Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 74 (2023) 1239–1245

Transportation Research Procedia

www.elsevier.com/locate/procedia

TRANSCOM 2023: 15th International Scientific Conference on Sustainable, Modern and Safe Transport

The Role of Auditors in Critical Infrastructure Protection: Case in Czech Republic

Mimi Enakome Oka[a], Martin Hromada[a*]

[a]*Tomas Bata University, Department of Security Engineering, Zlin 76001, Czech Republic*

Abstract

Recent changes in security and technology environment such as Russia's invasion against Ukraine, the rapid development of technology, internet of things, remote working due to the covid-19 pandemic, has led to an increase in cyber-attacks. The emergence of quantum cryptography could give rise to breaches in quantum security in years to come with national security being affected. Delays or disruptions in the supply chain have led to an increase in the risk of supply chain theft. Personal identity theft is on the increase and as such, the role of auditors in critical infrastructures protection cannot be over- emphasized as this has become a high priority at national and EU level. This review paper examines the role of auditors in protecting critical infrastructures in Czech Republic. It adopted a study carried out by P. Lois et al. (2021), evaluated factors relating to audit and security of information systems. The results of the study concluded that advisory roles of auditors and policy- standards affect the security of information systems.

Keywords: Cybersecurity, Auditor, Cyberthreat, European Union Agency for Cybesecurity (ENISA), European Program for Critical Infrastructure Protection (EP-CIP), Critical Information Infrastructure Protection (CIIP);

1. Introduction

No critical infrastructure in cyber space is untouchable, regardless of the country where it is located (Karabacak et al., 2016). According to Directive EU 2022/2557 of the European parliament and of the Council of 14th December

* Corresponding author.
E-mail address: hromada@utb.cz

10.1016/j.trpro.2023.11.267

2022, Critical infrastructure (CI) means an asset, a facility, equipment, a network, or a system, or a part of an asset, a facility, equipment, a network, or a system, which is necessary for the provision of an essential service. The Directive stated that member States should identify critical infrastructures and ensure the resilience of critical entities by following a risk-based approach, focusing on the entities most relevant for the performance of vital societal functions (EU Directive 2022/2557). To ensure a harmonized framework among member states, there should be an assessment of the relevant risks, both natural and man-made, including those of a cross-sectoral or cross-border nature, that could affect the provision of essential services (EU Directive 2022/2557).

The criteria for risk assessment should be developed as set out in Directive (EU) 2016/1148 of the European Parliament and of the Council to determine the significance and impact of an incidence (EU Directive 2022/2557).

The Organization for Economic Co-operation and Development (OECD) in its 2008 recommendation defines critical information infrastructure or 'CII' as those interconnected information systems and networks of which the disruption or destruction would have a serious impact on the health, safety, security, or economic well-being of its citizens or on the effective functioning of government or the economy (Markopoulou and Papakonstantinou, 2021). The Directive (EU) 2022/2555, requires critical entities belonging to the digital infrastructure sector to take appropriate measures to manage the risks posed to the security of network and information systems and to notify significant incidents and cyber threats by applying an all-hazard approach that includes both the resilience of the network and information systems, the physical components, and the environmental components of those systems (EU Directive 2022/2557).

Failure in critical infrastructures can have impact within the system when failure in one sector cascades into another sector or affect the economy as a whole, depending on the intensity and duration of the threat (Vichova et al., 2017).

Critical infrastructure protection in the Czech Republic is guided by the ACT 430/2010 Coll, Amending Act. No 240/2000 Coll., on Crisis Management and on Amendments to Certain Acts (Crisis Act), as amended, which is seen as the implementation of council directive 2008/114/- EC on the identification and designation of European critical infrastructures and improving their protection, a framework for creating a common European access to critical infrastructure protection (Hromada and Lukas, 2012). Although, Directive 2008/114/EC is being repealed effective from 18th October 2024, because the evaluation of the Directive in 2019 established that due to an increasingly interconnected and cross border nature of operations of CI, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place (EU Directive 2022/2557).

Previous studies showed that the protection of critical infrastructures from disruptive events is achieved through resilience. Resilience in a critical infrastructure system is a cyclical process of continuous improvement of the prevention, absorption, recovery, and adaptation of the system (Splichalova, 2020).

