine and	abstract_cluster_2.txt
5	technology is one of the core technologies of IoT deployments in the healthcare	abstract_cluster_4.txt
6	then move on to the newer technologies of social media and apps. This	abstract_cluster_4.txt
1	or change individuals' initial trust in technology. In this study, a research model	abstract_cluster_1.txt
2	that focused on the use of technology in supporting people with dementia to	abstract_cluster_1.txt
3	and health workers. Innovations in information technology in the past decade or two	abstract_cluster_2.txt
4	framework for understanding the role of technology in intelligence. The focus is on	abstract_cluster_2.txt
5	and health workers. Innovations in information technology in the past decade or two	abstract_cluster_2.txt
6	the various security requirements of RFID technology in IoT, many RFID authentication scheme	abstract_cluster_4.txt
7	to adopt innovative forms of information technology in order to survive and flourish.	abstract_cluster_4.txt
8	try to overcome such conflicts: through technology. In West Africa, the secure 'Seahorse'	abstract_cluster_4.txt
9	work that analyses the implementation of technology in enterprises in emerging countries, t	abstract_cluster_4.txt

	Concordance Analysis Results: technology and, technologies and	Range
1	ing personality, cognitive, calculative, and both technology and organizational factors of the insti	abstract_cluster_1.txt

	Concordance Analysis Results: technology and, technologies and	Range
2	M. Hendriks, S. Grant (Eds.) Information technology and indigenous people, Idea Group Publi	abstract_cluster_2.txt
3	sites facilitates the distribution of military technology and strategy across numerous scales of	abstract_cluster_2.txt
4	subject to the coercive power of technology, and appropriate the narrow technologic	abstract_cluster_2.txt
5	reflect a broader celebratory ethos of technology and commerce. To understand technologie	abstract_cluster_2.txt
6	GII. As a result, the associated technology and information systems become targets	abstract_cluster_2.txt
7	National Institute of Standards and Technology) and academic databases (e.g. Google	abstract_cluster_3.txt
8	makes extensive use of spatial information technology and can be widely applied to	abstract_cluster_3.txt
9	as spokespersons for the interactive data technology and the retail investor. We examine	abstract_cluster_4.txt
10	is an attempt to introduce a technology and a business model for centralising	abstract_cluster_4.txt
11	was affected through advances in modern technology and promises of wealth and material	abstract_cluster_4.txt
12	cyberspace. Failure to engage with information technology, and globally mediated sex, is discusse	abstract_cluster_4.txt
13	namely, law, economics, sociology, information technology and information resources management fo	abstract_cluster_4.txt
14	source, intrinsic criteria of data, communication technology, and integrity among various criteria.	abstract_cluster_4.txt
15	It has its roots in internet technology, and like the Internet, it is	abstract_cluster_4.txt
16	in the area of science and technology and integrated forecasting of socio-eco	abstract_cluster_4.txt
1	governance of populations occurs through new technologies and techniques of social control. Con	abstract_cluster_2.txt
2	driven by continued demographic growth, new technologies and the desire of many as	abstract_cluster_2.txt
3	especially in the light of developing technologies and the growth of e-commerce.	abstract_cluster_2.txt
4	The effects of information and communication technologies and technological innovation after en	abstract_cluster_3.txt
5	of life, one building on information technologies and critical functions of infrastruct	abstract_cluster_4.txt
6	1970s, to current debates over emerging technologies and global innovation, the academic c	abstract_cluster_4.txt

