International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 12, Issue 12, 2020

Cyber Security and the Higher Education Literature: A Bibliometric Analysis

Nazahah Rahim[a*], Zaleha Othman[b], Fathilatul Zakimi Hamid[c], [a,b]Othman Yeop Abdullah Graduate School of Business, Universiti Utara Malaysia 06010 UUM Sintok, Kedah, Malaysia, [c]Tunku Puteri Intan Safinaz School of Accountancy, Universiti Utara Malaysia 06010 UUM Sintok, Kedah, Malaysia, Email: [a*]nazahah@uum.edu.my

This article describes the trends of the literature on cyber security and higher education research from the year 2008 to 2018 using bibliometric analysis that has been indexed in Scopus database. Analysed parameters include access types and number of publications, document types, subject areas, authorship as well as geographical distribution of publications. It was found that in the last 10 years, only 418 documents were published and most of the documents published were conference papers where only six documents were open-access. The findings show that publications reached its peak during 2017 and English language is the dominant publication language. Most of the literature was found within the subject area of Computer Science and mostly from the United States of America. This article presents a groundwork for other researchers to probe into the area of cyber security and the higher education, as well as trigger further debates on the topic.

Key words: *Bibliometric analysis, cyber security, higher education, university.*

Introduction

The world population totals more than seven billion people, and as of February 2019 there were over four billion internet users in the world (Internet World Stats). Approximately two billion of these internet users are in Asia. With a growth rate of 1,704% from the year 2000 to 2018, the Asian region has seen a tremendous increase in internet usage (Internet World Stats). Malaysia as an example, a country in the Asian region, recorded an overwhelming growth of 880% from 2006 to 2017, when it also witnessed an increase in the number of internet users from 2.5 million people to 24.5 million people (Povera, 2018). This pattern

depicts that people all around the world are widely utilizing internet capabilities in their daily lives, as more and more people are engaged in cyber space to perform their daily activities; therefore, cyber security is crucial.

One of the contributing factors to this phenomenon is the developments in information and communication technology (ICT) which offers new opportunities and possibilities to users. While there are significant advances in ICT and its infrastructure, the cyber space is still far from being completely secured, as it is vulnerable to cyber threats. As an example, although Malaysia is highly committed to cyber security and was ranked third among 193 countries, there were 6,274 cases related to cyber-attacks recorded in 2017 (Aruna, 2017). This reflects that the cyberspace cannot be fully protected; hence the concern about cyber security is highly important due to the growing reliance on computer systems and the internet. Again, taking Malaysia as an example, a study by Microsoft, a well known technology company, revealed that the potential economic loss due to cyber security threats can hit a shocking USD12.2 billion, which is equivalent to more than 4% of Malaysia's total gross domestic product (GDP) of USD 296 billion (Para-masivam, 2018). The study also discovered that a large-sized organisation in Malaysia can incur an economic loss of USD22.8 million, whereby the loss is 630 times higher than the average economic loss for a medium-sized organisation (Paramasivam, 2018). Although there is a serious cyber security concern, a huge amount of data and information is still shared around the globe via the cyber space.

The dominance and extensive growth of the computer systems and the internet capabilities make cyber security an attractive topic. One of the sectors under threat is higher education. There were reported cases of universities facing cyber-attacks where data was compromised. The users in higher education institutions use portable devices that make them highly mobile. This allows them to be accustomed to networking, and thus they are able to access the network anytime and anywhere, on any device. As a result, cyber security at higher education institutions is extremely difficult to secure due to the practice of openness and allowing easy access to data and information (Ramim & Levy, 2006; Davidson & Hasledalen, 2014).

The insufficient cyber security exposes the higher education to threats and the presence of various types of academic research data have turned educational institutions into an attractive target for cyber attackers (Chabrow, 2015). This portrays that the higher education institutions such as universities are currently susceptible to cyber security issues. They become vulnerable because most universities practice open access and an information-sharing culture. This is an alarming situation to the higher education sector as cyber threats such as hacking can halt academic activities. Hackers deploy useful information from universities, and, hackers can easily trade the data as data becomes a commodity (Chabrow, 2015). The online system implemented in universities is a potential target for cyber security threats such as hacking (Chabrow, 2015). This is because the system implemented in universities contains

sensitive personal data of students and staff, as well as a wealth of intellectual property from academics. The culture of open communication and collaboration that exists within the university community comprising students, administrative staff, academics, and research groups make the system even more vulnerable to threats.

