EXACTA Engenharia de Produção eISSN 1983-9308

Editor: Dr. Luiz Fernando Rodrigues Pinto, Universidade Nove de Julho, Uninove / São Paulo - SP, Brasil

Submissões para este periódico

ABORDAGENS DE PESQUISAS DE AVALIAÇÃO DE RISCOS CIBERNÉTICOS: UM ESTUDO BIBLIOMÉTRICO

Versão do autor aceita publicada online: 27 fev. 2023

Publicado online: 08 mar. 2023

Como citar esse artigo - American Psychological Association (APA):

Silva, D. S., Oliveira, F. P., Ribeiro, J. S. A. N, Ribeiro, J. C. B., & Andrade, D. L. (2023). Abordagens de pesquisas de avaliação de riscos cibernéticos: um estudo bibliométrico. *Exacta*. doi: https://doi.org/10.5585/2023.21072

Daniel Sathler Silva

Universidade FUMEC / Brasil - *Contato principal para correspondência.*

Fabio Pires de Oliveira

Universidade FUMEC / Brasil

Jurema Suely de Araújo Nery Ribeiro

Universidade FUMEC / Brasil

Juliana Caldeira Bicalho Ribeiro

Universidade FUMEC / Brasil

Denilsio Lino Andrade

Universidade FUMEC / Brasil

Resumo

Diversas abordagens podem ser utilizadas em pesquisas sobre a avaliação de riscos cibernéticos e a falta de padronização e de definição dificulta a aplicação e a organização de conceitos sobre o tema. É com esse argumento que surge a motivação deste estudo: quais são os termos, métodos e tipos de pesquisa utilizados por trabalhos relacionados à avaliação de riscos cibernéticos na literatura científica internacional? Este artigo, a partir de uma metodologia de caráter bibliométrico, busca explorar as abordagens empregadas quanto aos métodos, tipos de pesquisa e termos adotados. O objetivo proposto foi alcançado por meio de análises de conteúdo com o intuito de identificar e quantificar características nas publicações. Foi possível observar um aumento do volume de publicações que utilizam métodos qualitativos/quantitativos a partir de 2013. Para os trabalhos que buscam a melhoria de métodos de avaliação de riscos cibernéticos, 79% destes trabalhos visam aprimorar métodos quantitativos.

Palavras-chave: Avaliação de Riscos Cibernéticos. Gerenciamento de Riscos. Segurança da Informação.

Cyber Risk Assessment Research Approaches: A Bibliometric Study

Abstract

Different approaches can be used in cyber risk assessment research. It is harder to use and organize the risk assessment concepts due the lack of standardization and definition. With this argument the motivation for this study arises: what are the terms, methods and types of research used by works related to risk assessment in the international scientific literature? This article, based on a bibliometric methodology, explores in works that have the theme of risk assessment which approaches are used in terms of methods, types of research and terminology adopted. The objective was achieved through the content analysis in order to identify and quantify characteristics in the publications. In addition, it was observed an increase in the volume of publications that use qualitative/quantitative methods from 2013 onwards. For works that seek to improve cyber risk analysis methods, 79% of the works uses quantitative methods, which have greater complexity of use and application.

Key words: Information Security. Risk Assessment. Cyber Risk Management.

1 INTRODUÇÃO

Nas últimas décadas, os dados se transformaram no elemento de maior importância para organizações de diferentes segmentos. Dados contábeis, pessoais, perfis de consumo, entre outros, são armazenados em dispositivos de alto poder computacional que, por sua vez, são vulneráveis a diferentes tipos de ameaças, as quais podem afetar a disponibilidade desses dados. O cenário apresentado resulta em riscos que devem ser observados pelas organizações. A identificação, a mitigação e a análise dos riscos desses dispositivos e sistemas são pontos que devem ser considerados pelas corporações em seus processos de gerenciamento de riscos empresariais (Rahman & Donahue, 2010).

Os riscos e as ameaças modificam-se todos os dias. As práticas de segurança da informação das organizações devem adotar uma abordagem de gerenciamento de risco, o qual é benéfico para a governança de tecnologia da informação (TI), visto que a governança deve garantir a

continuidade do negócio contra interrupções e falhas, bem como a conformidade com aspectos legais ou regulatórios.

Práticas de avaliação de riscos apresentam variações entre diferentes áreas, disciplinas e, até mesmo, dentro de uma mesma organização (Wangen, Hallstensen & Snekkenes, 2018). Diversas abordagens podem ser utilizadas em pesquisas sobre a avaliação de riscos, visto que autores vêm utilizando diferentes termos para referir-se ao tema citado e os trabalhos podem diferir-se quantos aos métodos utilizados e aos tipos de pesquisas.

Andronache e Althonayan (2018) apontam que variações na terminologia podem gerar confusão e ocasionar o uso indevido de termos por autores. Por sua vez, a falta de padronização e de definição dificulta a aplicação e a organização de conceitos sobre o tema. É com esse argumento que surge a motivação deste estudo: quais são os termos, métodos e tipos de pesquisa utilizados por trabalhos relacionados à avaliação de riscos cibernéticos na literatura científica internacional?

Este artigo, a partir de uma metodologia de caráter bibliométrico, busca explorar em trabalhos que possuem a temática de avaliação de riscos cibernéticos quais são as abordagens empregadas quanto aos métodos, tipos de pesquisa e termos adotados. Diante do cenário apresentado, três hipóteses foram formuladas: i) os termos mais utilizados para referir-se a trabalhos de avaliação de riscos cibernéticos são, respectivamente, *information security* e *cybsersecurity*; ii) a maior parte das pesquisas relacionadas à avaliação de riscos faz o uso de métodos quantitativos; iii) o tipo de pesquisa com maior incidência é o de melhoria de métodos de avaliação de riscos.

Além da presente seção introdutória, este trabalho é composto pelo item 2, correspondendo à revisão da literatura. Já a metodologia utilizada é apresentada na seção 3. Por sua vez, a análise dos resultados é apresentada na seção 4. Por fim, as conclusões estão dispostas no item 5.

2 REVISÃO DA LITERATURA

A seção “revisão da literatura” encontra-se dividida em três subseções, a saber: (2.1) avaliação de riscos, (2.2) gerenciamento de riscos (2.3) riscos cibernéticos e (2.4) segurança da informação.

