Research Article

Biomedical Science and Clinical Research

Investigating Potential Vulnerability of Critical Infrastructure and Way Forward – Recommendations to Enhance Security and Resilience

Henock Mulugeta Melaku

Henock Mulugeta, School of Information Technology and Engineering, Addis Ababa Institute of Technology, Addis Ababa University

***Corresponding author:**
Henock Mulugeta Melaku, Henock Mulugeta, School of Information Technology and Engineering, Addis Ababa Institute of Technology, Addis Ababa University

Submitted: 28 Dec 2022; **Accepted**: 09 Jan 2023 ; **Published**: 25 Jan 2023

Citations: Melaku, H.M. (2023). Investigating Potential Vulnerability of Critical Infrastructure and Way Forward – Recommendations to Enhance Security and Resilience. *Biomed Sci Clin Res,* 2(1), 61-67.

Abstract

In this research, firstly critical infrastructures (CIs) that are found in Ethiopia are identified. Then, potential security vulnerabilities of these CIs are identified by performing strategic and tactical level risk and vulnerability assessments. To perform the stated assessments, questionnaires were prepared using different standards. Moreover, on-site interviews, existing document and literature reviews were conducted. By performing the above research methodologies, the security vulnerabilities of selected CIs were thoroughly investigated. Finally, factors that contribute to the security vulnerabilities are critically identified and way forward recommendations are given to fill the identified security gaps and vulnerabilities.

Keywords: CI, Cybersecurity, Governance, Vulnerabilities, Risk, Incident

This research is supported by Addis Ababa University and has been done in collaboration with Information Network Security Administration (INSA). I hereby confirm that there are no relevant financial or non-financial competing interests to report.

In this paper the author's (Henock Mulugeta) contribution is summarized as follows:

1. The research was done in Ethiopia and the study was mainly focused on selected critical infrastructures (CIs) of the nation.
2. Relevant security related information was collected; different types of **questionnaires** according to the context of CI and different organizations (public and privately owned organizations) were prepared.
3. To collect useful information from different organizations, **on-site interview** was made on selected organizations and universities.
4. Through **document review** was also made to collect various important information.
5. **Literature review:** The most relevant previously published journals, conference proceedings, industrial standards were investigated and reviewed thoroughly.
6. Security level of selected critical infrastructure of the nation and organizations wa thoroughly investigated.
7. We have also identified and assessed potential vulnerabilities of selected CI and critical information infrastructures (CIIs) of the nation and organizations.
8. It is also determined factors that contribute to the vulnerabilities of company's IT infrastructure.
9. Finally, forwarded recommendations towards improving the security and resilience level of CI and CII of the nation and organizations.
10. In this research, data are collected and available. However, for confidentiality purpose, these data are not disclosed.

Introduction

Cybersecurity is the protection and security of cyberspace or digital ecosystem from a wide variety of cyber threats and attacks in order to ensure business continuity, minimize business risk, maximize return on investment, and business opportunities [1, 2]. These days, nations and organizations should protect and secure CIs such as banking and finance, energy and telecom sectors, government, higher education, information and ICT, defense and many more using international cybersecurity standards [3, 4]. These days, information systems and networking infrastructures of nations and different organizations are faced with various security threats from a wide range of sources. Among the various cyber-attacks, cybercrime and terrorism has accelerated significantly during recent years [5, 6]. They are well-organized, wellfinanced, and advanced technically [7-9]. Cybercrime has adopted a new perspective. The old view was quick entry and exit in a given cyberspace. However,

the new outlook is a hidden long term presence that affects the cyber system for a long period of time. As a nation here in Ethiopia as an example, we are not yet well prepared for cyber-war, but today it is economic war [9].

As we have researched, the key cybersecurity challenges in developing countries such as Ethiopia are: lack of comprehensive cybersecurity governance and management framework; lack of national and regional legal framework; lack of adequate cybersecurity professionals, competency, and skills; lack of basic awareness among end users; lack of national and international cooperation etc.[10-12].

Cybersecurity should be seen and well addressed from three different but interrelated perspectives. 1Cyber security technological solutions, 2- Cyber security management and 3- The human factor. Thus the following sections briefly present all of the three core sections of cybersecuity solutions for the existing security problems and vulnerabilities in Ethiopia.