The higher education institutions use computer systems and the internet extensively in almost all processes. The higher education systems are connected to the cyber world, but the cyber space is unsafe due to fraud and misconduct, leading to cyber security threats. Cyber security entails the protection of computer-related systems, including the hardware, software, and electronic data, from theft, damage, disruption, or misdirection. Generally, prior studies have already discussed about the various issues related to cyber security and suggested multiple ways to combat them, but due to the implementation of online learning and e-learning, only lately have scholars focused on how significant this issue is in education or academic setting. Therefore, this article attempts to observe the trends of studies conducted in the area of cyber security and higher education, specifically to analyse the trends of the literature within the last 10 years by using a bibliometric approach. It aims to explore what is out there and describe the evolution of the literature, as well as suggest implications for future research.

This article is organized as follows: The literature review will be presented in the next section, followed by the methodology. The methodology section describes the methods used comprising the source, dataset, data collection, and main elements of the analysis. Then, the results section contains an analysis of the data through several bibliometric analyses, followed by the discussion. Finally, the conclusions section contains suggestions for future research and concluding remarks.

Literature Review

Cyber security is a concept that was introduced during the post Cold War period in response to a mixture of technological innovations and changing geopolitical conditions (Hansen & Nissenbaum, 2009). It was made popular in the early 1990s by computer scientists to underline a series of insecurities related to networked computers. In recent years, new threats derived from digital technologies have made cyber security even more significant (Nissenbaum, 2005). These are called cyber threats. This moves in tandem with the advances in ICT and the increase in network connectivity and internet users. The effects of ICT introduce not only technical threats, but also content-related threats. These threats include offensive and abusive contents, such as hate speech, radical and offensive statements, and seditious and defamatory content, which can threaten national security and public safety (Nissenbaum, 2005; Hansen & Nissenbaum, 2009).

The rapid development of ICT has brought with it many new applications, such as e-commerce and global business, along with various risks. Cyber security is supposed to be a mechanism to protect computer-based equipment, information, and services from threats or risks, such as from illegal and unauthorised access. One of the sectors that is in danger of threats is the higher education sector. Inadequate cyber security has exposed university's open-access systems to threats and attackers. The presence of cutting-edge academic research data makes higher education institutions an attractive target for attackers (Chabrow, 2015). As higher education institutions store a large amount of data, the effects of cyber threats on higher education is becoming a serious matter and should not be taken lightly.

The majority of literature related to cyber security and the higher education has discussed its impact on e-learning or online learning systems. This has been documented by numerous studies (e.g., Ramim & Levy, 2006; Levy, Ramim, & Hackney, 2013; Bandara, Ioras, & Maher, 2014; Davidson & Hasledalen, 2014). Ramim and Levy (2006) found that the security of e-learning systems imposes a challenge because the systems are accessed and managed by thousands of users via the internet over hundreds of networks. The internet itself poses security threats, such as unauthorized access, hacking or cracking, obtaining sensitive information, altering data and configuration, and enabling academic misconduct incidents (Bandara et al., 2014).

Using a classic Delphi technique conducted via email, a study in the United States found that online education is vulnerable to cyber-attacks (Davidson & Hasledalen, 2014). A series of themes emerged from the study, including the vulnerability of data, the need for improved authentication, outdated hardware and software, encryption, leader concerns, and training for staff as well as students. The study also discovered that nearly 7 million students who used the online learning platform in the United States were potential targets of cyber threats.

Past researchers have concluded that cyber security threat to online learning systems is problematic and needs to be addressed by using leading-edge methods. The handling of online learning systems lacks technology and trained staff, and hence the systems become soft targets for cyber threats (Ramim & Levy, 2006; Davidson & Hasledalen, 2014). The consequences can be significant, as security breaches of university systems can result in the loss of millions of dollars for the affected universities. Hacking is found to be one of the most prominent cyber issues within the higher education system (Bandara et al., 2014). Hackers use various methods to manipulate data and information, including hacking, malware, skimming hardware, and insider attacks (Coleman & Purcell, 2015). Prior studies have looked into hacking activities whereby computer hackers are now becoming a real danger, especially when more computer systems are adopting online processing and improved telecommunications.

Furthermore, prior studies have also examined the challenges in preventing cyber security in terms of the role of IT education (Rowe, Lunt, & Ekstrom, 2011), the required IT skills (Ayyagari & Tyks, 2012), and the need for ICT security (Ayub, Haolader, & Rahman, 2013). Rowe et al. (2011) discussed the role of IT education in cyber security awareness programs. Meanwhile, Ayyagari and Tyks (2012) argued that security and disaster training should be the main IT skills embedded in the curriculum at higher education institutions, especially when information security and privacy have become core concepts in IT education. This aspiration is echoed by Ayub et al. (2013), emphasizing the need for ICT security in universities to prevent cyber security breaches. According to them, the breach can affect academic progress at the higher education level thus affecting students' results and performance. There is a strong relationship between academic activities and ICT security; therefore, without well-secured ICT, a university can come to a halt. Nonetheless, the effort seems difficult because it poses new challenges to universities in terms of budget constraints. Providing IT security can be demanding, particularly to small academic institutions. With a tight budget, these institutions are challenged with balancing the cost with the effectiveness of security efforts (Ayyagari & Tyks, 2012).