2.1 Avaliação de Riscos

Risco é a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. Pode ser uma oportunidade ou uma ameaça aos objetivos da organização, sendo que uma afeta negativamente e a outra, positivamente os objetivos do projeto (Monteiro, 2017).

A probabilidade de ocorrência e de impacto que o risco exerce sobre os objetivos organizacionais é o que o define. Portanto, quanto maior for a probabilidade e o impacto, maior será o nível desse risco para a organização. Enquanto a probabilidade está associada às chances de o evento acontecer, o impacto está associado ao efeito que o evento ocorrido exerce sobre os objetivos, ou seja, a materialização do risco (Fraporti & Barreto, 2018).

Os métodos de avaliação de riscos concentram-se em como uma organização identifica os riscos individuais definidos como a probabilidade de uma ocorrência negativa que ameaça a realização dos objetivos (Slay & Koronios, 2006). Esses métodos podem ser implementados, por exemplo, através de um questionário administrado a um grupo de pessoas que interagem com aspectos relacionados à segurança da informação (Shamala, Ahmad, Zolait & Sahib, 2015). A avaliação de riscos é uma das atividades previstas durante o processo de gerenciamento de riscos, o qual será abordado no próximo tópico.

2.2 Gerenciamento de Riscos

Uma das funções essenciais da governança de TI é o gerenciamento de riscos, uma vez que deve possibilitar a implantação de mecanismos que garantam a continuidade do negócio contra interrupções e falhas. O gerenciamento de riscos apoia a investigação e a análise do ambiente de TI, para verificar se a organização atende aos requisitos regulatórios e de negócios considerados prioritários (Molinaro & Ramos, 2011).

A gestão da segurança de ativos informacionais deve contemplar o gerenciamento de riscos, visto que possibilita a minimização do impacto de eventos potencialmente negativos. O próximo tópico abordará os conceitos relacionados à segurança da informação.

2.3 Riscos Cibernéticos

Os ativos informacionais estão sujeitos a diversos ricos cibernéticos, os quais podem comprometer a confidencialidade, disponibilidade e integridade de seus dados. Nesse contexto, é necessário entender os conceitos de ameaça e de vulnerabilidade. Machado (2014) define ameaça como uma causa potencial de um incidente indesejado, que pode resultar em dano para um

sistema ou organização. Já vulnerabilidade é definida pelo autor como uma fragilidade de um ativo ou um grupo de ativos que pode ser explorada por uma ou mais ameaças.

Agentes maliciosos podem colocar em prática planos de fraude e exploração de sistemas com o objetivo de usufruir de dados roubados. Dentre as ameaças virtuais, destaca-se a espionagem via Internet, também conhecida como espionagem cibernética, normalmente surgem de invasores contratados para atacar determinada organização e passam facilmente despercebidas, pois seu foco de infecção não é uma rede inteira, mas, sim, um computador específico de um funcionário comum, mas que compartilha a rede com máquinas importantes. Já o furto de identidade e violação de dados ocorre quando alguém pratica fraudes com os dados alheios para obtenção de vantagem indevida, o que envolve, por exemplo, informações pessoais, números de cartões, senhas, nomes de usuários e dados bancários (HSC, 2019).

Em um experimento, Walker-Roberts et al. (2020) utilizaram um banco de dados de ciberincidentes para investigar os riscos de incidentes no mundo físico e observaram como resultado que um dos ativos mais comumente atacados era a informação por meio de métodos de abuso de privilégios e que as principais caraterísticas eram as violações internas na própria organização, muitas vezes provenientes de erro humano (Sotolani, Galegale & Feitosa, 2022)

2.4 Segurança da Informação

A segurança da informação consiste na determinação de diretrizes e ações referentes à segurança dos aplicativos, da infraestrutura, dos dados, das pessoas e das organizações (Fernandes & Abreu, 2012). Fontes (2006) define como o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

Os três princípios centrais em todo e qualquer programa de segurança da informação são: confidencialidade (capacidade de garantir que o nível necessário de sigilo seja aplicado em cada junção de dados em processamento), integridade (garantia de rigor e confiabilidade das informações e dos sistemas e de que não ocorrerão modificações não autorizadas de dados) e disponibilidade (capacidade que os sistemas e as redes devem ter para executar e disponibilizar os dados de forma previsível e adequada às necessidades), também conhecidos como a tríade CIA (Machado, 2014). As significantes informações criadas, processadas e manipuladas pelos processos tecnológicos demandam uma forte camada de segurança da informação observando os seus pilares: integridade, confidencialidade e disponibilidade (Sotolani, Galegale & Feitosa, 2022).

Lenstra e Voss (2004) propuseram um modelo quantitativo para avaliar e agregar riscos de segurança da informação, bem como encontrar uma estratégia de mitigação de risco que seja ótima em relação ao modelo utilizado e ao orçamento disponível.

3 MÉTODO E MATERIAIS DE PESQUISA

O presente trabalho é parte de um estudo desenvolvido entre os meses de junho e julho de 2021. Foram buscados, em relevantes bases de dados, artigos científicos sobre a temática proposta, conforme descrição apresentada no Quadro 1. A metodologia apresenta caráter bibliométrico, uma vez que tem como objetivo, a partir de exploração preliminar, identificar e quantificar temas e tendências no material (Rodrigues, Tavar, Nogueira & Librelotto, 2016).

Quadro 1 – Descrição metodológica.

Critério	**Descrição**
Descritores pesquisados	A expressão utilizada é composta por dois termos, unidos pelo operador "AND": 1. Título: a. "Computer Security" OR "IT Security" OR "Electronic Security" OR "Digital Security" OR "Internet Security" OR "IT Risk Management" OR "Data Security" OR "Information Security" OR "Information Assurance" OR "Information Security Management Systems" OR "Cyber Threat Management" OR "Cybercrime Security" OR "Cyber Security" OR "Cybersecurity" OR "Cybersecurity Risk Management" OR "Cybersecurity Management" b. "Risk Management" OR "Risk Assessment"
Categoria	Artigos científicos publicados em periódicos.
Idiomas	Qualquer.
Bases de dados	Scopus e Scielo.
Critérios de exclusão	Artigos não disponíveis para *download*.
Contexto	Práticas de avaliação de riscos apresentam variações entre diferentes áreas, disciplinas e, até mesmo, dentro de uma mesma organização.
Justificativa	Variações na terminologia podem gerar confusão e o uso indevido de termos por autores. Diferentes métodos e tipos de pesquisas podem ser utilizados por trabalhos, a falta de padronização e de definição dificulta a aplicação e a organização de conceitos sobre o tema.