The first research area is cybersecurity technological solutions. The goal of the first component of the research is to investigate the shortcoming of security trends as a nation and organizations and to provide possible mitigation options. To achieve the outlined objectives, various assessments and surveys were conducted to have a deep understanding of how public and private organizations are protecting and securing their information technology (IT) infrastructures that support various business operations. The study also aimed to assess the usage of cybersecurity technological tools optimally at national and organizational level and to have come up with better and comprehensive security techniques of information and infrastructure systems. In view of the above goal, the first step was to focus on the technological solution of cybersecurity [10, 11].

The second objective of this study was to investigate the proper usage and implementation of various cybersecurity governance and management frameworks [11-13]. Here in Ethiopia, both private and public sectors are highly dependent on technological solutions (buying more tools and techniques) to protect their information and technological infrastructures. However, since the width and depth of the cyber-attack dimension is growing faster than ever, technology alone can provide some help but will not be a possible solution for the fastest growing cyber-attack scenarios [14, 15]. To this end, cybersecurity is well addressed by designing and implementing appropriate sets of governance, management, processes, controls, policies, procedures, and organizational security structures to make sure that security and business objectives are met without having security problems [16-18]. In light of the above facts, in this research study, different cybersecurity management solutions are recommended. As an example, there is a need to design a cybersecurity governance framework that should be associated with the business mission of nations and organizations. Cybersecurity management is also the major breakthrough in the cybersecurity realm, which includes planning, budgeting, performance management, etc [19].

Research Methodology

The following major research activities were performed to investigate the security vulnerabilities of different organizations.

Identifying Critical Infrastructures (CIs) of the nation: More than twelve governments owned CIs were selected for the study. Moreover, five regional ICT directorate offices, and three higher educations (universities) were considered in this study. For the stated CIs, strategic and tactical level risk assessment and vulnerability assessment were performed to see the existing security problems and vulnerability of the CIs.

Collecting relevant information: To collect data, different types of questionnaires were prepared according to the context of CIs. These questionnaires were prepared using different industrial standards such as NIST (National Institute of Standard and Technology) cybersecurity framework, ITU (International Telecommunication Union) standards, ISO/IEC, etc. According to the context of the CIs, the questionnaires were given to different information security officers, managers, employees, users, and clients.

On-site interview: To collect useful information from different organizations, on-site interviews were also made on selected organizations and universities.

Through document review was also made to collect important security related information. Reviewing various documents used by different organizations helped the researcher to know what kind of security controls are used by organizations for the IT system that supports business operation of the organizations. The following security document types were exhaustively reviewed and examined. Security policy and procedure documents such as legislative documents and directives; System documents such as system design and requirement guidelines, system user guideline, system administrative manual; security related documentations such as risk assessment reports, security audit reports, system test reports; system vulnerability reports such as report of system security testing, security requirement checklists; system certification test and evaluation reports, vendor's white paper, etc.

Literature review: The most relevant previously published journals, conference proceedings, industrial standards were investigated and reviewed thoroughly [20-24].

Investigating the Security Level of Selected Critical Infrastructure of the Nation and Organizations

Upon completion of analyzing the data, which are collected using different techniques that are mentioned up there, the following major security challenges were identified both at national and organizational level.

- Lack of appropriate organizational security structures to address the issue of cyber incidents.
- Lack of coordinated contingency plan, incident management plan, business continuity and disaster recovery plans and teams in most organizations. Except for some financial firms, there is a lack of disaster recovery sites for critical business continuity operations.
- Lack of SETA (Security education training and awareness) programs.
- Lack of organizational security structures for the constantly evolving cyber threat landscape. By far, financial sectors do have security structures within their overall organization.
- Inefficient sharing of threat and vulnerability information among different stakeholders. As an example, between national security agency and different CIs of the nation, and among different sectors.
- Lack of adequate information security professionals in different industries. By far, financial sectors are better equipped with trained security officials and managers than other industries.
- Ineffectiveness of the implementation of security policy that was developed by national security agencies among different organizations to see security holistically. Even most public and private organizations including universities that were investigated are unaware of the existence of security policy and strategy at national level.
- Currently, cybersecurity is seen as a technology solution by most institutions. It is not yet seen as a multi-dimensional cross-sector issue. To give a bit more detail, as it is researched in different organizations, the cybersecurity management part is almost missed by different organizations except financial industries, airline, telecom, and power sectors. Cybersecurity management is composed of risk assessment, developing and implementing security policy and strategy, governance, incident management, business continuity planning, disaster recovery planning, change management, etc. Today, cybersecurity is shifted from a technological solution paradigm to a risk based approach. However, in most organizations the stated management part of security is not yet fully practiced.

