Kalpa Publications in Computing

Volume 12, 2019, Pages 169–179

Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019

An Ontology Based Model for Cyber Security Awareness Education

Nthabiseng Modiba [1], Ojo Sunday [2], Zenzo Ncube [3]
Sol Plaatje University, Kimberley [1]
Tshwane University of Technology, Pretoria[2]
University of Mpumalanga, Malahleni[3]

Abstract

The internet has become a crucial part of our everyday lives so it is important to ensure that one is secure when surfing on it since personal information can be exchanged. Cyber security awareness is the key to internet security. The research discussed in this paper aims to develop an ontology model for cyber security awareness for educational purposes, to enable users to take responsibility for their own safety online. It aims to fill a gap in understanding of the cyber security awareness (CSA) education and to bridge the consensus gap between the Body of Knowledge (BoK) contributors. The research study was conducted using CURONTO (which is a curriculum ontology) model, to develop our CSA education ontology model that we propose. There are many attempts being made to allow for CSA education, but there remains a challenge of lack of consensus or common understanding of the CSA body of knowledge. There is need for a common model and format aimed at bringing together and putting in place, measures to address cybersecurity attacks. This will assist organizations and countries to close the gap and difference in the available CSA information globally, and to especially assist countries and organizations that are still developing cybersecurity protection measures, to have the information that they need readily available (Takahashi, Kadobayashi, 2011). We used an ontology because it will also be available to the academic community also to refine, extend or apply to other domains and also an ontology is both sharable and interoperable. In this paper we used the CURONTO model to develop our CSA ontology model for educational purposes, we expanded the one class of the model called syllabus and we added more classes so that it can serve for the CSA education. Then we did a literature study to develop a CSA syllabus from, the acquired syllabus was then represented in the model.

1. Introduction

When cyber users are not informed about cybercrimes, they can easily become victims to cyber criminals. Users online behave in an unsecure manner which makes them easy targets of exploitation (Kortjan & Von Solms, 2014). This behaviour is brought about by the lack of awareness of cyber safety by users. The best way to address the knowledge shortcoming is to first establish a stable knowledge base in Cyber Security awareness education. If this does not happen, organizations will continue to lose money due to cyber-attacks which could be averted by awareness programs. To empower a community, one needs to educate that community, and education serves as a powerful weapon in the hands of any community. People need to be aware of cybercriminals' activities so that they may be able to apply appropriate safety measures to protect themselves and their organizations against cyber-crime.

Dlamini & Modise, (2012). Mentioned several examples of organizations that lost money due to insufficient online security, such as the Road Accident Fund (RAF) from which money was stolen through the utilization of key loggers, amounting to the value of R15 million. The second example is the Amalgamated Banks of South Africa (ABSA) fraud occurrences on the internet, which cost up to R30 million. Fraud incidents that occurred at Landbank recorded up to R150 millions and the South African Revenue Services (SARS) internet fraud accounted for up to R100 million in the year 2010. To capture the Body of Knowledge (BoK) for the CSA education, an ontology was utilised due to its immense benefits for any domain knowledge.

(Bucci et al. 2011) define ontology as an official presentation of a collection of concepts linked to the domain concerned. They further explain that ontologies are aimed at acquiring domain knowledge, rendering a commonly agreed understanding which is reusable and can be shared throughout CSA platforms, making interoperability, reusability of knowledge, machine readability, and reasoning about information through inferencing possible. Ontology helps in defining a model that depict the relationship between the various CSA educational components.

Section 2 is the literature review, whilst section 3 is the theoretical background that gives a detailed description of the CURONTO model that we used in developing our CSA ontology educational model. In Section 4 we discuss the methodology of soliciting the contents of the CSA ontology model from different literature, Section 5 is where a detailed discussion on the proposed CSA ontology model that was derived from CURONTO takes place. The last section Section 6 is the results of Section 4 methodology; we discuss the contents of the proposed CSA model. Then the article is concluded in section 7.

