Prioritizing Cybersecurity Management Guidelines using Analytical Hierarchy Process (AHP) Decision Technique

Article history

Received:
15 Nov 2021

Received in revised form:
15 Feb 2022

Accepted:
28 Feb 2022

Published online:
20 May 2022

*Corresponding author
shaini@tms.uitm.edu.my

Norkhushaini Awang[1, *], Ganthan A/L Narayana Samy[2], Noor Hafizah Hassan[3]

[1,*]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Malaysia*
[2,3]*Razak Faculty of Technology and Informatics, Level 5, Menara Razak, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, Kuala Lumpur, Malaysia*
[1]*shaini@tmsk.uitm.edu.my*
[2]*ganthan.kl@utm.my*, [3]*noorhafizah.kl@utm.my*

Abstract

Decision theory is a set of concepts, principles, tools, and techniques that help decision-makers deal with complex and uncertain decision-making problems. The theory of decisions provides a systematic basis for making reasonable choices in a situation of uncertainty. This research implements an Analytical Hierarchy Process (AHP) decision technique in determining the effectiveness of choices in making a decision. The proposed systematic approach also discusses detailed guidelines using Analytical Hierarchy Process (AHP) techniques to help organizations conduct risk assessment effectively by prioritizing the proposed cybersecurity management guideline. A survey has been conducted by interviewing cybersecurity experts to get feedback on the proposed cybersecurity management guideline. The proposed cybersecurity management guideline uses the AHP decision technique to perform selection and prioritization in reducing the decision bias. In managing cybersecurity threats, this study proposed three criteria categories: human resource, logistical, and technical aspects. This criterion is a mechanism for university policymakers in managing university networks. The research study is continued with a discussion on the use of AHP decision tools to malware, network intrusion, and web intrusion management guideline. The use of AHP as a decision tool can help to reduce decision bias, ensure that every opinion is heard, and actively build consensus among decision-makers in solving problems. Collaborative decisions with multiple people can produce better results with strong commitment from decision-makers.

Keywords: *decision technique, cybersecurity risk analysis, Analytical Hierarchy Process*

1. Introduction

Analytical Hierarchy Process (AHP) is one of the decision theory models to have an accurate decision by quantifying the weights of decision criteria. Research from Brunelli [1] stated that decision analytics help decision-makers based on feelings and instincts, use analytic and quantitative tools, and analyze the decisions on a groundwork. Analytical Hierarchy Process is a theory and methodology for relative measurement which not interested in the exact measurement of some quantities, but rather on the proportions between them. According to Epstein & Harding [2] stated that in treating risk, it can be controlled in the organization internally in determining

[*] *Corresponding author. shaini@tmsk.uitm.edu.my*

the effectiveness of choices that have been made in decision making. A research from Önder & Hepsen [3] mention that Analytical Hierarchy Process (AHP) is one of the effective decision making technique especially when there is subjectivity and this technique is also suitable for solving a problem in which decision alternatives can be arranged hierarchically into sub-criteria. In this study, researcher assessed the risks for selected university in Malaysia by looking at the threats that occur in the university network. From Joshi & Singh [4] stated that in university network, they found that SQL injection, weak password and cross-site request forgery attack is the most attack capture from their analysis. Data transmission and storage increase the risks of data theft and virus infection in university network [5]. According to Lazar *et al.* [6] mention about their study performed to domain server found that cybersecurity threats occur in networks by masquerading as legitimate websites known as phishing attacks. This attack occurs by taking the vulnerabilities found in the user's web browser. Research on cybersecurity threats on the university network were also conducted by Yevseiev *et al.* [7] mention that in their research, they focusing on web infrastructure where the findings from this study found that the university network is vulnerable to cybersecurity threats through the web as it is access to applications in the university today.

