Journal of Universal Computer Science, vol. 26, no. 7 (2020), 764-782
submitted: 11/1/20, accepted: 13/2/20, appeared: 28/7/20

Bibliometric Mapping of Research on User Training for Secure Use of Information Systems

Damjan Fujs
(University of Ljubljana, Slovenia
damjan.fujs@fri.uni-lj.si)

Simon Vrhovec
(University of Maribor, Slovenia
simon.vrhovec@um.si)

Damjan Vavpotič
(University of Ljubljana, Slovenia
damjan.vavpotic@fri.uni-lj.si)

Abstract: Information systems are pervasive in organizations of all sizes. To use them securely, users must be properly trained. Because of the pervasiveness of information systems the number of scientific publications reporting on user training for secure use of information systems is increasing year by year. To overcome the issue of manually surveying such a vast body of knowledge and to keep up with research trends, we conducted bibliometric mapping of research on user training for secure use of information systems. A total of $N = 1955$ records published between 1991 and 2019 were retrieved from the Web of Science bibliographic database on 21 November 2019. Top contributing authors, organizations, countries and research field were identified with the Web of Science built-in results analysis tool. Additionally, keyword mapping was performed with VOSviewer software. The analysis of the network and overlay keyword maps revealed six clusters: healthcare, technology adoption, management, information security, technical solutions and physical security. The results of this study suggest attractive research directions to be pursued in the future, such as information security training in healthcare and individualized user training alternatives to one-size-fits-all user training approach.

Key Words: literature survey, literature review, cybersecurity, cyber security, computer security, education, bibliometrics, scientometrics, visualization
Category: A.1, H.0, K.3.2, K.4.3, K.6.5, L.2

1 Introduction

People are or should be involved in education from a young age since learning is a normal course of human development. The roots of educational research reach all the way back to the ancient Greek philosopher Plato who was interested in the fundamental questions of education: who and how should be educated [Noddings, 2012]. The answer to the first question seems quite straight forward – everyone should get some form of education. This is also true for cybersecurity and more specifically information systems security. Users of information systems need to be adequately trained to use them securely [Choi et al., 2018]. Organizations seek to train their employees to avoid cyberthreats and to protect the interests of organizations [Aldawood and Skinner, 2019]. However, one-size-fits-all training approaches may not be appropriate in all situations and some approaches may be more fitting to certain situations than others [D'Arcy and Hovav, 2009]. For example, approaches may consider the differences in level of cybersecurity-related knowledge of information systems users [Vasileiou and Furnell, 2018; Friesel et al., 2014] or the teaching approaches that users are most familiar with [Vavpotič et al., 2013]. Such approaches may increase the efficiency of training and lower the probability or scale of the resistance to training [Vrhovec et al., 2015].

In recent years, various literature surveys of cybersecurity and education research areas were conducted. For example, Fujs et al. [Fujs et al., 2019] surveyed the use of qualitative approaches in cybersecurity which included research on security education and training and Kokol et al. [Kokol et al., 2018] explored health informatics competences crucial for information technology education. However, it appears that there is a research gap as none of these literature surveys focused explicitly on cybersecurity education, nor more specifically on user training for secure use of information systems. Traditional literature surveys typically involve reading relevant articles adding an element of researchers' subjective judgement to them. This subjectivity may be reduced by a keyword analysis (i.e., bibliometric mapping) since it leans on automatic quantitative analysis with a predefined algorithm [Fergnani, 2019]. Recently, bibliometrics started to get traction in various research disciplines (e.g., health sciences [Holman et al., 2018], tourism [Garrigos-Simon et al., 2018] and computer science [Blanco-Mesa et al., 2019]).

To address the presented research gap, apply bibliometrics and identify the trends in research on user training for secure use of information systems, we conducted bibliometric mapping [van Eck and Waltman, 2019] which enables the identification of research trends and brings to light the most prominent research contributions. This literature survey may help cybersecurity researchers and practitioners to focus on relevant trends in research on user training for secure use of information systems and find directions where to progress beyond the state-of-the-art. To achieve this, this paper explores the following research questions:

RQ1: Who are the most productive authors, countries, organizations and research fields related to research on user training for secure use of information systems?

RQ2: Which keywords appear most often in research on user training for secure use of information systems?

RQ3: Which keywords appeared earlier and which later in research on user training for secure use of information systems?

2 Theoretical background

2.1 User training for secure use of information systems

Information systems can be defined as an entity that consists of users who perform information-related tasks, and various information technologies that are being used to perform these tasks [Vavpotič and Vasilecas, 2012]. Therefore, information systems include a variety of components, such as personal computers, social networks, ATMs, smartphones for business or personal use, etc. Already some early studies in information systems research focused on information system users training (e.g., computer-aided instructions for training) [Meliopoulos et al., 1987; Chowdhury and Clark, 1992]. Newer studies focused on information system users implementing security measures [Sasse et al., 2001; Stanton et al., 2005]. Recently, the breadth of cybersecurity education research has widened with innovative teaching approaches, such as security games [Cone et al., 2007], personalized security training [Vasileiou and Furnell, 2019] and augmented reality [Logofatu and Visan, 2015].