Another factor to consider in protecting critical infrastructures is vulnerability. It is the inability of the system to prevent damage and can be defined as the tendency of an object or a system against any specific risk with certain intensity (Slivkova et al., 2017).

The aim of this paper is to evaluate the role auditors can play in protecting critical infrastructures. It provides answers to research questions on the relationship between the advisory role of auditors, co-operation/collaboration of auditors with IT department, technical knowledge of auditors, policies and standards, information and training of personnels, and the security of information systems.

1.1 Identification of Critical Infrastructure

Critical infrastructures can be divided into technical and socio-economic infrastructures depending on their functions (Rehak et al., 2020). Identification of these critical infrastructures is the first step in protecting them (Markopoulou and Papakonstantinou, 2021). After the critical infrastructures have been identified, the next step is to evaluate their resilience or vulnerability to disruptive events. Academics and policy makers have resorted to the use of concepts and risk analysis to evaluate failure of infrastructures due to accidents or intentional act in a structured manner (DiMauro et al., 2010). However, it is difficult to determine threats posed by accidents or intentional acts in terms of probability. In risk analysis, there is a need to assign a value (either qualitative or quantitative) to the impact and significance of damage done to infrastructures and these are typically assessed in terms of expected loss, however, there are no defined methods to establish the acceptable threshold (DiMauro et al., 2010).

Previous studies have assigned a value for potential impact on critical infrastructures based on selected criteria for identifying and determining critical infrastructure elements (Rehak et al., 2020). Many other studies in the field have assessed critical infrastructures using pragmatic approaches based on indicators and criteria (DiMauro et al., 2010).

The top-down concept of the cross-cutting criteria is characterized by systematically categorizing components into specialized protection systems based on the impact which an infrastructure may cause by its non-functionality while the bottom-up systemic approach is characterized by assessing the criticality of infrastructure component from the smallest component i.e., from the bottom up (Rehak et al., 2017). When using the bottom-up approach, factors that could indicate the disruption of resilience for interconnected sectors should be determined (Vichova et al., 2017). European member states have different degrees of preparedness which has led countries to use different approaches across the European union and as a result there is an unequal level of protection of infrastructures, which undermines the overall security of critical infrastructures (Zygierewicz, 2020).

According to information on essential services, the cross-cutting criteria applied in the Czech Republic are as follows:

- Any disruption that would affect a large number of people, greater than 25,000 at the minimum (https://www.nukib.cz/).
- Disruption of another critical infrastructure element where the impact of that incident threatens an essential service identified in another country in the European Union (https://www.nukib.cz).
- Disruption which causes economic loss greater than 0.25% of Gross Domestic Product (GDP) from business disruptions, fines and penalties, property damage, injuries, and other cost (https://www.nukib.cz/).
- Unavailability of service to more than 1,600 people except in the electricity, gas, thermal industry, and banking sector, where there is a need for immediate provision of services for many users (https://www.nukib.cz/).
- A large number of casualties or injured people in need of medical treatment caused by the disruption of the given service (https://www.nukib.cz/).
- Disruption of public safety in an administrative territory of a municipal which may require rescue operations by the fire services, police are medical rescue service (https://www.nukib.cz/).
- Disclosure of sensitive data greater than 200,000 people in the health sector (https://www.nukib.cz/).

1.2 Indication of Crisis of Critical Infrastructures

According to Rehak et al., 2017, factors that indicate crisis can arise are as follows: origin of an extraordinary event with direct impact on the respective sub-sector, origin of an extraordinary event in the respective sub-sector, the need to regulate consumption and supply in the respective sub-sector, acquisition of intelligence information indicating a risk of terrorist attack, and insufficient preparedness of public administration authorities for organized and logistical solution to the situation. Factors that indicate the imminent risk of a crisis are as follows: authorities implementing special forces in the respective sub-sector, limitation, or interruption of supplies in the respective territory, activation of an integrated rescue system, probability of origin of secondary crisis situations, acquisition of intelligence, information confirming a realistic risk of terrorist attack, and assessment of the international-political situation. Factors that indicate that an event is a crisis includes surmounting and clean-up of consequences of a state of emergency which is not within the abilities of the operator of the respective sub-sector, limitation, or interruption of supplies of strategic commodities, and services that affects a substantial part of the territory.