2. Literature review

People are increasingly entering the cyberspace daily, which leaves cyber criminals with more people to victimise. According to Dube (2015), 5 million South Africans enter the cyberspace each year, and there is an annual loss of 6 billion Rands as they become victims of this type of crime. These statistics are proof that, if measures to combat cybercrime are not put in place, private and public organizations stand to lose much monetary resources. There are new cases of cyber-attacks reported on a regular basis according to the The times (2015), they further mention that computer forensic expert Danny Myburg receives at least five new cases of e-mail hacks monthly. In the same article, Hawks (Hawks are South Africa's new Directorate for Priority Crime Investigation) spokesman, Hangwani Mulaudzi, speaks of syndicates behind ransomware that are targeting wealthy South Africans and also parastatals, government, big businesses on a daily basis. For the cyber-attacks to work effectively, they need someone on the inside to trigger them. Sometimes people trigger these attacks unintentionally, out of ignorance or human error. People can only avert this attacks when they have been educated through the CSA programs.

Dlamini et al. (2011), defined cyber security awareness (CSA) as the safety training that is used to encourage, stimulate, build and instill cyber security skills and expected safety regulations from the users. Von Solms and Van Niekerk (2013) are of a similar view, that the intention of awareness is to help individuals see IT security challenges and react accordingly, and to be able to know what to do in case of a threat. The main reason for security awareness is to get users to be amenable to change . CSA is having users being completely conscious of the cyber environment, their actions and other users' actions. It is meant to encourage users to act responsibly and cautiously online, and also to know how to defend themselves against attacks. According to Programs (2017), cybersecurity is a computer field which requires humans, technology, processes and information to ensure functionality. It is a mixture of fields which features law, human factors, ethics and risk management.

It is a process of making, operating and testing safe computer systems (Programs, 2017). This field is known to be one of the most vital subjects at all levels of education. All professionals and citizens are to engage in CSA for their safety online. Ontologies are known for being the best in representing any knowledge domain, CSA is not an exception, in this paper we use an ontology to represent the CSA BoK for educational programs.

Researchers like Kapoor and Sharma (2010) are of the view that ontologies' main purpose is to attain domain knowledge in a general manner, to give a commonly agreed understanding of a domain. The same authors expand their view by saying that ontologies represent a shared conceptualization of a domain. They can, at times, also have depictions of these conceptualizations, the authors are referring to as graphical presentation of the ontology. Ontologies are meant to support sharing and reutilization of knowledge. An ontology is a model built to present facts, and is a theory of the world; more practically, a hypothesis of a domain (Raskin, et al., 2012). (Bucci. Sandrucci. & Vicario., 2011) defined ontology as an official presentation of a collection of concepts linked to the domain concerned. They further explain that ontologies are aimed at acquiring domain knowledge, rendering a commonly agreed understanding which is reusable and can be shared throughout CSA platforms, making interoperability, reusability of knowledge, machine readability, and reasoning about information through inferencing possible. An ontology in this paper, is a platform or tool meant to share the body of knowledge produced as one of the deliverables of this study. There are also other benefits that come with the ontology as stated by Van Vuuren, Van, Leenen, and Zaaiman, (2012), like:

- Sharing mutual understanding of the structure of information. This is the main goal of the ontology that is of interested in this paper. The aim is for every one of the CS stakeholders to have a mutual realization of the structure of CSA information.
- Facilitating reuse of domain knowledge.
- Clarify domain assumptions.
- Distinguish between domain knowledge and operational knowledge.
- Analyzing domain knowledge.

There is a number of curriculum ontology models in literature such as Chung and Kim' s (2016) four layered integrated learning ontology. A description of two of these models is given next. The first model is called the four-layered integrated learning ontology (Chung, Kim,. 2016). The four layers provided for are: Level 0- Curriculum Ontology layer, Level 1 - Syllabus Ontology layer, Level 2 - Subject Ontology layer, and Level 3 - Resource Ontology layer.

