

TOOMAS VIIRA

LESSONS LEARNED: CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

HOW TO PROTECT CRITICAL
INFORMATION INFRASTRUCTURE



Copyright
Provided by IHS Markit under license with IT Governance Ltd
No reproduction or networking permitted without license from IHS
Full document details: ITG 2018

<http://www.itgovernance.com>

Licensee=, Users=
Not for Resale,



Documents
Document Sharing Pro

Lessons Learned: Critical Information Infrastructure Protection

**How to protect
critical information infrastructure**

Lessons Learned: Critical Information Infrastructure Protection

How to protect
critical information infrastructure

TOOMAS VIIRA



IT Governance Publishing

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher or, in the case of reprographic reproduction, in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at the following address:

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

© Toomas Viira 2018

The author has asserted the rights of the author under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

First published in the United Kingdom in 2018
by IT Governance Publishing.

ISBN 978-1-84928-959-7
Mobi 978-1-84928-960-3

ABOUT THE AUTHOR

Toomas Viira has worked in cyber security for more than 20 years. In 2004 he joined RIA (www.ria.ee) (Estonian information system authority), in 2005 he began activities to create CERT Estonia, and in 2007 he was a member of the team that protected Estonia from large scale cyber attacks. Viira is also one of the authors of the Estonian Cyber Security Strategy. In 2009 he was appointed head of the Critical Information Infrastructure Protection department in RIA. He managed several national critical information infrastructure (CII) projects such as CII mapping, CII risk analysis and CII operators' penetration tests, developing risk analysis and response plans for large-scale state-level emergencies, and more. He has the following certifications: CISSP, CISA, CISM, CRISC, ISO 27001 CIS LI, ITIL® Foundation and ITIL Service Strategy. Viira is the founder of www.ciipunit.com.

ACKNOWLEDGEMENTS

I would like to express my thanks to Heli Tiirmaa-Klaar, Jaak Tepandi, Janno Kase, Kaimar Karu, Rünno Reinu, Siim Aben, Maarten Souw, Giuseppe G. Zorzino and Christopher Wright, who read and reviewed the manuscript, providing very useful comments and feedback. I would like to extend a special thanks to Mari Seeba, who read every sentence and analysed the content of the manuscript with the utmost care.

I'd like to thank the IT Governance Publishing team and the members who worked on this book: Jonathan Todd, Luke Milner and especially Vicki Utting, who managed me through the full publishing process and gave me very useful guidance.

I would like to express my thanks to all the colleagues I have worked with over the years and with whom I have had the opportunity to make great things in the field of cyber security.

CONTENTS

Introduction.....	9
Part 1: Critical infrastructure	12
Chapter 1: Critical infrastructure services	13
Chapter 2: Description of service and service level	15
Chapter 3: Providers of critical infrastructure services	18
Chapter 4: Critical activities and required resources	21
Chapter 5: Interdependencies of services	24
Chapter 6: Visualisation of information	28
Part 2: Critical information infrastructure	30
Chapter 7: Identification of important information systems	31
Chapter 8: Interdependencies of information systems	34
Chapter 9: Focusing and prioritisation.....	38
Part 3: Threats, vulnerabilities, risks, impacts	41
Chapter 10: Threats and vulnerabilities of information systems	42
Chapter 11: Assessment of the impact of service disruptions	45
Chapter 12: Risk assessment.....	48
Part 4: Protection activities.....	51
Chapter 13: Implementation of security measures	52
Chapter 14: Organisation required to protect critical information infrastructure	55

Contents

Chapter 15: NIS Directive.....	58
Chapter 16: Assessment of the security level	62
Chapter 17: Network scanning.....	65
Chapter 18: Business continuity plan and testing.....	68
Part 5: Protection system supporting activities.....	71
Chapter 19: Reliable relations and maintaining them.....	72
Chapter 20: Sharing information	74
Chapter 21: Training people.....	77
Part 6: Perfecting the system	80
Chapter 22: Improvement of the system	81
Part 7: Backup plan	83
Chapter 23: Life without IT.....	84
Appendix 1: Lessons learned	88
ITG Resources	90

