Co-funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ERASMUS+ cooperation partnership

Digital education tools for

SECURITY RISK MANAGEMENT

BEST PRACTICES ON SECURITY RISK MANAGEMENT

INTRODUCTION

During the past years, security has emerged as an important issue for many European countries. The world is grappling with a wide range of challenges, including migration, cyber-attacks, and other emerging difficulties such as the crisis caused by the virus and the ongoing war in Ukraine.

Consequently, it is evident that there is a pressing need not only for high-quality training for young security specialists but also for training that will enable them to better prepare for crises and potentially mitigate numerous threats before they escalate into full-blown crises.

This need prompted the formation of a consortium consisting of seven partner organizations from six countries. The primary objective of this consortium is to develop diverse digital teaching and learning materials focused on security risk management.

ABOUT THE PROJECT

Partners from Latvia, Lithuania, Finland, the Netherlands, Norway and Spain joined their knowledge and expertise and developed ERASMUS+ cooperation partnership project which aims to develop various teaching materials on security risk management.

This project aims to establish a sustainable security specialists' network, which can cooperate on a long term basis. During the project partners developed recommendations for Universities which are preparing security specialists in Europe. Also, the partnership developed comprehensive and up-to-date digital teaching materials and tools, gathered on one web platform which contains the most updated information on security risk management aspects available for all security experts, students and academics.

Find more materials on project website: https://security.turiba.lv/

ABOUT THIS PUBLICATION

This publication, titled "European Best Practices on Security Risk Management," serves as a comprehensive compilation of various subtopics within the realm of security risk management. It is designed to provide readers with valuable reading material that includes articles highlighting best practices, practical case examples, and expert advice.

Within this material, you will find articles covering a range of subtopics, including early-stage security threat identification, security risk aspects associated with public events, the role of artificial intelligence in security risk management, and crisis management.

The target audience for this material includes students who have a keen interest in security risk management, as well as lecturers and professionals working within the field of security.

CONTENT

IMPLEMENTING SECURITY RISK MANAGEMENT FOR AN ORGANIZATION OPERATING AS AN ELECTRICITY GRID MANAGER IN THE CRITICAL INFRASTRUCTURE

Lambert Bambach / Avans University of Applied Science / 2023

ABSTRACT

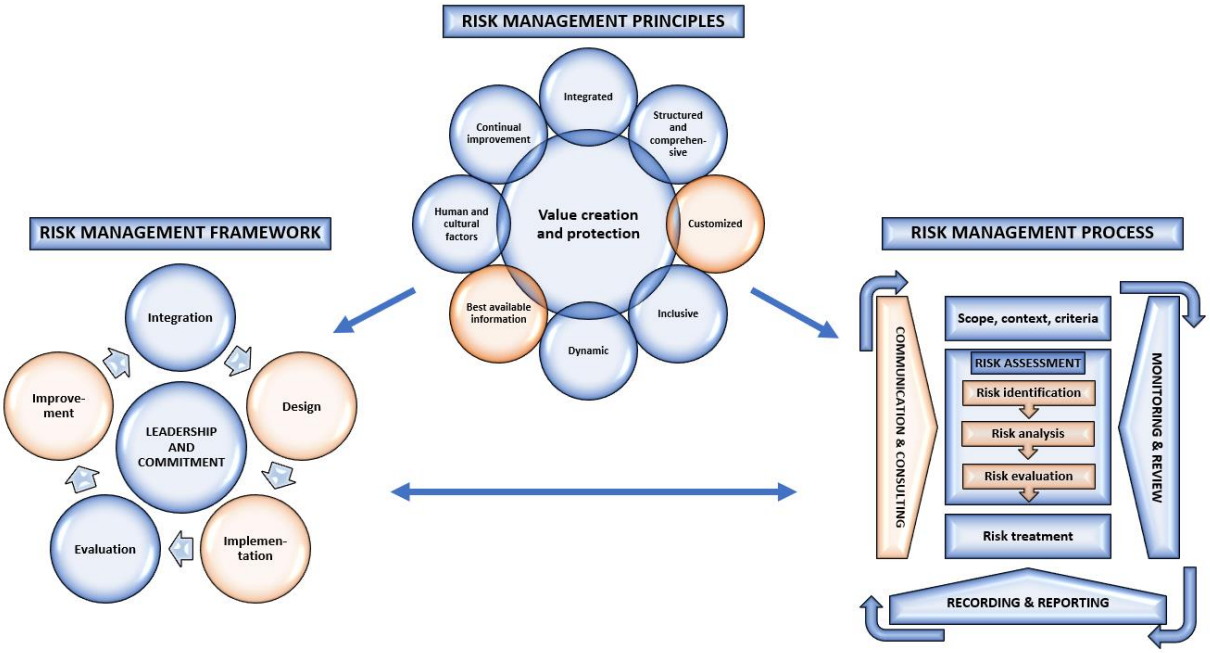
Threats of nation state actors and organized crime are changing the threat landscape of the critical infrastructure in which organizations operate as electricity grid managers. Examples of the threats are hacking, theft, destruction and manipulation of the electricity grid. To deal with these threats, it is important to have an asset protection programme that is up to date. This is achieved by mapping the various assets to be protected in line with the organizations objectives, performing threat and risk analysis in collaboration with government actors at European and National level, competing fellow electricity grid operators at national level and several departments within the organization itself.

Keywords

Objectives of the organization; Different types of assets; Threat and risk analysis; Risk evaluation; Law and regulations; Stakeholders.

Link to ISO 31000

Improvement, design, Implementation, best available information, customized, communication & consulting, risk identification, risk analysis and risk evaluation.



1. Introduction

A junior security employee in the Asset Protection department of an electricity grid manager, will be asked to provide insight into a possible method for renewing the Asset Protection Programme for 40,000 decentralized unmanned assets ranging from low voltage, medium voltage spaces , high-voltage cables and two central locations where large data centers are located.

The interest of the organization is that the asset protection programme must be established in collaboration with internal and external stakeholders to provide protection against threats to assets in the fields of Information Security, Operational Technology and Physical Protection.

With the renewed asset protection programme, a level of security must be realized that, in collaboration with various actors, copes with a changing threat landscape in which State Actors, organized crime and pilferers increasingly pose threats to the realization of the objectives. Also posing a threat to the primary objective of the organization: 'at all times distributing energy across all their grids every single day'.

The organization wonders how the asset protection programme can be achieved.

2. Case

The organization functions as electricity grid manager, responsible for properly distributing energy across all their grids every single day. Through cables and pipes, over three million Dutch households and companies are supplied with electricity. For this, 40,000 decentralized unmanned assets ranging from low voltage, medium voltage rooms, high voltage cables and two central locations where large data centers are located are used. The organization wants its grid to remain among the world's most reliable, and maintain dependability, affordability and accessibility of the grid for their customers.

The security risk manager explains that the asset protection programme should be able to cope with the changing threat landscape so that the goals of the organization can continue to be realized. In this changing threat landscape of terrorism, the likelihood of operating systems getting hacked by Nation State Actors and the stealing of valuable materials by organized crime and pilferers is increasing.

The security manager also knows that the number of assets that need to be protected is not only extensive but also diverse in nature. It concerns both assets that are OT and IT related. In doing so, he has to deal with several stakeholders who play roles and with whom cooperation is required. These actors do not always have the same interests as the organization. It is also not yet clear how the various laws and regulations can best be complied with.

For all these reasons, you are asked to provide insight into a possible method to realize the asset protection program. In doing so, it is important to take into account: a) the purpose of the organization; (c) threats and risk analysis; (d); (e) various stakeholders.

3. Best practices

3.1 Purpose of the organization

The primary objective of the organization, to be able to distribute energy across all their grids at all times every single day, to keep their grid one of the most reliable in the world.

3.2 Different types of assets

The organization has Assets in the decentralized field and centrally. In the decentralized field, the organization has to deal with assets such as control cabinets, transformers. Operational Technology (OT) plays an important role in these assets. Where Operational Technology is characterized by the fact that it is all set up with only one goal: 'It must run as long as possible and with as little downtime as possible. It is therefore equipment that lasts a long time, which usually does not meet the standards that we set today, because it was once built to the standards that applied 30 years ago. In addition, an OT asset cannot protect itself digitally.

Centrally, the organization deals with assets such as office buildings and data centres that are more Information Technology (IT) related. With an IT environment you assume that an information asset must be able to protect itself. You also assume that you need flexibility with it, you are mainly working on it functionally. It must support the business goals and these are all quickly flexible, short lifespan.