	Concordance Analysis Results: information systems and information system	Range
1	This paper extends an area of information systems research into a marketing of	abstract_cluster_1.txt
2	developed. Recent trust research in the information systems (IS) field has described trust	abstract_cluster_1.txt
3	lementing e-government systems and organizational information systems in general. This exploratory s	abstract_cluster_1.txt
4	to be „the weakest link" in information systems (IS) security management in th	abstract_cluster_1.txt
5	and action and the security of information systems are increasingly a focus of	abstract_cluster_1.txt
6	identifies four security issues (access to Information Systems, secure communication, securit	abstract_cluster_1.txt
7	ation, security management, development of secure Information Systems), and examines the extent to	abstract_cluster_1.txt
8	three viewpoints: a meta-model for information systems, the research approaches used,	abstract_cluster_1.txt
9	for studying information security from an information systems viewpoint, with respect to res	abstract_cluster_1.txt
10	and philosophy), are particularly necessary. Most information systems research takes for granted the	abstract_cluster_1.txt
11	uences shape organizational actions for improving information systems security. A case study of	abstract_cluster_1.txt
12	also enrich existing research models on information systems continuance. Moreover, the Saa	abstract_cluster_1.txt
13	nformation security awareness of staff, including information systems decision makers, in higher edu	abstract_cluster_1.txt
14	insidious motivators for organizations to adopt information systems security (ISS) approaches. Ext	abstract_cluster_1.txt
15	paper investigates the social representations of Information Systems (IS) security of different com	abstract_cluster_2.txt
16	discussed the framework and value of information systems (IS) security standards and ce	abstract_cluster_2.txt
17	the evolution of an Ireland-India information systems offshoring relationship. By tr	abstract_cluster_2.txt
18	and agenda in the development of information systems to support the process of	abstract_cluster_2.txt
19	adulthood. Digital technologies like geographic information systems (GIS) pose new problems for	abstract_cluster_2.txt
20	a research agenda, Cartography and Geographic Information Systems. 22 (1) (1995) 5-16]. Such imp	abstract_cluster_2.txt
21	States Bureau of Indian Affairs, geographic information systems, and cultural assimilation, in	abstract_cluster_2.txt
22	coherent system of controls consisting of information systems and procedures. This system-ba	abstract_cluster_2.txt

	Concordance Analysis Results: information systems and information system	Range
23	of this article is to identify information systems security risks in local govern	abstract_cluster_2.txt
24	information. Some of the most important information systems are those that produce the	abstract_cluster_2.txt
25	a result, the associated technology and information systems become targets for information	abstract_cluster_2.txt
26	on increasing the development of secure information systems. In particular, we introduce a	abstract_cluster_2.txt
27	related to the development of secure information systems; we identify limitations of ex	abstract_cluster_2.txt
28	discipline for the development of secure information systems, its principles and the challe	abstract_cluster_2.txt
29	of the most widespread problems affecting information systems. Security breaches at companie	abstract_cluster_2.txt
30	problem. For prompt deployment in legacy information systems, it would be desirable to	abstract_cluster_3.txt
31	in terms of the threat to information systems (IS) security. While there is	abstract_cluster_3.txt
32	is related to the misuse of information systems resources) and a three-item	abstract_cluster_3.txt
33	intent. Market surveillance systems (MSSs) are information systems that monitor financial markets	abstract_cluster_3.txt
34	factors are information technology (IT) tools, information systems integration and information se	abstract_cluster_4.txt
35	given the highest importance to the information systems integration. Then, IT tools an	abstract_cluster_4.txt
36	considered. In addition, findings indicate that information systems integration has the highest co	abstract_cluster_4.txt
37	in supply chain, key indices for information systems integration and information se	abstract_cluster_4.txt
38	Latin American countries like Chile. Hospital information systems (HISs) accelerate hospital-rel	abstract_cluster_4.txt
39	nity demographic and discourse data, geographical information systems maps, and comprehensive photog	abstract_cluster_4.txt
40	to identify what the most effective information systems are for the self-builders	abstract_cluster_4.txt
41	consumers' trust. Intentional insider misuse of information systems resources (i.e., IS misuse)	asbtract_big_three.txt
42	work from criminology, social psychology, and information systems. The model posits that user	asbtract_big_three.txt
43	findings of this research contribute to information systems security research, human-compu	asbtract_big_three.txt
1	trust in a more complex, organizational information system, there are a number of	abstract_cluster_1.txt