Over the last decade, the importance of user training for secure use of information systems appears to be rising [Švábenský et al., 2020]. Inadequate user training for secure use of information systems in organizations concerns both users with poor knowledge regarding secure use of information systems on one hand, and training staff with lacking teaching skills on the other. Cybersecurity is generally considered in the domain of IT departments. The staff in IT departments is typically well aware of cyberthreats and countermeasures from a technological standpoint. However, IT staff often lacks the skills needed to train information system users and users routinely fail to implement the required cybersecurity measures as they consider cybersecurity to be a responsibility of the IT department. Even in case of separate information security departments, this remains an issue as cybersecurity education of information system users often remains neglected due to a lack of cybersecurity workforce [(ISC)2, 2019]. These issues seem to manifest on the large scale. For example, almost a half of organizations in UK reported that their cybersecurity issues were related to a lack of skills of their employees [Furnell et al., 2017]. Therefore, it may be crucial that all employees in an organization, not just its IT staff, are sufficiently trained for secure use of information systems. It may be also crucial to develop an organizational culture where cybersecurity is considered everyone's responsibility and not a privilege.

2.2 Bibliometrics and related approaches

Bibliometrics has its roots in statistics and bibliography, and can be described as a quantitative literature bibliography study (e.g., associations between publications and their references) [Hood and Wilson, 2001]. Bibliometrics allows the analysis of chosen topic back for many decades (e.g., 30 years [López-Robles et al., 2019], 50 years [Iqbal et al., 2019]) therefore capturing a significant amount of data and gaining a deeper insight into the evolution of the topic under study.

There are two other trendy publication metrics related terms: scientometrics and informetrics [Hood and Wilson, 2001]. *Scientometrics* is often used in information systems security related studies with quantitative metrics of scientific activities (e.g., journal impact factor, journal h-index, journal quartile, publication year, citations) and can be used to determine the influence of the authors [Hood and Wilson, 2001]. For example, a recent scientometrics study found that scientific publications with longer abstracts and publications with more references receive higher number of citations in the information security research area [Wendzel et al., 2020].

Informetrics is the most widely used method in computer science as it is not only concerned with bibliographic information [Hood and Wilson, 2001] but includes various metrics which focus on information productivity [Sengupta, 1992]. Informetrics is not only concerned with scientific metrics and is also applicable in various fields where information can be analyzed [Hoffman et al., 2019]. Various scientific and other databases provide informetrics. There are however problems with consistency of metrics across different databases. For example, Google Scholar provides a different citation count for publications than Web of Science. To address this issue, there are some solutions emerging in the literature, such as using smart papers and blockchain technology allowing decentralized publishing and informetrics calculation [Hoffman et al., 2019].

New approaches, such as *intermediacy of publications*, are also emerging. These approaches enable comparisons between older and more recent publications, and can help to monitor the evolution of scientific knowledge based on a network of citations [Šubelj et al., 2020]. Since scientific productivity is growing, tools and methods that enable effective analysis of mass data will increase in their importance [Markscheffel et al., 2019].

3 Method

The employed research methodology is outlined in Figure 1 and presented in-detail in the following subsections.

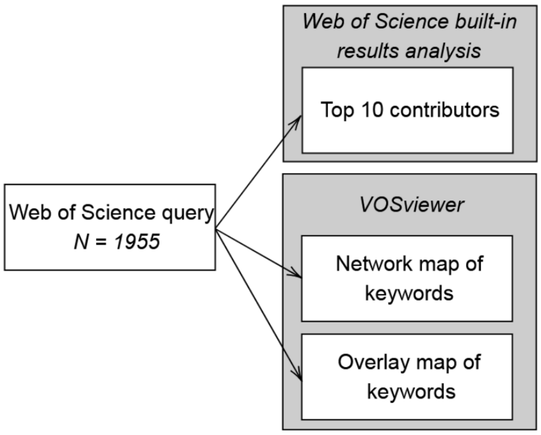

Figure 1: Data collection and analysis.

3.1 Data collection

To reach the most relevant papers on user training for secure use of information systems, we included the following topics for surveying the bibliographic databases: information systems, security training, and security education. The terms education and training are both relevant because users can either learn on their own or learn by being guided through training. The above-mentioned topics were used to form the query which was used to retrieve relevant records in the Web of Science[1] bibliographic database:

> TOPIC:(*information systems* AND (*security training* OR *security education*))

The chosen topics were intentionally very broad in order to expand the comprehensive picture of the observed research field. The results were further refined by document types *ARTICLE* or *PROCEEDINGS PAPER*. This enabled us to search for journal and conference papers related to information systems security education. Bibliographic records (N = 1955) were obtained on 21 November 2019.

3.2 Data analysis

First, bibliographic records were analyzed with the Web of Science built-in results analysis tool to identify the top 10 contributing authors, organizations,

[1] https://apps.webofknowledge.com/

countries and research areas. Result analysis reports include the total number of publications (N), the share of all publications included in our survey they represent (%), the most cited publication not excluding self-citations (Ref_N), authors of the most cited publication, and the number of citations for the most cited publication (TC_R). Publications may be overlapping between different authors, countries and research fields. For example, authors A and B may both have the same number of indexed publications (e.g., 7 publications). This may mean that they did not co-author any of them and all publications are different (e.g., $7 + 7 = 14$ publications), they co-authored all of them and all publications overlap (e.g., 7 publications), or they co-authored some publications (e.g., anything between 8 and 13 publications).