1.3 Security Audit

According to the stocktaking, analysis, and recommendations on critical infrastructures by ENISA, organizations should conduct security audits and report major IT security incidents if there are possible effects on critical services. In the survey conducted by ENISA, it was observed that security audits were not placed as high priorities in most European countries. However, it should be noted that most audits performed by internal auditors in organizations do not cover cybersecurity risk (Deliotte, 2017). Internal audit effectiveness arguably depends on four factors: quality of internal audit, attributes of auditee, organizational setting, and management support (Mihret and Yismaw, 2007). Internal audit ensures an organization's compliance with rules and regulations that regulates its operations (Deliotte, 2017).

2. Methodology

This paper adopts the model by P. Lois et al., (2021) which evaluated the factors relating to audit and security of information systems.

- **Advisory role of internal auditors:** According to Steinbart et al (2015), the contribution of internal audit to the security of information systems relies on the fact that the auditor is independent of the creation of these systems to audit them properly.
  - H_1: The advisory role is directly proportional to the number of violations.

- **Co-operation/ collaboration with auditors and IT department:** The results of research conducted by Bauer and Estep (2018) showed that when there is a good relationship between the auditors and the IT department, the audit is effective and timely.
  - H_2: The cooperation between internal audit and IT professionals is directly proportional to the number of violations.
- **Technological knowledge:** Richard et al (2005) argued that internal auditors should have basic IT knowledge to carryout audit functions.
  - H_3: The existence of specialized technological knowledge on the part of internal auditors is directly proportional to the number of violations.
- **Policies and standards:** Kayworth and Whitten (2010) conducted interviews with business security executives and argued that internal audit independently evaluate security policies.
  - H_4: Internal audit security standards are directly proportional to the number of violations.
- **Information and training of personnel:** Abawajy (2014) emphasized the need for personnels to have adequate information on safety rules through leaflets, seminars, or videos to reduce violations.
  - H_5: Information and training of personnel is directly proportional to the number of violations.

According to P. Lois et al., (2021) the study was conducted in Greece, Athens. Companies listed on the Athens stock exchange were selected. Questionnaires designed to examine the variables relating to internal audit and security were sent to the internal auditors of those companies. The selected samples were chosen from internal auditors working in entities listed on the Athens stock exchange.

$$Y= b+ b_1X_1 +b_2X_2 +b_3X_3 + b_4X_4 + b_5X_5 + \varepsilon \quad (1)$$

Dependent variable, Y = the security of information systems.

X_1, X_2, X_3, X_4, X_5 = independent variables i.e., advisory roles of internal auditors, co-operation/ collaboration with auditors and IT department, technological knowledge, policies and standards, and information and training of personnel respectively.

Coefficients = b_1, b_2, b_3, b_4, b_5. They represent the parameters that express the relationship between the independent variables and the dependant variable, and how much the dependant variable is expected to change if the independent variable changes by one unit provided other parameters remain constant. While ε represents the prediction error (P. Lois et al., 2021)

3. Results

The survey results according to P. Lois et al., (2021) backed by correlation testing performed with Pearson index showed that there is a statistically significant linear correlation between the dependent variable, security of information systems and the independent variable, policies- standards ($r = 0.4777$, p-value < 0.05). There is also a significant linear correlation between the dependent variable, security of information systems and the independent variable, advisory roles ($r = 0.674$, p-value < 0.05). There is no statistically significant correlation between the dependent variable, security of information systems with other independent variables (P. Lois et al., 2021).

TABLE 1 Correlations

	Security of Online Services	Advisory roles	Co-operation	Technological knowledge	Policies and procedures	Information and training
Security of Online Services	1					
Advisory roles	0.674	1				
Co-operation	-0.033	-0.329	1			
Technological knowledge	-0.157	-0.478	0.782	1		
Policies and procedures	0.477	0.122	0.572	0.584	1	
Information and training	-0.002	-0.266	0.7	0.676	0.572	1