The research on cybersecurity threats in university network also been discussed by Roberts [8] emphasized that many university users do not comprehend the risks to basic information security. In the report, author list seven (7) cybersecurity threats that can be found in university network. The threats that have been reported in university network are key loggers, viruses, worms and Trojans, denial of service attacks, sniffers, wireless sniffing, file sharing threats and abundance of bandwidth. All of these threats occur through the use of applications on the web. In the past, University of California banned Windows and Windows NT from being used by all campus users. This policy is made because numerous security threats of viruses, worms and denial-of-service attacks were reported and caused many outages of the university network. Support staff argued that it was difficult to maintain student computers installed in a stable way. A research conducted by Georgetown University [9] listed ten (10) types of threats which found in university network. The threats are includes technology with weak security, social media attacks, mobile malware, third-party entry, neglecting proper configuration, outdated security software, social engineering, lack of encryption, corporate data on personal devices and inadequate security technology. From these ten threats, most threats occur within the network and the rest occur on software.

University is a place provided with various technologies in preparing for student learning including Wi-Fi technology facilities, online learning, digital library, and web conferencing. The widespread use of the internet within university networks leaves universities vulnerable to cybersecurity threats. Attacks that took place on the university network were also discussed by Naagas *et al.* [10]mention about twenty six (26) threats that might happen in university network which are spoofing, sniffing, session hijacking, denial of service, viruses, foot printing, password cracking, arbitrary code execution, buffer overflow, cross-site scripting, SQL injection, network eavesdropping, elevation of privilege, brute force attacks, dictionary attacks, man in the middle, information disclosure, attacker exploits, war driving and wireless attack. In their study, random black box penetration testing was implemented in assessing the university network. From the 26 threats identified by researchers, researcher classified these threats into 3 categories, which are threats from viruses, from web applications and also intrusion into the network.

This discussion is continued on cybersecurity threats in university network, Joshi [11] explained that university campus exposed to the following security threats as groups such as phishing, ransomware, and malware, viruses spreading through social media, mobile devices operating system vulnerability and embedded devices connectivity. All cyber threats obtained from previous studies point to some general classifications. This research can conclude that cyber security threats can be categorized into network intrusion, malware and web application threats. In this research study, researcher conducted an interview with experts in administering cybersecurity threats in university network. The threats have the same with others researchers found or the new threats depends on the campus users activities using the information system in campus network.

2. Motivation

a. Cybersecurity Risk Analysis

University network is a critical asset for an organization to protect from cybersecurity threats. Cybersecurity threats is a current of common risk factors which effect of loss of data integrity [12]. There are challenges involves in implementing protecting cybersecurity in an organization. However, by implementing systematic cybersecurity risk management in analyzing the risks can control the risks for business continuity [13]. The main principles of network security are confidentiality, integrity, and availability (CIA) that forms the basis of asset protection, authenticity, accountability, reliability, and non-repudiation [14]. Compromising these principles leaves systems at risk. In this research study, to manage cybersecurity threats, this research looked at asset protection, authenticity, accountability, reliability, and non-repudiation as things that should be emphasized in the risk management recommendations.

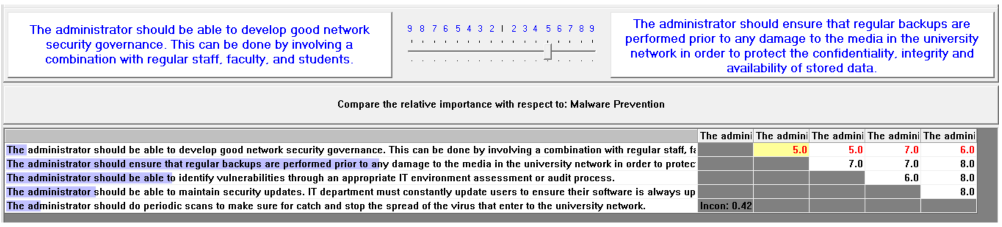
University network have many technologies that are adapted for student development. However, it also contributes to the occurrence of cyber threats, which in turn exposes the risk to the network. According to Joshi & Singh [15] emphasize that more access to technology give valued to learning environment. However, on the other hand access to technology can expose to vulnerability to computing environment with cybersecurity threats. It is crucial to secure the university network and have a fast recovery from risks. According to Yeh & Chang [16] mention that there are two types of security risks in the information security, both internal and external. Internal functions focused on technical issues, whereas external functions stressed managerial and operating security, or nontechnical issues. In assessing the security risks, managerial dimension can be deployed in an environment [17]. Authors stated that by looked at the time when the threats happen, organization can have a better assessment in managing the network.