It seems for one to capture and represent the cyber security awareness Body of Knowledge for educational purposes, an Ontology will serve as a great tool to define the domain knowledge. It will bring a common understanding of cyber security education, and link competencies with roles in the cyber security course. Due to its sharable, reusable and interoperable abilities, an ontology can produce the desired unanimity in the CSA domain amongst all the stakeholders. From our literature study we observed that there are many organizations that are offering cyber security awareness (CSA) education but there is no knowledge consensus among them all. Therefore, before the ontology construction, it is important to engage in an intense literature study to elicit the syllabus from different private and state organizations from all over the globe.

There are a number of previous and current efforts to establish skills frameworks, key topic areas and curricular guidelines for cyber security for example the United States of America's Veterans Affairs offices who offer their CSA course online. The course is intended to take an estimated one hour. The course helps people to realize their role to protect VA's information assets, more so the veterans' private information. The course also points out ways to meet these responsibilities. There are 11 topics that are covered for cyber security awareness for Veterans Affairs (Cinnamon. 2011). The STOP.THINK. CONNECT by APWG & NCSA (2017) is a worldwide online safety awareness campaign to assist users stay safer and more secure online. It covers a variety of topics and subtopics as part of the advice and tips.

SACSAA is an alliance of academic research groups from Nelson Mandela Metropolitan University (NMMU), the University of Johannesburg (UJ) and the University of South Africa (UNISA) (Dlamini & Modise , 2012). This is a platform where the alliance engages with the community on today's cybersecurity issues, knowledge and practices. It also provides education on cyber security and security knowledge and practices at no cost. These are some of the CSA programs that we used to acquire the Syllabus content from, the contents of the syllabus are discussed in Section 6.

3. Theoretical background

3.1. CURONTO Model

In order to produce a model for Cybersecurity Awareness, a model called CURONTO was adopted to be utilized in this paper. CURONTO is an Ontological Model for Curriculum Representation which is developed by Al-Yahya, Al-Faries,. and George (2013). This model consists of eight inter related classes for a full curriculum representation, these classes are illustrated in Figure 1 below. A course has a set of CLO (Course Learning Outcomes) of which each CLO is mapped to a PSO (Program Student Outcomes). After mapping PSO to CLO, then the PSO are mapped to PEO (Program Educational Objectives). A course consists also of a course description and it also has a syllabus. The course also has related book(s) either prescribed or reference books and it also has a faculty that it belongs to.

The CURONTO ontology model is utilized as a base of our model in this paper, but it does not entirely accommodate the whole of the syllabus ontology layer, that is; it does not accommodate the KAs, KUs and their topics. This study therefore, created an extension on the syllabus ontology layer in the CURONTO.

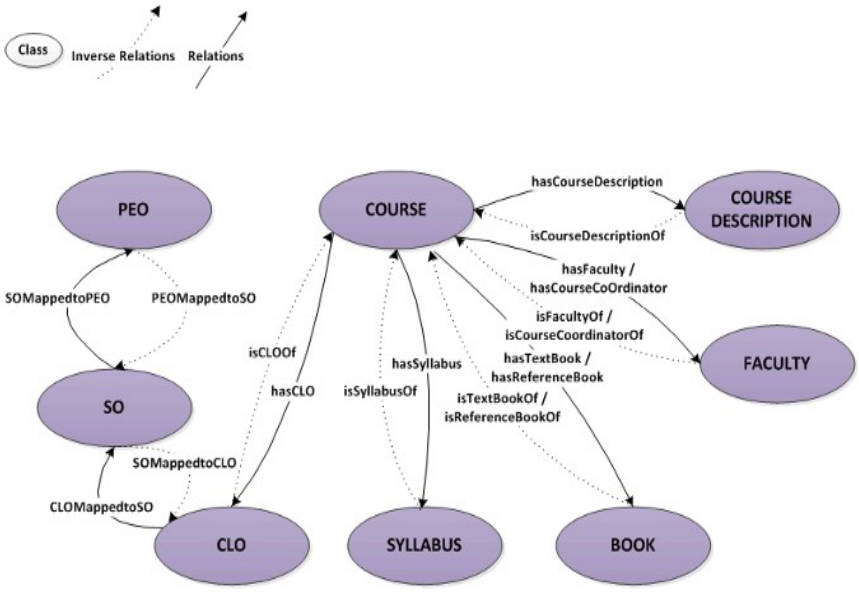

Figure 1. CURONTO

The diagram in Figure 1 is the original CURONTO model which has been adopted and expanded in order to fit this study. The main reason for the expansion is that, the class syllabus is compacted with a lot of other classes inside. This study makes an effort to unpack the syllabus class.