Second, bibliographic records were analyzed with VOSviewer software (version 1.6.13) developed by [van Eck and Waltman, 2010]. Two different bibliographical visualizations were created, namely network and overlay maps of keywords. *Network map of keywords* shows the correlations between keywords and involves the creation of graphs where each keyword is visualized with a node whose size is proportional to the number of publications where the keyword appears. Links between nodes indicate related keywords, i.e., keywords that usually occur together in a publication [van Eck and Waltman, 2010]. *Overlay map of keywords* incorporates the time dimension into a network graph by indicating early and late appearances of keywords in publications. We conducted a cluster analysis on 331 (out of 7340) keywords that appear at least 5 times in the studied publications for both maps of keywords. Visualization of thematic areas based on keywords co-occurrence [van Eck and Waltman, 2010] enables both qualitative and quantitative analyses and is a useful tool that facilitates the identification of relevant research areas although a systematic literature review should be conducted for a detailed analysis of a certain research area.

4 Results

This section first presents the analysis of the top contributing authors, organizations, countries and dominating research areas in research on user training for secure use of information systems. Next, network and overlay maps of keywords are presented and analyzed.

4.1 Top contributors

According to Table 1, all top contributing authors published a similar number of publications. Nevertheless, we can divide them into three groups, namely authors

Table 1: Top 10 contributing authors.

Author	N	%	Ref_N	Authors of Ref_N	TC_R
Tugnait JK	7	0.35	[Tugnait, 2015]	*Tugnait JK*	34
Kim J	7	0.35	[Park et al., 2017]	Park HE, *Kim J*, Park YS	8
Wang C	6	0.30	[Wang et al., 2015]	Wang HM, *Wang C*, Ng DWK	49
Li X	6	0.30	[Wu et al., 2017]	Wu Y, Weng J, Tang Z, *Li X*	9
Du Q	6	0.30	[Xu et al., 2017]	Xu D, Ren P, Wang Y, *Du Q*, Sun L	2
Ren P	6	0.30	[Xu et al., 2017]	Xu D, *Ren P*, Wang Y, Du Q, Sun L	2
Sun L	6	0.30	[Xu et al., 2017]	Xu D, Ren P, Wang Y, Du Q, *Sun L*	2
Wang Y	6	0.30	[Xu et al., 2017]	Xu D, Ren P, *Wang Y*, Du Q, Sun L	2
Chen L	5	0.25	[Liu et al., 2016]	Liu X, Lu R, Ma J, *Chen L*, Qin B	55
Chen W	5	0.25	[Hsu et al., 2016]	Hsu J, Liu D, Yiu YM, Zhao HT, Chen ZR, Li J, *Chen W*	21

with 7, 6 and 5 publications. In addition, it is reasonable to consider the number of citations as they can be a suggestive indicator of an author's quality in addition to the number of publications. Two authors stand out with publications with a higher number of citations, namely Chen L. with 55 citations [Liu et al., 2016] and Wang C. with 49 citations [Wang et al., 2015]. Both papers are relatively recent despite having a high number of citations additionally indicating that they are both of good quality despite a high share of self-citations (25.4 and 26.5 percent, respectively).

Table 2 presents the top contributing organizations. University of California System seems to be the most productive organization and University System of

Table 2: Top 10 contributing organizations.

Organization	N	%	Ref_N	TC_R
University of California System	28	1.43	[Gottlieb et al., 2015]	58
Chinese Academy of Sciences	23	1.17	[Peng et al., 2016]	132
State University of Florida	22	1.12	[Biros et al., 2002]	40
University of Texas System	18	0.92	[Siponen et al., 2014]	129
Bejing Jiaotong University	17	0.86	[Zhu et al., 2016]	7
Penn State University	16	0.81	[D'Arcy et al., 2009]	335
United States Department of Defense	16	0.81	[Biros et al., 2002]	40
University System of Georgia	16	0.81	[Straub and Welke, 1998]	399
Bejing University of Posts Telecommunications	14	0.71	[Peng et al., 2016]	132
University of London	13	0.71	[Perera et al., 2016]	95

Table 3: Top 10 contributing countries.

Country	N	%	Ref_N	TC_R
USA	486	24.84	[Straub and Welke, 1998]	399
China	326	16.66	[Yuan et al., 2016]	171
India	116	5.93	[Subashini and Kavitha, 2011]	958
England	88	4.49	[Willison and Warkentin, 2013]	134
Australia	83	4.24	[Minasny et al., 2013]	147
Russia	72	3.68	[Klimova et al., 2016]	26
Germany	67	3.42	[Baumgart, 2005]	85
South Korea	63	3.22	[D'Arcy et al., 2009]	335
Canada	59	3.01	[Stern et al., 2003]	109
Spain	51	2.60	[Fernández-Alemán et al., 2013]	190

Georgia the most influential among organizations according to the number of cites to the most cited publication. None of the authors in Table 2 seem to be a top contributing author which indicates that the most productive researchers do not necessarily come from the most productive research organizations.

As can be seen from Table 3, the USA has the highest number of publications and is relatively closely followed by China. In addition to these two countries, India is the only country with over 100 publications. The country with the most cited publication among the top contributing countries is India, followed by USA and South Korea.

Table 4 shows the most dominating research areas. Computer science and

Table 4: Top 10 contributing research areas.