b. Analytical Hierarchy Process (AHP) Decision Theory

Analytical Hierarchy Process (AHP) is one of the theory in decision making where this method uses mathematical model to support decision technique. According to N´emeth *et al.* [18] mention that AHP was used in their study to reduce the potential for bias in decision making by using resource intensity and reducing the burden on participants in decision making. The use of AHP in the field of healthcare where researchers consider different levels of criteria to measure relevancy. In this study researchers also mention by conducted a questionnaire, AHP can reduce the number of questions that need to be answered by decision makers, but can present the results of the study with a better strategy. The advantage of this method is that it can adjust the size to accommodate the decision-making problems because the structure of AHP is hierarchical, and the approach is clear. AHP is also capable of dealing with larger problems making it ideal for problems comparing performance between a large numbers of alternatives.

A study from Dash & Sar [19] looking at GIS systems, used Multi-Criteria Decision Analysis (MCDA) method named AHP is effective in mapping flood hazards and subsequently making decisions in flood management. Researchers have merged criteria and parameter evaluations based on AHP to make decisions in complex relationships. From the study, researchers have identified eight parameters related to hydro-geomorphological features in the GIS environment and grouped into five groups to set the assessment based on its influence on flooding. The conclusion from this study, shows that the analysis confirms the credibility of the method used, in identifying flood danger areas.

The application of AHP decision technique begins by listing the alternatives into a hierarchy of criteria. This is to facilitate analysis and comparison in an independent way. Once this logical hierarchy is built, the decision makers where in this research study we have listed experts in cybersecurity to evaluate alternatives systematically by making comparisons based on pairs for each selected criteria. In this research study, Expert Choice is used as the AHP decision tool as in Figure 1 and Figure 2.

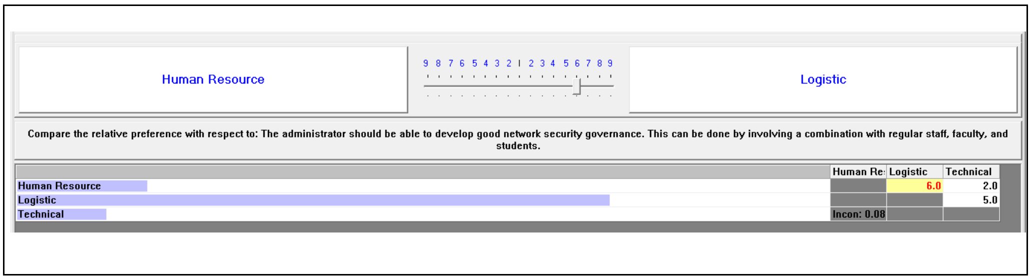

The administrator should be able to develop good network security governance. This can be done by involving a combination with regular staff, faculty, and students.

The administrator should ensure that regular backups are performed prior to any damage to the media in the university network in order to protect the confidentiality, integrity and availability of stored data.

Compare the relative importance with respect to: Malware Prevention

	The admini	The admini	The admini	The admini	The admini
The administrator should be able to develop good network security governance. This can be done by involving a combination with regular staff, fa		5.0	5.0	7.0	6.0
The administrator should ensure that regular backups are performed prior to any damage to the media in the university network in order to protec			7.0	7.0	8.0
The administrator should be able to identify vulnerabilities through an appropriate IT environment assessment or audit process.				6.0	8.0
The administrator should be able to maintain security updates. IT department must constantly update users to ensure their software is always up					8.0
The administrator should do periodic scans to make sure for catch and stop the spread of the virus that enter to the university network.	Incon: 0.42				

Figure 1. Alternatives Input in Expert Choice



Compare the relative preference with respect to: The administrator should be able to develop good network security governance. This can be done by involving a combination with regular staff, faculty, and students.