Identifying and Assessing Potential Vulnerabilities of Selected Cis of the Nation and Organizations

From the studied organizations, most of the organizations except financial companies, Airlines, partly in Telecom Company, and power sector, they didn't yet put cybersecurity as their main agenda at board and executive management level. The following existing problems are identified as a nation and organizations. At the national level, mostly the government of Ethiopia is working at a tactical level, not seeing cybersecurity strategically. Recently, the national security agency at national level prepared a draft security policy and strategy and one of the researchers was invited to review the draft security policy of the nation.

Some challenges and weaknesses were observed 1) in the development process; only few stakeholders were involved for the preparation of the draft security policy. 2) The challenge is on how to implement the security policy and strategy by different stakeholders both at public and private organizations. From an organization perspective, it is observed that there is a lack of interest and sense of ownership in the implementation of the policy. From a government perspective, it needs strong leadership and commitment to make sure that the cybersecurity policy will be implemented by both public and private organizations. Harmonization of security policy and strategy at national level is of paramount advantage. However, it is missing in Ethiopia. As an example, different organizations are using different security governance and policy frameworks independently. These results in either a security gap or overlap as a nation and organization. Even different ministry offices are using different security policies and procedures. This existed security problem has the following significant effect:

a. At the top of government (e.g. prime minister, parliament, and presidential offices) don't know that good security practices are being exercised nationally in a comprehensive approach.
b. Since different ministry offices are using different security policies and procedures, at national level they don't know what is left out that leads to security breaches.
c. Monitoring and evaluation of security practices that are being used by different organizations are difficult.
d. Security gaps result in security vulnerabilities, which in turn lead to a long list of consequences including information breaches and audit findings.

Most organizations are also working at a tactical level without having strategic cybersecurity frameworks. As an example, organizations are still buying more security technologies and tools such as installing tools, configuring routers and firewalls, configuring systems, etc. The following potential vulnerabilities of different organizations were identified by researchers.

- Improper configuration and usage of real time security monitoring tools (Sim-tools) that is responsible for monitoring different IT infrastructures including data centers.
- In most CIs, once firewalls are configured, they are not periodically upgraded and updated, which results in weakness in their defense mechanism. This problem was observed in some banking industries, universities, and other institutions.
- Lack of appropriate operational, administrative, technical, and physical security.
- Improper usage of backup strategies following security incidents and disasters. Example, improper implementation of hot-site, warm-site, and cold-site by performing cost benefit analysis for disaster recovery and business continuity operations.
- In most CIs there is lack of incident management, disaster recovery, and business continuity plans. Even at national level so far there is no. However, near Debre Birhan city, the national security agency is building one national disaster recovery site.
- Lack of appropriate security policy, procedures, guidelines, baselines, and standards.
- Improper configuration and implementation of access control management system according to organizational security

policy. As an example, it is observed that access permission and authorization are not managed according to the least privilege principle and separation of duties.

- Lack of the implementation of proper vulnerability assessment, penetration testing and management systems.
- Lack of performing periodic security audits (both internal and external audits) to see vulnerabilities.

Determining Factors that Contribute to the Vulnerabilities of CIs.

The following major factors that lead to security vulnerabilities were identified.
- There is a lack of conducting a proper and appropriate risk assessment. Unless there is proper risk assessment that should be performed periodically by organizations, it is impossible to see their vulnerabilities and what type of threats they are facing. It is also impossible for organizations to clearly identify the level of risk the organization is facing and the impact of the risk on IT systems and business functions that are supported by IT systems. Even though some institutions such as banks and airlines are conducting risk assessment, the following problems are identified. Lack of mechanism to properly classify their company assets that lead to wrong risk profile, poor articulation of risk scenarios, identification of risks using a set of predefined standards, lack of integration of their risk management in to overall organizational risk management process, assessing cyber-risks based on heuristics and past events as well as treating it with irrelevant controls.
- Lack of performing periodic security audits (internal or external). If organizations perform a security audit, they can clearly see their vulnerabilities (weakness in their defense mechanism). - Most organizations don't secure their IT system using industry standards and compliance.
- Lack of top management commitment and allocating appropriate budgets for cybersecurity.
- Lack of adequate operational and physical security.
- Application and data security weakness.
- Lack of controls of port addresses and services, enabling unused protocols.
- Lack of access log
- Lack of mail server protection
- Lack of secure software development life cycle (SDLC) for secure usage of web applications
- Lack of maintenance and upgrading of different security techniques
- Non secure communication among different branch offices, departments, etc.
- Lack of security awareness, training, and education for end users, employees, higher security officials, and top management.