Nonetheless, the higher education sector has additional security challenges. Other challenges include data breaches and human errors, but the 'relaxed' working environments and less formalised policies and procedures at some universities might not help much in promoting cyber security within the higher education sector. Prior studies have documented that the majority of data breaches have occurred in the academic settings since the year 2005 and are becoming more common (Ayyagari & Tyks, 2012; Coleman & Purcell, 2015). The information and data that are prone to threats in the higher education sector include students' grades, personal information, financial data, and research data. Likewise, the most common types of data breaches occurring within the higher education systems are hacking and malware, unintentional disclosure, and portable device breaches, such as through mobile phones. The resulting aftermath of a data breach has placed a significant financial burden on higher education institutions, as they are not prepared to handle information security disasters (Ramim & Levy, 2006; Davidson & Hasledalen, 2014).

A number of issues are documented regarding cyber security at the university and management levels. Coleman and Purcell (2015) conducted a study on four universities (Pennsylvania State University, University of Maryland, North Dakota State University, and Butler University), in which each of the universities has experienced a major data breach. They claimed that university administrators need to be prepared for data breaches and they suggested that universities should devise plans to secure against a breach as well as to react to a breach. In other words, universities need to be proactive and reactive towards securing data. Being proactive can be achieved through tight security and communication of policies as

preventive measures, whereas reactive measures can be taken through cyber insurance, timely notification, and free fraud protection.

It is identified that human errors can contribute to numerous challenges in promoting cyber security. As an example, smartphone users, especially among students, are capable of promoting cyber threats. This is a common means of exploiting cyber security. Users are advised to reduce the risk of unauthorized access to sensitive information stored on smartphones and mobile devices to enhance security. There is a need to mitigate the risks that smartphone users pose to university members and the university community. The risk of gaining unauthorized access to sensitive information can wreak havoc or might later be used as a tool for more severe cyber-attacks (Coleman & Purcell, 2015).

Prior studies on cyber security have also focused on examining users' experience and perception. Agha and Magsi (2017) examined cyber harassment experiences of 100 female students of two public universities in Sindh, Pakistan. The incidents of harassment showed that the female students were threatened and blackmailed frequently on the university campuses, mostly by aggressors known to them. However, the users were reluctant to report the harassment to their parents or to bring the matter to the attention of their respective university authorities because of a lack of trust and fear of hurting the family's social standing. On the other hand, Lubis et al. (2018) investigated user perception of security aspects of Wi-Fi performance in a university in Malaysia. The aim of the study was to provide insights on the indicators to be considered by network administrators of the university. The study found that the majority of students had a good perception of various security aspects in the campus network. To some extent, the users' perception can provide good initial steps to produce and implement cyber security measures.

Although prior studies have highlighted the various topics related to cyber security, studies from the perspective of managing cyber security within higher education institutions are still scarce. In order to provide a starting point to the discussion in this area, this article provides documentation on the trends derived from literature across the higher education context, discusses actions to be taken and hope that it will spark interest and produce further debate in the area. It is also hoped that this article will stimulate debates among practitioners and researchers, and that it will help to prevent unwanted cyber-related incidents from occurring within the higher education sector.

Research Methods

In order to describe the trends in cyber security and higher education literatures, a bibliometric analysis was conducted. This study is descriptive in nature, and so bibliometric analysis is an effective method to detect and investigate the emergence of the research area.

Even though this study provides a basic analysis, it contributes to knowledge and practice whereby it is among the first to analyse 10 years of literature on cyber security and higher education. The list of publications has been obtained through Scopus database search engine as at 28th February 2019. Scopus (scopus.com), an online database, contains the largest abstract and citation database of peer-reviewed literature. The database has 1.4 billion cited references dating back to the 1970s and it is a prominent source used in other bibliometric analysis studies. Various types of documented evidence and publications, such as scientific journals, articles, books, and conference proceedings, were examined.

This study focuses only on the last 10 years of publications and so the online database search was limited to cover a period from the year 2008 to 2018. Since the central focus of discussion in this article was on cyber security and higher education, the following search terms were used: cyber security, cybersecurity, cyber-security, higher education, and university. With these terms, the database was searched in the following categories: title, keywords, and abstract. The online search yielded 418 datasets, which were then used for further analysis. The results were then categorized based on the access types and number of publications, document types, subject areas, authorship, and geographical distribution of the literature found. The following section addresses the results and discussion of the analyses which are presented in graphical illustrations and organized views of the referred research works.

Result and Discussion

This section discusses the access types and number of publications that appeared across time, the document types, the subject areas in which the documents were published, the most prominent authors as well as the authorship, and the countries where the research originated / the geographical distribution of the publications.