	Human Re:	Logistic	Technical
Human Resource		6.0	2.0
Logistic			5.0
Technical	Incon: 0.08		

Figure 2. Criteria Input in Expert Choice

In managing cybersecurity incidents, as mention by Antonucci [20] stated that there are 3 aspects that can be seen, namely human resource, logistics and technical aspects. Author also explained that the human resource aspects are the identification of important people, decision-making mechanisms, and training and enforce cybersecurity policies and procedures. Logistical aspect is by looking at specialized workspaces, crisis directories and helpdesk. Lastly is the technical aspect where this aspect looks at defense and investigation capabilities, tools and equipment in managing the cybersecurity. These three aspects are used in decision making as input criteria in the AHP decision tool. This can be shown as in Figure 2.

In another study also discussed the use of AHP in facilitated to make decisions in risk management in the supply chain Zekhnini *et al.* [21] . The researcher found that AHP combines qualitative and quantitative approach analysis and integrates it as a single analysis problem. AHP also uses a qualitative approach to turn issues into hierarchies. The researcher also stated how AHP helps analysts in making the best decisions and also gives good reasons for the choices to be made. Therefore, the AHP methodology was used in their study to rank and prioritize risks in the supply chain research area.

Discussion from Baylan [22] stated on the use of AHP in risk assessment planning. Researcher used hybrid algorithms in which they adapted AHP and TOPSIS in the study in decision making after identifying the risks of project activities. This method has provided a platform to researchers that project risk can be analyzed using quantitative methods in comparison with previous methods where when studying risk, qualitative methods are widely used.

3. Research Methodology

A discussion from British Standard [23] stated that the relevance information is needed to support top management achieved the organization objectives and conducting the decision-making. The proposed research conducted to optimize and suggest solutions to reduce the risks. AHP decision technique is used in this phase in ranking the proposed Cybersecurity Management Guideline gathered from risk treatment. The main purpose of using this technique is to solve problem in making a decision. AHP decision technique also provides a framework in making the decisions by measuring its alternative and criteria provided.

a. Expert Feedback

As mention before, AHP decision technique is a multi-criteria decision-making where it measures criteria and alternatives to improve traditional decision problem solving. Traditional problem solving taken a long time to measure in getting accurate results. In this research study, expert interview in conducted to gather solution and propose a Cybersecurity Management Guideline. The application of AHP decision technique begins by listing the alternatives into a hierarchy of criteria. This is to facilitate analysis and comparison in an independent way. Once this logical hierarchy is built, the decision makers where in this research study we have listed experts in cybersecurity to evaluate alternatives systematically by making comparisons based on pairs for each selected criteria. This research implementing an Analytical Hierarchy Process (AHP) decision technique in determining the effectiveness of choices in making a decision. A survey have been conducted from interviewing 9 experts from ICT Security Division, ICT Infrastructure Division, ICT Operations Division, ICT Policy & Strategic Division, Information System Division, Cloud and Security Computing Company and Cybersecurity Malaysia to get feedback on the proposed cybersecurity management guideline as in Table 1.

Table 1. Proposed Cybersecurity Management Guideline

NO	MALWARE PREVENTION	NETWORK INTRUSION PREVENTATION	WEB INTRUSION PREVENTATION
1.	The administrator should develop a good network security governance. This can be done by involving a combination with regular staff, faculty, and students.	The administrator should communicate with IT teams from other institutions or universities to compare the effectiveness of security protocols being used.	The administrator should educate university users about their responsibilities in using and sharing information to external users.
2.	The administrator should ensure the regular backups are performed prior to any damage to the media in the university network in order to protect the confidentiality, integrity and availability of stored data.	The administrator should install the appropriate software and hardware according to the requirements of the university.	The administrator should guarantee network access at the university is secure with network encryption by adding an extra layer of security for remote operation.
3.	The administrator should identify vulnerabilities through an appropriate IT environment assessment or audit process.	The administrator should perform adequate penetration testing to identify vulnerabilities.	The administrator should enforce university users to use strong password and change it every semester.
4.	The administrator should maintain security updates. IT department must constantly update users to ensure their software is always up to date.	The administrator should monitor network communication to make sure there are no simultaneous sessions and stop sharing passwords from internal users.	The administrator should configure the VPN for university user devices correctly with virtual connections to the university network.
5.	The administrator should do periodic scans to make sure for catch and stop the spread of the virus that enter to the university network.	The administrator should give instructions and support to university users by explaining about shared responsibilities.	The administrator should train professionals in both cybersecurity engineering and cybersecurity operations and leadership.