4. Methodology

The methods of investigation in this paper included
•Literature study to elicit CSA syllabus Ontology engineering of the CSA syllabus.
•Ontology Modelling of CSA syllabus.

The course syllabus was elicited from literature. A study was conducted were we studied a number of CSA education initiatives and their contents, Table 1 was elicited from the study as part of the content that will be utilized in our content. Different literature was utilized to elicit the CSA syllabus. This paper drew on research and studies conducted by different authors in order to realize its objectives as discussed in section 2. The South African Cyber Security Academic Alliance (SACSAA) was found to have the best basic CSA areas of knowledge (KAs) and the units of knowledge (KUs), and topics. Criteria for assessment was derived from the topics. These were obtained from a study by Dlamini and Modise (2012) from their website: http://www.cyberaware.org.za/. Some sources utilized in developing the CSA syllabus were the US Veteran office (Cinnamon, 2011), Stop. Think. Connect (APWG & NCSA, 2017) and Get safe online (Get safe online, 2017).
The CURONTO model was then used to develop our proposed model to represent our syllabus in.

Table 1. Information used in CSA content from three initiatives

Initiative	**Information used in CSA content**
Stop. Think. Connect	Protect your personal information (Password as KU, never share personal information as KU)
	Connect with care (Wi-Fi safety as KA)
US veteran office	Password as KU
Get safe online	Protect your computer as KU
	Banking and payments (Internet banking safety as KA)
	Social networking (Social media safely as KA)

5. Proposed model

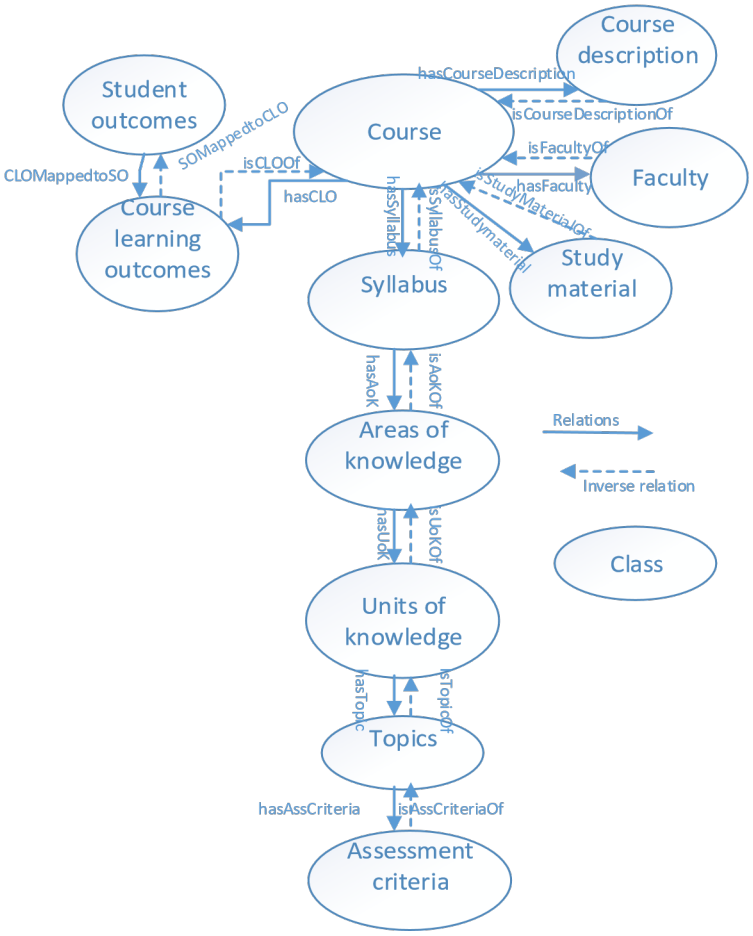

Figure 2. Proposed model for CSA

In this paper, we utilized the information extracted from the CURONTO model described above. The relationship of these classes are described below in the regard of the CSA BOK. Below is the full description of the expanded CURONTO model for CSA in Figure 2. Below is the description of Figure 2.

- The class "Course" has a course description called "Course description", inversely "Course description" is course description of "Course".
- Again "Course" has a faculty which it belongs to called "Faculty", "Faculty" is a faculty of a "Course".
- "Course" has study material which students utilizes namely "Study material", the "Study material" is the study material which belongs to a "Course".

- Lastly "Course" has "Course learning outcomes", and "Course learning outcomes" is the course learning outcomes of the "Course".

- The “Course learning outcomes” class is mapped to Student outcomes labeled “Student outcomes” and “Student outcomes” is also mapped to “Course learning outcomes”
- “Course” has areas of knowledge called “Areas of knowledge”, and “Areas of knowledge” is area of knowledge of “Course”.
- “Knowledge units” has topics “Topics” inversely the “Topics” class is topics of “Knowledge units”.
- A class “Topics” has assessment criteria and the “Assessment criteria” class is the assessment criteria of “Topics”.

We discuss the actual classes for our proposed model in the following section.

5.1. Course

The name of the course is outlined here; in this case the course name is called: Basic Cybersecurity Awareness.

5.2. Course Description

The description is meant to give a clear understanding of what the course is about, or what the course aims to achieve. This course introduces students to the basics of Cybersecurity Awareness (CSA). Basic CSA focuses on the basics of threads and vulnerability of one’s information online and the infrastructure supporting it. The course provides knowledge on the basic cyber intrusion methods and the basic cybersecurity countermeasures to assist in the prevention of cyber-attacks. Students are equipped with the knowledge and ability to interact in a safe and effective way on the cyberspace and securely utilizing the cyber assets. After completion the students will know how to protect themselves on the cyberspace, the skills will help to prevent cyber-attacks and on how to protect their systems and information on the cyberspace.

5.3. Faculty

The faculty that will take responsibility for this course in the organization i.e. the people who will provide the educators, the teaching space, study material or direct students to where they can get the study materials. The custodians of these course are the ICT faculty.

5.4. Study Material

Here the material that the students are going to use to study is outlined. It either be a book, hand out notes, CDs or DVDs or online material etc.

5.5. Syllabus

Syllabus is made up of four classes, which are described below. The CSA syllabus is described in Figure 2.

a) Knowledge areas (KA) – here the knowledge that is available is split up into different sections and labeled.
b) Knowledge units (KU) - The units of knowledge are knowledge pieces inside bigger structure i.e. areas of knowledge, this unit are much narrower, structured and focused than the areas of knowledge which are very broad.
c) Topics - Topics are the subject of conversation or discussion inside the units of knowledge.
d) Assessment criteria - Assessment is the systematic process of gathering information from many sources to make appropriate educational decisions

5.6. Course Learning Outcomes (CLO)

The course learning outcomes defines what the course offers to the students. They actually outline objectives of the course. These outcomes are mapped to the Student outcomes i.e. the student outcomes below are derived from these course learning outcomes.

a) Outline the different methods that can be utilized to protect yourself while online.
b) Fully describe the basics of public Wi-Fi safety.
c) Explain internet banking safety in details.
d) Indicate ways which you can utilize the social network securely.

5.7. Program Student Outcomes (PSO)

Student outcomes are the knowledge, skills, and work practices that students are supposed to gain by the end of the teaching term, such as a course, program, or school year. The student outcomes for the CSA course are as follow:

a) Student will be able to describe ways in which one can protect themselves on the cyber space.
b) Student will be able to outline the different methods that can be utilized to protect themselves from dangers when surfing on the public Wi-Fi.
c) Student will be able to explain how safely manage your internet banking accounts.
d) Student will be able to indicate ways which you can utilize the different social media networks securely.

6. CSA model content

Figure 3. below shows the content of the CSA model that was propose in the previous section. The content was elicited using the methodology described in section 4.

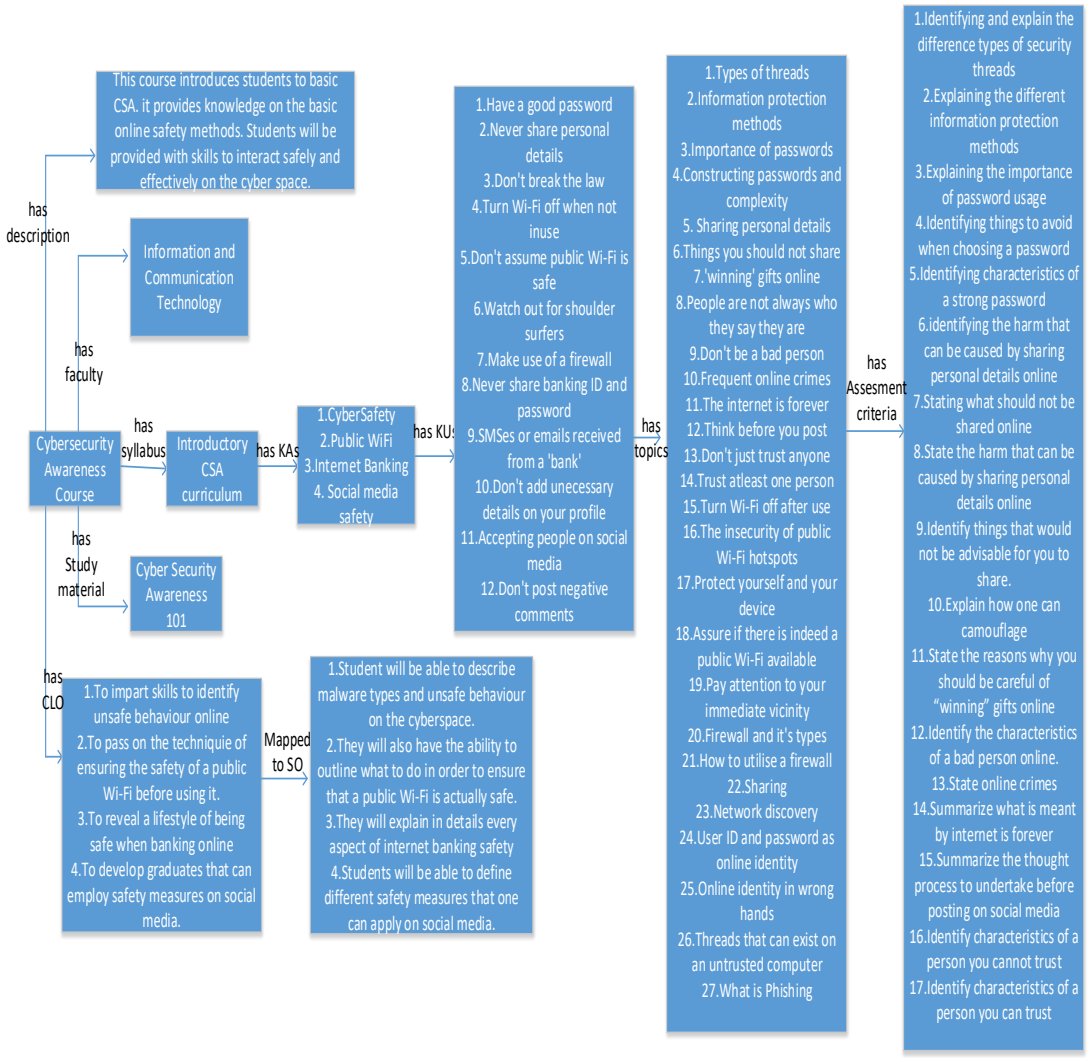

Figure 3. CSA model contents

7. Conclusion

This research aims to develop an ontology which will be used as a base for reaching a consensus on the CSA BoK. From here the ontology model can be implemented using one of the ontology development tool, then it can be applied to different organizations to test if it can really change the CSA in users.

