PROFESSIONAL PAPER

Annals of Disaster Risk Sciences

Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure

Implementing Cybersecurity Measures in Transport Organisation

Silvana Tomić Rotim, University of Applied Sciences Velika Gorica, ZIH

Address for correspondence: Silvana Tomić Rotim, University of Applied Sciences Velika Gorica, ZIH d.o.o., Croatia, e-mail: stomic@zih.hr

Abstract

The Article describes the phases of implementing the necessary measures according to Cybersecurity Regulation for critical infrastructure and ISO 27032 standard. As a base for identification of the necessary measures in transport organization the risk assessment has been done. The Risk Management Methodology has been described as well as the results of the risk assessment. The main aspects of risk treatment with the most suitable measures for Cyber risks are identified. Also as very important aspect of protecting critical transport infrastructure we have identified the critical services and prepared business continuity plans. The main steps and results in providing the acceptable level of availability and opportunities for continuity are presented and explained.

Keywords

Critical Infrastructure, Cybersecurity Regulation, ISO 27032, Risk Management, Business Continuity

1. Introduction

In the last decades a lot of organizations have experienced different types of Cybersecurity attacks, such as Ransomware, Internet of Things Botnets, Phishing and Whaling attacks, Business Process Compromise Attacks, Machine Learning enabled attacks etc (Goud, 2017).

European Union has taken various steps to help companies and the critical infrastructure providers to implement the necessary measures for achieving the acceptable level of security and continuity in delivering their services. The Cybersecurity Regulation for critical infrastructure is in place and all providers have to conform to it. Because of that the paper covers the most important phases of implementing the necessary measures according to this Regulation and available international standards (ISO 27032, ISO27001, ISO 22301), and the practical case study for Rail Infrastructure.

2. Methods

Some qualitative, as well as quantitative methods were been using in this paper. Relevant studies addressing the issue of the different types of Cybersecurity attacks and their consequences will be analysed at the global level. Observations will be systematized via the synthesis method. Also, existing methods (RA – Risk Assessment, BIA – Business Impact Analysis, etc.) will be analysed, as well as the relevant literature that addresses the issues

of Cybersecurity. The descriptive method was used for investigation and understanding types of Cybersecurity attacks generally, and the specifics for critical infrastructure.

RA method has been applied for investigation of the most critical risks for Rail Infrastructure, and BIA for identification of the most important services that Rail Infrastructure offers and that could be interrupted by Cyber-attacks. The highly structured questionnaires were used in conducting risk assessment and business impact analysis. The participants involved in applying these methods on rail infrastructure were the business processes owners. With the analytic-synthetic method the relationship between the results of these methods (RA and BIA), and suggested security measures was established through Risk Treatment Plan and Business Continuity Strategy.

2.1 Risk Assessment Method

For risk assessment in the Railways Infrastructure company I prepared the methodology based on the guidelines of ISO 31000 and ISO 27005. It is entirely suited to the needs of the organization to conduct a cyber risks assessment.

Risk assessment was conducted to assess the likelihood of threats occurring with respect to the preventive security measures implemented to mitigate the vulnerability and the impact once the threat occurs.

Likelihood is expressed using a predetermined method of grading the probability of occurrence of an event. Because the distribution of the likelihood of threats occurring is widespread in practice (ranging from daily unwanted events such as the occurrence of spam to events such as fires or terrorist attacks that occur once every few decades), the scale will qualify as indicated in Table 1.

Table 1. Threat occurrence likelihood levels

Level	Likelihood of threat
High	This event is expected to occur in most cases.
Moderate	Events can sometimes occur.
Low	Occurrence of an event is not likely.

Once the likelihood of a threat occurrence has been determined, it is necessary to evaluate the negative impact that could appear if the threat successfully exploits the vulnerabilities. In this assessment one should use previously obtained values of information assets, the purpose of the system, the importance of data for an organization's operations, the sensitivity of data and the security measures that reduce the impact once the threat occurs.

Impact assessment refers to the loss or compromise of any fundamental information system principles or a combination of these principles, loss of the revenue, system repair costs, loss of public reputation, etc.

The impact value is qualified as defined in Table 2.