Research area	N	%	Ref_N	TC_R
Computer science	830	42.4	[Subashini and Kavitha, 2011]	958
Engineering	568	29.0	[Ming et al., 2007]	157
Education & educational research	219	11.2	[Einterz et al., 2007]	165
Telecommunications	179	9.2	[Yuan et al., 2016]	171
Business economics	121	6.2	[Straub and Welke, 1998]	399
Health care sciences & services	86	4.4	[Wu et al., 2007]	242
Information science & library science	79	4.0	[Straub and Welke, 1998]	399
Medical informatics	72	3.7	[Wu et al., 2007]	242
Public, environmental & occupational health	59	3.0	[Stern et al., 2003]	109
Social sciences, other topics	55	2.77	[D'Arcy and Hovav, 2009]	44

engineering research areas are clearly dominating according to the number of publications as they cover more than two thirds of all publications.

4.2 Keywords mapping and cluster analysis

To gain a deeper insight and identify the research hotspots, bibliographic data was visualized. The more connected keywords are shown closer together which indicates that there are only minor differences between them and that they have a higher co-occurrence. Six major clusters shown in Figure 2 were identified: *healthcare* (red), *technology adoption* (light blue), *management* (yellow), *information security* (blue), *technical solutions* (green) and *physical security* (orange).

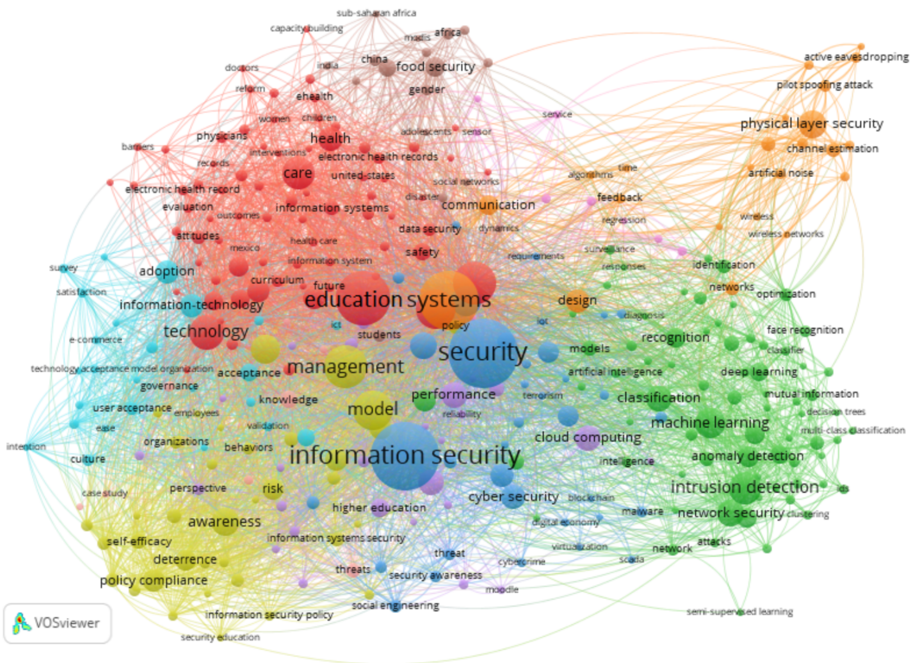

Figure 2: Network map of keywords with colored keyword clusters.

The most prominent keywords in research on user training for secure use of information systems are "information security", "management", "awareness", "machine learning", "intrusion detection", "design", "network security", and "cyber security". The map also suggests the presence of two different poles. The left pole predominantly represents the human-related topics and the right one the technological topics. However, it seems that some topics are positioned in the opposite pole of the expected one. For example, "technology" is positioned in the left pole representing the human-related topics which may be due to the fact that it is a phrase with a wide meaning (e.g., as in technology adoption) and can be therefore closely related to the topics from both poles. It is also interesting that "education" is positioned in the *healthcare* cluster. This indicates the importance of sensitive personal data protection in healthcare. Therefore, information systems users need to be well-educated in information security and data protection in this sector.

The keyword "education" is strongly connected to "information security" in the *information security* cluster, "adoption" and "acceptance" in the *technology adoption* cluster, and "security policy compliance", "management" and "awareness" in the *management* cluster. In the *technical solutions* cluster, "education" is linked to "classification" and "attacks", and to "system", "time" and "design" in the *physical security* cluster. The keyword "security" seems to be predominantly related to the technical pole and less to the sociological pole. This suggests that more emphasis is need on socio-technological research in the future. The data presented in Table 4 also supports this as publications in sociological sciences appear to reach a smaller number of citations indicating a lower attractiveness of the topic.

Next, we included the time dimension in the analysis. Figure 3 shows the overlay map of keywords where the six keyword clusters identified above are marked. To display the time dimension of these terms, a color palette from purple to yellow is used. Purple means that a keyword appeared already in the 1990s while yellow means that it appeared only recently. Most older keywords are in the *management* and the *technical solutions* clusters. The nodes of recent keywords, such as "security education", "social engineering", "security awareness", "culture", "intention", "identification" and "responses", are further away from the center indicating that they are less connected.

From both keyword maps it can be determined that most keywords in the *healthcare* cluster appear relatively recently, that they include the keyword "education", and that they are strongly connected to the *information security* cluster. This clearly points to the importance of information security education in healthcare. This may be mainly due to the recent informatization efforts in the healthcare sector where a significant share of employees were not sufficiently trained in information security or simply lack the motivation to adhere to the information security policy. For example, the primary responsibility of physicians is to improve the health conditions of their patients while everything else is often considered of secondary importance despite dealing with very sensitive medical data. Healthcare employees are also typically less information security savvy than employees in other sectors

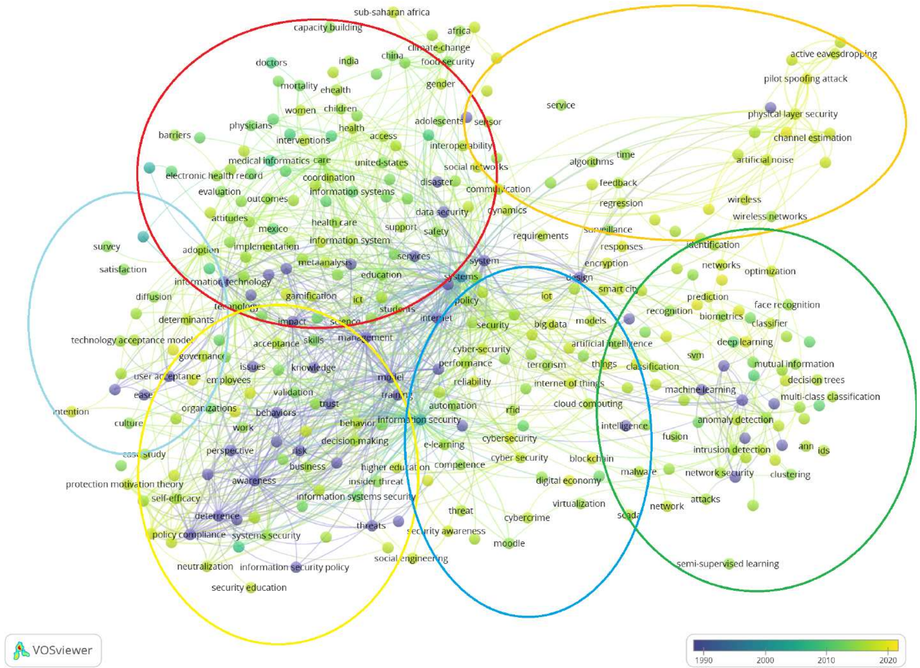

Figure 3: Overlay map of keywords with marked keyword clusters.

with a longer history of informatization [Vrhovec and Markelj, 2018]. It may be also important to note that information security related knowledge may vary considerably between employees in the same organization [van Niekerk, 2005]. The importance of personalized user training is further emphasized by keywords in the *management* cluster. Keywords, such as "culture", "behavior", "awareness" and "satisfaction", indicate that user's adoption of security measures does not dependent only on his or her knowledge and competences but also on other human-related aspects. These aspects importantly influence whether users will perceive training as appropriate and worth the effort [Dincelli and Goel, 2015]. It appears that this kind of visualization points to a recent trend in research. The combinations of recent terms suggest personalized learning to be a perspective future research direction. Researchers may pursue ways to adapt user training for secure use of information systems to the level of knowledge and competencies of individual employees. It may be even more important to do so in sectors often dealing with highly sensitive data, such as healthcare. This kind of research is already emerging (e.g., [Friesel et al., 2014; Vasileiou and Furnell, 2018, 2019]) since widely used one-size-fits-all user training approaches may not be optimal [D'Arcy and Hovav, 2009].

The *technical solutions* cluster is also a cluster with a number of recent keywords that are well-connected to the keywords in the *information security* cluster. This implicates the potential of certain technologies to importantly contribute to secure use of information systems. For example, "deep learning", "intrusion detection", "artificial intelligence" and keywords related to advanced statistical approaches all facilitate and advance cyberthreat prevention, detection and response. However, opportunities for future research do not lie just in these areas but in user training for secure use of information systems as well. Currently, "education" is connected only to keywords "authentication", "classification" and "attacks" while there do not appear be any noteworthy associations to "artificial intelligence", "machine learning" or "deep learning". This points to a research gap and an opportunity to be addressed in future research. Links between nodes can be however interpreted in both directions. This further indicates that there is a need for research on how to train users about using advanced technological solutions. Therefore, the importance of user training may increase with a wider adoption of big data, smart cities, the Internet of Things and other emerging advanced technologies. Additionally, the pervasiveness of these technologies in future information systems will create an even greater need for personalized user training for their secure use.

5 Discussion

5.1 Theoretical and practical implications

This paper investigates the state-of-the-art in research on user training for secure use of information systems. This is a complex research field with several contributing research areas, such as computer science, education, economics, management, etc. This paper makes several theoretical and practical implications based on our study. First, the analysis of keywords shows some interesting areas to address in the future, especially information security in specific contexts, such as healthcare. Nevertheless, it is worth highlighting that higher keyword incidence and correlation does not automatically mean quality of publications, i.e., volume does not bring quality *per se* however it may help a research field to gradually evolve and eventually mature [Hicks et al., 2015]. Second, the "top-10" tables are provided. These tables identify the contributors (i.e., authors, organizations, countries and research areas) in research on user training for secure use of information systems. These tables can be used as a starting point in future studies evaluating the quality of works in the studied research areas complementing the results of our study. Third, based on the keywords, we find that education or learning can be implemented at both human (e.g., e-learning as an activity [Vavpotič et al., 2013]) and technological levels (e.g., machine learning). In both cases, there is the human element present – either as the human who is learning or the human who is creating the learning machine. Fourth, the results of our study indicate that a greater emphasis will be needed on personalized training for secure use of information systems in the future.