	Concordance Analysis Results: information systems and information system	Range
2	to hinge on top management championing information system security initiatives and propag	abstract_cluster_1.txt
3	of risk and its effect on information system (IS) risk management. Design/me	abstract_cluster_2.txt
4	they require new business, operational and information system models that extend 30 years or	abstract_cluster_2.txt
5	project was the creation of an information system to ascertain and characterise a	abstract_cluster_2.txt
6	and the Police Computer Network and Information System of Turkey (POLNET). By delineat	abstract_cluster_2.txt
7	technology (remote sensing (RS) and geographic information system (GIS). We constructed an ecolo	abstract_cluster_3.txt
8	source of the security of an information system, rather than rational design ch	abstract_cluster_3.txt
9	The main modification involved integrating an information system with the MBWA in order	abstract_cluster_3.txt
10	as many tours as managers). The information system collected information about saf	abstract_cluster_3.txt
11	on examples relating to the Visa Information System, I show that processes of	abstract_cluster_4.txt
12	data on kin connectivity with geographical information system (GIS) data in a rural	abstract_cluster_4.txt
13	risk assessment (ERA) based on geographic information system (GIS) was built. To identify	abstract_cluster_4.txt
14	Electronic health network (EHN) is an information system providing functions involved in	abstract_cluster_4.txt
15	prefer to use either the Integrated Information System (IIS) that the Ministry of	abstract_cluster_4.txt
16	of Labour has initiated or Payroll Information System (PIS) that is proposed by	abstract_cluster_4.txt
17	in computer science (CS) and computer information system (IS) programmes. The course del	abstract_cluster_4.txt
18	towards Europe, namely Eurodac, the Schengen Information System (SIS II) and the Visa	abstract_cluster_4.txt
19	System (SIS II) and the Visa Information System (VIS). This paper tries to	abstract_cluster_4.txt

	Concordance Analysis Results: information systems security	Range
1	uences shape organizational actions for improving information systems security. A case study of	abstract_cluster_1.txt
2	insidious motivators for organizations to adopt information systems security (ISS) approaches. Ext	abstract_cluster_1.txt
3	of this article is to identify information systems security risks in local govern	abstract_cluster_2.txt

	Concordance Analysis Results: information systems security	Range
4	of the most widespread problems affecting information systems. Security breaches at companie	abstract_cluster_2.txt
5	findings of this research contribute to information systems security research, human-compu	asbtract_big_three.txt

	Concordance Analysis Results: information security policy and information security policies	Range
1	between the uptake and application of information security policies and the accompanying	abstract_cluster_2.txt
2	significant relationships between the adoption of information security policies and the incidence or	abstract_cluster_2.txt
3	paper, we investigate the tension between information security policies and information secu	abstract_cluster_2.txt
4	learning cues influence employee awareness of information security policies and ultimately diffe	abstract_cluster_4.txt
5	utsourcing. Purpose – Employees' compliance with information security policies is considered an ess	abstract_cluster_4.txt
1	availability. While the importance of the information security policy (InSPy) in ensuring th	abstract_cluster_2.txt
2	gement, particularly development and execution of information security policy, awareness, compliance	abstract_cluster_3.txt
3	and situational factors that lead to information security policy violation intentions.	abstract_cluster_3.txt
4	situational factors and intentions to violate information security policy. This study represents	abstract_cluster_3.txt
5	meta-traits and their influence on information security policy violation intentions.	abstract_cluster_3.txt
6	in-house employees in terms of information security policy awareness. Based on da	abstract_cluster_4.txt
7	thereby resulting in diminished levels of information security policy awareness. These findi	abstract_cluster_4.txt
8	advance social cognitive theory by incorporating information security policy awareness as an import	abstract_cluster_4.txt

	Concordance Analysis Results: information security management	Range
1	its implications for the practice of information security management. Copyright This p	abstract_cluster_2.txt
2	he evaluation model include project construction, information security management, special construct	abstract_cluster_2.txt
3	incorporating the identified key issues into information security management systems (ISMS). Or	abstract_cluster_2.txt
4	opportunistic behaviour, therefore, confidence in information security management can be achieved. T	abstract_cluster_2.txt

