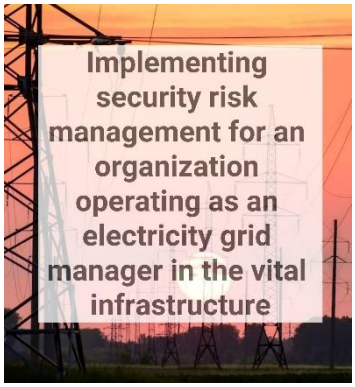
Funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

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

Lambert Bambach / Avans University of Applied Science, the Netherlands / 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 organization's 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.

Link to ISO 31000

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

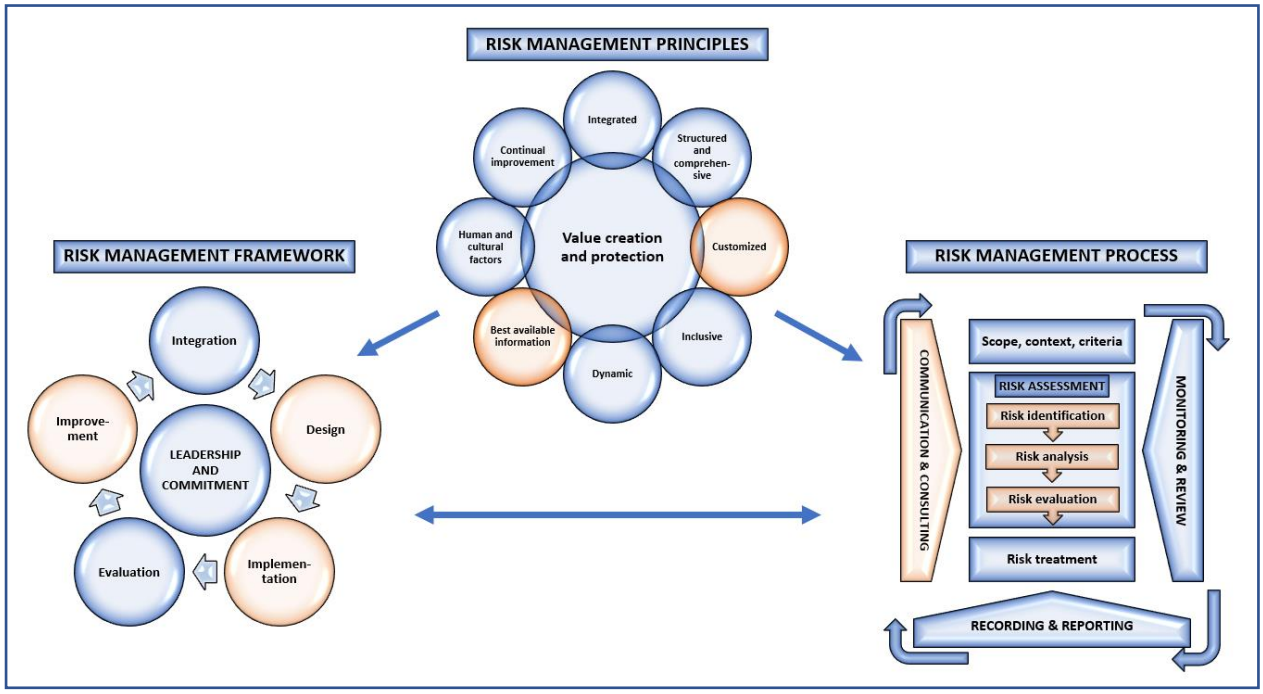


Figure 1. Risk management framework, Risk management principles and Risk management process according to ISO 31000:2018

1. Introduction

A junior security employee in the Asset Protection department of an electricity grid manager, is 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 ones, 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. 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 programme. In doing so, it is important to take into account: a) the purpose of the organization; (b) threats and risk analysis; (c); (d) 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 ones in the world.

3.2 Different types of assets

The organization has Assets both in the decentralized field and centrally. In the decentralized field, the organization deals with assets such as control cabinets, transformers. Operational Technology (OT) plays an important role in these assets. Operational Technology is characterized by the fact that it is all set up with only one goal: 'It must run for as long as possible and with as little downtime as possible. It is therefore equipment that lasts a long time, which often 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 with it functionally. It must support the business goals and these are all quickly flexible, having short lifespans.

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 means that you must build the measures around it to protect such an asset. However, the three fundamental basic principles of information technology 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 expect to always keep their communication systems up and running. If the police are no longer able to communicate in times of crisis, 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 distributing energy across all their grids at all times 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, using camera systems, fences and

reinforced access control. For this, the organization is also continuously developing and assessing 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 are 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 Dutch vital infrastructure. NIS is the directive on the security of network and information systems (NIS Directive), as 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 standardizations have helped the physical and information security department to be able to advise objectively. Standardization also helps to speak a universal language internally, for example with management, but also with external actors 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 injudicious 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 setting 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 advice to be given.

To establish effective requirements, the organization considers the following: 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 need 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

The 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, in order 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 to or perhaps better than those of the competitors, because the criminal still looks for 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