4. Result & Discussion

In managing cybersecurity incidents, as mention by Antonucci [20] stated that there are 3 aspects that can be seen, namely human resource, logistics and technical aspects. Author also explained that the human resource aspects are the identification of important people, decision-making mechanisms, and training and enforce cybersecurity policies and procedures. Logistical aspect is by looking at specialized workspaces, crisis directories and helpdesk. Lastly is the technical aspect where this aspect looks at defense and investigation capabilities, tools and equipment in managing the cybersecurity. These three aspects are used in decision making as input criteria in the AHP decision tool.

The use of the AHP decision tool is used on the proposed malware management guideline to optimize and prioritize solutions in overcoming the risks. The results obtained from Table 2 assist the network administrator manage the correct and consistent alternatives in coordinating strategies to reduce the occurrence of malware attack in the university network. The result shows, the first prioritize step that has been selected is network administrators should back up the media that available in university network. Next, network administrator should develop a network security governance involving administrative staff, faculty members, and students. The next safety steps is network administrator should identify network vulnerabilities through an appropriate IT environment assessment or audit process. Next priority guideline that has been chosen is network administrator should do periodic scans to stop the spread of the malware that enter to the university network. In conclusion, the administrator should be able to maintain security updates by constantly update users to ensure their software is always up to date. As a whole, in managing malware attack, experts agreed that technical criteria is more important than human resources and logistics. The results as discussed are obtained from the use of the AHP decision tool on the proposed malware management guideline to prioritize and optimize solutions in overcoming the risks.

Table 2. Malware Management Guideline Result

RANKING	MALWARE PREVENTION	CRITERIA
P1	The administrator should ensure the regular backups are performed prior to any damage to the media in the university network in order to protect the confidentiality, integrity and availability of stored data.	1. Technical Aspect 2. Human Resource Aspect 3. Logistic Aspect
P2	The administrator should develop a good network security governance. This can be done by involving a combination with regular staff, faculty, and students.	
P3	The administrator should identify vulnerabilities through an appropriate IT environment assessment or audit process.	
P4	The administrator should do periodic scans to make sure for catch and stop the spread of the virus that enter to the university network.	
P5	The administrator should be able to maintain security updates. IT department must constantly update users to ensure their software is always up to date.	

The use of the AHP decision tool is used on the proposed network intrusion management guideline to optimize and prioritize solutions in overcoming the risks. The results obtained from Table 3 assist the network administrator manage the correct and consistent alternatives in coordinating strategies to reduce the occurrence of network intrusion in the university network.

The result shows, the first prioritize step that has been selected is network administrators should perform adequate penetration testing to identify vulnerabilities happen in the university network. Next, network administrator should give instructions and support to university users by explaining about shared responsibilities in using university resources. The next safety steps is network administrator should communicate with IT teams from other institutions or universities to compare the effectiveness of security protocols being used in the network environment. Next priority guideline that has been chosen is network administrator should install the appropriate software and hardware according to the requirements of the university. In conclusion, the administrator should monitor network communication to make sure there are no simultaneous sessions and stop sharing passwords from internal users. As a whole, in managing malware attack, experts agreed that technical criteria is more important than human resources and logistics. The results as discussed are obtained from the use of the AHP decision tool on the proposed network intrusion management guideline to prioritize and optimize solutions in overcoming the risks.

Table 3. Network Intrusion Management Guideline Result

RANKING	NETWORK INTRUSION PREVENTION	CRITERIA
P1	The administrator should perform adequate penetration testing to identify vulnerabilities.	1. Technical Aspect 2. Human Resource Aspect 3. Logistic Aspect
P2	The administrator should give instructions and support to university users by explaining about shared responsibilities.	
P3	The administrator should communicate with IT teams from other institutions or universities to compare the effectiveness of security protocols being used.	
P4	The administrator should install the appropriate software and hardware according to the requirements of the university.	
P5	The administrator should monitor network communication to make sure there are no simultaneous sessions and stop sharing passwords from internal users.	