	Concordance Analysis Results: information security management	**Range**
5	to explore the management role in information security management. Various studies h	abstract_cluster_3.txt
6	for a more holistic approach to information security management. In this paper, us	abstract_cluster_3.txt
7	explore specific managerial activities to enhance information security management. We found that num	abstract_cluster_3.txt
8	is considered an essential component of information security management. The research aims	abstract_cluster_4.txt
9	priori assumption about user intent, P3. Information security management and choice of coun	abstract_cluster_4.txt
10	propositions can form a basis for information security management, making the object	abstract_cluster_4.txt
11	(IT) tools, information systems integration and information security management. The findings indi	abstract_cluster_4.txt
12	integration. Then, IT tools and, ultimately, information security management are considered. In	abstract_cluster_4.txt
13	indices for information systems integration and information security management are also referred.	abstract_cluster_4.txt
14	the mechanisms which structure e-democracy. Information Security Management System (ISMS) is a	abstract_cluster_4.txt
15	management, Crisis management, Change management, Information Security Management System, etc. Risk	abstract_cluster_4.txt

	Concordance Analysis Results: security and privacy, privacy and security	**Range**
1	these tools also raised significant national security and privacy considerations. Finally, the	abstract_cluster_1.txt
2	usability, transparency, quality-assured content, security, and privacy) vary in their impact	abstract_cluster_2.txt
3	Mobile applications build part of their security and privacy on a declarative permission	abstract_cluster_3.txt
4	the declarative permissions model on which security and privacy services of Android rely	abstract_cluster_3.txt
5	method bias cannot be completely eliminated. Security and privacy are the two major	abstract_cluster_3.txt
6	hallenged ethical issues about users' information security and privacy. SNS users are concerned	abstract_cluster_3.txt
7	we devise mechanisms covering three important security and privacy issues of EHN including	abstract_cluster_4.txt
8	attain legitimacy. Given the rising IT security and privacy concerns, organizations are i	abstract_cluster_4.txt
9	lack of confidence in ICT's security and privacy, a perception of ICT	abstract_cluster_4.txt

	Concordance Analysis Results: security and privacy, privacy and security	**Range**
1	and the public at large. Accordingly, privacy and security are active topics of	abstract_cluster_1.txt
2	contribute toward a broad understanding of privacy and security not simply as technical	abstract_cluster_1.txt
3	embedded in social and cultural contexts. Privacy and security are difficult concepts to	abstract_cluster_1.txt
4	move away from narrow views of privacy and security and toward a holistic	abstract_cluster_1.txt
5	technologies designed to support self-expression, privacy, and security for global civic networks.	abstract_cluster_2.txt
6	a deeper understanding of customers' perceived privacy and security (CPPS) by investigating priva	abstract_cluster_4.txt
7	organisations to do this because when privacy and security practices are clearly disclos	abstract_cluster_4.txt
8	ones being the digital divide, the privacy and security concerns and the availability	abstract_cluster_4.txt
9	followed by a section on data privacy and security issues. The concluding sectio	abstract_cluster_4.txt

	Concordance Analysis Results: threat to, and safety and security	**Range**
1	contrast, external rivals pose a lower threat to personal status, so people are	abstract_cluster_1.txt
2	and society in terms of the threat to information systems (IS) security. While	abstract_cluster_3.txt
3	be required to combat this growing threat to IS security. As we approach 2015	abstract_cluster_3.txt
4	(ISDB) of employees is a serious threat to organizations. However, not much empiric	abstract_cluster_3.txt
5	to privacy). Insiders represent a major threat to the security of an organization'	abstract_cluster_3.txt
6	systematically treated as a national security threat to the United States. The scope	abstract_cluster_3.txt
7	or social engineering, is an omnipresent threat to a large number of commercial	abstract_cluster_4.txt
8	terrorism primarily as a crime, a threat to the state's security or	abstract_cluster_4.txt
9	study area and the degree of threat to the coastline. The sustainable civilizat	abstract_cluster_4.txt
10	.e., IS misuse) represents a significant threat to organizations. For example, industry sta	asbtract_big_three.txt
1	classrooms, elbow room, as well as safety and security. The swiftness and considerab	abstract_cluster_2.txt