5.2 Limitations and future work

This paper has some limitations that the reader should note. First, it should be noted that the data were collected from the Web of Science bibliographic database which includes the most influential publication venues with the highest standards [Garrigos-Simon et al., 2018]. Future work searching in other bibliographic databases, such as Scopus, ACM DL and IEEE Xplore, would be beneficial as they are often used by security researchers. Second, the Web of Science bibliographic database offers institutions varying subscriptions. Even though the same search query is executed in the same Web of Science indexes, the search will return different results at different institutions if their subscriptions differ. The search query was executed in the Web of Science Core Collection which includes the following indexes: SCI-EXPANDED (1900–present), SSCI (1900–present), A&HCI (1975–present), CPCI-S (2011–present), SPCI-SSH (2011–present), BKCI-S (2011–present), BKCI-SSH (2011–present), ESCI (2015–present), CCR-EXPANDED (2011–present), and IC (2011–present). This indicates that a number of conference papers published between 1991 and 2010 were not included in this study. Third, science mapping cannot be a substitute for systematic literature surveys [Hallinger, 2019] however it offers an alternative analysis and insight into research trends. Such analyzes are dynamic, i.e., they may change over time. This may be considered both a limitation and a direction for further studies at a certain point in time.

References

[Aldawood and Skinner, 2019] Aldawood, H. and Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 11(3):73.

[Baumgart, 2005] Baumgart, D. C. (2005). Personal digital assistants in health care: experienced clinicians in the palm of your hand? The Lancet, 366(9492):1210–1222.

[Biros et al., 2002] Biros, D. P., George, J. F., and Zmud, R. W. (2002). Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study. MIS Quarterly, 26(2):119.

[Blanco-Mesa et al., 2019] Blanco-Mesa, F., León-Castro, E., and Merigó, J. M. (2019). A bibliometric analysis of aggregation operators. Applied Soft Computing, 81:105488.

[Yuan et al., 2016] Yuan, Chengsheng, Sun, Xingming, and Lv, Rui (2016). Fingerprint liveness detection based on multi-scale LPQ and PCA. China Communications, 13(7):60–65.

[Choi et al., 2018] Choi, S., Martins, J. T., and Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. Journal of Information Science, 44(6):752–767.

[Chowdhury and Clark, 1992] Chowdhury, B. and Clark, D. (1992). COPERITE computer-aided tool for power engineering research, instruction, training and education. IEEE Transactions on Power Systems, 7(4):1565–1570.

[Cone et al., 2007] Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. (2007). A video game for cyber security training and awareness. Computers and Security, 26(1):63–72.

[D'Arcy and Hovav, 2009] D'Arcy, J. and Hovav, A. (2009). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. Journal of Business Ethics, 89(S1):59–71.

[D'Arcy et al., 2009] D'Arcy, J., Hovav, A., and Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, 20(1):79–98.

[Dincelli and Goel, 2015] Dincelli, E. and Goel, S. (2015). Research Design for Study of Cultural and Societal Influence on Online Privacy Behavior. In Proceedings of 2015 IPIP 8.11/11.13 Dewald Roode Information Security Research Workshop, pages 1–18, Newark, Delaware.

[Einterz et al., 2007] Einterz, R. M., Kimaiyo, S., Mengech, H. N., Khwa-Otsyula, B. O., Esamai, F., Quigley, F., and Mamlin, J. J. (2007). Responding to the HIV Pandemic: The Power of an Academic Medical Partnership. Academic Medicine, 82(8):812–818.

[Fergnani, 2019] Fergnani, A. (2019). Mapping futures studies scholarship from 1968 to present: A bibliometric review of thematic clusters, research trends, and research gaps. Futures, 105(September 2018):104–123.

[Fernández-Alemán et al., 2013] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. á. O., and Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3):541–562.

[Friesel et al., 2014] Friesel, A., Ward, A., Welzer, T., Poboroniuc, M., and Mrozek, Z. (2014). Building a shared understanding of the skills and competences in order to respond to the current global technical challenges. In 2014 IEEE Global Engineering Education Conference (EDUCON), pages 676–679, Istanbul. IEEE.

[Fujs et al., 2019] Fujs, D., Mihelič, A., and Vrhovec, S. L. R. (2019). The power of interpretation. In Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19, pages 1–10, New York, New York, USA. ACM Press.

[Furnell et al., 2017] Furnell, S., Fischer, P., and Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. Computer Fraud & Security, 2017(2):5–10.

[Garrigos-Simon et al., 2018] Garrigos-Simon, F., Narangajavana-Kaosiri, Y., and Lengua-Lengua, I. (2018). Tourism and Sustainability: A Bibliometric and Visualization Analysis. Sustainability, 10(6):1976.

[Gottlieb et al., 2015] Gottlieb, L. M., Tirozzi, K. J., Manchanda, R., Burns, A. R., and Sandel, M. T. (2015). Moving Electronic Medical Records Upstream. American Journal of Preventive Medicine, 48(2):215–218.

[Hallinger, 2019] Hallinger, P. (2019). Science mapping the knowledge base on educational leadership and management in Africa, 1960–2018. School Leadership & Management, 39(5):537–560.