Access Types and Number of Publications

Data obtained were firstly being analysed based on the access types and number of publications. Table 1 depicts the access types where, it was found that 2.4% of the documents published on the topic of cyber security and the higher education between 2008 and 2018 were open-access, and the rest were non-open access. This means that it would be challenging for researchers to retrieve and access resources, data, and information from sources such as journal articles, conference papers, and theses, as the research outputs are not distributed openly online and sometimes are not free of cost. It is evident that, on average, the number of publications remained fairly consistent from 2008 until about the year 2013, where there was a drop in the number of publications. After that year, a fairly steady increase in the number of publications can be observed. This could reflect the increased interest in the topic. This also

raises the question of whether the interest in cyber security studies especially focusing on the higher education sector, is seasonal in nature. The highest productivity was observed in 2017 with a total of 86 (20.6%). The details statistic about the number of research publications published is summarized in Table 2.

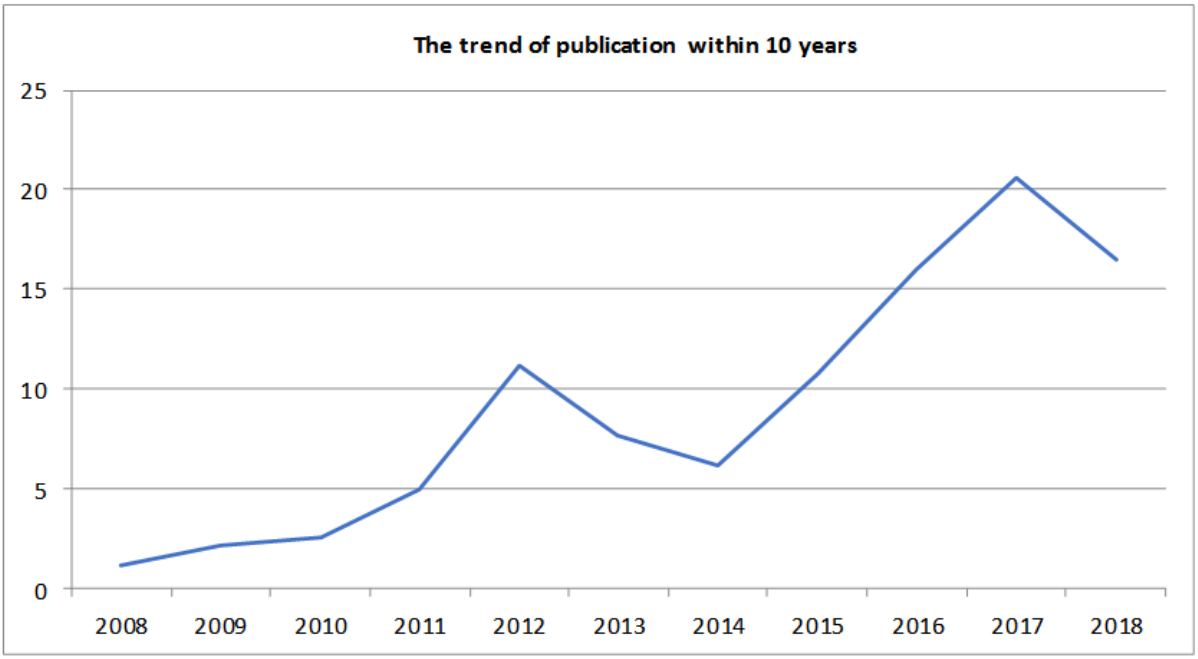
Table 1: Access type

Access type	**Frequency**	**% (N=418)**
Open access	10	2.4
Other (non-open access)	408	97.6
Total	418	100%

Table 2: Number of publications according to year

Publication Year	**Frequency**	**% (N=418)**
2018	69	16.5
2017	86	20.6
2016	67	16.0
2015	45	10.8
2014	26	6.2
2013	32	7.7
2012	47	11.2
2011	21	5.0
2010	11	2.6
2009	9	2.2
2008	5	1.2
Total	418	100%

Figure 1. The trend of publication within 10 years, from 2008 until 2018 (as at 28 February 2019)



Document Types

Table 3 depicts the document types, of which 47.8% of the documents published from 2008 to 2018 were conference papers, followed by 28.7% journal articles and 6.7% book chapters, while the rest were conference reviews, reviews, books, articles in press, short surveys, editorials, notes, and erratum. Within the period of 10 years, 200 conference papers on the topic of cyber security and higher education were published mainly as proceedings in various avenues, such as the ASEE Annual Conference and Exposition Conference Proceedings, ACM Inter-national Conference Proceeding Series, and Proceedings Frontiers in Education Conference Fie. Nevertheless, specialist journals, such as the Journal of Cyber Security, Advances in Cyber Security Technology Operations and Experiences, and Dynamic Networks and Cyber Security, were not the preferred publishing avenues among most researchers, as these journals published the lowest number of publications within the 10 year period. This could be due to the publishing standards and requirements of journal publishers to ensure that their journals are on par with other established and quality journals.