P. Lois et al., (2021) Internal auditing and Cybersecurity: Audit role and procedural contribution.

TABLE 2 Coefficients

Model	Unstandardized coefficients		Standard coefficients		
	β	Std. error	βeta	t	Sig
Constant	1.438	0.433		3.324	0.001
Advisory role	0.416	0.087	0.481	4.787	0
Co-operation	0.044	0.105	0.051	0.413	0.681
Technological knowledge	-0.175	0.116	-2.22	-1.508	0.136
Policies and standards	0.605	0.113	0.613	5.348	0
Information and training	-0.17	0.107	-1.62	-1.584	0.118

P. Lois et al., (2021) Internal auditing and Cybersecurity: Audit role and procedural contribution.

According to P. Lois et al., (2021) the multiple linear regression is as follows:

Security of information systems = 1.438 + 0.416 * advisory role + 0.044 * co-operation- 0.175* technological knowledge +0.605 * policies and standards - 0.170 * information and training (2)

Table 1 shows that there is a positive correlation between the dependent variable security of information systems and the independent variables, advisory roles, and policies- standards.

Table 2 shows that the first independent variable “advisory role” has a t value = 4.787 and p value=0.000 < 0.005. The fourth independent variable “policies and standards” has a t value = 5.348 and significance p value= 0.000 < 0.005. Therefore, we reject the null hypothesis and accept the alternative hypothesis that the variables “advisory roles” and policies- standards” affect the security of information systems (P. Lois et al., 2021).

4. Discussions

The overall results indicate that the advisory roles of internal auditors and policy- standards in organizations have a positive relationship with security of information systems. This implies that as the management implements auditors’ recommendations and staff members adhere to the organization’s standard policies and procedures then information systems would be secure. All other factors in the study such as collaboration between the auditors and IT department, technical knowledge of auditors, and information and training do not affect the security of information systems. The findings of this study are restricted to the private sector in Greece, however, in the Czech Republic security falls under the responsibility of the Ministry of Interior and National Cyber and Security Agency (NUKIB), which is a public sector. Notwithstanding, the results can be relied on as there is co-operation and exchange of information on cyberspace protection between the private and the public sector in the European Union (I. Lella et al, 2021). It would be interesting to carry out further research on the effect of advisory roles of auditors and policy- standards in critical entities that have reported incidents in the Czech Republic.

5. Conclusions

Auditors have an important role to play in the protection of critical infrastructures. This review paper adopted the methodology in a study conducted by P. Lois et al., (2021). The two important variables that affect security of information systems are advisory roles of the auditors and policy-standards. Auditors in organizations whether external or internal should continue to play advisory roles to the management and ensure policy- standards are being adhered to. In the European Union, ENISA provides the tools and publications for institutions to follow. Cyber threats, incidents and events should be shared with NUKIB in the Czech Republic. To maintain the national security or the security of critical entities, sensitive information should be accessed, exchanged, and handled prudently giving detailed attention to the transmission channels and storage capacities (EU Directive 2022/2557).

References

Alzeban Abdulaziz, G. D. (2014). Factors affecting the internal audit effectiveness: A survey of Saudi public sector. *International Accounting Auditing and Taxation, 23(2)*, 74-86.

Arena M, A. G. Internal audit effectiveness: Relevant drivers of auditees satisfaction. *Internal Journal of Auditing, 13*, 43-60.

Deloitte (2016): The changing role of audit committee and internal audit deloitte.

Cohen, A., & Sayag, G. (2010). The effectiveness of internal auditing: An empirical examination of its determinants in Israeli organisations. *Australian Accounting Review, 20*(3), 296-307. doi:10.1111/j.1835-2561.2010.00092.x

COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (text with EEA relevance)

S., Bernatik, A., Senovsky, P., Senovsky, M., & Rehak, D. (2013). Territorial risk analysis and mapping. *Chemical Engineering Transactions, 31* doi:10.3303/CET1331014

DiMauro, C., Bouchon, S., Logtmeijer, C., Pride, R. D., Hartung, T., & Nordivik, J. P. (2010). A structured approach to identifying European critical infrastructures. *International Journal of Critical Infrastructures, 6*(3), 277-292. doi:10.1504/IJCIS.2010.033340

Directive EU 2022/2557. Retrieved from https://eur-lex.europa.eu/eli/dir/2022/2557/oj

Drogalas George, Karagioras Theotanis, Arampatzis Konstatinos. (2015). Factors associated with internal audit effectiveness: Evidence from Greece . *Journal of Accounting and Taxation, 7 (7)*, 113-122.