[Hicks et al., 2015] Hicks, D., Wouters, P., Waltman, L., de Rijcke, S., and Rafols, I. (2015). Bibliometrics: The Leiden Manifesto for research metrics. Nature, 520(7548):429–431.

[Hoffman et al., 2019] Hoffman, M. R., Ibáñez, L.-D., and Simperl, E. (2019). Scholarly publishing on the blockchain – from smart papers to smart informetrics. Data Science, 2(1-2):291–310.

[Holman et al., 2018] Holman, D., Lynch, R., and Reeves, A. (2018). How do health behaviour interventions take account of social context? A literature trend and co-citation analysis. Health: An Interdisciplinary Journal for the Social Study of Health, Illness and Medicine, 22(4):389–410.

[Hood and Wilson, 2001] Hood, Wiliam W., Wilson, Concepción S. (2001). The literature of bibliometrics, scientometrics,and informetrics. Scientometrics, 52(2):291–314.

[Hsu et al., 2016] Hsu, J., Liu, D., Yu, Y. M., Zhao, H. T., Chen, Z. R., Li, J., and Chen, W. (2016). The Top Chinese Mobile Health Apps: A Systematic Investigation. Journal of Medical Internet Research, 18(8):e222.

[Iqbal et al., 2019] Iqbal, W., Javed, R. T., Qadir, J., Mian, A. N., Tyson, G., Hassan, S. U., and Crowcroft, J. (2019). Five decades of the ACM Special Interest Group on Data Communications (SIGCOMM): A bibliometric perspective. Computer Communication Review, 49(5):29–37.

[(ISC)2, 2019] (ISC)2 (2019). Strategies for Building and Growing Strong Cybersecurity Teams. Technical report, (ISC)2.

[Klimova et al., 2016] Klimova, A., Rondeau, E., Andersson, K., Porras, J., Rybin, A., and Zaslavsky, A. (2016). An international Master's program in green ICT as a contribution to sustainable development. Journal of Cleaner Production, 135:223–239.

[Kokol et al., 2018] Kokol, P., Saranto, K., and Blažun Vošner, H. (2018). eHealth and health informatics competences: A systemic analysis of literature production based on bibliometrics. Kybernetes, 47(5):1018–1030.

[Liu et al., 2016] Liu, X., Lu, R., Ma, J., Chen, L., and Qin, B. (2016). Privacy-Preserving Patient-Centric Clinical Decision Support System on Naive Bayesian Classification. IEEE Journal of Biomedical and Health Informatics, 20(2):655–668.

[Logofatu and Visan, 2015] Logofatu, B. and Visan, A. (2015). New trends in the educational area. Case study regarding the usability of google apps tools within the department for distance learning. In The 11th International Scientific Conference eLearning and Software for Education, pages 526–531, Bucharest.

[López-Robles et al., 2019] López-Robles, J., Otegi-Olaso, J., Porto Gómez, I., and Cobo, M. (2019). 30 years of intelligence models in management and business: A bibliometric review. International Journal of Information Management, 48(January):22–38.

[Markscheffel et al., 2019] Markscheffel, B., Kretschmer, H., and Pichappan, P. (2019). Report of 14 th International Conference on Webometrics, Informetrics and Scientometrics (WIS) & 19th COLLNET Meeting 05 to 08 December 2018, University of Macau, Macau. COLLNET Journal of Scientometrics and Information Management, 13(1):3–6.

[Meliopoulos et al., 1987] Meliopoulos, A. P. S., Cokkinides, G. J., and Contaxis, G. C. (1987). Computer Aided Instruction of Power System Security Control Functions. IEEE Transactions on Power Systems, 2(1):232–238.

[Minasny et al., 2013] Minasny, B., McBratney, A. B., Malone, B. P., and Wheeler, I. (2013). Digital Mapping of Soil Carbon. In Advances in Agronomy, volume 118, pages 1–47. Elsevier.

[Ming et al., 2007] Ming, J., Hazen, T. J., Glass, J. R., and Reynolds, D. A. (2007). Robust Speaker Recognition in Noisy Conditions. IEEE Transactions on Audio, Speech and Language Processing, 15(5):1711–1723.

[Noddings, 2012] Noddings, N. (2012). Philosophy of Education. In Encyclopedia of the Social and Cultural Foundations of Education, pages 1–156. SAGE Publications, Inc., 2455 TellerRoad, Thousand Oaks California 91320 United States.

[Park et al., 2017] Park, E. H., Kim, J., and Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. Computers & Security, 65:64–76.

[Peng et al., 2016] Peng, M., Sun, Y., Li, X., Mao, Z., and Wang, C. (2016). Recent Advances in Cloud Radio Access Networks: System Architectures, Key

Techniques, and Open Issues. IEEE Communications Surveys & Tutorials, 18(3):2282–2308.

[Perera et al., 2016] Perera, G., Broadbent, M., Callard, F., Chang, C.-K., Downs, J., Dutta, R., Fernandes, A., Hayes, R. D., Henderson, M., Jackson, R., Jewell, A., Kadra, G., Little, R., Pritchard, M., Shetty, H., Tulloch, A., and Stewart, R. (2016). Cohort profile of the South London and Maudsley NHS Foundation Trust Biomedical Research Centre (SLaM BRC) Case Register: current status and recent enhancement of an Electronic Mental Health Record-derived data resource. BMJ Open, 6(3):e008721.

[Sasse et al., 2001] Sasse, M. A., Brostoff, S., and Weirich, D. (2001). Transforming the 'weakest link' - A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3):122–131.

[Sengupta, 1992] Sengupta, I. N. (1992). Bibliometrics, Informetrics, Scientometrics and Librametrics: An Overview. Libri, 42(2):75–98.

[Siponen et al., 2014] Siponen, M., Adam Mahmood, M., and Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2):217–224.

[Stanton et al., 2005] Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2):124–133.

[Stern et al., 2003] Stern, N. J., Hiett, K. L., Alfredsson, G. A., Kristinsson, K. G., Reirsen, J., Haedardottir, H., Briem, H., Gunnarsson, E., Georgsson, F., Lowman, R., Berndtson, E., Lammerding, A. M., Paoli, G. M., and Musgrove, M. T. (2003). Campylobacter spp. in Icelandic poultry operations and human disease. Epidemiology and Infection, 130(1):23–32.

[Straub and Welke, 1998] Straub, D. W. and Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 22(4):441.

[Subashini and Kavitha, 2011] Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1):1–11.

[Šubelj et al., 2020] Šubelj, L., Waltman, L., Traag, V., and van Eck, N. J. (2020). Intermediacy of publications. Royal Society Open Science, 7(1):190207:1–16.

[Švábenský et al., 2020] Švábenský, V., Vykopal, J., and Čeleda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20).

[Tugnait, 2015] Tugnait, J. K. (2015). Self-Contamination for Detection of Pilot Contamination Attack in Multiple Antenna Systems. IEEE Wireless Communications Letters, 4(5):525–528.

[van Eck and Waltman, 2010] van Eck, N. J. and Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2):523–538.

[van Eck and Waltman, 2019] van Eck, N. J. and Waltman, L. (2019). VOSviewer Manual. Technical Report September, Universiteit Leiden, CWTS MEaningful metrics.

[van Niekerk, 2005] van Niekerk, J. (2005). Establishing an Information Security Culture in Organizations: An Outcomes Based Education Approach. Dissertation, Nelson Mandela Metropolitan University.

[Vasileiou and Furnell, 2018] Vasileiou, I. and Furnell, S. (2018). Enhancing security education recognising threshold concepts and other influencing factors. In ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy, pages 398–403, Funchal, Madeira, Portugal.

[Vasileiou and Furnell, 2019] Vasileiou, I. and Furnell, S. (2019). Personalising Security Education: Factors Influencing Individual Awareness and AC. In Mori, P., Furnell, S., and Camp, O., editors, Information Systems Security and Privacy: 4th International Conference, ICISSP 2018, pages 315–321, Funchal - Madeira, Portugal. Springer.

[Vavpotič and Vasilecas, 2012] Vavpotič, D. and Vasilecas, O. (2012). Selecting a methodology for business information systems development: Decision model and tool support. Computer Science and Information Systems, 9(1):135–164.

[Vavpotič et al., 2013] Vavpotič, D., Žvanut, B., and Trobec, I. (2013). A comparative evaluation of e-learning and traditional pedagogical process elements. Educational Technology and Society, 16(3):76–87.

[Vrhovec and Markelj, 2018] Vrhovec, S. and Markelj, B. (2018). Relating mobile device use and adherence to information security policy with data breach consequences in hospitals. Journal of Universal Computer Science, 24(5):634–645.

[Vrhovec et al., 2015] Vrhovec, S. L., Hovelja, T., Vavpotič, D., and Krisper, M. (2015). Diagnosing organizational risks in software projects: Stakeholder resistance. International Journal of Project Management, 33(6):1262–1273.

[Wang et al., 2015] Wang, H.-M., Wang, C., and Ng, D. W. K. (2015). Artificial Noise Assisted Secure Transmission Under Training and Feedback. IEEE Transactions on Signal Processing, 63(23):6285–6298.

[Wendzel et al., 2020] Wendzel, S., Lévy-Bencheton, C., and Caviglione, L. (2020). Not all areas are equal: analysis of citations in information security research. Scientometrics, 122(1):267–286.

[Willison and Warkentin, 2013] Willison, R. and Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Quarterly, 37(1):1–20.

[Wu et al., 2007] Wu, J.-H., Wang, S.-C., and Lin, L.-M. (2007). Mobile computing acceptance factors in the healthcare industry: A structural equation model. International Journal of Medical Informatics, 76(1):66–77.

[Wu et al., 2017] Wu, Y., Weng, J., Tang, Z., Li, X., and Deng, R. H. (2017). Vulnerabilities, Attacks, and Countermeasures in Balise-Based Train Control Systems. IEEE Transactions on Intelligent Transportation Systems, 18(4):814–823.

[Xu et al., 2017] Xu, D., Ren, P., Wang, Y., Du, Q., and Sun, L. (2017). ICA-SBDC: A channel estimation and identification mechanism for MISO-OFDM systems under pilot spoofing attack. In 2017 IEEE International Conference on Communications (ICC), pages 1–6. IEEE.

[Zhu et al., 2016] Zhu, L., Yu, F. R., Tang, T., and Ning, B. (2016). An Integrated Train–Ground Communication System Using Wireless Network Virtualization: Security and Quality of Service Provisioning. IEEE Transactions on Vehicular Technology, 65(12):9607–9616.