That means that you need to look at OT assets differently than IT assets. As a rule, an OT asset can also be considered as an asset that cannot protect itself, so that also means that you must build the measures around it to protect such an asset. However the three fundamental basic principles of information security are: integrity, confidentiality and availability. Periodic downtime is accepted. In operational technology, the valuation of these basic principles is different, namely: availability, integrity and finally confidentiality. Downtime is not accepted.

3.3 Threat and risk analysis

3.3.1 Identification and analysis of risks

The main threats are Nation State Actors, organized crime and pilferers which can lead to compromising the primary objective of the organization by hacking, theft, destruction and manipulation of the electricity grid.

3.3.2 Risk Assessment

In the case of the Nation State Actor it is difficult to mitigate this threat because these actors often have unlimited resources. It is an accepted risk. But the critical infrastructure may not be compromised and has to be available all the time, because many other public services and organizations depend on it. For example, the police expects to always keep their communication systems up and running. If the police are no longer able to communicate in times of crises, then the organization has a problem because this poses a national security problem and the organization does not achieve its primary objective: 'security of supply'. This means at all times distributing energy across all their grids every single day.

In the case of organized crime, the organization needs to take some more security measures. Especially for the OT assets because these assets cannot protect themselves, that also means

that measures must be built around them to protect such assets. By means of camera systems, fences and reinforced access control. For this, the organization is also continuously developing and accessing annually whether the security baseline is still sufficient or not and whether it needs to be adjusted or not? For the pilferer, the standard measures to mitigate this threat is often sufficient. The pilferer is characterized by the fact that the chance of participating in criminal activities increases if the opportunity is there. So if the opportunity is limited, there is a high probability that the pilferer will not continue their activities.

3.4 Laws and regulations

3.4.1. Legislation

In the case of this organization, one of the most important stakeholders is the legislature. The organization is supervised by the National Inspectorate of Digital Infrastructure of the Ministry of Economic Affairs and Climate because the organization is regulated under the NIS 1 and will be regulated in the near future under the NIS 2, as they are part of the vital infrastructure. NIS is the directive on security of network and information systems (NIS Directive) ordered by the European Union Agency for Cybersecurity (ENISA).

3.4. 2. Regulation

In addition, the organization has also certified itself in accordance with ISO 27001 together with ISO 27019.

ISO standardization have helped the physical and information security department to be able to advise objectively, the standardization also helps to speak an universal language internally, for example with management, but also with external factors such as a regulator and it helps in the continuous search for improvements within the organization.

3.5 Stakeholders

The various stakeholders form sources on which the organization relies to map the threat landscape and risk appetite of its own organization and to test whether they are on the right track to gain insights in the threats and to work together to mitigate the threats.

3.5.1 Internal stakeholders

3.5.1.1 Management

Management makes choices as to whether it will actually implement measures. It makes its decisions based on the threat landscape advised to it by the physical and information security department. An ISMS has been set up for this purpose, which falls directly under the Board of Directors. That is the highest body where all the final decisions for the organization are taken. The moment the organization faces an irresponsible risk, the physical and information security department can report that to the Board of Directors, after which resources can be shifted to address the problem to be able to do the right things. The questions are: Are we actually going to implement all the measures and in what period of time are we going to do that? Or perhaps we are not going to adjust the requirements accordingly, so that perhaps something will be weakened? Or perhaps even more effort will be made on measures.

3.5.1.2 Department of physical and information security

The physical and information security departments are working together. In the organization, the departments fall directly under the Board of Directors. For the organization it is actually the only place where security belongs and also the only place where the departments can carry out their independent role, because security is on the one hand requirement settling and on the other hand controlling, but never executive. Very often one sees that in organizations it is placed in an executive department, then the security departments can never be independent in the advises to be given.

In order to be able to be requirement settling, the organization looks at: a) What are we actually going to protect? b) What are we protecting at the moment? c) What are our crown jewels?

An important task here is to help staff members become aware of the fact that the threat landscape has actually changed and that this leads to new measures. It is also about involving them in the changes regarding security. We get new information assets, what does this mean for your work as security measures will also change. That does not mean that you merely have to be technically trained for that, but also that we should put other management measures in place and let staff members know why we do that. In this respect enabling security awareness is important.

3.5.2 External stakeholder

3.5.2.1 Europe

European Network of Transport System Operators of Electricity (ENTSO-E), is the partnership in which all European network operators active in the synchronized network of Europe are represented. The organization is a member of ENTSO-E to exchange knowledge about the changing threat landscape.

3.5.2.2. National Government

To obtain information for the threat and risk analysis, the organization cooperates with the National Cyber Security Center of the Ministry of Justice and Security, the National Coordinator for Counterterrorism and Security of the Ministry of Justice and Security and the General Intelligence and Security Service of the Ministry of the Interior and Kingdom relations. Additionally, it is supervised by the National Digital Infrastructure Inspectorate of the Ministry of Economic Affairs and Climate Policy, which monitors the execution of the imposed tasks.

3.5.2.3 Competing fellow electricity grid operators

The organization works together with 3 network distributors. They share the same interest in protecting the vital infrastructure but are competing organizations as well. They work together to lay down a minimum security baseline that needs to be reviewed periodically, in order to keep in line with the most current threat landscape and to know whether the security measures of the organization itself and the others are in place. From a commercial point of view, it is important to which extent the organization invests in security measures, but also whether your security measures are at least equal or perhaps better than those of the competitors, because the criminal still looks at the weakest link.

References

Cybersecurity And Nation-State Threats: What Businesses Need To Know. Accessed 31.05.2023
Cybersecurity And Nation-State Threats: What Businesses Need To Know (forbes.com)

European association for the cooperation of transmission system operators. Accessed 30.05.2023
Home (entsoe.eu)

European Union Agency for Cybersecurity. Accessed 31.05.2023
https://www.enisa.europa.eu/

How do OT and IT differ? Accessed 31.05.2023
https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html

Identify Your "Crown Jewels". Accessed 30.05.2023
https://staysafeonline.org/cybersecurity-for-business/identify-your-crown-jewels/#:~:text=Crown%20jewels%20are%20the%20data,high%2Dvalue%20target%20for%20cybercriminals.

Information security management system (ISMS). Accessed 30.05.2023
https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS

ISO/IEC 27001. Accessed 31.05.2023
ISO/IEC 27001 - Wikipedia

ISO/IEC 27019. Accessed 30.05.2023
https://en.wikipedia.org/wiki/ISO/IEC_27019

Information Technology. Accessed 31.05.2023
Information technology - Wikipedia

NIS Directive Accessed 31.05.2023
https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Operational Technology. Accessed 31.05.2023
https://en.wikipedia.org/wiki/Operational_technology

COLLABORATIVE RESPONSE DURING GJERDRUM LANDSLIDE IN NORWAY

Ensieh Roud / Nord University / 2023

ABSTRACT

This article presents some successful elements of collaboration during an emergency response to a landslide happened in Gjerdrum, Norway. It will further shed light on the pivotal role of communication and knowledge sharing within organizations, planning versus improvisation, and formal versus informal connections. Effective collaboration networks, characterised by discursive properties such as reciprocity, participatory decision making, and collaborative leadership, are identified as successful element in this incident.

1. Introduction

Countries and communities need to develop adaptation solutions and implement action to respond to the impacts of climate change that are already happening, as well as prepare for future impacts'. These words are from the UN Climate Change Secretariat (UNFCCC, 2021), discussing adaptation to climate change. However, natural disasters are not isolated events, as they are often the result of complex interactions between social and environmental (Boin et al., 2020). To address this multifaceted issue, the article will address the ISO 31000 principles and refer to ASIS handbook Domain Seven.

Collaboration across multiple geographic and organisational boundaries is one of the key part of enhancing risk management and resilience that enable effective response and recovery activities in a natural disaster (Therrien, Beauregard, & Valiquette-L'Heureux, 2015). The evaluation reports of several disasters, such as Hurricane Katrina, the California wildfires, and the flood in Germany in 2021 , indicate that a more organised inter-organisational collaboration would have reduced the destructive effects of these events. The dynamic situation in natural disasters and responding to complex events often require emergency organisations to deviate from established organizational structures to address a novel context and new tasks (Andreassen & Borch, 2020). Responding to natural disasters requires organisations to collaborate because a single organisation may not respond independently due to rapid changes in the environment, a lack of experience, the scope of the task, and insufficient resources (Kapucu & Garayev, 2011). This inter-organizational collaboration can be ensured by the systematic sharing of information possessed by each organization and by combining their goals (Therrien, Beauregard, & Valiquette-L'Heureux, 2015). Therefore, in such collaborative emergency response, several organisations, such as police departments, paramedic services, and rescue agencies, may be involved. In addition, depending on the scale of the emergency, local authorities, government departments, military forces, and various businesses from different nations may also be engaged. Therefore, resilience enhancement in a natural disaster requires an integrated hazard mitigation and resilience plan that includes inter-organisational collaboration among interdependent organisations (Godschalk, 2003).