INTRODUCTION

The way organisations operate and provide services has changed considerably over the past decades. Their capability to produce something has also grown significantly. This has become possible largely due to information technology solutions, which have become indispensable and a natural part of business. Those who try to manage without them achieve only limited performance and functionality. It often seems that doing things without IT solutions is plain impossible. Information plays an important role in management decisions and in business processes. IT solutions have allowed organisations to increase their efficiency in order to be competitive. However, do we even know and realise what happens when IT solutions are not working – when they simply don't function at all or not in the way we expect them to?

People and organisations consume electricity generated by various types of power plants: nuclear, hydroelectric, thermal, wind, solar and others. We consume the services of communications service providers, such as voice telephony and data communication. We cannot get by without transport service providers – we need companies that operate in aviation, marine transport or on railways. We need operational water supply companies to get water from the tap. Hospitals, clinics and ambulance crews must work to provide medical help to people. Financial service providers must be operational so we can withdraw money from ATMs or make bank transfers. Most of these companies use information systems to provide their services. It wouldn't be possible without them.

Introduction

However, these systems must be very well protected against cyber attacks. Cyber attacks¹ could interrupt² all or part of critical infrastructure services for several hours or days, bringing health, safety, economical, environmental and reputational consequences³.

Risks should also be minimised in terms of technological faults and human error. Are the systems that provide critical infrastructure services protected? How well are they protected? Considering today's threats and attack capabilities, it feels like many of these systems are not adequately protected.

Billions of people use the services of these companies, and this number is increasing rapidly. There are fewer and fewer places where people don't consume any services provided with the help of IT solutions.

But how is it possible that services consumed by so many people are provided using relatively vulnerable systems? In many instances, even the most basic security measures have not been implemented.

I have been working in the field of protecting CII since 2005 and organised the relevant activities in a country where the use of e-services and dependence on information

¹ A Stuxnet cyber attack on a steel mill caused damage to Germany's industrial infrastructure by destroying human machine interaction components: www.sentryo.net/cyberattack-on-a-german-steel-mill

² In December 2015 a successful cyber attack on a power grid in the Ukraine compromised information systems and disrupted electricity supplies to end consumers: https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

³ The NonPetya ransomware attack is estimated to have cost shipping giant Maersk \$300m and forced it to halt operations at 76 port terminals around the world. They were just one of the companies affected globally: www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shiiping_giant_maersk/

Introduction

technology is among the highest in the world. People often ask me the same questions: How is CII protected in Estonia and what have you learned?

The current weak protection of CII, the threats and attack capabilities lurking in cyberspace, and the questions people have asked prompted me to write this book. My goal is to help you be as successful as possible in protecting your CII, and do so as quickly and with as little effort as possible, irrespective of whether you work for a critical infrastructure service provider, a company that organises the provision of critical infrastructure services, a company that provides services to a provider of critical infrastructure or somewhere else.

The book is aimed at people who organise the protection of critical infrastructure, such as chief executive officers, business managers, risk managers, IT managers, information security managers, business continuity managers, and civil servants from ministerial level to analyst level. Most of the principles and recommendations I describe are also valid in organisations that are not critical infrastructure service providers.

There are several hyperlinks throughout the book. If you are reading the print version, please visit www.ciipunit.com/lessonslearned where you will find an online library for easier access to the links. On the same website, I have also provided links to several CII incident pages and CII audit checklists, and will regularly update the website with content related to the book.

PART 1: CRITICAL INFRASTRUCTURE

CHAPTER 1: CRITICAL INFRASTRUCTURE SERVICES

‘The next Pearl Harbor we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems.’⁴ – Leon Panetta

People have a variety of needs in their daily lives: water, food, clean air, a home and electricity. We also consume many other benefits such as transport services, communication services, television and radio programmes, medical services and banking services. Without some of them, we probably wouldn’t survive – not for long, anyway. Some services are more important to different people at different times – transport connections, communications and medical services may be more or less essential, depending on your circumstances. A common understanding of primary needs is relatively easy to achieve, but when pinpointing vital services we may often end up with different opinions. Defining such services depends on geographic location, climate, season, people’s way of life and other factors. There are services that people have become used to over decades, and their absence causes uncertainty or puts our security at risk. Mobile communication is a good example of this: it is important for people to be in contact with their loved ones, but 30 years ago we managed just fine without mobile phones. We’ve become increasingly used to them and our dependence on them has grown. Many of us feel like we can’t live without social networks.

⁴ www.huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html

1: Critical Infrastructure Services

The lines between vital, socially important and other services consumed by us cannot be clearly and unequivocally defined. From the viewpoint of protecting critical infrastructure, it is important that such services are defined and written down somewhere. Every country should have a specific law that regulates this field. Defining critical services is bound to lead to discussions and possibly arguments about whether or not a specific service is critical, or why one service is critical and another is not. Preparing the list of services is still in its early stages in terms of the entire process of protecting critical infrastructure and CII, and there is still a lot to do. The law can be amended if an important service was left out or a service that was deemed critical shouldn't actually be regarded as such.

These critical services must be operational:

- power supply
- oil and gas supply
- water supply and sewerage
- harbours
- rail traffic
- air traffic
- data telephony
- data communication
- settlements and cash withdrawals
- law enforcement
- medical assistance.

The list is not final, and the circumstances, characteristics and needs of each country should be taken into account.

Lesson 1: Define critical infrastructure services.

CHAPTER 2: DESCRIPTION OF SERVICE AND SERVICE LEVEL

‘Critical infrastructure is vitally important to all of us because it provides the necessities: water and food; the electricity and gas; the telecommunications and broadcasting services that keep us in touch and help us to conduct our business; the health services that keep us alive; the banking and finance system that keeps our economy running; and the transport system that gets us – and the goods we need – from A to B.’⁵ – George Brandis

Preparing the list of critical infrastructure services described in the previous chapter is the first step. However, the list alone is not enough for planning the activities that follow. It is also important to describe the critical infrastructure services. How and on what basis can we say that a critical infrastructure service is functioning? How do we know what a specific critical service is and what characterises it? If we don’t know what a functioning service looks like, then it’s impossible for us to objectively assess whether or not it is functioning. Does a service function as needed?

Every critical service should be described. The description of a critical infrastructure service should allow the service provider, consumers and other stakeholders to understand what can and cannot be expected from the specific service. All critical infrastructure services can be characterised with different criteria and parameters. The requirements for and

⁵ www.attorneygeneral.gov.au/Speeches/Pages/2014/Second%20Quarter%202014/6June2014-OpeningAddressOfTheCriticalInfrastructureResilienceConference.aspx

2: Description of Service and Service Level

service level of a critical infrastructure service should also be determined. Power coming from the grid always has the same tension and frequency, and we're used to this. It's possible that these parameters have been determined in regulations. Power supply companies enter into contracts with their clients. These contracts or the general conditions of services may also contain other aspects that describe the service and service level. They might contain the number to call in the event of faults, determine how quickly the company has to react to faults, how quickly faults have to be eliminated, etc. Sometimes they state the length of a power cut from which the client is not charged for the service. In these cases, we can say that a service level has been determined between the service provider and the client. However, the service level of a critical infrastructure service should be determined from the viewpoint of the state.

It's likely that there are many services that have not been adequately described and for which the necessary service level has not been determined. Or, if a service level has been determined, it was not done in consideration of the fact that the service is a critical infrastructure service and its consumers may have higher expectations regarding the continuous operation of the service.