	Concordance Analysis Results: threat to, and safety and security	Range
2	ips, personal values, cultural identity, physical safety and security, aesthetic preferences, and un	abstract_cluster_2.txt
3	by a case study of the safety and security measures adopted in the	abstract_cluster_2.txt
4	2010 FIFA World Cup partners, is the safety and security of local and international	abstract_cluster_2.txt
5	the authors argue that such a safety and security strategy should be informed	abstract_cluster_2.txt
6	is often assumed that perceptions of safety and security may influence individuals' des	abstract_cluster_2.txt
7	be used, what components (quality, quantity, safety, and cultural acceptability) they were inte	abstract_cluster_3.txt
8	anxiety among the public concerning the safety and security of their personal and	abstract_cluster_4.txt
9	the state's ability to provide safety and security online. This disparity present	abstract_cluster_4.txt
10	accept the trade-off between increased safety and diminished control that accompanies a	abstract_cluster_4.txt
11	commentary that addresses issues pertaining to safety and security to garner an overarching	abstract_cluster_4.txt

	Concordance Analysis Results: socio-technical	Range
1	evaluation model with 5 dimensions based on Socio-Technical model and Stakeholder Theory, whic	abstract_cluster_2.txt
2	this research is to analyse the socio-technical consequences deriving from the dig	abstract_cluster_2.txt
3	is an overview of the possible socio-technical risks that a panel of	abstract_cluster_3.txt
4	a high frequency of occurrence of socio-technical information security risks caused	abstract_cluster_3.txt
5	operate within the context of larger socio-technical systems, wherein they interact – b	abstract_cluster_3.txt
6	with a thorough analysis of its socio-technical context, thereby considering not o	abstract_cluster_3.txt
7	interactions among the actors in the socio-technical system. The requirements models of	abstract_cluster_3.txt
8	a central role in advancing the socio-technical project that is constituted by	abstract_cluster_4.txt
9	This paper looks at cities as socio-technical systems consisting of patterns of	abstract_cluster_4.txt
10	them down into an agent-based socio-technical model. This method is useful	abstract_cluster_4.txt
11	evaluation of the informational stability of socio-technical systems, which are influenced by	abstract_cluster_4.txt

	Concordance Analysis Results: information society	Range
1	while neither the general literature on information society nor security studies pay any	abstract_cluster_2.txt
2	international norms to deal with the “information society,” so that “risk society” does	abstract_cluster_2.txt
3	market of electronic commerce. In the information society, to promote private dynamism a	abstract_cluster_2.txt
4	quite a late achievement of the information society, although, in theory, it could	abstract_cluster_4.txt
5	of Russia’s moving towards the information society, new possibilities open up of	abstract_cluster_4.txt
6	of the opportunities offered by the information society. A methodology is formulated o	abstract_cluster_4.txt
7	of education in the conditions of information society. A concept is put forward	abstract_cluster_4.txt
8	In the globalization era and the information society, data security and protection	abstract_cluster_4.txt

	Concordance Analysis Results: construction of	Range
16	interests are closely aligned in the construction of regulatory institutions at the int	abstract_cluster_4.txt
17	This paper focuses on the discursive construction of ‘security’ in a particular context	abstract_cluster_4.txt
18	Part of the project is a construction of a future intelligent city named	abstract_cluster_4.txt
19	a much larger exercise involving the construction of four new science buildings around	abstract_cluster_4.txt
20	are to better understand the ‘social construction’ of the problem and subsequent policy	abstract_cluster_4.txt
21	through an examination of the social construction of the Heartbleed bug. It demonstrate	abstract_cluster_4.txt
22	vehicle of public participation in the construction of a new political order. This	abstract_cluster_4.txt
23	contribution of this study is the construction of structural and measurement models	abstract_cluster_4.txt
24	using contemporary street maps, and the construction of a comprehensive database by using	abstract_cluster_4.txt
25	synthesis of the management objective, the construction of a dynamic expert system, ensuring	abstract_cluster_4.txt
26	Coordination emerges in SEOP through the construction of a new institutional design, articu	abstract_cluster_4.txt
27	of date of planting, land terracing, construction of drainages, cover cropping and maki	abstract_cluster_4.txt
28	trees, planting of cover crops and construction of drainages across farmland. Age, ac	abstract_cluster_4.txt
29	at different levels of internationalization and construction of the world system’s new	abstract_cluster_4.txt