The use of the AHP decision tool is used on the proposed web intrusion management guideline to optimize and prioritize solutions in overcoming the risks. The results obtained from Table 4 assist the network administrator manage the correct and consistent alternatives in coordinating strategies to reduce the occurrence of web intrusion in the university network.

The result shows, the first prioritize step that has been selected is network administrators should guarantee network access at the university is secure with network encryption by adding an extra layer of security for remote operation. Next, network administrator should educate university users about their responsibilities in using and sharing information to external users. The next safety steps is network administrator should train professionals in both cybersecurity engineering and cybersecurity operations and leadership. Next priority guideline that has been chosen is network administrator should enforce university users to use strong password and change it every semester. In conclusion, the administrator should configure the VPN for university user devices correctly with virtual connections to the university network. As a whole, in managing web intrusion, experts agreed that technical criteria is more important than logistics and human resources.

Table 4. Web Intrusion Management Guideline Result

RANKING	WEB INTRUSION PREVENTION	CRITERIA
P1	The administrator should guarantee network access at the university is secure with network encryption by adding an extra layer of security for remote operation.	1. Technical Aspect 2. Logistic Aspect 3. Human Resource Aspect
P2	The administrator should educate university users about their responsibilities in using and sharing information to external users.	
P3	The administrator should train professionals in both cybersecurity engineering and cybersecurity operations and leadership.	
P4	The administrator should enforce university users to use strong password and change it every semester.	
P5	The administrator should configure the VPN for university user devices correctly with virtual connections to the university network.	

The results as discussed are obtained from the use of the AHP decision tool on the proposed web intrusion management guideline to prioritize and optimize solutions in overcoming the risks.

5. Conclusions

The proposed method implemented an Analytical Hierarchy Process (AHP) decision technique in determining the effectiveness of choices in making a decision. This technique helped network administrator prioritize the decisions acquired from expert interviews conducted in the study. As mention before, AHP decision technique is a multi-criteria decision-making where it measures criteria and alternatives to improve traditional decision problem solving. Traditional problem solving taken a long time to measure in getting accurate results. The proposed method implemented a systematic approach to help organizations in conducting risk assessment effectively by giving priority to the proposed Cybersecurity Management Guideline.

References

[1] Brunelli, Matteo. 2015. Introduction to the Analytic Hierarchy Process.

[2] Epstein, Alice L., and Gary H. Harding. 2019. Risk Management. Clinical Engineering Handbook, Second Edition. Second Edi. Vol. 627. Elsevier Inc. https://doi.org/10.1016/B978-0-12-813467-2.00052-3.

[3] Önder, Emrah, and Ali Hepsen. 2013. "Combining Time Series Analysis and Multi Criteria Decision Making Techniques for Forecasting Financial Performance of Banks in Turkey." In International Journal of Latest Trends in Finance and Economic Sciences, 3:26. https://doi.org/10.2047/ijltfesvol3iss3-26.

[4] Singh, Umesh Kumar, and Chanchala Joshi. 2017. "Information Security Risk Management Framework for University Computing Environment." International Journal of Network Security 19 (5): 742–51.

[5] Guo, Jinlan. 2019. "Big Data Security and Privacy Protection in Colleges and Universities." Application of Intelligent Systems in Multi-Modal Information Analytics 929: 727–35. https://doi.org/10.1007/978-3-030-15740-1.

[6] Lazar, David, Kobi Cohen, Alon Freund, Avishay Bartik, and Aviv Ron. 2021. "IMDoC: Identification of Malicious Domain Campaigns via DNS and Communicating Files." IEEE Access 9: 45242–58. https://doi.org/10.1109/ACCESS.2021.3066957.

[7] Yevseiev, Serhii, Volodymyr Aleksiyev, Svitlana Balakireva, Yevhen Peleshok, Oleksandr Milov, Oleksii Petrov, Olena Rayevnyeva, Bogdan Tomashevsky, Ivan Tyshyk, and Olexander Shmatko. 2019. "Development of a Methodology for Building an Information Security System in the Corporate Research and Education System in the Context of University Autonomy." Eastern-European Journal of Enterprise Technologies 3 (9–99): 49–63. https://doi.org/10.15587/1729-4061.2019.169527.