A Way Forward Recommendations to Improve the Security and Resilience Level of Cis

As it is researched, cybersecurity is well achieved by implementing a suitable set of:
A. Cybersecurity governance and management frameworks
B. Cybersecurity risk management and assessment frameworks
C. Cybersecurity strategies and policy
D. Incident management frameworks
E. Business continuity and disaster recovery strategies and frameworks
F. Various types of controls such as administrative, technical, operational, and physical controls.
G. Security procedures, industry standards, guidelines, baselines, and applying best practices.
H. Organizational security structures that should be integrated with the overall organizational structures.

All of the above stated recommendations are presented below.

A. Cybersecurity Governance and Management Frameworks

Cybersecurity governance framework should mainly focus on the responsibilities and practices that should be exercised and addressed by top level management of organizations (board and executive management) having the following main goals: provide strategic direction towards securing the IT system that supports the business function; ensuring that security objectives are well defined and achieved; making sure that security risks are assessed and managed properly and validating that enterprise resources are well spent for securing the assets. Cybersecurity governance framework plays a vital role in achieving the security objectives of an organization for both current issues and future challenges.

To address current security issues, the researcher recommends for the security governance framework to cover the following issues:

If there is already an existing security policy, it needs amendment and review periodically. If there is no security policy, it is recommended to develop security policy at national and organizational level; the implementation of appropriate technological controls; implementation of periodic security audit and assessment; to design and provide security awareness and training programs among citizens.

For future cybersecurity challenges, the security governance framework should address the following points and are recommended here; consider the emerging threat factor; address the fastest moving technological revolution; continually work on people's attitude towards security to create a cyber-aware workforce; focus on the work culture transformation.
In general, it is recommended for the cybersecurity governance framework to incorporate the following component.
- A cybersecurity risk management and assessment methodology
- A comprehensive cybersecurity strategy that should be in line with business and IT objectives
- Appropriate security policies that transform and address each aspect of security strategies.
- A complete set of security standards for each security policy to be transformed into a suitable set of security procedures and guidelines.

- Monitoring mechanism to ensure compliance and the effectiveness of the framework.
- A suitable set of processes to continually evaluate and update the security policies, standards, guidelines, and procedures.
- Designing effective and efficient organizational security structure.

It is also **recommended** for the governance framework to include roles and responsibilities, and accountabilities of various stakeholders, which includes the following:

- Designing SETA program (security awareness training and education program)
- Enhancing research and development programs towards cybersecurity at national and organizational level (in collaboration with universities and center of excellence)
- Designing international and regional collaboration framework
- Designing framework to enhance public-private partnership collaboration.
- Enhancing incident management capabilities.
- Enhancing business continuity and disaster recovery capabilities.
- Enhancing change management capabilities.

To design the outlined security governance framework, **the following major tasks are identified and recommended**

• Develop cybersecurity strategies, which are relevant to the country.
• To effectively implement security strategy, there is a need to design cybersecurity policy
• Define mechanism to obtain senior management's commitment
• Define roles and responsibilities at national and organizational level
• Establish communication and reporting mechanisms, which will support security governance framework
• Develop security procedures and guidelines using standards that support the security policy.
• Establish legal and regulatory framework.

B. Cybersecurity Risk Management and Assessment Frameworks

The researcher strongly recommends that any organization should perform risk assessment periodically to alleviate the ever increasing cyber-attack dimensions. As an initial risk management framework recommendation, the following guidelines are recommended that can be refined according to organizational context.

1. Formation of a risk assessment team from different departments in a given organization and even at country level is the first step.
2. Assignments of responsibilities and creation of awareness and training on risk management framework
3. There is a need to understand and have a clear view of the institution's security setup and readiness.
4. Identifying security holes or vulnerabilities (weakness in their defense mechanism) are important steps that should be performed intensively.
5. Develop a new and/or adopt risk management framework from international standards according to the context of the country.
6. Establish and maintain incident management, disaster recovery, and business continuity programs.

In general, the following three major risk management practices are recommended: 1) to design risk assessment methods, 2) to propose risk mitigation techniques; and 3) to devise mechanisms to periodically evaluate the assessment and mitigation plans and procedures.