This article present some best practices of the inter-organizational relationships in the landslide event in the small town of Ask in the Gjerdurm municipality in Norway. Due to its coastline and wide mountain ranges, Norway is highly exposed to changing weather conditions. The report "Climate in Norway 2100", provided by the Norwegian Centre for Climate Services (NCCS, 2017), indicates that gradually increasing temperature, increased precipitation and extreme rainfall, and increased floods in the future climate may cause more quick clay slides in certain areas in Norway (p.34). In addition, some flood and landslide events have been studied to improve risk and crisis management related to natural hazards.

2. Case

The 2020 Gjerdrum landslide occurred in Norway, at Ask village, Gjerdrum's administrative center. This quick clay landslide spanned an area of 300 by 700 meters and caused debris flow to affect an additional 9 hectares. While some individuals were rescued and others evacuated themselves, 10 people lost their lives and several buildings were destroyed, resulting in an estimated economic cost exceeding $100 million (Nikel, 2021). The Joint Rescue Coordination Center (JRCC) report states that during the early phase of the Gjerdrum landslide, the primary challenge was to acquire a comprehensive understanding of its extent and to request appropriate resources (JRCC, 2021). Emergency situations are often characterized by uncertainty and limited information, and incidents occurring during the night or under adverse weather conditions, such as the Gjerdrum landslide at night during the Christmas period, exacerbate the challenge of gaining an overview. The incident necessitated a demanding search and rescue (SAR) operation due to the significant number of people requiring immediate attention, and the subsequent breakdowns in infrastructure, such as water, sewage, roads, and electricity in the area, added to the complexity of the operation (JRCC, 2021).

3. Best practices

The response to Gjerdrum landslide is considered as fairly successful. It could have been ended as a tragedy. Reviewing the evaluation reports and interviewing the involved actors revealed some elements of great collaboration. In Norway, after the terrorist attack in 2011, several reforms have happened and collaboration was added to the crisis management principles. Since then organization have gone through exercises together to enhance interorganizational collaboration. The municipality in Gjerdrum planned an exercises based on landslide scenario but due to the outbreak of Covid, unfortunately they could not execute it. And if they have done that, the interorganizational challenges that they faced would have been minimized. This revealed the importance of joint exercises and how it can positively influences on ***information dissemination, communication, clarity of roles, establishing common operating terms and allocation of resources***.

During the incidents, fire brigades invited their upper level, Norwegian Directorate for Civil Protection (DSB), to listen to their meeting at operating center. This is the first time they have done it and it is identified as an efficient way of passing the information to decision maker at higher level without creating any confusion. However, DSB believes this should be

an invite from lower level and not a command from them. This example highlights the importance of flexibility and trust among involved organization and across levels.

Moreover, having a liaison who has decision making authority was identified a facilitator element in collaborative emergency response. This might save huge amount of time during crisis.

The crisis management structure of Norway is found to function very well during the landslide because police was the leader of operation and there were almost no conflict when it comes to decision making and clarity of roles. There were two operation centers - side by side during the days of a rescue operation, and one of which continued its operation for two months after the first one ended. One operation center was focused on the rescue operation, the other on all the other tasks that also had to be taken care of, but which did not fall directly under the rescue operation. The tasks that were solved from the second operation center also very important tasks and had an impact on life and health. There were, for example, farms with several hundred animals within the evacuated zone, there was a need for measures to improve infrastructure such as water and roads and there was a need to retrieve important assets from evacuated buildings. This has been identified as an innovative approach to handle crisis and prevent overloading of information in one center and categorize the tasks during operation to facilitate collaboration.

This case revealed how critical is to have personal and informal contact during crisis. For example, municipality explained that due to covid there faced so many obstacles and all the roads were destroyed, therefore they had problem with transferring people to a safe place. It was almost impossible to get public transport in order, so the person in charge had some contact in private transport companies and call him for assistance.

All above examples are in line with the findings from round table that emphasis how significant are the soft skills such as communication, continuous interaction, cooperation and making innovative decisions.

References

ASIS International Board Certification Handbook. Accessed 20.04.2023 https://www.asisonline.org/globalassets/certification/documents/certification-handbook_final.pdf

Andreassen, N., Borch, O. J., & Sydnes, A. K. (2020). Information sharing and emergency response coordination. *Safety Science*, *130*, 104895.

Boin, A., Ekengren, M., & Rhinard, M. (2020). Hiding in plain sight: Conceptualizing the creeping crisis. *Risk, Hazards & Crisis in Public Policy*, *11*(2), 116-138.

Climate in Norway 2100 (2017). Accessed 25.05.2023 https://www.miljodirektoratet.no/globalassets/publikasjoner/M741/M741.pdf

Godschalk, D. R. (2003). Urban hazard mitigation: Creating resilient cities. *Natural hazards review*, *4*(3), 136-143.

JRCC (2021). Evaluation report of the rescue operation and the emergency management under quick clay landslide at Gjerdrum. Accessed 25.05.2023. https://www.regjeringen.no/contentassets/52d43dc95b5b44fd80293c2b3515713b/rapport-gjerdrum-hovedredningssentralen-03-06-2021-digital-1.pdf

Kapucu, N., & Garayev, V. (2011). Collaborative decision-making in emergency and disaster management. *International Journal of Public Administration*, *34*(6), 366-375.

Nikel, D. (2021). Norway Landslide Insurance Bill Tops $100 Million [Press release]. Retrieved from https://www.forbes.com/sites/davidnikel/2021/01/08/norway-landslide-insurance-bill-tops-100-million/

Therrien, M. C., Beauregard, S., & Valiquette-L'Heureux, A. (2015). Iterative factors favoring collaboration for interorganizational resilience: The case of the greater Montréal transportation infrastructure. *International Journal of Disaster Risk Science*, *6*, 75-86.

United nations climate change annual report (2021). Accessed 25.05.2023 https://unfccc.int/sites/default/files/resource/UNFCCC_Annual_Report_2021.pdf

ARTIFICIAL INTELLIGENCE AND BIOMETRIC FACIAL IDENTIFICATION IN THE SECURITY FIELD

Javier Dorado / School of Prevention and Integral Safety and security / 2023

ABSTRACT

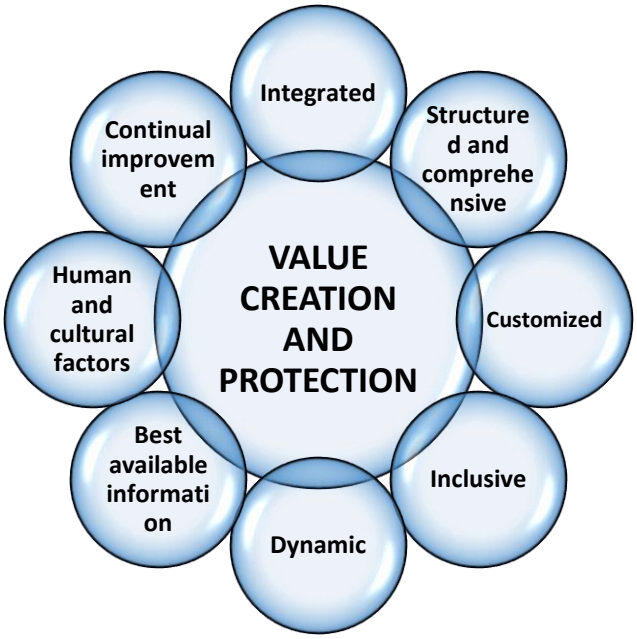
The use of biometric facial identification technologies in public and private institutions for security purposes is a reality. Examples are detection and prevention in access control, or the identification of suspects or wanted persons. Nonetheless, the use of these techniques that operate with artificial intelligence and automated decisions presents several problems, not only in terms of regulatory legitimacy from the point of view of the protection of fundamental rights, but also from an operational perspective. In this sense, biometric identification must be approached from a dual analysis: the technical-operational and the legal-regulatory, as both dimensions can entail risks for the organisation and the physical integrity of individuals.

Keywords

Biometric identification, Artificial Intelligence, automated decisions, false positives, false negatives, fundamental rights, sanctions, risk analysis and assessment.

Link to ISO 31000

ISO 31000 processes: Risk assessment, risk treatment, monitoring, and review.



1. Introduction

A company entrusts you with the task of analysing the risks involved in implementing a biometric identification camera for access control purposes on its premises. However, they are not only concerned about the possible failures that this technology could generate, which

could endanger private security purposes, but also about the possible administrative sanctions that this could entail within the framework of data protection.

With regard to technical-operational issues, the company needs to detect a number of persons who have previously been convicted of theft or burglary. For these persons, the company has biometric facial identification templates. However, the company has concerns about the possibility of incidents (false positives or false negatives) with this technology.

In terms of regulatory issues, the company is unclear to what extent and under what conditions it can use this technology without incurring a data protection infringement.

2. Case

The company in question is a jewelry shop and, as mentioned above. It has a database with the facial templates of people (15 in total) who have been previously convicted by the criminal courts in the last three years, specifically for theft or burglary in the establishments of this business.

The manager of the jewelry shop explains that the biometric identification camera, if positive, will inform the state security forces and bodies, so that they can go and arrest those identified, as they have a restraining order against the establishments, issued by the criminal jurisdiction.

However, the manager knows that this type of technology sometimes fails, either because of false positives (mistaken identifications) or false negatives (failure to detect the reported person in the database). In the first case, the company does not want to have problems with customers, as a false positive could lead to a complicated situation, as the system is designed to alert the police, when, in this case, the person identified has no criminal record. In the second case, on the contrary, if the identification fails, there would be a possible risk to the physical integrity of the employees, and/or to the company's assets, depending on whether the individuals in question are punished for robbery with violence or theft, respectively.

Furthermore, it is not clear to the company whether they can use this type of technology legally or whether there are risks of sanctions, which could lead to financial problems for the company.

For all these reasons, you are entrusted with the task of issuing a report with a dual perspective: a) a technical-operational report on the risks and advantages that the use of biometric identification cameras for access control purposes may entail; and b) a regulatory report on the conditions under which this technology can be used without violating data protection regulations.

3. Best practices

3.1 Technical-operational risks: a) False positives; b) False negatives

3.1.1 Identification and analysis of risks

The main risks to be reported to the company are indeed the possibility of occurrences of the technology such as false positives or false negatives.

3.1.2 Risk assessment

In the first case, it is important that the company providing this technology informs us of the probability of its software generating this type of failure. Once this point has been clarified, and considering that the bug cannot be neutralised, a two-step protocol should be put in place, in order to ensure that no one who does not meet the requirements is stopped. In this regard, it is recommended that a switchboard should filter out suspicious positives, i.e., those where there is doubt as to the identification of suspects.

In the case of false negatives, it is clear that it is difficult to implement an ex-ante access control process, as it is precisely this that has failed. Therefore, again, human verification is needed. If artificial intelligence fails, human intelligence can make up for it. This could be done by training employees, so that they can appeal to the competent public authority when they suspect that a customer's behaviour is inappropriate and may pose a risk to the physical integrity of employees or the company's assets.

3.2 Regulatory risks: GDPR sanctions

3.2.1 Identification and analysis of risks

On the legal-regulatory level, the company's assignment presents even more problems. The first thing we need to make clear to the company is that Art. 9 GDPR establishes a prohibitive rule regarding the use of "biometric data intended to uniquely identify a natural person". This prohibitive rule is accompanied by a series of assumptions that legitimise the use of personal data through these technologies. These assumptions include a) explicit consent; b) vital interests of the data subject or another natural person; c) exercise of legal actions; d) essential public interest.

3.2.2 Risk assessment

Regarding consent, it can hardly be given, in the terms of the **GDPR** (art. 7), in the context of the establishment. We cannot ask for explicit, specific consent, for the purposes of processing, from every single customer entering the establishment. As for the essential public interest, we must rule it out, as we are in the field of private security.

On the other hand, the other two enabling grounds (vital interests and legal action) can lift the ban on the processing of biometric data for access control purposes.

However, considering the millions of administrative penalties that would result from unlawful use of such data without respecting the principle of lawfulness (Art. 83.5 **GDPR**: administrative fines of up to EUR 20 000 000 or, in the case of a company, an amount equivalent to up to 4% of the total annual global turnover of the previous financial year), we recommend that a consultation with the national data protection agency be carried out. In the meantime, we recommend that the company does not make use of these technologies,

as the enabling grounds that may legitimise the use of these technologies may not be sufficient to make a fully lawful use of them.

References

ISO 31000 Risk management. In: ManagementMania.com [online]. Wilmington (DE) 2011-2023, 11/11/2016 [cit. 05/30/2023]. Available at: https://managementmania.com/en/iso-31000-risk-management

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

COLLABORATION IN EVENT SAFETY AND SECURITY RISK PREVENTION: CASE RUISROCK

Anja Aatsinki & Hanna Iisakkila Rojas / Laurea University of Applied Sciences / 2023

ABSTRACT

The purpose of this article is to demonstrate the importance and process of collaboration in event safety and security. The best practice demonstrates the model used by South-West Finland´s authorities when collaborating with event organizers. The process follows ISO 31000:2018 risk management process. The representatives of Finnish police and South-West Finland rescue authority have been consulted and interviewed for this article.

1. Introduction

Event organizer is responsible for preventing and managing the risks and collaborating with different actors and authorities. Event safety and security is heavily legislated in Finland and for that reason planning the event safety and security in time is essential. The most essential legislation in Finland includes Assembly Act, Rescue Act and Land Use and Building Act. In every event the organizer has to prevent and manage the risks of the particular event. The size and the risk profile affect the demands but basically all events where the risks are considered bigger the emergency plan is obligatory.

This article concentrates in event risk prevention in summer festival Ruisrock held in Finland. Ruisrock is one of oldest festivals in Finland. It is held in Ruissalo island that is part of city of Turku (Ruisrock 2022a). Ruissalo is a unique site for events because its nature is heavily protected and the location on the island creates its own challenges for risk management. The island is connected to the mainland via one bridge. Ruisrock is a three-day festival and approximately 100000 people visit the event during the weekend (Ruisrock 2022b). In this article the collaboration model between organizer and different authorities is presented. The process adapts to the ISO 31000:2018 standard risk management process.

2. Case

Planning annual big events like Ruisrock is usually continuous and planning the next year event starts right after the previous event is finished. Finnish Assembly Act (530/1999) regulates that event organizer needs to notify police at least five days in advance of the event but in case of the bigger events collaboration, planning and consulting is practically constant all year round. Recue Act (379/2011) in Finland requires that all public events that have 200 or more persons present at the same time, needs to draw up an emergency plan. Responsibility lies with the organizer.

Organizing the event also requires collaboration with other stakeholders like the performing artists with their organizations and different companies that offer services at the event. Planning is done in close collaboration with organizers event security provider, police, rescue services and health service provider. In this article the best practice presented is the

rewarded collaboration model with South-West Finland authorities (Varsinais-Suomen pelastuslaitos 2019).

In this article this model is presented via ISO 31000:2018 Risk-management framework (Figure 1).

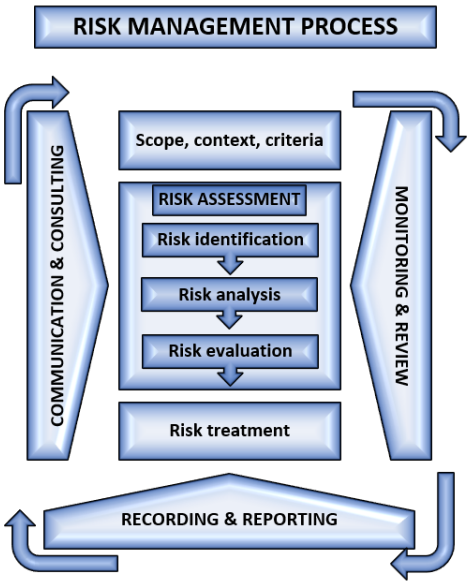


Figure 1. Risk management process (adapted from ISO 31000:2018)

3. Best practice

Communication and consultation

For safe and secure event close and immediate multi-authority cooperation is essential, as well as continuous interaction with the event organizer. Due to cooperation with the authorities, expertise is available in a wide area of event safety, which is combined with up-to-date information with the organizer. Safety and security planning is started early enough by the event organizer. It also requires and assures that concrete preparations for the event are made in time. In big events it's usually necessary for the event organizer to consult experts in safety and security, rather than doing everything by themselves. It's important to be able to recognize the areas where own expertise isn't sufficient. The authorities will advise on the basics, but the responsibility lies on the organizer. Beside the supervision, authorities also provide information and guidance. Regardless of the collaboration, the juridical responsibility lays on the event organizer. Therefore, the organizer shall submit the rescue plan of the event to the regional rescue authorities no later than 14 days before the start of the event (Rescue Act 379/2011).

Functional safety and security measurements are fundamental for successful event, so therefore it's vital that organizer is motivated and understanding towards safety and security culture, even though it would mean investing more money or resources.

Scope, context, criteria

When the group for Ruisrock´s risk assessment is formed, the following aspects are considered to find enough expertise to cover the specific risks and features:

- The specific characteristics of the area (water, location on an island, heavy traffic, elevation differences, urban environment, public transport, etc.)
- Number of people participating in the event (environmental maintenance, security stewarding, guidance, services, exits, etc.)
- Nature of the event (whether there are topics or performers that stir up the mind, people with disabilities, children, the elderly)
- Whether there are any special programs or equipment at the event that require special safety planning and expertise, the availability of the organizer/ resources of public authorities.

According to the Rescue Act (379/2011) the dangers and risks concerning the event need to be detailed and assessed. All measures in the emergency plan must be based on this risk assessment. The event organizer must take care that all needed legislation is taken into consideration.

Risk assessment

First in the risk assessment process the overall situational picture is drawn up. It includes the structures, program, environmental management and placement, human resources, and all other essential factors. Identification of the risks is based on the specific features of the event and the lessons learned from a previous years. Analysis of the risks is done by recognizing causes and consequences for each risk. After this the analysis is used to evaluate the magnitude of risks. All key authorities affecting event safety must participate in risk assessment in the form of a joint meeting. The organizer presents the factors affecting the situational picture to the authorities, and together the severity of risks and the level of preparedness for them are considered. Organizer makes a preliminary emergency plan that can be discussed with authorities.

Recognized causes and consequences are used for creating event specific treatment measures. Event organizer needs to have a reliable criterion and demonstrate that their risk management measures are risk-orientated and compliant with the legislation. Authorities evaluate if the measures presented in the rescue plan are sufficient and they can ask event organizer to enhance the event safety and security plan.

In addition, regarding the overall security of society, the authorities must then carry out an assessment of the risks posed by the event and how the authorities should prepare for identified risks that are not directly the responsibility of the event organizer. This preparedness may include increasing authorities´ resources, reserving additional spaces, ensuring the internal flow of information, and providing information etc. In addition to the event area, the mega-scale event has a wider impact on society, and the risk assessment generated by its impact is the responsibility of the authorities.

Risk treatment

The risk treatment is combination of structural, technical and operational measures that are based on risk assessment. Preventing crimes and other deliberate harmful acts is largely directed by legislation. Different laws regulate the powers of different actors (security stewards, security guards, police). For example, the security checks and searches on persons, removal from the area and apprehension are regulated by law. In bigger events like Ruisrock besides rescue plan multiple other plans must be drawn up and they are part of the risk treatment.

Monitoring and review

Monitoring in Ruisrock is done with an official inspection just before the start of the event. During the event onsite monitoring is done with both authorities and security service provider. Security service and health service providers are also obliged to keep a logbook of the service events that help organizer to develop and plan the event for the future. After the event debriefing session is held with the organizer. Information is also obtained from the media and other public sources. All this information and sources are helping to review and develop the Ruisrock festival.

The authorities always go through the most significant events together afterwards. Often, debriefing is also carried out together with the organizer. If criminal investigation measures must be carried out, the aim is to bring the responsible persons to criminal responsibility for their negligence.

Recording and reporting

In all phases authorities take notes, so that after a year, the shortcomings identified are considered at the planning stage. During the process there are multiple mandatory documents that must be made. These include for example:

- Fire inspection minutes
- Event logs
- Meeting minutes

Dynamic and continuously improving emergency plan serves also as a recording and reporting tool.

References

Finland Assembly Act 530/1999. Accessed 10.2.2023. https://www.finlex.fi/fi/laki/kaannokset/1999/en19990530_20020824.pdf

Finland Rescue Act 379/2011. Accessed 10.2.2023. https://www.finlex.fi/en/laki/kaannokset/2011/en20110379.pdf

Ruisrock. 2022a. Accecced 3.12.2022. https://ruisrock.fi/en/info/

Ruisrock. 2022b. Accessed 3.12.2022. https://ruisrock.fi/en/sold-out-ruisrock-makes-a-stellar-comeback-attracting-a-total-of-105-000-visitors/

Varsinais-Suomen pelastuslaitos 2019. Accessed 10.2.2022. https://www.vspelastus.fi/uutinen/2019-10-02_valtakunnallinen-turvallisuuspalkinto-varsinais-suomeen

HOW TO DEVELOP AND IMPLEMENT A SECURITY CULTURE IN YOUR ORGANIZATION

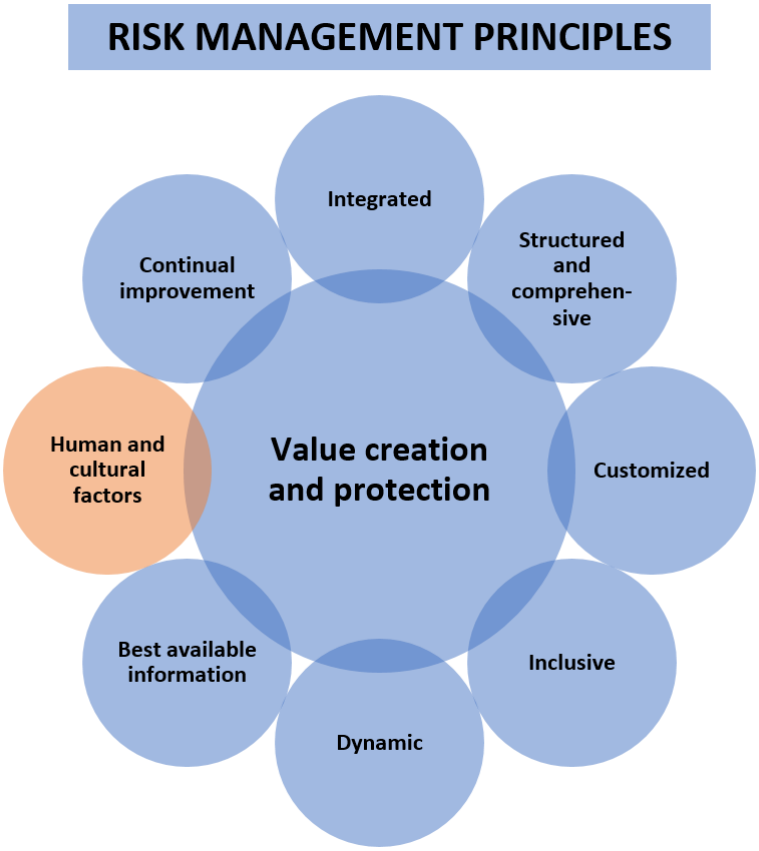
Kārlis Apalups / Turiba University / 2023

ABSTRACT

Development of security culture in an organization can be a challenge, but there are some steps for success that should be considered once a decision is made to develop a culture of security. Such decision should come from the top management as without such support no significant development of organizational culture can take place. Likewise it's important to establish clear and consistent security policies for them to be followed as a standard throughout the organization. Once support and policies are set in place, the next step should be to train your organization on the policies and best practices for security. For it to be an up-to-date culture, there also needs to be a monitoring and measurement of security culture and this can also be achieved by setting in place specific metrics to measure the success of security culture and to get an ROI.

Link to ISO 31000

ISO 31000 Risk management principles: Human and culture factors.



1. Introduction

Security culture is the set of ideas, customs and social behaviors that influence the security of an organization. It is the most important element in an organization's security strategy, as it affects how employees perceive and respond to security threats and incidents. A strong security culture can reduce risk and save money by preventing data breaches, complying with regulations, and protecting the reputation of the organization.

However, developing and implementing a security culture is not a simple task. It requires a strategic, long-term approach that involves top management support, clear and consistent security policies, effective awareness and training programs, and continuous measurement and improvement. In this article, we will discuss some best practices for creating and maintaining a security culture in your organization. For the purpose of this article, we will be studying the case of “Latvijas finieris” which works in an international environment and has security as one of its core values.

2. Case

Latvijas Finieris is the leading plywood and its products' manufacturer in Baltic States and Finland. The company is also active in forest management, logging and the production of synthetic resins and phenol films.

In 2014 “Latvijas finieris” had a huge fire in one of Rīga-based factories. After this event, the holding company decided to implement security culture and develop it. As part of its efforts was the creation of Safety management service (SMS) that managed security risks in such areas as – fire safety, occupational health and work safety, environmental protection and physical security. Before the fires there was a high amount of work related accidents which led to losses of working power, insurance costs and a decrease in feelings of safety among workers.

The efforts of SMS allowed to develop such a security culture that drastically lowered work related incidents, increase the ROI from security and safety investment and increase the overall organization culture.

3. Best practices

3.1. Get top management support. Obtaining the support of senior leaders is the first step in building a security culture. It is important that they communicate the significance and value of security and safety to all employees, allocate sufficient resources and budget for security initiatives, and hold themselves and others accountable for security performance. This support can also help create a positive tone at the top, where security is seen as a strategic priority and a shared responsibility, not just another budget expense position.

3.2. Establish clear and consistent security policies. Security policy is like a standard for the organization. It’s the rules that define the expected behavior and actions of employees regarding security. Policy should cover topics such as access control, password management, data protection, incident response, and compliance requirements. Security policies should be aligned with the organization's goals and values, as well as with the relevant laws and

regulations. They should also be written in simple and understandable language, communicated to all employees, and enforced consistently.

3.3. Provide effective awareness and training programs. Awareness and training programs are essential for educating employees about the security risks they face, the policies they need to follow, and the best practices they need to adopt. They should be tailored to the specific needs and roles of different groups of employees, such as IT staff, managers, or end users. Awareness and training programs should be delivered regularly and updated frequently to keep up with the changing threat landscape.

3.4. Measure and improve security culture. Security culture is not a static state, but a dynamic process that needs to be monitored and evaluated over time (Just like risk management). There are various tools and methods that can be used to measure security culture, such as questionnaires, surveys, interviews, or audits. These can help to assess the current state of security culture, identify strengths and weaknesses, and track progress and changes. Based on the results of these measurements, security culture can be improved by addressing gaps, reinforcing positive behaviors, rewarding good performance, or correcting bad habits.

3.5. **Get an ROI of security culture.** Security culture is not only a cost center, but also a value driver for an organization. By developing and implementing a security culture, an organization can achieve various benefits such as:

- Reducing the likelihood and impact of security incidents
- Enhancing customer trust and loyalty
- Improving employee engagement and retention
- Increasing operational efficiency and productivity
- Complying with legal and regulatory obligations
- Gaining competitive advantage in the market

To quantify these benefits, an organization can use metrics such as:
- Number of security incidents prevented or detected
- Amount of money saved or recovered from security incidents
- Customer satisfaction or retention rate
- Employee satisfaction or turnover rate
- Time or resources saved or optimized by security measures
- Compliance status or audit results
- Market share or revenue growth

By measuring these metrics before and after implementing a security culture program, an organization can calculate the return on investment (ROI) of its security culture efforts.

By following these best practices, an organization can build and maintain a strong security culture.

References

The Importance Of A Strong Security Culture And How To Build One - Forbes https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/

Building a Culture of Security - ISACA https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security

Developing a cyber security culture: Current practices and future directions - ScienceDirect https://www.sciencedirect.com/science/article/pii/S016740482100211X

https://www.finieris.com/en/home

https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks

HYBRID THREATS AND SECURITY RISK MANAGEMENT

Prof. dr. Raimundas Kalesnykas / Kazimieras Simonavičius University/ 2023

ABSTRACT

Hybrid threats is one of the most complex challenges in the security management system faced by the European Union (EU) and its Member States, public sector organizations and business companies. States and their organizations are looking for innovative security solutions in order to quickly respond and be resilient against such threats as cyber-attacks, irregular migration, cross-border crime, disinformation.

The case of instrumentalization of migrants organized by the Belarusian authorities at the EU's Eastern borders is presented in this article. It illustrates that organizations (state border security, private companies implementing security solutions) must establish a security risk management system based on the response mechanism from hybrid threats.

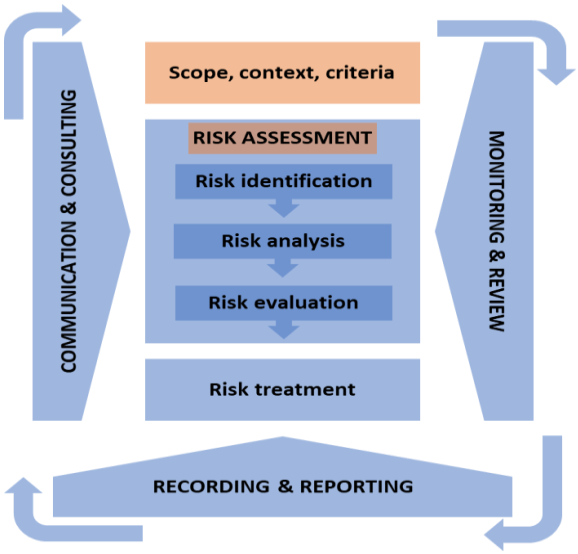
The risk management process requires an understanding of external and internal factors in order to assess risk in the field of border protection. Managing risks that pose a threat to border security includes risk identification, analysis and evaluation.

Keywords

Hybrid attack, instrumentalization of migrants, border security, risk identification and analysis

Link to ISO 31000: 2018

Establishing the context, defining the external and internal parameters for managing risk, risk assessment, legal and regulatory requirements



1. Introduction

In recent years, the topic of *Hybrid Threats* has dominated the security landscape in the EU. The state and institutions that take care of its security looking for new security tools and technologies to address vulnerabilities across multiple domains. The concept of *Hybrid Threats* has been increasingly transformed from military context to public security realm.

The term *Hybrid Thre*at refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. *Hybrid Threats* are characterized as: (a) coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means (e.g. hybrid attacks using people, technologies, false information), (b) activities that exploit the thresholds of detection and attribution, as well as the different interfaces (internal-external security, local-state, and national-international).

Countering hybrid threats relates to national security and the maintenance of law and order. Efforts to respond to hybrid threats have to be underpinned by a capacity to detect early malicious hybrid activities, internal and external factors, and to understand the possible links between often seemingly unconnected events.

This first changed with the hybrid aggression by Belarus in mid-2021 through the creation of an artificial migration route to EU Eastern countries (Latvia, Lithuania, Poland) - which brought thousands of refugees at the EU's doorsteps, and EU/national security and border management challenges for years to come[1]. These may include a rise in trafficking in human beings, especially women and children, rise of smuggling in weapons and other illegal goods, as well as terrorism and radicalization.

When managing security risk raised from hybrid threats, organizations (state or non-state) should establish external and internal environment in which the organization seeks to achieve its security objectives. In this context, it is important to understand and determine external and internal parameters, which should be taken into account when managing risk: (a) social and cultural, political, legal, regulatory, financial, technological and economic environment, whether international, national, regional or local; (b) key drivers and trends having impact on the security objectives of the organization; (c) relationships with stakeholders; (d) governance, organizational structure, roles and accountabilities; (e) policies and the strategies that are in place to achieve security goals; (f) capabilities and knowledge (e.g. budget, people, processes, information systems and technologies), etc.

2. Case

From June 2021 onwards, the number of migrants seeking to cross from Belarus into the territory of neighbouring Latvia, Lithuania and Poland in an irregular manner increased dramatically. The Belarusian authorities contributed by organizing the transfer of refugees

[1] Irregular border crossings to the EU increased significantly in 2022, as FRONTEX – the EU's border agency – noted a rise of 64% from the previous year estimating "around 330 000 irregular border crossings were detected at EU's external border, according to preliminary calculations. Last year, EU and Schengen associated countries faced unprecedented challenges at their external borders. These have ranged from the state-organized migration perpetrated by Belarus from 2021 onward to Russia's invasion of Ukraine in February 2022.

and immigrants from Iraq, Afghanistan, and other countries of the Middle East and Africa across the Belarusian-Lithuanian and Belarusian-Polish-Latvian border.

According to statistics, the number of unauthorized attempts to enter Poland stood at 3,500 in August, 7,700 in September and 17,300 in October 2021, and Polish border services recorded approximately 2 thousand attempts to cross the Polish-Belarusian border every month illegally (Statista, 2023).

In 2021, the number of people crossing the Lithuania-Belarus border increased more than thirtyfold compared to the previous year. Between 1 January 2021 and 31 January 2022, 4 150 irregular migrants (including 2 891 persons in July 2021 alone) were de facto detained in Lithuania (State Data, 2023). According to the Lithuanian Border Guard Service, 20,679 migrants were prevented from entering Lithuania between 3 August 2021 and 1 July 2023 (Lithuanian State Border Guard Service, 2023).

In Latvia, the number of persons detained for irregular border crossing was almost 15 times higher in 2021 (446 attempts) compared to 2020 (30 attempts), 10,394 instances of border-crossing deterrence (i.e. push-backs) were recorded from 2021 until 20 July 2023 (Latvia State Border Guard, 2023).

The majority of migrants were citizens from Middle Eastern and African countries (Iraq (Kurds and Yazidis, Iraqi Arabs) Syria, Iran, Afghanistan, Congo, Cameroon, Sri Lanka).

The Belarus–European Union border crisis was recognized as a “hybrid attacks” by the Belarusian authorities resulting in increased pressures relating to migration and asylum at the Belarus border with Latvia, Lithuania and Poland (CoE Parliamentary Assembly Resolution 2404 (2021). The migrant crisis was triggered by the severe deterioration in Belarus–EU relations, following the 2020 Belarusian presidential election, the 2020–2021 Belarusian protests, the Ryanair Flight 4978 incident and subsequent sanctions on Belarus. The “hybrid attacks” began around July 7 2021, when Belarus's President threatened to "flood" the EU with "drugs and migrants". Those who arrived in Belarus were then given instructions about how and where to trespass the EU border, and what to tell the border guards on the other side of the border.

Poland, Lithuania, and Latvia have described the migrant crisis as a “hybrid attack”, using migrants as weapons and calling the migrant crisis an incident of human trafficking of migrants, waged by Belarus against the EU. In the EU agenda, this phenomenon was named as “the instrumentalization of migration” - capacity to control irregular migratory flows (Rashe, 2022), and response mechanism was initiated by 3 EU Eastern countries in order to establish risk management system for external border security. Migration is increasingly framed as a security issue because immigrants are presumed to bring risks of terrorism, human trafficking, cross-border crime and illegal immigration (Dekkers et al., 2016). This situation indicates that contemporary security challenges are highly complex and inter-related, requiring more cross-sectoral, transdisciplinary and cross-country cooperation in all risk management phases both at the EU and Member States levels.

3. Best practices on EU external – Eastern borders' security management

3.1. Risk Analysis and Controls

External border security is affected by phenomena such as geopolitics, migration, cross-border crime, terrorism, and hybrid threats that are fluid and multidimensional in nature, thus requiring a flexible approach to their understanding, analysis and management.

Border Security Agencies within EU Member States are used Common Integrated Risk Analysis Model (CIRAM)[2], which focus on the security threat dimension. The analysis of different risk categories provides a comprehensive picture of challenges and threats that jeopardize the security and functioning of the EU's external borders. Risks are grouped into three broad categories: irregular migration (clandestine entry, document fraud), , secondary movements and returns, and cross-border crime (smuggling of illicit drugs, firearms smuggling, detection of stolen vehicles and vehicle parts, tobacco smuggling, trafficking in human beings).

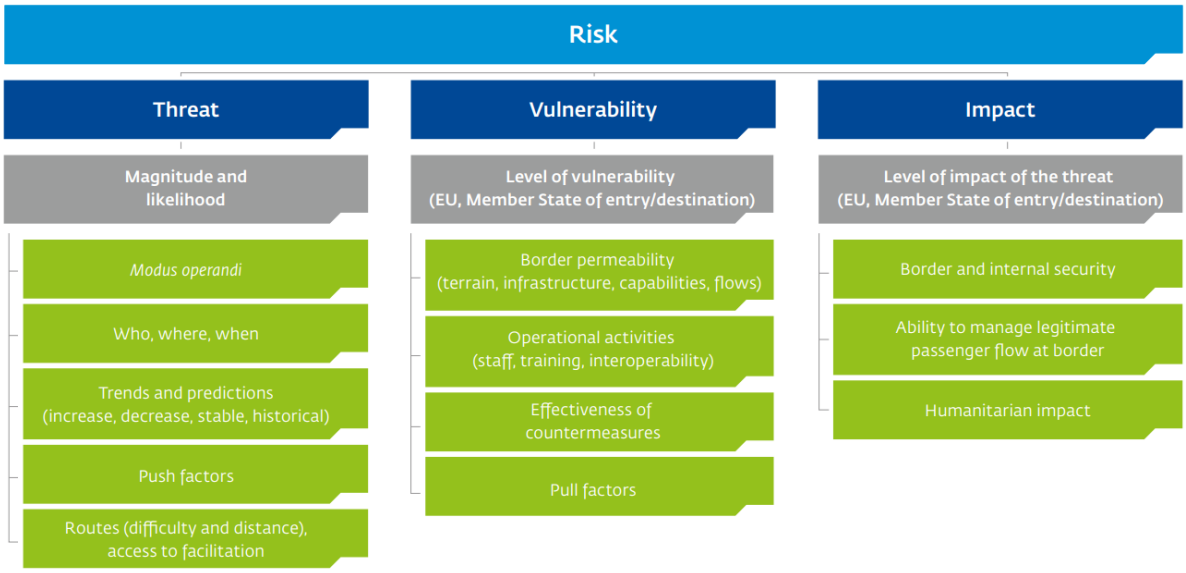
Security Risk Management is the ongoing process of identifying these border security risks and implementing plans to address them. *Risk Analysis* refers to the systematic examination of components of risks to inform decision-making. For the management of the security of external borders, *risk* is defined as the magnitude and likelihood of a threat occurring at the external borders, given the measures in place at the national borders and within the EU, which will affect the EU internal security and national security of Member States.

Risk in the context of the management of the security of external borders can be viewed as having 3 components: (1) the threat that will be assessed in terms of magnitude and likelihood; (2) the vulnerability to the threat – in other words the level and efficiency of response to the threat; and (3) the impacts – should the threat occur on the EU internal and/or Member States' national security, on the security of the external borders, as well as the bearing on the efficient management of bona fide border crossing.

Risks are identified and assessed, in view of their level of threat, vulnerability and impact, and then communicated to the decision-makers. While the analysts are responsible to identify and assess the threat, decision-makers are responsible, within the remit of their decision-making capacities, to manage the risks. Risk analysis implies a reference period – a day, a week, a month or a year – consistent with the level of decision-making it is to inform.

[2] Common Integrated Risk Analysis Model (CIRAM) developed by FRONTEX, the European Border and Coast Guard Agency. The purpose of the CIRAM is to establish a clear and transparent methodology for risk analysis in order to facilitate efficient information exchange and cooperation in the field of border security. See: Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.1 (2021), FRONTEX - European Border and Coast Guard Agency, https://prd.frontex.europa.eu/document/common-integrated-risk-analysis-model-2-1/

Scheme for the Risk Analysis using CIRAM tool[3]



Example of Controls. Risk analysts of national border security agencies communicate risks to the Management Board, so that it can take informed decisions about annual budget allocation among a variety of risks. Risk analysts at border crossing point (BCP) level communicate operational risks to the head of the BCP, so that he or she can take informed decisions when allocating staff for controls and surveillance. Risk analysts should state that the threat of illegal border-crossing between BCP X and BCP Y is very likely, given evidence from the past and intelligence currently available, whereas it is unlikely between BCP Y and BCP Z. This information enables decision-makers to allocate resources as well as to the area between BCP X and BCP Y as a priority.

National integrated border surveillance systems driven by risk analysis should have a stable capacity (organizational, administrative and technical) and in a continuous state of alert. This is necessary to prevent and detect unauthorized border crossings, to apprehend persons who have crossed the border illegally and to ensure that such persons are subject to coherent and comprehensive referral procedures (i.e. screening procedures) that respect their fundamental rights, to intercept transportation means, such as vessels, used for illegal border crossing, to counter cross-border crime, such as smuggling, trafficking in human beings and terrorism, as well as to respond to threats of a hybrid nature.

3.2. Response to Hybrid Threats

3.2.1. Operational support by EU agencies

In the peak of irregular migration influx (July 2021), Lithuanian Government requested support from specialized EU agencies – FRONTEX (European Border and Coast Guard Agency) and EUAA (EU Agency for Asylum). FRONTEX and EUAA in dealing with irregular migrants

[3] Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.0 (2013), FRONTEX - European Border and Coast Guard Agency, https://frontex.europa.eu/what-we-do/monitoring-and-risk-analysis/ciram/

related problems is aimed at preventing the flow of irregular migrants through Lithuania to Western EU countries.

The FRONTEX quickly launched a Rapid Border Intervention in order to bring immediate assistance to an EU Member State that is under urgent and exceptional pressure at its external border, especially related to large numbers of non-EU nationals trying to enter its territory illegally. During the Rapid Border Intervention, the FRONTEX deployed about 120 officers, 36 patrol cars and 2 helicopters to conduct border surveillance and control activities in support of Lithuanian State Border Guard Service (SGBS). FRONTEX officers also assisted in data gathering on irregular border crossings and exchange of operational information.

The EUAA has been providing operational support and deployed 73 personnel working in the areas of registration and processing of asylum applications – including by conducting interviews and drafting opinions – and enhancing the capacity to manage the reception of applicants. Also, Lithuanian State Border Guard Service (SBGS) received support to enhance management of first line reception in particular on site management, communication, information provision and vulnerability, as well as assisting in expanding reception capacities.