8. References

Abburu, S., Babu, G. (2013) 'Survey on Ontology Construction Tools', *International Journal of Scientific & Engineering Research.* Retrieved from https://pdfs.semanticscholar.org/9748/12a625e0e89036f1969b42e70a3af258d7e1.pdf

Al-Yahya, M., Al-Faries, A. and George, R., (2013, July). *'CURONTO: An ontological model for curriculum representation'*. In Proceedings of the 18th ACM conference on Innovation and technology in computer science education (pp. 358-358). ACM.

Bucci. G, Sandrucci. V and Vicario. E .(2011). *Ontologies and Bayesian Networks in Medical Diagnosis.* Retrieved from https://ieeexplore.ieee.org/abstract/document/5718690
Cinnamon. T., (2011), *How the Department of Veterans Affairs is Implementing the NICE Cybersecurity Framework.* Retrieved from https://www.nist.gov/

Chung, H. and Kim, J. (2016). *An Ontological Approach for Semantic Modeling of Curriculum and Syllabus in Higher Education., International Journal of Information and Education Technology.* Retrived from https://pdfs.semanticscholar.org/

Dlamini, Z., Modise, M. (2012). *Cyber security awareness initiatives in South Africa: a synergy approach*, 7th International Conference on Information Warfare and Security, 10. doi: 10.1007

Get Safe Online. 2017 [Online] available from https://www.getsafeonline.org/ [Accessed: 30 April 2018].

Kapoor B., Sharma S. (2010), *A Comparative Study Ontology Building Tools for Semantic Web Applications.* Retrieved from: Reserchgate.net

Kortjan, N. and Von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1), pp.29-41. Retrieved from https://www.ingentaconnect.com/content/sabinet/comp/2014/00000052/00000001/art00004

Noy, N. F. and McGuinness, D. L. (2001) 'Ontology Development 101: A Guide to Creating Your First Ontology', *Stanford Knowledge Systems Laboratory*, Retrieved from http://www.corais.org/

Programs, P. D. (2017). *Cybersecurity Curricula* 2017, 1(November), pp. 1–111. Retrived from http://www.ncsl.org/documents/taskforces/CSEC_Overview.pdf

Raskin, V., Hempelmann, F., Triezenberg, E. & Nirenburg, S. (2012). *Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool.* Retrieved from https://www.researchgate.net/publication/

Stojanovic L., Motic B.(2002) . *Ontology evolution within ontology editors, international conference on knowledge management,* Retrieved from http://citeseerx.ist.psu.edu/viewdoc/

Takahashi, T. & Kadobayashi, Y. (2011) '3-5 Cybersecurity information exchange techniques: Cybersecurity information ontology and CYBEX', *Journal of the National Institute of Information and Communications Technology*, 58(3–4), 127–135. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/

The times, Crafty cybercriminals are stalking South Africans online, studying their every move via their e-mail accounts – and stealing millions…Library review [Online]Available from: http://www.msn.com/en-za/money/technology. 11 November 2015 [Accessed: 13th November 2015].

Thirugnanam, M. (2013) 'An Ontology Based System for Predicting Disease Using SWRL Rules', *International Journal of Computer Science and Business Informatics*. Retrieved from http://www.ijcsbi.org/index.php/ijcsbi/article.

Van Vuuren, J. C. J. Van, Leenen, L. and Zaaiman, J. J. (2012), Using *an ontology as a model for the implementation of the National Cybersecurity Policy Framework for South Africa*, Retrived from https://researchspace.csir.co.za/dspace/handle/10204/7869

Von Solms, R. Von and Van Niekerk, J. (2013). *From information security to cyber security*, Retrieved from https://www.sciencedirect.com/science/article/pii/S016740481300080