Table 3: Document types

Document Type	Frequency	% (N=418)
Conference paper	200	47.8
Journal article	120	28.7
Book chapter	28	6.7
Conference review	25	6.0
Review	17	4.1
Book	14	3.3
Article in press	4	1.0
Short survey	4	1.0
Editorial	3	0.7
Note	2	0.5
Erratum	1	0.2
Total	418	100%

Subject Areas

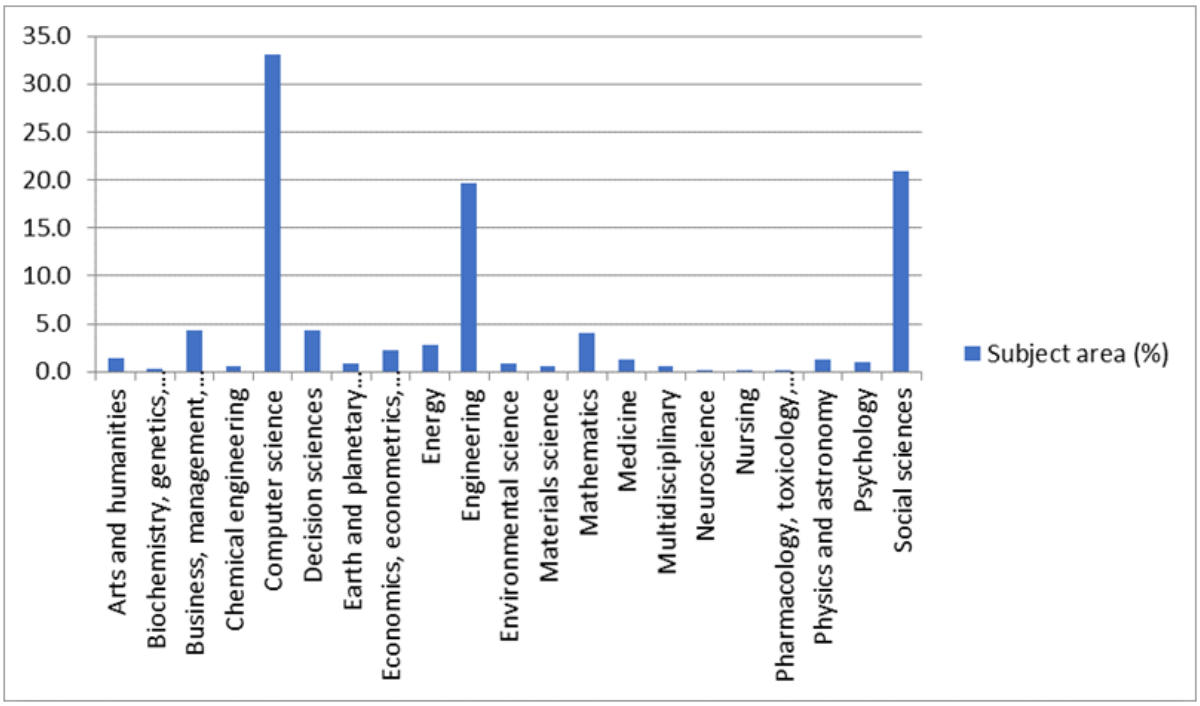
Table 4 and Figure 2 illustrate the subject areas of the works published from 2008 to 2018. The classification of subject areas is based on the aims and scope of the document source, and on the content it publishes (Scopus.com). It is evident that 33.1% of the documents published on cyber security and the higher education can be found within the subject area of Computer Science. This is followed by 21% within the subject area of Social Sciences and 19.6% within the subject area of Engineering. The works of previous authors could also be found in the areas of Decision Science; Business, Management and Accounting; as well as in Arts and Humanities. This suggests that the complexity of the topic and its multidisciplinary nature are significant across multiple areas. This is an interesting finding, as the topic of cyber security covers an array of subject areas, not only in Computer Science, which looks into the theory, experimentation, applications, and engineering for the design and use of computers, but also into areas such as Social Sciences and Humanities.

Table 4: Subject areas

Subject Areas	**Frequency***	**% (N=744)**
Arts and humanities	10	1.3
Biochemistry, genetics, and molecular biology	2	0.3
Business, management, and accounting	32	4.3
Chemical engineering	4	0.5
Computer science	246	33.1
Decision sciences	32	4.3
Earth and planetary sciences	6	0.8
Economics, econometrics, and finance	17	2.3
Energy	21	2.8
Engineering	146	19.6
Environmental science	6	0.8
Materials science	4	0.5
Mathematics	30	4.0
Medicine	9	1.2
Multidisciplinary	4	0.5
Neuroscience	1	0.1
Nursing	1	0.1
Pharmacology, toxicology, and pharmaceutics	1	0.1
Physics and astronomy	9	1.2
Psychology	7	0.9
Social sciences	156	21.0
Total	744*	100%

*Some documents were categorised under more than one subject area.