These parameters should be determined for every critical infrastructure service:

- maximum tolerable downtime
- recovery time objective.

Maximum tolerable downtime is the downtime that an organisation, specific sector or country can tolerate. 'Maximum tolerable' can be defined at business, sector or

2: Description of Service and Service Level

country level and these could be different. A critical infrastructure service provider should follow the shortest defined downtime.

Recovery time objective is the defined time during which systems and services should be brought up and running.

Service-specific indicators that characterise the operating level of the service must be defined for the majority of services: a minimal quantity of calls in a mobile communications network, the quantity of banknotes withdrawn from an ATM in a certain unit of time, the guaranteed minimal water pressure at specific measurement points, the minimal number of passengers served by a harbour in a certain unit of time, etc.

The above is the so-called primary requirement in the process of building a critical infrastructure protection system. We should then think about the operational needs of critical services in the event of crises of different severity and define them if possible. What are the critical infrastructure services that should definitely work in the event of a crisis and at what level should they operate?

Lesson 2: Describe the critical infrastructure service and determine its service level.

CHAPTER 3: PROVIDERS OF CRITICAL INFRASTRUCTURE SERVICES

‘Critical infrastructure is diverse and complex not only because of the variety of sectors it covers, from communications, emergency services, information technology to nuclear reactors and transportation systems; it is complex also due to the special nature of its ownership.’⁶ – Dean Thompson

Once the list of critical infrastructure services has been prepared, they have all been described and their service levels determined, the next step is to identify the providers. Critical infrastructure service providers are not only public-sector organisations. In many countries, essential elements of critical infrastructure are owned and operated by private companies. Depending on the service, market, regulations and many other factors, a service may be provided by one or several service providers. Some countries may only have one provider of a certain service if the service provider is a monopoly, or only one service provider may have the right to provide a certain service in a certain region. The number of monopolies has decreased in the past 20 or 30 years. Many countries have opened their markets in the communication and energy sectors, which in the past were often controlled by monopolies.

In the case of a monopoly when there is only one service provider on the market, this service provider must be considered the critical infrastructure service provider.

⁶ <https://ro.usembassy.gov/remarks-by-u-s-charge-daffaires-ad-interim-dean-thompson-at-the-critical-infrastructure-protection-forum/>

3: Providers of Critical Infrastructure Services

What happens when there is more than one service provider on the market? Many other factors should be considered, such as the number of clients to whom the service is provided, market share, production volume and capacity, number of clients in a certain geographic region, etc.

Which service providers will be considered critical infrastructure service providers and which ones will not? Depending on the sector, services and possible criteria for defining critical infrastructure services, as well as reaching the relevant agreements, identifying these service providers may take a lot of time.

For example, if there are many voice telephony service providers, which of them should be considered critical infrastructure service providers? There may also be situations where some providers only operate in a certain geographic region and don't provide their service nationwide. Some of these service providers may have the biggest market share in a specific region and not provide their services in another. This means that geography must be considered when defining the criteria for a critical infrastructure service provider.

Possible criteria for qualifying an organisation as a critical infrastructure services provider:

- Number of clients nationwide.
- Number of clients in a certain region.
- Number of people living in a certain administrative district.
- Market share of the service provider according to turnover.
- Production volume, capacity, etc.

3: Providers of Critical Infrastructure Services

- Number of service points in the country or a certain administrative district.
- Client or clients to whom the service is provided (e.g. a communications operator that provides services to other critical infrastructure service providers).
- A service provider of transnational importance (e.g. a critical infrastructure service provider in the EU – an operator that provides a service to a significant number of clients abroad).
- An operator that provides international connections, etc.

The list of critical infrastructure providers should be reviewed and updated at least annually or after essential changes.

Lesson 3: Define the providers of critical infrastructure services.