3.2.2. Physical Barrier

By implementing the Law on Installation of a Physical Barrier (2021), The Lithuanian Government approved the installation of a physical barrier in the end of August in 2021, after the Belarusian regime launched a hybrid attack against Lithuania, resulting in an influx of illegal migrants into the country. The physical barrier is being installed in accordance with the requirements of the State Border Guard Service (SBGS) – a concertina prism was installed on the national border, and fence segments topped with concertina spiral coil are being built next to it. The total height of the fence with the concertina is approximately 4 meters above ground. During the construction of the physical barrier, 530 kilometers of new fence segments were installed, and 357 kilometers of concertina prism were built. The total length of the Lithuanian border with Belarus is 679 kilometers. More than 100 kilometers of the national border runs along the banks of rivers and lakes, where there are no plans to install physical barriers.

3.2.3. Automated state border surveillance system

In order to maximize a state border protection, it is essential to ensure that the entire section of the border with Belarus is monitored using the latest technologies. Lithuania has installed the automated state border monitoring system, equipped with CCTV cameras and motion detectors, on a 640 km stretch and will monitor 100% of the state borders with Belarus. Also, Lithuanian State Border Guard Service uses drones, reconnaissance aircraft, offshore sensors and satellite remote sensing to track illegal migration.

3.2.4. Refuse to entry

In early July 2021, the Lithuanian Parliament declared that the country is in a state-level emergency due to a massive influx of migrants. Lithuanian Parliament adopted amendments to the Law on the State Border and Protection (25 April 2023) legalizing the turning away of irregular migrants at the border under a state-level extreme situation regime or a state of emergency.

The amendments to the Law on the State Border and Protection (2023) introduce a possibility to refuse entry to Lithuania during a state-level extreme situation, and due to an influx of foreigners; also to those foreign nationals who intend to cross or have crossed the state border at places that are not designated for that purpose or at places designated for that purpose but having violated the procedure for crossing the state border. The officers of Lithuanian State Border Guard Service (SBGS) have the right to turn away irregular migrants only along the border – up to 5 km inland.

The provision on turning away migrants applied individually to each foreigner and would not apply in certain cases to ensure entry or humanitarian access to Lithuania's territory for foreigners fleeing military aggression or persecution. An assessment of the need for assistance carried out for foreigners who have not been allowed to enter. If found to be in need, migrants would have to be provided with necessary urgent medical or other assistance.

The amendments to the Law on the State Border and Protection (2023) make a clear distinction between natural migration and the instrumentalised migration facilitated by the Belarusian regime and that the legislation is necessary to safeguard Lithuania's national security interests.

3.3. Legal Framework for Risk Management of Border Security

In October 2021, the European Council invited the Commission to propose any necessary changes to the EU's legal framework to respond to the state-sponsored instrumentalization of people at the EU's external border with Belarus. Article 78(3) of the Treaty on the Functioning of the European Union (TFEU) provides for the adoption of provisional measures in emergency migratory situations at the EU's external borders. The objective of the proposal is to support Latvia, Lithuania and Poland by providing for the measures and operational support necessary to manage in a humane, orderly and dignified manner, fully respectful of fundamental rights, the arrival of persons being instrumentalised by Belarus.

The main features of the emergency migration and asylum management procedure at the EU external borders (Lithuania, Latvia, and Poland):

- possibility for the Member States concerned to register an asylum application and offer the possibility for its effective lodging only at specific registration points located at the vicinity of the border including the border crossing points designated for that purpose
- registration deadline for applications for international protection extended to up to four weeks
- possibility to apply the accelerated procedure at the border for all applications, and thus limiting the possibility for Belarus to target for instrumentalization third-country nationals to whom the border procedure cannot be applied
- return procedure at the external borders
- material reception conditions –to cover only basic needs. Latvia, Lithuania and Poland need to ensure that any actions respect basic humanitarian guarantees, such as providing third-country nationals on their territory with food, water, clothing, adequate medical care, assistance to vulnerable persons and temporary shelter

The European Commission's proposal is in line with the comprehensive approach set out in the New Pact on Migration and Asylum. The Pact is designed to establish a common

approach to migration and asylum that is based on solidarity, responsibility, and respect for human rights. The Pact has delivered various outcomes, e.g. determines EU mechanism for preparedness and management of crises related to migration, developed an early warning and forecasting system allowing prompt identification of migration situations, enabling effective preparedness and response, addressed situations of crisis and force majeure in the field of migration and asylum, established the EU integrated border management system - coordinated framework from border surveillance to anti-smuggling and to returns of migrants.

The European Commission's forthcoming proposals to reform the Schengen Borders Code will include strengthening the EU's legal framework to give better tools to Member States to protect the external borders in situations of instrumentalization of migrants, while ensuring full respect for fundamental rights. They will also contain measures that will help those Member States who see unauthorized movements of migrants including the repercussions of instrumentalization far away from the external border.

The European Commission's proposal is the latest in a series of coordinated EU actions that include: targeted measures for transport operators that facilitate or engage in smuggling; diplomatic and external action; stepping up humanitarian assistance and support for border security and migration management.

References

1. Amendments to the Law on the State Border and Protection, adopted by the Parliament of the Republic of Lithuania, 25 April 2023, No. XIV-1891, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ff701250e35a11eda305cb3bdf2af4d8?jfwid=fwi8z9chx
2. Blažytė, G. et al. (2022). Comparative report on the influx of irregular migrants across the Belarus border: the response by the Governments of Lithuania and Latvia. *Diversity Development Group and PROVIDUS Center for Public Policy*, https://ec.europa.eu/migrant-integration/library-document/niem-comparative-report-influx-irregular-migrants-across-belarus-border_en
3. Building walls, restricting rights: Lithuania's response to the EU-Belarus border 'crisis', *Statewatch, 1 February 2022,* https://www.statewatch.org/analyses/2022/building-walls-restricting-rights-lithuania-s-response-to-the-eu-belarus-border-crisis/
4. Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum (COM/2020/609 final), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0609
5. Communication from the European Commission to the European Parliament the Council on Establishing the multiannual strategic policy for European integrated border management (COM(2023) 146 final), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0146
6. Dekker R., et al. (2016). The use of online media in migration networks. *Population, Space and Place, 22, 539–551.*
7. Evans, J. (2021). "Belarus dictator threatens to 'flood EU with drugs and migrants'". *The Week, 28 May 2021,* https://www.theweek.co.uk/news/world-news/europe/952979/belarus-dictator-threatens-flood-eu-with-drugs-migrants-avoid-sanctions
8. FRONTEX - European Border and Coast Guard Agency: Risk Analysis for 2022/2023 (2022), https://frontex.europa.eu/publications/risk-analysis-for-2022-2023-RfJIVQ
9. Giannopoulos, G. et al. (2021). The Landscape of Hybrid Threats: A conceptual model. *Publications Office of the European Union, Luxembourg.*
10. Hybrid Threats as a Concept. *The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE),* https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
11. Joint Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Responding to

state-sponsored instrumentalization of migrants at the EU external border (JOIN(2021) 32 final), https://commission.europa.eu/document/4d0c173e-709f-4832-b12f-31792cd10bff_lt
12. Joint Communication from the European Commission to the European Parliament and the Council on Joint Framework on countering hybrid threats - a European Union response (JOIN/2016/018 final), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
13. Latvia State Border Guard. Statistics at the state border and within the country (from 1 August 2021 to 1 July 2023), https://www.rs.gov.lv/en
14. Law on Installation of a Physical Barrier in the territory of the Republic of Lithuania near the External Border of the European Union with the Republic of Belarus, adopted by the Parliament of the Republic of Lithuania, 10 August 2021, No. XIV-513, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/4763ca32fa7211ebb4af84e751d2e0c9?positionInSearchResults=1&searchModelUUID=e617cf00-5855-4e3f-afc8-d9021687a307
15. Lithuanian State Data Management IS. Monitoring of illegal migration (from 01.01.2011) & Registered illegal migrants, https://ls-ospsdg.maps.arcgis.com/apps/dashboards/9b0a008b1fff41a88c5efcc61a876be2
16. Parliamentary Assembly of the Council of the Europe Resolution 2404 (2021) "Instrumentalised migration pressure on the borders of Latvia, Lithuania and Poland with Belarus", https://pace.coe.int/en/files/29537/html
17. Rashe, L. (2022). The instrumentalization of migration – how should the EU respond? *Jacques Delors Centre, Hertie School, Germany,* https://www.delorscentre.eu/en/publications/the-instrumentalisation-of-migration
18. Sari, A. (2023). Instrumentalized migration and the Belarus crisis: Strategies of legal coercion. *The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)*
19. Statista. Number of attempts to illegally cross the Polish-Belarusian border in Poland from August 2021 to June 2023, https://www.statista.com/statistics/1271292/poland-attempts-of-illegal-crossing-of-the-polish-belarusian-border/
20. The European Commission's proposal for a Council Decision on Provisional emergency measures for the benefit of Latvia, Lithuania and Poland (COM/2021/752 final), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A752%3AFIN&qid=1638547296962