Figure 2. Subject areas



Authorship

The data collection process of this study has generated various datasets, which were documented and written by 158 different authors. The datasets yielded insights concerning the most productive authors who have published many research works. Based on the results, there were two productive authors who published four publications each within the period of 10 years on the issues concerning cyber security and higher education. They were Manimaran Govindarasu, who is a Professor of Electrical and Computer Engineering from Iowa State University, and Adam Hahn, who is a Professor of Computer Science from Washington State University. Both prominent authors have recorded thousands of citations across the globe. Their studies contributed massively to knowledge and theory, especially to the context of developed countries. Other authors who have produced in the cyber security and higher education literature include Aditya Ashok from Iowa State University, Dale C. Rowe from Brigham Young University, and Michel Cukier from the University of Maryland.

Geographical Distribution of Publications

This category reflects the number or proportion of papers published by authors affiliated with a given country. The increasing proportion of international journals of a country provides new venues for papers from a particular country to be seen by other researchers worldwide. In terms of the geographical distribution, the majority of publications (48.7%) came from a

developed country, particularly from the United States of America. This might be due to the abundance of sources and the existence of experts from the United States itself such as Professor Manimaran Govindarasu and Professor Adam Hahn. This is followed by China and the United Kingdom with 5.3% each, then Australia with 3.6%. The documents were mostly written in English (405 papers), while 10 documents were written in the Chinese language, 2 documents in Russian, and 1 in Turkish. This clearly indicates that studies on cyber security and higher education are not well published yet and not common among researchers within the developing countries. The analysis also revealed that the total dataset is 470 which are higher than the initial data obtained. Upon further investigation, this is due to some documents that were produced by more than one author from different countries. Researchers from more than 55 different countries contributed to the publication of retrieved documents. All countries that contribute to the literature in cyber security and higher education are listed in Table 5. The United States of America (USA) ranked first with a total of 229 (48.7%) documents followed by China and the United Kingdom (UK) with 25 documents each (10.6%).

Table 5: Countries contributed to the publication

Publishing country	**Frequency***	**% (N=470)**
United States	229	48.7
China	25	5.3
United Kingdom	25	5.3
Australia	17	3.6
Germany	9	1.9
France	8	1.7
Canada	7	1.5
Finland	6	1.3
Malaysia	6	1.3
Romania	6	1.3
Russian Federation	6	1.3
South Korea	5	1.1
Czech Republic	4	0.9
Estonia	4	0.9
India	4	0.9
Japan	4	0.9
Portugal	4	0.9
Singapore	4	0.9
South Africa	4	0.9
Spain	4	0.9
Indonesia	3	0.6
Ireland	3	0.6

Italy	3	0.6
Poland	3	0.6
Austria	2	0.4
Brazil	2	0.4
Bulgaria	2	0.4
Lithuania	2	0.4
New Zealand	2	0.4
Qatar	2	0.4
Sweden	2	0.4
Taiwan	2	0.4
Turkey	2	0.4
United Arab Emirates	2	0.4
Other countries (one publication each: Algeria, Bangladesh, Belarus, Colombia, Cuba, Cyprus, Denmark, Ecuador, Egypt, Georgia, Israel, Jordan, Netherlands, Norway, Nigeria, Oman, Pakistan, the Philippines, Slovenia, Switzerland, Thailand, Yemen)	21	4.2
Undefined	35	7.4
Total	470*	100%

*Some documents were produced by more than one author from different countries.

The analysis suggests that both developed and developing countries have exhibited interest and keenness in producing literature in cyber security and higher education. The documents which were published in various avenues produced by authors from more than 55 countries around the world show that the topic of cyber security and higher education have already been discussed for the past 10 years, however, it is still scarce.

Securing the electronic environment or the cyber space from intrusion can be challenging. In terms of practice, a continued effort towards cyber security is pertinent. It can be concluded that the higher education sector is vulnerable to cyber security threats. The environment of openness, collaboration among universities, and the easy access to portable devices can contribute to the breach of cyber security. This is a challenge as universities rely heavily on electronic data that are transmitted via the cyber space for the smooth operation of the higher education institution.

Another practical implication of this study is the need for better tools for cyber security management systems. In light of this, universities have a responsibility to develop cyber security models that target appropriate and proportionate security controls. Based on the work undertaken to date, it is believed that the technical expertise to implement appropriate controls to different components of the digital platform is already available to universities

(Nissenbaum, 2005; Hansen & Nissenbaum, 2009). However, the responsibility and awareness towards implementing an effective cyber security management system are still limited, so it is imperative that university administrators understand the need to invest in better tools for cyber security management.