Getie Mihret, D., & Wondim Yismaw, A. (2007). Internal audit effectiveness: An Ethiopian public sector case study. *Managerial Auditing Journal, 22*(5), 470-484. doi:10.1108/02686900710750757

Hromada, M., & Lukas, L. (2012). *Multicriterial evaluation of critical infrastructure element protection in Czech republic* Springer Berlin Heidelberg. doi:10.1007/978-3-642-35267-6_48

Information on the essential service

Internal audit an urgent call to action deloitte advisory 2017. (2017). ().

Kampova, K., Lovecek, T., & Rehak, D. (2020). Quantitative approach to physical protection systems assessment of critical infrastructure elements: Use case in the Slovak republic. *International Journal of Critical Infrastructure Protection, 30*, 100376. doi:10.1016/j.ijcip.2020.100376

Karabacak, B., Ozkan Yildirim, S., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of turkey. *The Computer Law and Security Report, 32*(3), 526-539. doi:10.1016/j.clsr.2016.02.005

Lella, I., Theocharidou, M., Tsekmezoglou, E., Malatras -European, A., Ardagna, C., Corbiaux, S., . . . Douligeris, C.*Enisa threat landscape 2021 editors* doi:10.2824/324797

Lois, P., Drogalas, G., Karagiorgos, A., Thrassou, A., & Vrontis, D. (2021). Internal auditing and cyber security: Audit role and procedural contribution. *International Journal of Managerial and Financial Accounting, 13*(1), 25-47. doi:10.1504/IJMFA.2021.116207

Malachová, H., & Oulehlová, A. (2016). Application of business continuity management system into the crisis management field. *Transactions of the VŠB-Technical University of Ostrava, Safety Engineering Series, 11*(2), 43-50. doi:10.1515/tvsbses-2016-0016

Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *The Computer Law and Security Report, 41*, 105502. doi:10.1016/j.clsr.2020.105502

Mort Dittenhofer. (2001). Internal auditing effectiveness: An expansion of present methods.*16(8)*, 443-450.

National cyber security center. Retrieved from https:// www.govcert.cz/en/act/regulation-and-audit

Nyaga Milton Kaboi, D. K., & Kamau George Riro. (2018). Influence of internal audit independence on internal audit effectiveness in the kirinyaga county government Kenya. *Internal Journal of Economics, Commerce and Management, VI*(5)

Pereira, T., & Santos, H. (2010). *A security audit framework to manage information system security* Springer Berlin Heidelberg. doi:10.1007/978-3-642-15717-2_2

Rehak, D., Hromada, M., & Ristvej, J. (2017). *Indication of critical infrastructure resilience failure* CRC Press. doi:10.1201/9781315210469-124

Rehak, D., Hromada, M., & Lovecek, T. (2020). Personnel threats in the electric power critical infrastructure sector and their effect on dependent sectors: Overview in the Czech republic. *Safety Science, 127*, 104698. doi:10.1016/j.ssci.2020.104698

Slivkova, S., Rehak, D., Nesporova, V., & Dopaterova, M. (2017). Correlation of core areas determining the resilience of critical infrastructure. *Procedia Engineering, 192*, 812-817. doi:10.1016/j.proeng.2017.06.140

Splichalova, A. (2020). *Managerial decision making in indicating a disruption of critical infrastructure element resilience* MDPI AG. doi:10.3390/admsci10030075

Stock taking analysis and recommendation on the protection of CIIs European union agency for network and information security. (). Retrieved from https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

Titko, M., Ristvej, J., & Zamiar, Z. (2021). Population preparedness for disasters and extreme weather events as a predictor of building a resilient society: The Slovak republic. *International Journal of Environmental Research and Public Health, 18*(5), 2311. doi:10.3390/ijerph18052311

Vichova, K., Hromada, M., & Rehak, D. (2017). The use of crisis management information systems in rescue operations of fire rescue service of the Czech republic. *Procedia Engineering, 192*, 947-952. doi:10.1016/j.proeng.2017.06.163

Zygierewicz Anna. (2020). *Directive on security of network and information systems, European parliamentary research service* . ().