[8] Roberts, Thomas L. 2013. "Information Security in Higher Education: Threats & Response." Global Information Assurance Certification Paper. SANS Institute. http://zma.es/Incident Handler/real-world-arp-spoofing/real-world-arp-spoofing_487.pdf. https://doi.org/10.6633/IJNS.201709.19(5).12.

[9] Georgetown University. 2017. "Top 10 Threats to Information Security."

[10] Naagas, Marlon A, and Thelma D Palaoag. 2018. "A Threat-Driven Approach to Modeling a Campus Network Security." In International Conference on Communications and Broadband Networking, 1–7. https://doi.org/10.1145/3193092.3193096.

[11] Kumar, Umesh, Chanchala Joshi, and Neha Gaud. 2016. "Measurement of Security Dangers in University Network." International Journal of Computer Applications 155 (1): 6–10. https://doi.org/10.5120/ijca2016911584.

[12] Tupa, Jiri, Jan Simota, and Frantisek Steiner. 2017. "Aspects of Risk Management Implementation for Industry 4 . 0." Procedia Manufacturing 11 (June): 1223–30. https://doi.org/10.1016/j.promfg.2017.07.248.

[13] Kure, Halima Ibrahim, Shareeful Islam, and Mohammad Abdur Razzaque. 2018. "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System." Applied Sciences 8 (898): 1–29. https://doi.org/10.3390/app8060898.

[14] Liu, Qisi, Liudong Xing, and Chaonan Wang. 2017. "Framework of Probabilistic Risk Assessment for Security and Reliability." 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), 619–24. https://doi.org/10.1109/DSC.2017.35.

[15] Joshi, Chanchala, and Umesh Kumar Singh. 2017. "Information Security Risks Management Framework – A Step Towards Mitigating Security Risks In University Network." Journal of Information Security and Applications 35: 128–37. https://doi.org/10.1016/j.jisa.2017.06.006.

[16] Yeh, Quey Jen, and Arthur Jung Ting Chang. 2007. "Threats and Countermeasures for Information System Security: A Cross-Industry Study." Information and Management 44 (5): 480–91. https://doi.org/10.1016/j.im.2007.05.003.

[17] Jouini, Mouna, Latifa Ben Arfa Rabai, and Ridha Khedri. 2015. "A Multidimensional Approach Towards a Quantitative Assessment of Security Threats." Procedia Computer Science 52 (1): 507–14. https://doi.org/10.1016/j.procs.2015.05.024.

[18] N´emeth, Bertalan, Anett Moln'ar, Kalman Wijaya, Andr´as Inotai, Jonathan D Campbell, and Zolt´an Kal´o. 2019. "Comparison of Weighting Methods Used in Multicriteria Decision Analysis Frameworks in Healthcare with Focus on Low- and Middle-Income Countries." Journal of Comparative Effectiveness Research 8 (4): 195–204.

[19] Dash, Pratik, and Jishnu Sar. 2020. "Identification and Validation of Potential Flood Hazard Area Using GIS-Based Multi-Criteria Analysis and Satellite Data-Derived Water Index." Journal of Flood RIsk Management, no. April: 1–14. https://doi.org/10.1111/jfr3.12620.

[20] Antonucci, Domenic. 2017. Cyber Risk Handbook. Wiley.

[21] Zekhnini, Kamar, Anass Cherrafi, Imane Bouhaddou, and Youssef Benghabrit. 2021. "Analytic Hierarchy Process (AHP) for Supply Chain 4.0 Risks Management." Advances in Intelligent Systems and Computing 1193: 89–102. https://doi.org/10.1007/978-3-030-51186-9_10.

[22] Baylan, Emin Başar. 2020. "A Novel Project Risk Assessment Method Development via AHP- TOPSIS Hybrid Algorithm." Emerging Science Journal 4 (5): 390–410. https://doi.org/10.28991/esj-2020-01239.

[23] British Standard. 2018. "ISO 31000 : 2018 BSI Standards Publication Risk Management — Guidelines." Switzerland. https://www.ashnasecure.com/uploads/standards/BS ISO 31000-2018.pdf.