Fonte: Elaborado pelos autores (2021).

Conforme apontado pelos autores Andronache e Althonayan (2018), diferentes termos vêm sendo utilizados para referir-se a temas relacionados à segurança cibernética e incluem: *Computer Security; IT Security; Electronic Security; Digital Security; Internet Security; IT Risk Management; Data Security; Information Security; Information Assurance; Information Security Management Systems; Cyber Threat Management"; Cybercrime Security; Cyber Security; Cybersecurity; Cybersecurity Risk Management* ou *Cybersecurity Management*. Os termos citados foram utilizados na construção da expressão de busca, informada no Quadro 1. Além disso, *Risk Management* e *Risk Assessment* foram adicionados a *string* de busca com o objetivo de filtrar os trabalhos relacionados ao gerenciamento de riscos.

A base de dados Scopus apresentou-se como a mais importante fonte de informações deste trabalho, uma vez que indicou 567 trabalhos na busca do campo título dos trabalhos, após aplicar o filtro de tipo de documento *article*, obteve-se 181 resultados e, após aplicar o filtro *Open Access*, foram encontrados 53 artigos científicos para *download*. Não foram adicionados filtros para a data de publicação e o artigo mais antigo encontrado foi publicado em 2004. A busca pela *string* foi realizada também na base de dados Scielo, porém não retornou nenhum resultado.

O *software* Microsoft Excel foi utilizado para a categorização dos 53 trabalhos da amostra resultante. Cada artigo foi identificado por um número, sendo explorados e registrados os seguintes metadados: autores, título, ano de publicação e palavras-chave.

As palavras-chave presentes em todos os artigos foram reunidas para a elaboração de uma nuvem de palavras, objetivando-se melhor compreensão dos termos adotados. Foi utilizado o *software* Microsoft PowerPoint, no qual foram desconsideradas as diferenças entre letras maiúsculas e minúsculas.

Já os métodos para avaliação de riscos podem ser classificados como qualitativos, quantitativos ou qualitativos/quantitativos (Valis &Koucky, 2009). O Quadro 2 descreve os métodos citados.

Quadro 2 – Métodos para a avaliação de riscos.

Método	**Descrição**
Qualitativos	Avaliação que comumente define o impacto, a probabilidade e o nível de risco, por meio de métricas de significância, como "alto", "médio" e "baixo", conforme critérios qualitativos.
Quantitativos	Avaliação em que valores numéricos, utilizando uma escala pré-definida, são atribuídos para o impacto, a probabilidade e o nível de risco.
Qualitativos/quantitativos	Avaliação em que são empregados valores numéricos para mensurar o impacto, a probabilidade e o nível de risco, entretanto critérios qualitativos são utilizados para a interpretação dos valores citados.

Fonte: Elaborado pelos autores (2021).

Conforme apresentado no Quadro 2, os métodos quantitativos atribuem valores numéricos para os elementos da avaliação de risco, processo que pode ser complexo e difícil de ser conduzido (Macek, Magdalenic & Redep, 2020). Já os métodos qualitativos são frequentemente baseados em julgamentos subjetivos dos membros da equipe de avaliação de risco (Kalinin, Krundyshev & Zegzhda, 2021). Por fim, as abordagens qualitativas/quantitativas apresentam uma solução de compromisso para as características dos métodos anteriormente citados, uma vez que preveem a utilização de valores numéricos para os elementos da avaliação de risco e permite a interpretação por meio de critérios qualitativos.

Por sua vez, é possível classificar o tipo da pesquisa de avaliação de riscos. Pan e Tomlinson (2016) propõem sete tipos para a classificação de trabalhos relacionados à temática citada, os quais são exibidos no Quadro 3.

Quadro 3 – Tipos de pesquisas de avaliação de riscos.

Tipo	Descrição
Métodos de identificação de riscos	Pesquisas que abordam métodos de identificação de riscos. Trata-se do processo de encontrar, reconhecer e descrever os riscos.
Comparação de métodos de avaliação de riscos	Pesquisas comparativas dos métodos de avaliação de risco, quantitativos ou qualitativos, considerando as suas vantagens e desvantagens.
Melhoria de métodos de avaliação de riscos	Pesquisas em que os autores propõem melhorias para as abordagens de avaliação de risco.
Comparação de *frameworks*	Pesquisas comparativas de *frameworks* existentes, considerando a sua estrutura e aplicabilidade.
Melhoria de *frameworks*	Pesquisas em que os autores propõem melhorias para processos a partir de *frameworks* já existentes.
Estudo de caso	Pesquisas que avaliam a temática citada em diferentes contextos e cenários.
Outros	Pesquisas pontuais sobre o tema como, por exemplo, a análise de impactos econômicos.

Fonte: Elaborado pelos autores (2021).

Conforme apresentado no Quadro 3, os tipos de pesquisas incluem o estudo de métodos de identificação de riscos; comparação e melhoria de métodos ou *frameworks* de avaliação de riscos; estudos de caso e outros, o que inclui temas pontuais sobre a avaliação de riscos, como a análise de impactos econômicos.

A partir dos métodos e os tipos de pesquisas de avaliação de riscos, foram realizadas análises de conteúdo com o objetivo de identificar e quantificar características nas publicações, servindo de base para inferências, conforme apresentado na seção de resultados. Apesar de alguns estudos apresentarem discussões que se referem a mais de um tipo de pesquisa, a classificação utilizada no presente trabalho considerou apenas os elementos centrais, associados diretamente à estrutura e aos objetivos.

4 APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

O resultado da busca realizada encontra-se apresentado no Quadro 4, no qual é apresentado o total de 53 artigos.

Quadro 4 – Artigos analisados.