Cyber security has its significant impact on the higher education sector, and this issue remains one of the major security concerns of nations around the world. It has proliferated significantly, and as a result, proper IT policies and procedures, especially those related to security of information systems, have become critical for higher education institutions. This is because the higher education world has now become wireless. The users in the higher education sector use e-books, Moodle, smartphones, wireless networks such as Bluetooth and Wi-Fi, as well as other gadgets and thus university administrators need to maintain a robust cyber security system. In order for a cyber security practice to be successful, organisations such as the higher education institutions need to consider the elements of people, process, and technology, and how these elements can contribute to the overall security of an organisation (Paramasivam, 2018). It was found that the literature related to cyber security and higher education were written by multiple authors, however, most prominent authors were affiliated with the developed countries such as the United States. This could pose a serious concern on the lack of experts from developing countries.

Cyber security is a requirement for digital transformation to guide and keep universities safe, especially in terms of data protection. The higher education sector needs to invest in strengthening its cyber security system. Over 90% of cyber incidents can be averted by maintaining the most basic best practices (Paramasivam, 2018). Some of the best practices suggested by Microsoft are maintaining strong passwords; conditional use of multi-factor authentication against suspicious authentications; and keeping device operating systems, software, and anti-malware protection up-to-date and genuine, which can rapidly raise the bar against cyber-attacks and hence help to protect the system (Paramasivam, 2018). This should include not just toolsets but also training and policies to support users at the higher education or university level. Moore (2010) outlined in detail the various challenges plaguing cyber security, which include misaligned incentives, information asymmetries, and externalities. He recommended introducing a change in policy to improve cyber security. This consists of mitigating malware infections via ISPs by subsidised clean-up, mandatory disclosure of fraud losses and security incidents, mandatory disclosure of control system incidents and intrusions, aggregation of reports of cyber espionage, and better reporting methods (Moore, 2010).

In addition, a report by Universities UK (2013) documented approaches to implementing cyber security in higher education institutions. The report is written from the perspective of management, exploring various ways to be cyber secure across the whole organisation. The

primary focus of the report is on overcoming the challenge of protecting against targeted unauthorised attempts to access information via cyberspace. It also looks at approaches on how to examine the risk associated with cyberspace and how these should inform the development of risk-based management of cyber security across an academic institution. According to the report, the main elements of developing cyber security at the higher education level include:

• evaluating the risk associated with cyber threats,
• creating effective oversight and reporting of information risks,
• executing appropriate general and specific network controls.

Conclusion

The analysis presented in this article is an approach towards creating awareness and interest for cyber security studies, particularly in the context of higher education institutions. It aims to explore and describe the development within a period of 10 years, from 2008 to 2018, and is hoped to trigger further debates on the topic in question. From the findings above, it is clearly seen that literature on cyber security focusing on the higher education is limited. Therefore, in terms of research, much effort needs to be made, such as conducting studies in the context of developing countries as the impact of cyber security is a global issue. Although the geographic dispersion of the literature related to cyber security and higher education shows that the United States has the largest number of publications as well as influence in terms of the authorship, most authors who have contributed to this area are from the developed countries such as the United States, China and the United Kingdom. Another implication is the accessibility issue, in which it is difficult to access documents related to studies on cyber security and higher education as most of the published works have limited access (non-open access). Most of the documents examined were conference papers, such as proceedings, which could not be seen as containing rich contents compared to full research papers. Further investigation through extended research works is required to truly understand the rationale behind this issue, allowing it to be confidently applied.

The exploration made in this article was motivated by two observations: first, cyber security issues have remained as a debated topic in the literature in recent years but is still a scarcely debated topic in the higher education, and second, managing cyber security in the higher education sector is challenging. Yet, no consensus about progress on this area has been achieved in the literature. This article started with an indication that there was not much clarity about the actual level of progress that has been made in the topic of cyber security and the higher education. In this article, a bibliometric approach has been used to trace the developments in this topic within published documents obtained from an online database.

This paper presents a bibliometric review to gain a clearer insight into the trends, historical review, forecasts and contributions of the cyber security literature focusing on higher education. The research on this topic has already started before the year 2008 and there is some progress where the peak of publications is seen in the year 2017 with a total of 86 publications compared to 69 publications in 2016. It is expected the total number of publication will increase more in 2018 where, as of February 2019 there are publications which have not yet been indexed by Scopus, hence not captured in the datasets.