	Concordance Analysis Results: construction of	Range
30	external factor on the anti-government construction of the issue. This study suggests	abstract_cluster_4.txt
31	at Korykos and Elaiussa Sebaste. The construction of isodomic towers is the only	abstract_cluster_4.txt
32	that this concern led to the construction of the isodomic towers. No archaeolog	abstract_cluster_4.txt
33	hypothesis. Eastern Rough Cilicia witnessed the construction of a road network and bridges	abstract_cluster_4.txt
34	led to a boom in the construction of public buildings in the cities	abstract_cluster_4.txt
35	is proposed. An approach to the construction of the so-called vector of	abstract_cluster_4.txt

References

[1] KOVÁCS L., NEMESLAKI A., ORBÓK Á., SZABÓ A.: Structuration Theory and Strategic Alignment in Information Security Management: Introduction of a Comprehensive Research Approach and Program. *AARMS,* 16 1 (2017), 5–16.

[2] SISMONDO, S.: Science and Technology Studies and an Engaged Program. In. *The Handbook of Science and Technology Studies, Third Edition.* Cambridge: MIT Press, 2008. 13–31.

[3] HACKETT, E., AMSTERDAMSKA, O., LYNCH, M., WAJCMAN, J.: *The Handbook of Science Technology Studies, Third Edition.* Cambridge: MIT Press, 2008.

[4] HOWCROFT, D., MITEV, N., WILSON, M.: What We May Learn from the Social Shaping of Technology Approach. In. *Social Theory and Philosophy for Information Systems.* Chichester: John Wiley & Sons, 2004. 329–371.

[5] SIMON, H.: *The Sciences of the Artificial.* Third edition. Cambridge: MIT Press, 1996.

[6] PEREZ, C.: Technological revolutions and techno-economic paradigms. *Cambridge Journal of Economics,* 34 1 (2010), 185–202. https://doi.org/10.1093/cje/bep051

[7] WINNER, L.: Do Artifacts Have Politics? In. *The Social Shaping of Technology.* 2 ed. London: Open University Press, 1999. 28–40.

[8] BOSS, S. R., GALLETTA, D. F., LOWRY, P. B., MOODY, G. D., POLAK, P.: What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly,* 39 4 (2015), 837–864.

[9] POSEY, C., ROBERTS, T. L., BENJAMIN, P., BENNETT, R. J., COURTNEY, J. F.: Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly,* 37 4 (2013), 1189–1210.

[10] YOO, Y.: Computing in everyday life: A call for experiental computing. *MIS Quarterly,* 34 2 (2010), 213–231. https://doi.org/10.2307/20721425

[11] KIM, S. H., KIM, B. C.: Differential Effects of Prior Experience on the Malware Resolution Process. *MIS Quarterly,* 38 3 (2014), 655–678.

[12] LI, C., PETERS, G. F., RICHARDSON, V. J., WATSON, M. W.: The Consequences of Information Technology Control Weaknesses on Management Information Systems:

The Case of Sarbanes-Oxley Internal Control Reports. *MIS Quarterly,* 36 1 (2012), 179–203.

[13] DAVIS, F. D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13 3 (1989), 319–340.

[14] VENKATESH, V., MORRIS, M. G., DAVIS G. B., DAVIS, F.:User acceptance of information echnology: Toward a unified view. *MIS Quarterly*, 27 3 (2003) 425–478.

[15] CECEZ-KECMANOVIC, D., GALLIERS, R. D., HENFRIDSSON, O,. NEWELL S., VIDGEN, R.: The sociomateriality of information systems: Current status, future directions. *MIS Quarterly*, 38 3 (2014), 809–830. https://doi.org/10.25300/MISQ/2014/38:3.3

[16] WANG, J., GUPTA, M., RAO, H. R.: Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly*, 39 1 (2015), 91–112.

[17] BULGURCU, B., CAVUSOGLU, H., BENBASAT, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34 3 (2010), 523–548. https://doi.org/10.2307/25750690

[18] KNAPP K. J., FERRANTE, C. J.: Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. *Journal of Management Policy and Practice*, 13 5 (2012), 66–80.

[19] BIJKER, W. E.: *Of Bicycles, Bakelites and Bulbs: Toward a Theory of Sociotechnical Change.* Cambridge: MIT Press, 1995.

[20] RAYSON, P.: From key words to key semantic domains. *International Journal of Corpus Linguistic*, 13 4 (2008), 519–549. https://doi.org/10.1075/ijcl.13.4.06ray