N°	Ano	Autores	Título
1	2004	Lenstra, A., Voss, T.	Information security risk assessment, aggregation, and mitigation
2	2009	Zawiła-Niedźwiecki, J., Byczkowski, M.	Information Security Aspect of Operational Risk Management
3	2010	Romanov, A., Tsubaki, H., Okamoto, E.	An approach to perform quantitative information security risk assessment in IT landscapes
4	2010	Beebe, N.L., Rao, S.V.	Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process
5	2011	Bolle, S.R., Hasvold, P., Henriksen, E.	Video calls from lay bystanders to dispatch centers - Risk assessment of information security
6	2011	Saleh, M.S., Alfantookh, A.	A new comprehensive framework for enterprise information security risk management
7	2011	Fenz, S., Ekelhart, A., Neubauer, T.	Information security risk management: In which security solutions is it worth investing?
8	2012	Song, J.-G., Lee, J.-W., Lee, C.-K., Kwon, K.-C., Lee, D.-Y.	A cyber security risk assessment for the design of I&C systems in nuclear power plants
9	2012	Shameli-Sendi, A., Shajari, M., Hassanabadi, M., Jabbarifar, M., Dagenais, M.	Fuzzy multi-criteria decision-making for information security risk assessment
10	2013	Liu, L., Bao, T., Yuan, J., Li, C.	Risk assessment of information security based on grey incidence and D-s theory of evidence
11	2013	Bojanc, R., Jerman-Blažič, B.	A quantitative model for information-security risk management

12	2014	Xiangmo, Z., Ming, D., Shuai, R., Luyao, L., Zongtao, D.	Risk assessment model of information security for transportation industry system based on risk matrix
13	2014	Lai, L.K.H., Chin, K.S.	Development of a failure mode and effects analysis based risk assessment tool for information security
14	2014	Webb, J., Maynard, S., Ahmad, A., Shanks, G.	Information security risk management: An intelligence-driven approach
15	2014	Markovic-Petrovic, J.D., Stojanovic, M.D.	An improved risk assessment method for SCADA information security
16	2014	Coronado, A.J., Wong, T.L.	Healthcare cybersecurity risk management: Keys to an effective plan
17	2015	Herland, K., Hmminen, H., Kekolahti, P.	Information security risk assessment of smartphones using bayesian networks
18	2015	Henshel, D., Cains, M.G., Hoffman, B., Kelley, T.	Trust as a Human Factor in Holistic Cyber Security Risk Assessment
19	2015	Chaitanya Krishna, B., Subrahmanyam, K., Kim, T.-H.	A dependency analysis for information security and risk management
20	2015	Shamala, P., Ahmad, R., Zolait, A.H., Sahib, S.B.	Collective information structure model for information security risk assessment (ISRA)
21	2015	Woo, P.S., Kim, B.H., Hur, D.	Towards cyber security risks assessment in electric utility SCADA systems
22	2016	Zarei, J., Sadoughi, F.	Information security risk management for computerized health information systems in hospitals: A case study of Iran
23	2016	Talabeigi, E., Jalali Naeeini, S.G.	Information security risk management and incompatible parts of organization
24	2016	Pan, L., Tomlinson, A.	A systematic review of information security risk assessment
25	2016	Shedden, P., Ahmad, A., Smith, W., Tscherning, H., Scheepers, R.	Asset identification in information security risk assessment: A business practice approach

26	2017	Wangen, G.	Information Security Risk Assessment: A Method Comparison
27	2018	Wangen, G., Hallstensen, C., Snekkenes, E.	A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF
28	2018	Zhu, Q., Qin, Y., Zhou, C., Gao, W.	Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems
29	2018	Fielder, A., König, S., Panaousis, E., Schauer, S., Rass, S.	Risk assessment uncertainties in cybersecurity investments
30	2018	Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., Hu, B.	A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems
31	2018	Kure, H.I., Islam, S., Razzaque, M.A.	An integrated cyber security risk management approach for a cyber-physical system
32	2018	Öbrand, L., Holmström, J., Newman, M.	Navigating Rumsfeld's quadrants: A performative perspective on IT risk management
33	2018	Musman, S., Turner, A.	A game theoretic approach to cyber security risk management
34	2018	Li, S., Bi, F., Chen, W., Miao, X., Liu, J., Tang, C.	An improved information security risk assessments method for cyber-physical-social computing and networking
35	2018	Hashim, N.A., Abidin, Z.Z., Zakaria, N.A., Ahmad, R., Puvanasvaran, A.P.	Risk assessment method for insider threats in cyber security: A review
36	2018	Alohali, M., Clarke, N., Furnell, S.	The design and evaluation of a user-centric information security risk assessment and response framework
37	2018	Kovácsné Mozsár, A.L., Michelberger, P.	It risk management and application portfolio management

38	2018	Xuepeng, H., Wei, X.	Method of information security risk assessment based on improved fuzzy theory of evidence
39	2019	Kure, H.I., Islam, S.	Assets focus risk management framework for critical infrastructure cybersecurity risk management
40	2019	Chen, Y.-T., Huang, C.-C.	Determining information security threats for an iot-based energy internet by adopting software engineering and risk management approaches
41	2019	Mokhor, V., Gonchar, S., Dybach, O.	Methods for the total risk assessment of cybersecurity of critical infrastructure facilities
42	2019	Turskis, Z., Goranin, N., Nurusheva, A., Boranbayev, S.	Information security risk assessment in critical infrastructure: A hybrid MCDM approach
43	2019	Haji, S., Tan, Q., Costa, R.S.	A hybrid model for information security risk assessment
44	2019	Shang, W., Gong, T., Chen, C., Hou, J., Zeng, P.	Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees
45	2020	Wang, Z., Chen, L., Song, S., Cong, P.X., Ruan, Q.	Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations
46	2020	Brunner, M., Sauerwein, C., Felderer, M., Breu, R.	Risk management practices in information security: Exploring the status quo in the DACH region
47	2020	Maček, D., Magdalenić, I., Ređep, N.B.	A systematic literature review on the application of multicriteria decision making methods for information security risk assessment
48	2020	Wang, J., Neil, M., Fenton, N.	A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model
49	2020	Liu, H.B., Liu, Y., Xu, L.	Dombi Interval-Valued Hesitant Fuzzy Aggregation Operators for Information Security Risk Assessment
50	2021	Yoo, Y., Park, H.-S.	Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship

51	2021	Kalinin, M., Krundyshev, V., Zegzhda, P.	Cybersecurity risk assessment in smart city infrastructures
52	2021	Bhuiyan, T.H., Medal, H.R., Nandi, A.K., Halappanavar, M.	Risk-averse bi-level stochastic network interdiction model for cyber-security risk management
53	2021	Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y., Wang, J.	A Systematic Risk Assessment Framework of Automotive Cybersecurity

Fonte: Elaborado pelos autores (2021).