This study has a few limitations that are inherent to the database used. Thus, it should be emphasized that even though Scopus is one of the largest databases, there are still journals and titles which have not been indexed, and therefore publications in these journals might have been ignored. Furthermore, this study only focuses on the topic related to cyber security and higher education based on the title of the documents, abstract and keywords. Thus, all the other literature that are related to the topic but are not explicitly categorised based on the article title, abstract and keywords were excluded. The total number of publications is only correct at the time of the search as the database is updated constantly. Despite all these limitations, this study is among the first to analyse the detailed bibliometric indicators of literature in cyber security focusing on the higher education context.

This study presents a groundwork on the topic of managing cyber security in the higher education that is hoped to inspire further debates. The findings should be able to provide insights to future researchers. It is suggested for future researchers to conduct textual analysis, which would certainly reveal additional and interesting findings. This is because this study employed specific search criteria; the article title, abstracts and keywords, which are available electronically via the Scopus platform, rather than full papers or complete documents. The data was collected through one database, Scopus. Although Scopus is the largest abstract and citation database of peer-reviewed literature, including scientific journals, books, and conference proceedings, future studies should include other databases to get complete and comprehensive findings on the documented works of authors around the globe. Future research may also want to incorporate a variety of research methods, such as interviews, group discussions, experiments, or other tactics, for the purpose of collecting data and gaining rich information.

Acknowledgement

The authors wish to thank the Ministry of Education Malaysia for funding this study. The grant is coded as 13598 Fundamental Research Grant Scheme.

REFERENCES

Agha, N., and H. Magsi. 2017. Need for creating secure cyber spaces: evidences of cyber harassment from female Pakistani university students. Pakistan Journal of Women's Studies. 24(1): 89.

Aruna, P. 2017. Combating cyber crimes. Available at https://www.thestar.com.my/business/business-news/2017/11/18/combating-cyber-crimes/

Ayub, B., F. A. Haolader, and M. M. Rahman. 2013. The influence of ICT security to academic environment at universities: case study Uganda. International Journal of Innovative Research in Science, Engineering and Technology. 2(8): 4866–4873.

Ayyagari, R., and J. Tyks. 2012. Disaster at a university: A case study in information security. Journal of Information Technology Education. 11: 85–96.

Bandara, I., F. Ioras, and K. Maher. 2014. Cyber security concerns in e-learning education. In Proceedings of ICERI2014 Conference, 17th-19th November.

Chabrow, E. 2015. China blamed for Penn State breach: Hackers remained undetected for more than two years. Available at http://www.databreachtoday.com/china-blamed-for-penn-state-breach-a-8230

Coleman, L., and B. Purcell. 2015. Data breaches in higher education. Journal of Business Cases and Applications. 15: 1–7.

Davidson, P., and K. Hasledalen. 2014. Cyber threats to online education: a Delphi study. In ICMLG2014 Proceedings of the 2nd International Conference on Management, Leadership and Governance: ICMLG 2014 (p. 68). Academic Conferences Limited.

Hansen, L., and H. Nissenbaum. 2009. Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly. 53(4): 1155–1175.

Internet World Stats. n.d. Usage and population statistics. Available at http://www.internetworldstats.com/asia/my.htm

Levy, Y., and M. M. Ramim. 2015. An assessment of competency-based simulations on e-learners' management skills enhancements. Interdisciplinary Journal of e-Skills and Lifelong Learning. 11: 179–190.

Levy, Y., M. M. Ramim, and R. A. Hackney. 2013. Assessing ethical severity of e-learning systems security attacks. Journal of Computer Information Systems. 53(3): 75–84.

Lubis, A. R., F. F. Fachrizal, M. Lubis, and H. M. Tahir. 2018. Wireless service at public university: a survey of users perception on security aspects, Proceedings of the 2018 International Conference on Information and Communications Technology (ICOIACT), March.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3-4): 103-117.

Nissenbaum, H. 2005. Where computer security meets national security. Ethics and Information Technology. 7(2): 61–73.

Paramasivam, S. 2018. Cybersecurity threats to cost organisations in Malaysia US$12.2 billion in economic losses. Available at https://news.microsoft.com/en-my/2018/07/12/cybersecurity-threats-to-cost-organisations-in-malaysia-us12-2-billion-in-economic-losses/

Povera, A. 2018. Internet users in Malaysia up from 2.5mil in 2006 to 24.5mil in 2017. Available at https://www.nst.com.my/news/nation/2018/02/331284/internet-users-malaysia-25mil-2006-245mil-2017

Ramim, M., and Y. Levy. 2006. Securing e-learning systems: a case of insider cyber attacks and novice IT management in a small university. Journal of Cases on Information Technology (JCIT). 8(4): 24–34.

Rowe, D. C., B. M. Lunt, and J. J. Ekstrom. 2011. The role of cyber-security in information technology education. In Proceedings of the 2011 Conference on Information Technology Education (pp. 113–122). ACM.

Universities UK. 2013. Cyber security and universities: managing the risk. Available at http://www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf