Systematic Review: Cybersecurity Risk Taxonomy

A.M. Rea-Guaman[1], T. San Feliu[1], J.A. Calvo-Manzano[1] and I.D. Sanchez-Garcia[2],

[1] Universidad Politécnica de Madrid, ETS Ingenieros Informáticos
Madrid, España
marcelo.rea.guaman@alumnos.upm.es
{tomas.sanfeliu, joseantonio.calvomanzano}@upm.es

[2] Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica
Ciudad de México, México
issanchez@ipn.mx

Abstract. In cybersecurity, the identification of risks is a fundamental part because this activity is not unique to cybersecurity and it is hard to know what the risks in this area are. This study aims to identify if there are some risk taxonomies in cybersecurity. For this, a systematic review of the studies published from 1990 to 2017 was carried out. We found 132 papers and some of them mention some risk taxonomies within the scope of IT (information technologies) cybersecurity, although only five primary elements were selected, identifying the main risk taxonomies. A classification of cybersecurity risk taxonomy types has been adapted, with the inclusion of new categories, categorized according to their perspective and domain. We have analysed the taxonomies form a proposed five level perspective. Finally, it has been observed that risk taxonomies may be shifting the focus from the asset level to service and business level.

1 Introduction

In recent years, interest in cybersecurity has been increasing. As our world becomes increasingly interconnected, real-time availability of systems becomes more and more necessary. Therefore, the impact that cyber threats can cause to organizations can be large, and the care and protection of information assets within organizations is of great importance. And the assets are important and crucial in critical business processes. Also, the information that is shared in the different technologies has an increasing value for consumers and users. The information contained in the systems is more valuable than the technologies that contain the systems, more and more private and governmental organizations have combined efforts to standardize the identification of risks that affect cybersecurity.

How organizations address the cybersecurity risks in their organizations is essential in order to implement effective, efficient and sustainable cybersecurity. Therefore, it is necessary to identify the risks that affect organizations in the area of cybersecurity. There are risks in almost all areas of the organizations. Risks that fall into cybersecurity and are difficult to identify, cybersecurity risk taxonomies assist in determining the risks that exist within the scope of cybersecurity.

Based on the above, a systematic review was carried out to identify the main taxonomies and classification of cybersecurity risks. Thus, this paper is organized as follows: Section 2 presents the concept of risks and it includes the cybersecurity risk, Section 3 presents the details of the systematic review process; Section 4 analyses and interprets the results of the systematic review; Section 5 reports on the results of the systematic review based on the different taxonomies of existing or applicable cybersecurity risks, includes the adaptation of a new classification of taxonomies with the inclusion of new categories, according to their perspective and, finally, Section 6 presents the conclusions.

2 Context

A definition of risk according to ISACA is: "The combination of the probability of an event and its consequence" [1]. This is a definition that applies to any field, whether it is an environmental risk, a work risk or a risk in the field of information technology. Different classifications have been made to identify the cybersecurity risks, for the different areas because have particular characteristics.

To better understand what a cybersecurity risk is, the following concepts are presented according to ISACA. To understand the term cybersecurity, we must first define the term cybersecurity risk. "Cybersecurity risk is not one specific risk. It is a group of risks, which differ in technology, attack vectors, means, etc. We address these risks as a group largely due to two similar characteristics: A) they all have a potentially great impact B) they were all once considered improbable" [2]. "Cybersecurity is the sum of efforts invested in addressing cybersecurity risk, much of which was, until recently, considered so improbable that it hardly required our attention" [2].

By the previous definitions, we know that the handling of a cybersecurity risk is different from the other types of risks and, in turn, the risks in cybersecurity are being very variable. It is therefore important to have a taxonomy that helps to identify and classify the risks inherent in cybersecurity.

In this paper, it is intended to answer through a systematic literature review the following question: Are there any risk taxonomy related to cybersecurity published?

In order to answer the question, the proposed systematic review technique by Kitchenham is used [3], [4]. A systematic review is a formal and verifiable process that the researcher performs to document the state of knowledge in a specific subject. The systematic review [4] makes possible to: (1) review the relevant work that has been done in the area of study, (2) examine the results, evaluate and contrast them, and (3) identify gaps in current research in order to do an appropriate proposal for a new research activity.

3 Systematic review

The systematic review includes the following activities: (A) identifying the needs, (B) proposing a review protocol, (C) conducting the review (identifying primary studies, evaluating studies, and synthesizing information), (D) analysing and interpreting the results, and (E) reporting the results of the systematic review.

Next, the process of the systematic review related to cybersecurity risk taxonomies published is detailed. Section 4 and 5 of the paper present the activities D and E of the systematic review.

3.1 Identification of the Needs for the Systematic Review

A systematic review was required to identify the different taxonomies of cybersecurity risks that have been published.

3.2 Review Protocol

At this point the following tasks were defined: Formulation of the questions to be asked, the criteria for selecting the database sources, the database sources to be used for the search, the elaboration of the search strings according to the defined criteria and the search in the sources, to locate and select the studies.

Formulation of the question. Question(s): What risk taxonomies have been proposed for cybersecurity?

The issues and questions related to the needs and objectives of the review were raised.

- Problem: there is a need to implement cybersecurity risk taxonomies in organizations, but it is not known which have been proposed. This also makes possible to determine a trend of implementation.
- Questions: What risk taxonomies have been proposed for cybersecurity?
- Population: publications related to risk taxonomies in cybersecurity, security management in information systems, and applications in organizations.
- Intervention: different taxonomies of cybersecurity risks that have been published/used.
- Effect: to know if there are any taxonomy that cover all areas of cybersecurity or not.
- Result measurement: proposed cybersecurity risk taxonomies, their descriptions and approaches.
- Application: to know the different taxonomies of cybersecurity risk, and their approaches.

Criteria for the selection of sources. The criteria for the selection of sources were: database that include journals and papers focused on cybersecurity risk taxonomy and have advanced search mechanisms, making use of the terms and synonyms used in

search queries; availability of full text papers; papers available on the web for free; specialized magazines are available in the library of the Universidad Politécnica de Madrid.

Identification of the sources. Specialized databases such as IEEE Computer, Science Direct, ACM Digital Library and Web of Knowledge are among the selected sources.
Search string. The terms used in the systematic review were constructed using the following criteria: (1) "Cybersecurity Risk Taxonomy", (2) "Cybersecurity Risk", (3) "Risk Taxonomy" and (4) "cyber risk taxonomy". These keywords, combined with the logical operators AND and OR, as well as the NOT operator to refine the search, were used in the search engines of the specialized databases.

The words used in the search string include: "Taxonomy", "cybersecurity", "risk", "cyber risk".

Search in the sources. We searched the sources using the criteria defined previously for their selection. All sources of the identified databases were included. Search strings were applied to electronic databases and other sources (journals and conferences). To evaluate the list of sources obtained, were involved two experts in cybersecurity risk taxonomies.

3.3 Review

At this point, the search of the papers in the databases selected with the predefined search strings is displayed. The review is done in three phases. The inclusion and exclusion criteria established below were applied to the search results.

Criteria for selecting studies and procedures for inclusion and exclusion within the primary studies. The Table 1 lists the inclusion and exclusion criteria that were applied to the results of the initial search. The selection of studies was focused on those related to cybersecurity risk taxonomies published.

Table 1. Inclusion and Exclusion Criteria.

Inclusión (I)	Exclusión (E)
I1. Empirical studies of cybersecurity risk taxonomies that have related content in showing some risk classification that applies to cybersecurity.	E1. Papers that are based only on a particular opinion that does not address cybersecurity.
I2. Papers that discuss taxonomies or classifications of cybersecurity risks.	E3. Studies that are not relevant to the research question or are not related to the particular study.
I3. Papers that use keywords.	E4. Studies that are unclear or ambiguous.
I4. Papers whose title, summary or content are related to the topic.	E5. Duplicate publications.
I5 Free access documents.	E6 Pre-1990 studies due to constant updating in the area.

In a first phase of the review, making use of the search engines of the identified databases and putting the search string elaborated in the task "the search string" of the activity "review protocol", a total of 132 studies were found.

In the second phase of the review, each study was reviewed taking into account the previous inclusion and exclusion criteria, obtaining a total of 14 relevant studies. To select the relevant studies, the following steps were taken: read the title, read the summary, read the conclusions and fill in template created, if they provide enough information, the study is selected and saved. Otherwise, it is deleted.

In the third phase of the review, five primary studies were obtained that answered the questions formulated initially. Table 2 shows the sources, the total number of papers, and the number of primary paper selected by source.

Table 2. Distribution of studies by source.

Source	Total	Relevant	Primary
IEEE Explore	11	3	2
Science Direct	6	0	0
ACM Digital Library	8	0	0
Web of Knowledge	107	11	3
Total	**132**	**14**	**5**

Evaluation of study quality. To assess the quality of the studies, the following questions were asked:

- Is the primary study relevant to the research being done?
- Do primary studies provide enough information for the results to benefit from the systematic review?

From the previous questions, it was verified that the five primary studies selected are relevant, provide sufficient information and add value to the systematic review.

Data extraction and synthesis. To extract the important information of each paper, a template was designed. The template contains the following fields: (1) paper identification, (2) reference (title, author, year), (3) type of paper (case study, survey, experiment, research), (4) purpose of the study, (5) context of the study, (6) type of study (improvement, deployment or both), (7) depth of analysis (high, medium, low), (8) cybersecurity risk taxonomies published, (9) area and approach to taxonomy, and (10) observations

For each paper selected, after reading the full text, the information was recorded on the form, which allowed for the subsequent analysis of the results.

4 Analysis and interpretation of the results of the systematic review

At the conclusion of the systematic review, the context of each document was analyzed, for those documents that proposed a taxonomy in cybersecurity, the proposed risk classification was analyzed, and its focus and scope.

According to their context they were classified in:

- Framework related risk.
- Concepts on how to perform a taxonomy.
- Taxonomy focused on a specific area.

There is one framework enterprise risk management (ERM), one concept on how to perform a taxonomy of information security risks and three taxonomies focused in: social engineering, software providers and information security risk.

The results of the systematic review are presented below, the primary items found are described in the Table 3 for further analysis.

Table 3. Primary studies

Paper	Context	Author
Three key enablers to successful enterprise risk management.	Risk management	Kanel (2010)
Taxonomy of information security risk assessment (ISRA)	Information security risk	Alireza (2016)
Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing	Perform a taxonomy of information security risks	Elnagdy (2016)
Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits Developing a Risk Management	Taxonomy focused on social engineering	Greitzer (2014)
Process and Risk Taxonomy for medium-sized it solution providers	Taxonomy focused on software providers	Herzfeldt (2012)

In order to obtain complementary studies, the technique of snowballing has been applied. This has allowed to obtain two additional studies from [8] and one additional study starting from [5]. Additionally, a search in Google Scholar provided two complementary taxonomies.

These complementary studies are shown in the Table 4.

Table 4. Primary studies

Paper	Context	Reference
A Taxonomy of Operational Cyber Security Risks.	Enterprise	Cebula (2010)
The structure of a cyber risk a scenario based approach in cyber risk assessment	Enterprise	Delmee (2016)
Securing smart grid: cyber attacks, countermeasures, and challenges	Smart grid	Li (2012)
Classification and trend analysis of threats origins to the security of power systems	Energy systems	Bompard (2013)
Development of methodical social engineering taxonomy	Social engineering	Larebee (2006)

5 Results report of systematic review

Once each of the primary studies was selected and analysed, the published cybersecurity risk taxonomies were identified, and the area and focus were determined, as well as the frameworks and risk management models.

- The document of Kanel, J [9] addresses a risk taxonomy that includes cybersecurity risks and financial risks in organizations based on the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework.
- In the document of Elnagdy, S [8], it was found a taxonomy of basic cyber-attacks in smart grid, and a classification of malicious threats.
- The document of Greitzer F [5] presents a taxonomy of risks focused on social engineering.
- We identified that the author Herzfeldt A [6] presented a taxonomy of shrouded risks and IT system vendors is provided, which categorize the risks from the need identification to the implementation and maintenance of the system.
- The paper of Cebula, J [10] presented a Taxonomy of Operational Cyber Security Risks that mentions an adequate taxonomy of risks in cybersecurity. This is divided into four classes: actions of people, systems and technology failures, failed internal processes, external events.
- The paper of Delmee, F [11] created a cyber risk taxonomy based on a scenario based risk approach. The scenarios are further elaborated with contextual information about the victim and threat agent to identify all the relevant concepts within the scenario.
- We identified that the author Li, X [12] presents a taxonomy of basic cyber-attacks in smart grid communication. In this taxonomy, there are four types of attacks: device attack, data attack, privacy attack, and network availability attack. They have different objectives and are often the building blocks of more sophisticated attacks.
- The paper of Bompard, E [13] due to the growing recognition of the importance of power systems in today's society, a classification of malicious threats is presented, there are three malicious threats: physical threat, human threat and cyber threat.
- We identified that the author Laribee, L [14] in his study presented a taxonomy for encoding social engineering attacks, proposes four main dimensions of interest in determining the type and severity of a social engineering attack. The first category is the target, the second category is the type of deception, the third category is the particular resource or target information, and the fourth category is the thrust ploy.

To analyze the results, we have extended a classification of taxonomy types obtained from Alireza, S [7]. The Alireza's classification has three levels of bottom-up abstractions that are asset, services, business. Although most taxonomies rely on asset level, new studies are shifting the focus and moving to the level of service and business. We have included source attacks and external events as two complementary categories. We have added these two new categories, due to the difficulty of matching the classification elements of the taxonomies found and which were difficult to fit into

the categories proposed by Alireza, S [7]. Each element of the analyzed taxonomies has been mapped to one of the five categories, the results of this mapping are shown in Table 5.

Table 5. Summary of taxonomies

Author	Domain	Perspective	Taxonomy Items
Kanel et al. (2010)	Enterprise	Asset + Service + Business + External	Sources and events Business objects and dynamics models Risk impacts
Li et al. (2012)	Smart grid	Asset + Attack + Business	Device Attack Data Attack Privacy Attack Network Availability attack
Bompard et al. (2013)	Energy Systems	Attack + Business + External	Physical threat Human threat Cyber threat
Greitzer et al. (2014)	Social engineering	Asset +Attack	Interaction personal Non Interaction personal
Laribee (2006)	Social engineering attacks	Asset + Attacks	Target Type of deception Resource or target information Trust ploy
Herzfeldt et al. (2012)	IT Solutions	Services + Business + External	Environment Provider Risk IT solution Risk Customer Risk
Cebula et al. (2010)	Enterprise	Asset + Service + Business + External	Actions of people Systems and technology failures Failed internal processes External Events
Delmee. (2016)	Enterprise	Asset + Service + Attack+ Business	General information Organization (victim) Threat agent Asset Threat event Business impact Vulnerabilities Control

The analysis indicates that all taxonomies take into account the Asset and Business level, with the exception of taxonomies specialized in social engineering. This is because they are focused on aspects of human interaction. It is noteworthy that specialized smart grid taxonomy, focuses solely on aspects of possible forms of attacks.

It is common in all other taxonomies besides the business aspect, take into account aspects of asset, service and external events. This is due to the need to identify threats

to both resources and business activities. External events must be taken into account as they have to be monitored.

The most modern taxonomy, such as Delmee, F. [11], combines the three levels of abstraction with the category of sources of attack. This could indicate that risk taxonomies could be shifting the focus form the asset level to the abstraction levels of services and business.

6 Conclusions

This paper reviewed the cybersecurity taxonomy documents published in the conferences and journals process to understand progress in cybersecurity risk taxonomies. The objective was to identify the studies with respect to risk taxonomies that have been proposed for cybersecurity.