Table 2. Impact level

Level	Impact
High	• Interruption of key services • Loss of significant assets • Serious environmental damage • Death • A significant loss of public reputation

	• Public pressure for changes in organization • Endangering the integrity of the traffic management, signal-safety or electrical-energy subsystem • 10 trains daily affected by the incident
Moderate	• Interruption of some basic services • Loss of property • Certain adverse effects on the environment • Severe injuries • Partial loss of public reputation • Negative public opinion in the media
Low	• Delay in deadline for less significant processes/services • Loss of property (small value) • Temporary adverse effects on the environment • First aid treatment • Slower gaining of public trust • Partly negative attitude of the public

Based on the likelihood of the occurrence and the impact of the threat on the asset, the ultimate value of the risk is determined. This is done according to the defined risk calculation matrix, listed in Table 3.

Table 3. Risk matrix

LIKELIHOOD	High (3)	3	6	Unacceptable risks
	Moderate (2)	2	4	6
	Low (1)	Acceptable risks	2	3
		Low (1)	Moderate (2)	High (3)
		IMPACT		

This risk matrix sets out the framework for selecting risk treatment options. For all unacceptable risks (risk level greater than or equal to 6) measures will be identified to address that risk.

2.2 Business Impact Analysis Method

To ensure continuity in the provision of key services, the BIA - Business Impact Analysis method will be used. Its purpose is to determine which business processes are necessary to ensure the continuity of key services in the event of a major incident, and to prioritize their renewal. During the BIA, the impact of interruptions of business process or activities on the overall organization's operations is analysed in detail. The goal of the analysis is to collect data that is critical for selecting a business continuity strategy, implementation of the solutions, and developing business continuity plans and procedures. The data mentioned, among other things include:

- Relationships and interdependencies of the process internally and externally,
- Tangible and intangible losses caused by interruption of the process,

- Recovery Time Objective (RTO),
- Recovery Point Objective (RPO),
- Minimum business continuity objective (MBCO)
- Maximum acceptable outage (MAO)
- The resources necessary to recover the functionality of process providing critical services in the event of interruption.

Interruptions of key services as a direct effect have losses compared to the normal, undisturbed operations of Rail Infrastructure company. There are two basic types of losses - tangible and intangible. The tangible losses include those losses that can be quantitatively expressed. Most often, these are financial losses (decrease or delay in revenue, increased operating expenses, etc.), since in most cases they can be estimated by analysing the organization's operations. Other types of tangible losses include the reduction of services offered, loss of market share, reduction of the number of users, penalties determined by the SLA contracts, etc.

Intangible losses are those losses that cannot be quantified but have a significant impact on the future performance of the organization. These are, for example, loss of reputation, loss of customer trust, loss of competitiveness, compromising customer safety, etc. For all identified losses, it is necessary to determine the level of impact on the business. The following is an overview of the parameters estimated at Rail Infrastructure company for each key service:

- Lost revenue due to process interruption
- Penalties for failure to comply with legal obligations
- Penalties for non-fulfillment of contractual obligations
- Operating costs of process renewal
- The possibility of permanent loss of contracts with key user
- Strategic importance for the owner
- Strategic importance for business environment
- Loss of reputation.

The assessment of each parameter was performed by a qualitative method according to the three-level scale of impact (large, moderate, small).

3. Problem Analysis

In the last decades a lot of organizations have experienced different types of Cybersecurity attacks, such as Ransomware, Internet of Things Botnets, Phishing and Whaling attacks, Business Process Compromise Attacks, Machine Learning enabled attacks etc (Goud, 2017). A Cybersecurity attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A Cybersecurity attack can maliciously disable computers, steal data, or use breached computers as a launch point for other attacks. Cybercriminals use a variety of methods to launch a Cybersecurity attack.

For Cybercriminals the very interesting subject of attack are critical infrastructures. The loss of service or the damage to customer and public confidence can have dramatic consequences. Critical infrastructures include health, emergency services, energy, financial services, food, government, water and transport. This paper is about how to solve the problem of potential cyber-attacks in the field of rail transport.

Railways, as critical infrastructures, are a highly tempting security breach target. And as railways are embracing automation by increasingly connected railway systems, this network creates a one-of-a-kind technical complexity where firewalls, signature-based mechanisms and other network perimeters are not enough to cope with internal or external cyber-threats. To determine how attacks on railways could be performed, British-based computer security firm Sophos, in cooperation with Koramis of Germany, created project Honeytrain, (Milne, A. 2017). A model was set up as a honeypot to hackers of a mythical virtual rail transport control and operating system, in order to gain information about the quality, quantity and aggressiveness of possible attacks. During its operation of six weeks, a total of 2,745,267 cyberattacks on railway systems from several countries identified.

Because of its critical role for rail safety and its increasing level of complexity, the signaling system, a critical safety system that directs and manages railway traffic, is the most sensitive system and a cyber-attack on this system could cause serious damage (e.g. human lives, economic losses, reputational damage, etc.). According to cybersecurity experts, it is the weakest link within railway systems, UNIFE (2019). This weakness is due to several factors, such as the prevalence of older equipment that is prohibitively expensive to upgrade, the combination of IT and OT networks and most importantly, the lack of railway-specific cybersecurity solutions to protect this critical system. Its vulnerability is increased due to the continued introduction of RIoT (Rail Internet of Things) sensors and tools and by moving to the cloud. Generally, cyberattacks are becoming more frequent and more sophisticated so it is very important to be able to identify them on time and to be prepared for preventing these attacks or in the worst case be able to answer to the incidents.

4. Discussion and Conclusions

4.1 Regulations and Standards

Based on the above presented problem analysis and the trends in Cybersecurity attacks on critical infrastructure, we can conclude that it is necessary to provide systematic approach in coping with this problem and finding the appropriate solution.

The European Union Parliament and the Council have adopted the Directive (EU) 2016/1148 concerning measures for high common level of security of network and information systems across the Union. According to this Directive, EU Directive (2016), all Member States have to adopt a national strategy on the security of network and information systems, create a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States, create a computer security incident response teams network in order to contribute to the development of trust and confidence between Member States, establish security and notification requirements for operators of essential services and for digital service providers, and designate national competent authorities. The Directive contains the list of entities that offer essential services, and among them is rail transport, including infrastructure.

Following this Directive Croatia has adopted the National Strategy for Cybersecurity that covers the following key areas of cyber security:

- Electronic communications and information infrastructure and services, which is further divided into public electronic communications, electronic government and electronic financial services,
- Critical communication and information infrastructure and cyber crisis management,
- Cybercrime.

Also Croatia has adopted the Regulation and the Act on cyber security for key service providers and digital service providers. This Act regulates procedures and measures to achieve a high level of cyber security for key services and digital service providers, as well as the criteria for identification of the incidents that have high impact to providing critical services.

This regulatory EU and national framework offer the basic elements that could be taken into consideration in the process of improving Cybersecurity measures implemented in critical services providers. Beside it, it is very useful to apply international standards for information security, especially ISO 27001 Information security management systems – Requirements ISO/IEC (2013), and ISO 27032 Guidelines for cybersecurity (ISO/IEC, 2012). The main steps of ISO 27032 implementation are, (Tomić Rotim, S. 2019):

- Identification of all physical and virtual, personal and organizational assets. Under the asset we mean information, software, hardware, services, people and some intangibles, such as reputation and image.
- Risk assessment that means identification and analysis of threats and vulnerabilities. The results of risk assessment are presented through Risk Assessment Report.
- Business impact analysis for the purpose of identifying the most critical processes and the acceptable time for recovering the critical services in the case of disaster.

- Determination and implementation of the appropriate cybersecurity measures. There are different kinds of cybersecurity controls, such as: Application-level controls, Server protection controls, End-user controls, Controls against social engineering attacks, Cybersecurity readiness controls and others.

The best option for all critical services providers is to combine the directions from the regulatory framework and the best practices from the international standards. In the case of Rail Infrastructure and its critical services this approach has been applied. The key performance indicators of the whole process and the implementing measures show that this approach is successful.

4.2 Risk Assessment

For the core activities in the process model of the provision of key services, a risk assessment was carried out and risk treatment measures were defined in accordance with the methodology described above. Table 4 provides an overview of the identified risks and security measures for the signal-safety system that is essential in providing the key railway infrastructure management and maintenance services, including traffic management.

The signal-safety system was selected because it plays a critical role in railway safety, as stated in the previous chapter.

Table 4. Overview of identified risks and security measures for management of the signal-safety system

No.	Risk	Security measure
1.	Unauthorized access to signal-safety devices	• Rules on Information Systems Safety Management (Physical Security) • Anti-theft locks • Instructions for workers of executive service with a signal-safety and telecommunication devices • Performing regular inspections and testing of signal-safety devices • Activities for the protection of property and premises
2.	Improper/disabled functioning of signal-safety devices	• Spare parts • Instructions for maintaining the signal-safety devices • Performing emergency maintenance, regular inspections and testing of signal-safety devices
3.	Tapping into a communication channel between individual parts of the signal-safety devices	• Traffic Regulations • Instructions for workers of executive service with a signal-safety and telecommunication devices • Rules on maintenance of signal-safety devices • Performing regular inspections and testing of signal-safety devices • Activities for the protection of property and premises
4.	Irresponsible management of critical assets and changes to	• Instructions for workers of executive service with a signal-safety and

	critical assets	telecommunication devices • Rules on maintenance of signal-safety devices • Performing regular inspections and testing of signal-safety devices • Compliance with and enforcement of the provisions of other general acts relating to property • Activities for the protection of property and premises
5.	Infrastructure Subsystem Monitoring Tool (CA Spectrum) Disabled	• Instruction for workers of executive service with a signal-safety and telecommunication devices • Rules on maintenance of signal-safety devices
6.	Abuse by authorized persons	• Rules on Information Systems Safety Management (Access Control) • Limited number of persons with access rights • Performing regular inspections and testing of signal-safety devices • Activities for the protection of property and premises • Staff awarness

Some of the security measures have already been implemented and some are in the process of implementation, after which a new risk assessment needs to be carried out and the initial risk levels reduced. Risk assessment and treatment ensures preventive action to reduce cyberattacks. Nevertheless, such attacks are still possible because the risks cannot be reduced to zero. To ensure good corrective action in the event of an attack, a process for managing cyber incidents and business continuity has been implemented. For incidents, the procedure for reporting an incident is described, as well as the method of incident response and reporting. The incident response process includes:

- collection of evidence as soon as possible after the event,
- conducting forensic analysis (if necessary),
- escalation (if necessary),
- assessing the need for corrective action,
- implementation of appropriate corrective actions,
- ensuring that all incident response activities are appropriately recorded for later analysis,
- communicating the incident with relevant details to internal and external persons and organizations on a need-to-know basis,
- formal closure of incident after resolution,
- checking if corrective actions are effective.

4.3 Business Impact Analysis

In order to prepare an adequate business continuity plan, the BIA was performed according to previously described methodology. For the key railway infrastructure management and maintenance service, including traffic management, all the processes on which that service depends are identified:

- Maintenance of telecommunications
- Maintenance of electro-energy system
- Maintenance of track upper and lower structure
- The organization and regulation of traffic
- Maintaining a business network
- Maintenance of the transport network
- Maintenance of signal-safety system

All resources for successful provision of this service have been identified. These include human resources, vendor services, required data, registry phones, trackside radio, trackside telephone cables, station-to-station signal ring, UHF and VHF system, wind sensors, SPEV (SCADA) system for EE system, SCADA remote control centers, energy telecommunication cables, transformer stations, etc. Table 5 provides a description of the key services.

Table 5. Description of the key services

Service	Dependency description
Registry phones	Record communications/conversations (on telecommunication premises or in traffic offices)
Trackside radios	Part of the radio dispatch system.
Trackside telephone cables	For connections between the signal-man at the railway stations, there are usually two lines on the same line.
Station-to-station signal ring	Part of the traffic management system. Train direction notification.
UHF and VHF systems	Communication between traffic staff within one station (for example. train manoeuvring between tracks). Maintenance people also use it if a physical connection has broken.
Wind sensors	The sensors are placed on the critical parts, gives information to the staff, the information goes to the railroad dispatcher via a cable connection.
Line cabinets and telephones - parts of traffic management systems	Line cabinets and telephones for communication with traffic offices.
Telephone exchanges	For tunnel work or bends, when outsourced companies do maintenance, then they answer by telephone (make a conference call)-and this is recorded.
Energy telecommunication cables	To power the telecommunications devices.
Video cameras and recorders (for traffic monitoring)	For video surveillance. Recorded locally on discs at stations.
SPEV (SCADA) system for EE system	Operation of power plants to provide electric power to the contact network.
SCADA remote control centers	When entering the SPEV facility the system records that the door is open.
Transformer stations	To power the stations. In case of power failure there are backup generators at the railway stations.