C. Security Strategies and Policies

Once risk assessment is performed at organizational and at national level, according to the risk profile, appropriate cybersecurity strategy and policy should be designed. The following *initial security strategy development framework is recommended:*

When cybersecurity strategy is developed at national level that can later on be refined into organizational level, the following key areas was identified by the researcher that should be incorporated in the strategy:

Key Cybersecurity Strategic Areas Include

1. *Governance framework* should be prepared at national and organizational level.
2. *Risk management methods.* In this strategic area, focuses can be to design risk management approach; identify mechanisms for the management of cyber-risk; the development of policies, standards, and regulations; development of sectorial or organizational risk management profile
3. *Incident management and preparedness plan:* which is composed of establishment of contingency plan for crisis management; establishment of incident handling and management capabilities to protect the national cyberspace and digital ecosystem; establishment of Computer Incident Response Teams (CIRTs) with national and organizational responsibility. There is ethio-CERT at national level. However, we recommend this CIRT to be decentralized at least at sectoral level; establishment of public-private partnership for incident detection and response capabilities; development of disaster recovery and business continuity plans.
4. *Securing critical infrastructures*
5. *Capacity development and awareness* that includes development of research and development towards cybersecurity; creation of cybersecurity awareness program; creation of training, education and skill development program; development and implementation of cybersecurity curricula at elementary, high school, and colleges and universities; legal and cybercriminal framework; development of legal frameworks; establishment and promotion of agency that will implement the legal framework; establishment of international cooperation towards cybercriminal; development of capacity building to law enforcement agencies.
6. *Regional and international collaboration*; establishment of cooperation and collaboration partnership with international and regional countries and security agencies.

7. *Institutional cybersecurity framework* that includes establishment of national security advisory board; establishment of agencies responsible for cybersecurity at national level.
8. *Government cybersecurity enhancement program,* which includes establishment of a digital ecosystem that is reliable and convenient for e-commerce and e-government with national public key infrastructure (PKI); development of public-private partnership framework (the partnership can be local and international).

The following additional strategic areas are also identified and are recommended as part of national cybersecurity strategic areas: data protection, privacy, rights, freedom of expression, and information sharing among different stakeholders; security strategies on new emerging technologies such as cloud computing security, security in internet of things (IoT), securing huge amount of data (big data analysis); national data security management and hosting; cyber-physical infrastructure regulatory framework development such as smart grids, industrial control system, robotics system, medical monitoring.
To implement the aforementioned strategic areas, researcher **recommends** the following initial cybersecurity strategy development guidelines that will be refined later on according to nation's context:
• Vision and *mission* of the organization and the nation should be clearly identified and presented.
• *Should follow a comprehensive and holistic approach; cy*bersecurity should be seen from multidimensional perspectives and it is a cross-sector issue that address areas such as law enforcement; national, regional, and international relationship and cooperation; trade negotiation; assuring sustainable economic, social development,…
• *Active participation of multiple stakeholders;* when security strategy is developed, active participation of multiple stakeholders should be involved and it should address their interests, needs along with definition of roles and responsibilities.
• *Consideration of economic and social prosperity;* one of the primary goals of cybsersecurity strategy is to create a cyberspace or digital ecosystem which is secured and resilient to any type of cyber threats. If this primary goal is achieved, it is possible to create economic and social prosperity. It is also possible to maximize the application of ICT to sustainable development.
• *Addressing fundamental human rights;* the strategy should respect all human rights that are agreed in regional and international laws.
• *Risk management and resilience;* the strategy should be developed in such a way that risk at national and regional level should be managed effectively and create a resilient environment.
• *Assignment of resources, roles, and responsibilities;* Assignment of roles and responsibilities at national and organizational level; Allocation of enough human and financial resources for the effective implementation of the strategy.
• *Establish a trusted digital ecosystem;* the strategy should enable to create a trusted cyberspace that can be trusted by business and citizens for the efficient delivery of e-commerce, e-government, and digital transactions.
Finally, for the development of national cybersecurity strategy, the researcher identified for the involvement and active participation of the following stakeholders: The government of Ethiopia (both the executive and legislative branch of government); CI owners and operators; The judiciary branch of the nation; Law enforcement agencies such as general attorney, police department, etc; Local and international vendors; Academia such as universities; International partners; Citizens that can be represented through parliament and civil societies.

D. Cybersecurity Policy Development

Once risk assessment is conducted both at national and organizational level and a set of strategy is developed, security policy will fall quickly in place. Cybersecurity policy can be determined based on feedback from risk assessment results. The risk assessment result will derive security policy creation on the following identified and recommended items such as: change management policy; access management policy; firewall and proxy policy; patch management policy; employee hiring and termination policy; system setup and configuration policy; backup policy; datacenter policy; data encryption policy; email, internet usage policy, etc.

In general, the researcher **recommends** the following types of policies that should be developed and implemented at national and organizational levels: general policy at national level; program policy at organizational level; issue-specific policy; system-specific policy; advisory policy; informative policy; regulatory policy; procedures, guidelines, standards, best practices, and guidelines.

Conclusion and Future Work

In this research study, CIs are identified. Vulnerabilities of these CIs are well assessed using vulnerability assessment and risk assessment techniques. To see security gaps of the CIs, different questionnaires, onsite interviews, document review, and literature review were performed. Investigating the security level of selected CIs of the nation and organizations. Then after, factors that contribute to the vulnerabilities of CIs were thoroughly investigated. Finally, recommendations and solutions were forwarded to improve the security and resilience level of these CIs of the nation.

As a future work, various types of cybersecurity frameworks will be designed according to the context of the nation such as cyebersecurity governance and management framework, cybersecurity risk assessment framework

References

1. Adams, S. A., Brokx, M., Dalla Corte, L., Galic, M., Koops, B. J., Leenes, R., ... & Skorvánek, I. (2015). The governance of cybersecurity.
2. Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.
3. Von Solms, B., & Kritzinger, E. (2012). Critical information

infrastructure protection (CIIP) and cyber security in Africa–Has the CIIP and cyber security Rubicon been crossed?. In International Conference on e-Infrastructure and e-Services for Developing Countries (pp. 116-124). Springer, Berlin, Heidelberg.
4. Gagliardone, I., & Sambuli, N. (2015). Cyber security and cyber resilience in East Africa.
5. Gashgari, G., Walters, R. J., & Wills, G. B. (2017, April). A Proposed Best-practice Framework for Information Security Governance. In IoTBDS (pp. 295-301).
6. Liu, X. F., Shahriar, M. R., Al Sunny, S. N., Leu, M. C., & Hu, L. (2017). Cyber-physical manufacturing cloud: Architecture, virtualization, communication, and testbed. Journal of Manufacturing Systems, 43, 352-364.
7. Liveri, D., & Sarri, A. (2014). An evaluation framework for national cyber security strategies. Heraklion: ENISA, 8.
8. Mod, U. (2011). The UK Cyber Security Strategy Protecting and Promoting the UK in a Digital World. London: Cabinet Office.
9. Morgan, S. "Official annual cybercrime report." Sausalito: Cybersecurity Ventures (2019).
10. Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. National Cybersecurity Institute Journal, 1(3), 9-19.
11. Orojloo, H., & Azgomi, M. A. (2017). A method for evaluating the consequence propagation of security attacks in cyber–physical systems. Future Generation Computer Systems, 67, 57-71.
12. Pernice, I. (2018). Global cybersecurity governance: A constitutionalist analysis. Global Constitutionalism, 7(1), 112-141.
13. Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security?. Journal of Intellectual Capital.
14. Rjaibi, N., & Rabai, L. B. A. (2017). Maximizing Security Management Performance and Decisions with the MFC Cyber Security Model: e-learning case study. EAI Endorsed Transactions on e-Learning, 4(15).
15. Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In 2017 International Conference on Information Systems and Computer Science (INCISCOS) (pp. 253-259). IEEE.
16. Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering, 5(5), 67.
17. Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int'l LJ, 50, 305.
18. Turskis, Z., Goranin, N., Nurusheva, A., & Boranbayev, S. (2019). A fuzzy WASPAS-based approach to determine critical information infrastructures of EU sustainable development. Sustainability, 11(2), 424.
19. Vincent, H., Wells, L., Tarazaga, P., & Camelio, J. (2015). Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. Procedia Manufacturing, 1, 77-85.
20. Melaku, H. M. (2022). Investigating Potential Vulnerability of Critical Infrastructure and way forward–recommendations to enhance security and resilience.
21. Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of cyber policy, 3(2), 258-283.
22. Barrett, M. P. (2018). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, Gaithersburg, MD. USA, Tech. Rep.
23. Ciglic, K., McKay, A., Hering, J., & Moore, T. (2018). Cybersecurity Policy Framework:"A practical guide to the development of national cybersecurity policy". Microsoft.
24. Ramon, M. C., & Zajac, D. A. (2018). Cybersecurity Literature Review and Efforts Report. Prepared for NCHRP Project, 03-127.