O Quadro 4 exibe os artigos identificados na busca considerando os respectivos anos de publicação, autores e títulos. Já a nuvem de palavras, criada a partir das palavras-chaves existentes nos artigos, está apresentada na Figura 1.

Figura 1 – Nuvem de palavras.

Fonte: Elaborado pelos autores (2021).

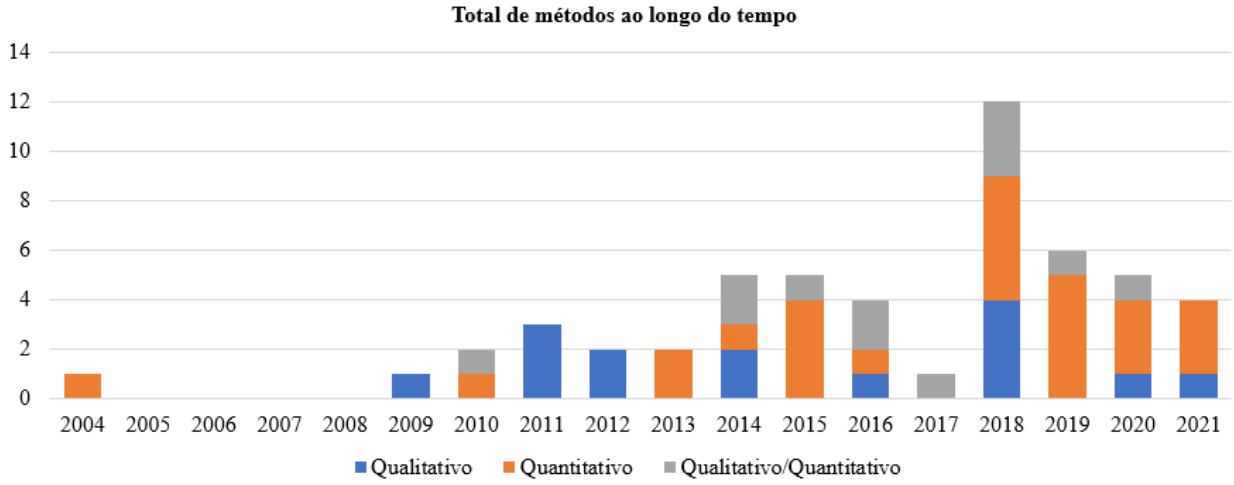
A partir da análise da Figura 1, é possível observar que os termos com maior utilização para referir-se a trabalhos de avaliação de riscos cibernéticos são, respectivamente, *information security* e *cybsersecurity*, o que confirma a primeira hipótese proposta para o presente trabalho. O termo *information security* comumente aborda a segurança de ativos informacionais conforme três propriedades de informação, que são a disponibilidade, a integridade e a confidencialidade (Machado, 2014).

Andronache e Althonayan (2018) citam que o termo *cybersecurity* desenvolveu-se a partir do conceito de *information security* e é uma abordagem mais ampla para proteger não apenas os

ativos de informação, mas também a tecnologia, ativos, processos, pessoas, organização e práticas com variáveis semelhantes. Steinberg (2020) também afirma que *cybersecurity* é uma ramificação de *information security* que trata de informações e sistemas de informação que armazenam e processam dados em formato eletrônico, entretanto *information security* abrange a segurança de todas as formas de dados – até mesmo arquivos em papel.

Em sequência, a classificação dos trabalhos foi realizada a partir dos métodos de avaliação de riscos cibernéticos e o resultado encontra-se apresentado na Figura 2.

Figura 2 – Total de métodos ao longo do tempo.



Fonte: Elaborado pelos autores (2021).

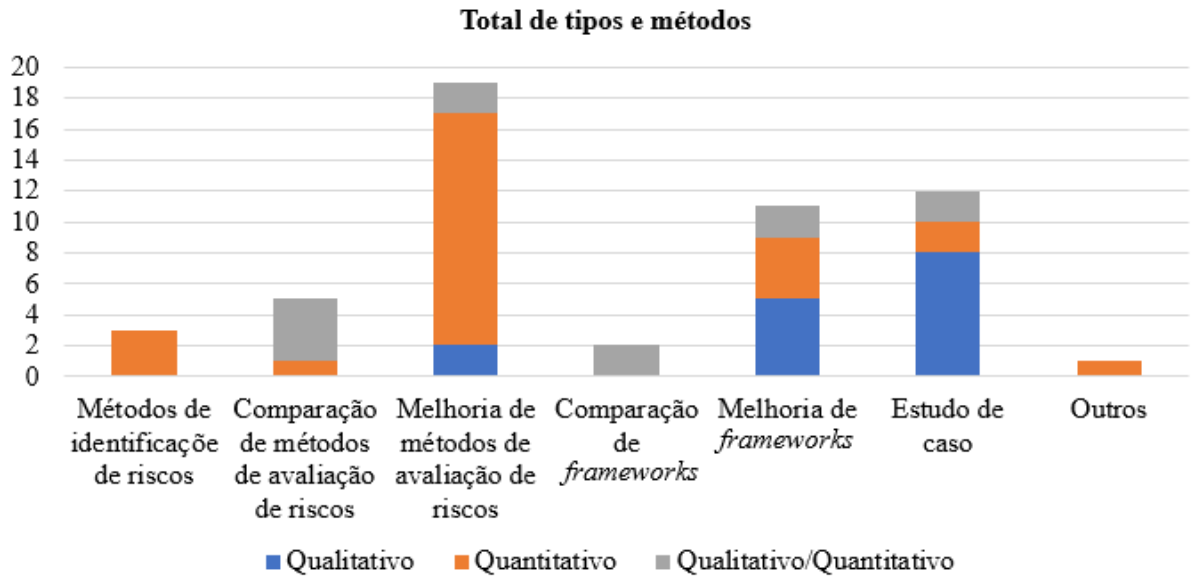
É possível observar na Figura 2 que o método com maior utilização é o quantitativo, com o total de 26 artigos. Em seguida, o método qualitativo foi empregado por 15 trabalhos. Por fim, o método qualitativo/quantitativo foi observado em 12 publicações. A maior parte das pesquisas relacionadas à avaliação de riscos faz o uso de métodos quantitativos, o que confirma a segunda hipótese formulada para o presente trabalho.

O artigo mais antigo encontrado foi publicado em 2004, entretanto a próxima publicação foi observada apenas em 2009. Além disso, é possível observar uma quantidade significativa de publicações relacionadas ao tema no ano de 2018, com o total de 12 trabalhos. Dentre os artigos publicados, Li *et al.* (2018), Hashim *et al.* (2018) e Alohali, Clarke e Furnell (2018) desenvolveram pesquisas que abordam fatores humanos para a avaliação de riscos. Neste mesmo período, Zhang *et al* (2018) e Xuepeng e Wei (2018) apresentaram em seus trabalhos métodos quantitativos que usam a teoria *fuzzy*.

O trabalho elaborado por Sulaman e Host (2013) aponta que a maioria das pesquisas identificadas utilizam métodos quantitativos de avaliação de risco. Vale ressaltar que os autores apontam a necessidade de mais pesquisas sobre métodos que combinem as vantagens de métodos quantitativos e qualitativos (qualitativos/quantitativos). A partir do resultado apresentado na Figura 2, é possível afirmar que a tendência de uso majoritário de métodos quantitativos permanece, entretanto, após 2013, houve a publicação de 11 trabalhos que utilizam métodos qualitativos/quantitativos.

A classificação conforme os tipos de pesquisa observados nos trabalhos encontra-se apresentada na Figura 3.

Figura 3 – Total de artigos por tipos e métodos.



Fonte: Elaborado pelos autores (2021).

É possível observar que os três tipos de pesquisa com maiores incidência são, respectivamente, melhoria de métodos de avaliação de riscos (19 artigos); estudo de caso (12 pesquisas) e melhoria de *frameworks* (11 trabalhos). A análise da Figura 3 confirma a terceira hipótese proposta para o presente trabalho.

Dentre os trabalhos relacionados à melhoria de métodos de avaliação de riscos, foi observado que 15 trabalhos utilizam o método quantitativo (79% do total). Esse levantamento indica que a maior parte dos autores da amostra buscam otimizar os métodos de avaliação de risco por meio de abordagens quantitativas. As abordagens quantitativas conhecidamente possuem maior complexidade de execução em comparação às demais (Macek,Magdalenic & Redep, 2020). Pan

e Tomlinson (2016) apontam que métodos quantitativos podem ser utilizados para melhoria do cálculo da probabilidade, reduzindo a subjetividade nos cálculos das pontuações de risco.
Foi observado que, dentre os trabalhos do tipo estudo de caso, oito artigos utilizam métodos qualitativos, ou seja, 66% do total de pesquisas do tipo citado. Os métodos qualitativos de avaliação de riscos apresentam maior facilidade de uso, entretanto critérios subjetivos são utilizados durante a avaliação, o que pode diminuir a sua eficácia (Kalinin, Krundyshev & Zegzhda, 2021).

5 CONCLUSÕES

Diversas abordagens podem ser utilizadas por pesquisas sobre a avaliação de riscos. A falta de padronização e de definição dificulta a aplicação e a organização de conceitos, visto que autores vêm utilizando diferentes termos para referir-se ao tema citado e os trabalhos podem diferir-se quantos aos métodos utilizados e aos tipos de pesquisas. O presente trabalho teve como objetivo explorar os aspectos citados em trabalhos que possuem a temática de avaliação de riscos cibernéticos. Esta pesquisa forneceu um panorama analítico sobre o tema nas bases de dados Scopus e Scielo por meio de um estudo bibliométrico dos documentos selecionados, utilizando uma *string* construída a partir dos termos comumente utilizados, por meio de um estudo bibliométrico dos documentos selecionados.
O objetivo proposto para o presente trabalho foi cumprido a partir da identificação dos termos, métodos e tipos de pesquisa presentes nos trabalhos da amostra selecionada. A primeira hipótese foi comprovada a partir da análise da Figura 1, na qual é possível observar que os principais termos, relacionados à avaliação de riscos cibernéticos, identificados na nuvem de palavras são, respectivamente, *information security* e *cybersecurity*.
Por sua vez, a segunda hipótese foi confirmada ao analisar a Figura 2, uma vez que a maioria dos trabalhos utilizam métodos quantitativos. Entretanto, vale ressaltar que é possível observar um aumento do volume de publicações que usam métodos qualitativos/quantitativos a partir de 2013.
Já a terceira hipótese foi comprovada a partir da análise da Figura 3, visto que a maioria dos trabalhos da presente amostra visam a melhoria de métodos de avaliação de riscos. Dentre os trabalhos do tipo estudo de caso, oito artigos utilizam métodos qualitativos, ou seja, 66% do total de pesquisas do tipo citado. Por outro lado, 79% dos trabalhos de melhoria de métodos de avaliação de riscos buscam aprimorar métodos quantitativos, os quais possuem maior complexidade de uso e aplicação

Ao término da presente pesquisa, foi possível constatar que algumas contribuições foram realizadas, dentre elas, vale ressaltar que no campo teórico, o estudo corroborou com as pesquisas apresentadas na revisão sistemática de literatura, as quais mostraram-se relevantes para a reflexão acerca da temática da pesquisa, visto que foi apontado que diferentes abordagens vêm sendo utilizadas para fazer referências a temas relacionados ao gerenciamento de riscos cibernéticos. O presente trabalho identificou e quantificou aspectos sobre as abordagens utilizadas em pesquisas relacionadas à avaliação de riscos na literatura científica internacional e apresentou as características observadas acerca dos termos, métodos e tipos de pesquisa. Como limitação, este artigo utilizou duas bases de dados e pode ser expandido com o uso de outras bases para realização das buscas, além da adoção apenas de artigos Open Access. Além disso, como trabalho futuro, sugere-se a realização de pesquisas comparativas entre os métodos quantitativos de avaliação de risco, com o objetivo de validar a eficiência e aplicabilidade dos novos métodos propostos. Outra sugestão para trabalhos futuros é refazer a busca, após o período de um ano, para verificar se as tendências observadas permanecem ativas.

REFERÊNCIAS

Alohali, M., Clarke, N. & Furnell, S. (2018). The design and evaluation of a user-centric information security risk assessment and response framework. *International Journal of Advanced Computer Science and Applications*, 9 (10), pp. 148-163.

Andronache, A.& Althonayan, A. (2018). Shifting From Information Security Towards A Cybersecurity Paradigm. Disponível em: <www.researchgate.net/publication/326400825>. Acesso em: 17 jul. 2021.

Beebe, N.L. & Rao, S.V. (2010). Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process. *Communications of the Association for Information Systems*, 26 (1), pp. 329-358.

Bhuiyan, T.H., Medal, H.R., Nandi, A.K. & Halappanavar, M. (2021). Risk-averse bi-level stochastic network interdiction model for cyber-security risk management. *International Journal of Critical Infrastructure Protection*, 32, art. no. 100408.

Bojanc, R. & Jerman-Blažič, B. (2013). A quantitative model for information-security risk management. EMJ - *Engineering Management Journal*, 25 (2), pp. 25-37.

Bolle, S.R., Hasvold, P., Henriksen, E. (2011). Video calls from lay bystanders to dispatch centers - Risk assessment of information security. *BMC Health Services Research*, 11, art. no. 244.

Brunner, M., Sauerwein, C., Felderer, M. & Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. 2020. *Computers and Security*, 92, art. no. 101776.

Coronado, A.J. & Wong, T.L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation and Technology*, 48, pp. 26-30.

Chaitanya Krishna, B., Subrahmanyam, K. & Kim, T.-H. (2015). A dependency analysis for information security and risk management. *International Journal of Security and its Applications*, 9 (8), pp. 205-210.

Chen, Y.-T. & Huang, C.-C. (2019). Determining information security threats for an iot-based energy internet by adopting software engineering and risk management approaches. *Inventions*, 4 (3), art. no. 53.

Fenz, S., Ekelhart, A. & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Communications of the Association for Information Systems*, 28 (1), pp. 329-356.

Fernandes, A. A.& Abreu, V. F. (2012). *Implantando a governança de TI: da estratégia à gestão de processos e serviços*. 3. ed. Rio de Janeiro: Brasport.

Fielder, A., König, S., Panaousis, E., Schauer, S. & Rass, (2018). S. Risk assessment uncertainties in cybersecurity investments. *Games*, 9 (2), art. no. 34.

Fontes, E. (2006). *Segurança da informação: o usuário faz a diferença.* São Paulo: Saraiva.

Fraporti, S. & Barreto, J. (2018). *Gerenciamento de riscos*. Sagah Educação S.A.

Haji, S., Tan, Q. & Costa, R.S. (2019). A hybrid model for information security risk assessment. *International Journal of Advanced Trends in Computer Science and Engineering*, 8 (1).

Hashim, N.A., Abidin, Z.Z., Zakaria, N.A.& Ahmad, R., Puvanasvaran, A.P. (2018). Risk assessment method for insider threats in cyber security: *A review. International Journal of Advanced Computer Science and Applications*, 9 (11), pp. 126-130.

HSC Brasil. *Ameaças persistentes avançadas: Como se proteger*. 2019. Disponível em: https://www.hscbrasil.com.br/ameacas-persistentes-avancadas/. Acesso em 24 jul. 2021.

Herland, K., Hmminen, H. & Kekolahti, P. (2015). Information security risk assessment of smartphones using bayesian networks. *Journal Cyber Security and Mobility*,4, p.65-86.

Henshel, D., Cains, M.G., Hoffman, B. & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, 3, pp. 1117-1124.

Kalinin, M., Krundyshev, V. & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, 9 (4), art. no. 78.

Kovácsné Mozsár, A.L. & Michelberger, P. (2018). It risk management and application portfolio management [Zarządzanie ryzykiem it i zarządzanie portfelem aplikacji]. *Polish Journal of Management Studies*, 17 (2), pp. 112-122.

Kure, H.I. & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. *IET Cyber-Physical Systems*. 4 (4), pp. 332-340.

Kure, H.I., Islam, S. & Razzaque, M.A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, 8 (6), art. no. 898.

Lai, L.K.H. & Chin, K.S. (2014). Development of a failure mode and effects analysis based risk assessment tool for information security. *Industrial Engineering and Management Systems*, 13 (1), pp. 87-100.

Lenstra, A. & Voss, T. (2004). Information security risk assessment, aggregation, and mitigation. *Lecture Notes in Computer Science* (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 3108, pp. 391-401.

Li, S., Bi, F., Chen, W., Miao, X., Liu, J. &Tang, C. (2018). An improved information security risk assessments method for cyber-physical-social computing and networking. *IEEE* Access, 6, pp. 10311-10319.

Liu, L., Bao, T., Yuan, J. & Li, C. (2013). Risk assessment of information security based on grey incidence and D-s theory of evidence. *Journal of Applied Sciences*, p. 1740-1745.

Liu, H.B., Liu, Y. & Xu, L. (2020). Dombi Interval-Valued Hesitant Fuzzy Aggregation Operators for Information Security Risk Assessment. *Mathematical Problems in Engineering*.

Macek, D., Magdalenic, I. & Redep, N.B. (2020). A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. *International Journal of Safety and Security Engineering*, 10 (2), pp. 161-174.

Machado, F. (2014). *Segurança da Informação: princípios e controle de ameaças*. 1. Ed. São Paulo: Érica.

Markovic-Petrovic, J.D. & Stojanovic, M.D. (2014). An improved risk assessment method for SCADA information security. *Elektronika ir Elektrotechnika*, 20 (7), pp. 69-72.

Mokhor, V., Gonchar, S. & Dybach, O. (2019). Methods for the total risk assessment of cybersecurity of critical infrastructure facilities. *Nuclear Radiation Safety*, p. 4-8.

Molinaro, L.& Ramos, K. (2011). *Gestão de tecnologia da informação: governança de TI: arquitetura e alinhamento entre sistemas de informação e o negócio*. Rio de Janeiro: LTC.

Monteiro, M. S. (2017). *A importância da gestão de riscos*. Belém: CONACI.

Musman, S. & Turner, A. (2018). A game theoretic approach to cyber security risk management. *Journal of Defense Modeling and Simulation*, 15 (2), pp. 127-146.

Öbrand, L., Holmström, J. & Newman, M. (2018). Navigating Rumsfeld's quadrants: A performative perspective on IT risk management. *Technology in Society*, 53, pp. 1-8.

Pan, L. & Tomlinson, A. (2018). A systematic review of information security risk assessment. *International Journal of Safety and Security Engineering*, 6 (2), pp. 270-281.

Rodrigues, A. R., Tavar, C., Nogueira, G. M. & Librelotto, R. F. (2016). A bibliometria como ferramenta de análise da produção intelectual: uma análise dos hot topics sobre sustentabilidade. *Biblionline*, v. 12, n. 3, p. 34-47.

Rahman, M. & Donahue, E. (2010). Convergence of Corporate and Information Security. *International Journal of Computer Science and Information Security*, Vol. 7, No. 1.

Romanov, A., Tsubaki, H. & Okamoto, E. (2010). Caan approach to perform quantitative information security risk assessment in IT landscapes. *Journal of Information Processing*, 18, pp. 213-226.

Saleh, M.S. & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics*, 9 (2).

Shamala, P., Ahmad, R., Zolait, A.H. & Sahib, S.B. (2015). Collective information structure model for information security risk assessment (ISRA). *Journal of Systems and Information Technology*, 17 (2), pp. 193-219.

Shameli-Sendi, A., Shajari, M., Hassanabadi, M., Jabbarifar, M. & Dagenais, M. (2012). Fuzzy multi-criteria decision-making for information security risk assessment. *Open Cybernetics and Systemics Journal*, 6 (1), pp. 26-37.

Shang, W., Gong, T., Chen, C., Hou, J. & Zeng, P. (2019). Information Security Risk Assessment Method for Ship Control System Based on Fuzzy Sets and Attack Trees. *Security and Communication Networks*, 2019, art. no. 3574675.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H.& Scheepers, R. (2016). Asset identification in information security risk assessment: A business practice approach. *Communications of the Association for Information Systems*, 39 (1), art. no. 15, pp. 297-320.

Slay, J., & A. Koronios. (2006). *Information technology security & risk management*. Milton, QLD: Wiley.

Sotolani, R. S., Menezes, I. D. A. C., Galegale, N. V., & Feitosa, M. D. (2022). Vulnerabilidades de Segurança da Informação na Indústria 4.0: Proposição de Critérios para o uso de Análise Multicritério. *Exacta*.

Song, J.-G., Lee, J.-W., Lee, C.-K., Kwon, K.-C. & Lee, D.-Y. (2012). A cyber security risk assessment for the design of Lamp; C systems in nuclear power plants. *Nuclear Engineering and Technology*, 44 (8), pp. 919-928.

Steinberg, J. (2020). *Cibersegurança Para Leigos*. 1 ed. Rio de Janeiro: Alta Books.

Talabeigi, E. & Jalali Naeeini, S.G. (2016). Information security risk management and incompatible parts of organization. *Journal of Industrial Engineering and Management*.

Turskis, Z., Goranin, N., Nurusheva & A., Boranbayev, S. (2019). security risk assessment in critical infrastructure: A hybrid MCDM approach. *Informatica* (Netherlands), 30 (1), pp. 187-211.

Valis, D. & Koucky, M. (2009). Selected overview of risk assessment techniques. *Probl. Eksploat*, 75, pp. 19–32.

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: understanding security threats in the era of cyberphysical systems. *Journal of Supercomputing*, 76(4), 2643–2664.

Wang, Z., Chen, L., Song, S., Cong, P.X. & Ruan, Q. (2020). Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations. *Alexandria Engineering Journal*, 59 (4), pp. 2725-2731.

Wang, J., Neil, M. & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers and Security*, 89.

Wang, Y., Wang, Y., Qin, H., Ji, H., Zhang, Y. & Wang, J. (2021). *A Systematic Risk Assessment Framework of Automotive Cybersecurity*. Automotive Innovation.

Wangen, G. (2017). Information Security Risk Assessment: A Method Comparison. *Computer*, 50 (4), art. no. 7912273, pp. 52-61.

Wangen, G., Hallstensen, C. & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, 17 (6), pp. 681-699.

Webb, J., Maynard, S., Ahmad, A. & Shanks, G. (2014). Information security risk management: An intelligence-driven approach. *Australasian Journal of Information Systems*, 18 (3), pp. 391-404.

Woo, P.S., Kim, B.H. & Hur, D. (2015). Towards cyber security risks assessment in electric utility SCADA systems. *Journal of Electrical Engineering and Technology*, 10 (3), pp. 888-894.

Xiangmo, Z., Ming, D., Shuai, R., Luyao, L. & Zongtao, D. (2014). Risk assesment model of information security for transportation industry system based on risk matrix. *Applied Mathematics and Information Sciences*, 8 (3), pp. 1301-1306.

Xuepeng, H. & Wei, X. (2018). Method of information security risk assessment based on improved fuzzy theory of evidence. *International Journal of Online Engineering*, 14 (3), p. 188-196.

Yoo, Y. & Park, H.-S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *Journal of Marine Science and Engineering*, 9 (6), art. no. 565.

Zarei, J. & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: A case study of Iran. *Risk Management and Healthcare Policy*, 9, pp. 75-85.

Zawiła-Niedźwiecki, J. & Byczkowski, M. (2009). Information Security Aspect of Operational Risk Management. *Foundations of Management*, 1 (2), pp. 45-60.

Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y. & Hu, B. (2018). A Fuzzy Probability Bayesian Network Approach for Dynamic Cybersecurity Risk Assessment in Industrial Control Systems. *IEEE Transactions on Industrial Informatics*, 14 (6), pp. 2497-2506.

Zhu, Q., Qin, Y., Zhou, C. & Gao, W. (2018). Extended multilevel flow model-based dynamic risk assessment for cybersecurity protection in industrial production systems. International *Journal of Distributed Sensor Networks*, 14 (6).