IST system	For maintenance of timetables of all trains (train data) – planned and actual routes are recorded. If system does not work for 1 day, data is retroactively entered – not connected with traffic management. A maximum of 3 days can be entered backwards if the IST does not work.
Mail	The telegrams are sent to inform about changes in relation to the plan; if the mail does not work then it is reported via phone.
Network devices	On railway stations in telecommunication cabinets. Remote access to telephone exchanges, registry phones, video cameras and recorders.
Optics (optic cables)	For connecting network devices and external operators with optic cable. There is a local cable along the main cable.
SS device	Devices for securing stations, open rails and railway crossings.
Railroad light signals	For allowing and prohibiting train rides. Two-filament bulbs are used to reduce risk. Bulbs have a detection system that detects if the bulb does not work.
Switches	Shift switches and control their position and accuracy. In the event of a malfunction, the switch can be switched manually.
Devices for securing railway crossings	They allow and prohibit the driving of road vehicles.
CA Spectrum	Incident reporting application system for Maintenance department. SS is not connected.

These analyses have identified the criticalities of certain IT services necessary for the operation of Rail Infrastructure, as well as the parameters describing the operational impact of the disruption of operation of individual IT services on business. The analysis also defines the business requirements according to the availability of IT services, in such a way that it determines the deadline within IT services can be recovered if unacceptable losses for the company are to be avoided. The data collected serves as a basis for considering possible BC strategies and selecting the most appropriate ones. The selection of the most appropriate strategies or solutions is made on the basis of several criteria, the most important of which are:

- Recovery Time Objective (RTO) - the timeframe for resuming minimum set of IT service functionality in order to avoid unacceptable losses and compromise business sustainability,
- Recovery Point Objective (RPO) - the point in time before which all stored data must be securely preserved (the target frequency of backing up data to reduce losses to an acceptable level).
- Implementation cost

Fulfillment of RPO parameters can be viewed from two aspects, the availability of data in case of failure and the preservation of integrity during its disruption. Data availability is achieved through redundant copies, whether on tapes, disk or any other medium.

Fulfillment of RTO parameters defines the difference in time that is currently required for the establishment of IT services after the outage and the one defined. Reducing IT service recovery time and approaching target recovery time (RTO) are achieved in various ways, the most common of which are:

- establishment of redundancy,
- preparing and ensuring the necessary preconditions for a faster recovery,
- preparation of backup equipment,
- education of employees,
- designing an IT architecture that can use the established redundancy automatically or semi-automatically.

The business continuity strategies to be considered are those that allow for renewal at a time equal to or less than the established RTO and whose implementation cost does not exceed the maximum cost that the organization has decided to tolerate in the event of an incident.

The Business Continuity Strategy covers all the resources necessary for the business, namely:

- staff,
- office space,
- equipment and ICT systems,
- information,
- services and suppliers,
- transportation,
- financial resources.

Key resources important to the business of Rail Infrastructure include numerous types of equipment, services and communication. The strategies are divided by the aforementioned resources - different resources, namely, require a different approach when developing a business continuity strategy. While, for example, for a typical data center, it is best to build an alternative location where servers and associated services and applications will be renewed, for resources such as data communications strategy is mostly confined to the realization of multiple or alternative communication links.

Based on the selected strategies, business continuity plans and DR procedures have been made which are necessary for the provision of key services.

References

EU Directive (2016): European Union Parliament and the Council, the Directive (EU) 2016/1148 concerning measures for high common level of security of network and information systems across the Union, 6 July 2016.

Goud, N. (2017): Most Dangerous Cyber Security Threats of 2017, https://www.cybersecurity-insiders.com/most-dangerous-cyber-security-threats-of-2017/

ISO/IEC (2012), ISO/IEC 27032 Information technology – Security techniques – Guidelines for Cybersecurity

ISO/IEC (2013), ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements

Milne, A. (2017): Hacking the railway, The European Rail Supply Industry Association, https://www.railengineer.co.uk/2017/05/30/hacking-the-railway/

National Strategy for Cybersecurity, 7 October 2015. (NN108/2015)

Tomić Rotim, S. (2019): The contemporary technological aspects of Cybersecurity: restrictions and opportunities posed by modern technology, 12th International Scientific and Professional Conference “Crisis Management Days”, Conference Proceedings, Šibenik, 2019.

UNIFE (2019): Vision Paper on Digitalization Digital Trends in the Rail Sector, http://www.unife.org/component/attachments/?task=download&id=984, published: 15 April 2019.