In order to obtain complementary studies, the technique of snowballing has been applied. This has allowed to obtain two additional studies from [8] and one additional study starting from [5],

The results are based on the results of five primary studies identified in the search engines selected for the review, two files identified in the snowballing of Elnagdy, S [8], one paper of Greitzer, F [5] and two primary files identified in the additional search in the Google Academic search engine, which may be a relatively low percentage of the total population of files obtained without applying the inclusion and exclusion criteria.

There are different types of risk taxonomies. Each of these taxonomies have been developed to meet a particular need. We have provided a general view and structure of risk taxonomies. Also, we have developed a new classification of taxonomy types. Based on this classification we have analyzed the taxonomies found and identified that most of them are of particular application and cannot be applied in other domains.

The taxonomies identified only abrogated specific risks such as social engineering risks, financial risks, operational risks, malicious threats and risks taxonomy based in certain specific scenarios.

In the paper of Elnagdy, S [8], it does not present a taxonomy, but it indicates the concepts necessary to be able to define a taxonomy of risks that can be applied in cybersecurity in the cloud.

The most modern taxonomy of cybersecurity risks is Delmee, F [11] study, based on a scenario based risk approach, and is distributed in eight different concepts and fifty-one characteristics.

Using the protocol of this systematic review as a starting point, additional searches from primary studies and new sources of studies will be reviewed in future iterations in order to complete the collection of taxonomies. We believe that this survey and study of risk taxonomies are important, in that it will help explain the different abstraction levels and could led to the development of more comprehensive and effective risk taxonomies.

References

1. ISACA Glosary (2016), https://www.isaca.org/Pages/Glossary.aspx?tid=1784&char=R.
2. ISACA, http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296.
3. Kitchenham, B., Dybå, T., Jørgensen, M.: "Evidence-based software engineering," Proceedings of the International Conference on Software Engineering, pp. 273–281 (2004)
4. Kitchenham, B.: "Guidelines for performing systematic literature reviews in software engineering," EBSE Technical Report EBSE-2007-01, Keele University (2007)
5. Greitzer, F., Strozer, J., Cohen, S., Moore, A., Mundie, D., Cowley, J.: Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. IEEE Security and Privacy Workshops, vol 35, 236-250 (2014)
6. Herzfeldt, A., Hausen, M., Briggs, R. O., Krcmar, H.: European Conference on Information Systems ECIS 2012. Developing a risk management process and risk taxonomy for medium-sized it solution providers. Association for Information Systems, Barcelona Spain (2012)
7. Alireza, S., Rouzbeh, B., Cheriet, M. (2016) Taxonomy of information security risk assessment (ISRA). Computers & security, vol 57, 14-30 (2016)
8. Elnagdy, S., Meikang, Q., Keke, G. (2016) Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing. IEEE International Conference on Cyber Security and Cloud Computing, vol 3, 295-300 (2016)
9. Kanel, J., Cope, E., Deleris, L., Nayak, N., Torok, R.: Three key enablers to successful enterprise risk management. IBM J. RES. & DEV, vol 54, 1-15 (2010)
10. Cebula, J., Young L.: A Taxonomy of Operational Cyber Security Risks. Software engineering institute. Recovered from: http://resources.sei.cmu.edu/ library/asset-view.cfm?assetid=91013 (2010)
11. Delmee, F.: Graduation research, The structure of a cyber risk a scenario based approach in cyber risk assessment. Utrecht University, Deloitte Nederland (2016)
12. Li, X., Liang, X., Lu, R., Lu, Shen, X., Lin, X., Zhu, H.: Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Communications Magazine, 50(8):38–45 (2012)
13. Bompard, E., Huang, T., Wu, Y., Cremenescu, M.: Classification and trend analysis of threats origins to the security of power systems. International Journal of Electrical Power & Energy Systems, 50:50– 64 (2013)
14. Laribee, L.: Development of methodical social engineering taxonomy. Master's Thesis, Monterey, CA: Naval Postgraduate School. Amazon Digital Services (2006)