CHAPTER 4: CRITICAL ACTIVITIES AND REQUIRED RESOURCES

‘Despite the fact that cyber-attacks occur with greater frequency and intensity around the world, many either go unreported or are under-reported, leaving the public with a false sense of security about the threat they pose and the lives and property they impact.’⁷ – Daniel Wagner

In order to provide a critical infrastructure service reliably, it is necessary to know how the service is provided. What kind of business processes must be operating so that the service provider can provide the service and the consumer can consume it? Providing critical infrastructure services often depends on various sub-services without which the service cannot be provided. Depending on the organisation and the service, such services may be provided internally: one department provides a service to another department. The other option is to outsource services from external providers. If the provision of services is organised internally, then the parties and business processes connected to the critical infrastructure service must be identified inside the company. In such cases, it is usually easier to understand which business processes are necessary to provide the critical infrastructure service, which resources are needed, what the connections between the different resources are like and how the whole system works.

⁷ www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyber-attacks/b_10114374.html

4: Critical Activities and Required Resources

However, the services consumed for service provision are often not all internal and the services of external providers are also needed. Critical infrastructure service providers often have several external service providers. They in turn often rely on subcontractors. There are many cases where a critical infrastructure service provider doesn't even know how long a certain supply chain is and who they actually depend on. Not to mention knowing the ability of a specific company to provide a specific service or sub-service, their capability in the event of a crisis, the background of the specific company, etc.

It is important to know what is needed to provide every critical infrastructure service at the required service level. What kind of business processes guarantee that the service is operational and which business processes are essential? In general, the business processes needed to provide critical infrastructure services can be divided into three categories:

- Business processes without which the service cannot be provided.
- Business processes that are necessary for providing the service, but the service can for some time be provided without such business processes being operational (possibly at reduced functionality and/or load).
- Business processes that do not have a significant role in the provision of the service, that is, the service can be provided without these processes being operational.

There are many companies where the processes needed to provide critical infrastructure services have not been described, there is no understanding of the connections between processes, and the operation of various processes is not measured. Sometimes the bigger the company, the more difficult the processes are to describe. However, as a

4: Critical Activities and Required Resources

company grows in size, it needs to give more attention to describing its processes and their efficiency.

The resources needed for different processes should be identified after the processes have been listed and described. The following questions should be asked:

- Who is responsible for operating each process?
- How is the smooth operation of processes guaranteed?
- What happens if there are faults or disruptions?
- What is the impact of disruptions on providing the main service?

It should also be clear whether the preconditions needed for providing a critical service at the required service level have even been created, whether the service levels of outsourced services have been agreed with subcontractors and whether the service levels have been agreed inside the organisation of the critical infrastructure service provider. Would all the above even make it possible to provide the service at the required level or should changes be made?

Lesson 4: Identify the critical activities, resources and responsible persons needed to provide the critical infrastructure service.

CHAPTER 5: INTERDEPENDENCIES OF SERVICES

‘By better understanding and quantifying the consequences, both economic and societal, of a severe cyber hazard on our country’s critical infrastructure, we underline the level of responsibility amongst each of the key stakeholders in this value chain. Through hyper-connectivity, we have created fantastic opportunities for smarter infrastructure use that also bring with them a complex set of cyber risks for the foreseeable future.’⁸ – Simon Ruffle

In the previous chapter, we determined that providing critical infrastructure services needs several business processes and took a look at this from the viewpoint of a critical infrastructure service provider. However, the big picture should also be analysed in terms of the functioning of the state. It is obvious that many critical infrastructure services depend on one another, on many other services that are not regarded as critical infrastructure services, and on power supply. In most countries, many critical infrastructure services also depend on the operation of services in the ICT sector, such as voice telephony, data communication or information systems. There are also

⁸ www.quicken.com/investing/stock-quotes/LMT/Lockheed-Martin-Corp/Collaboration-on-Critical-National-Infrastructure-Cybersecurity-Key-to-Minimising-UK-Economic-Risk-According-to-New-Study/600-201604120803PR_NEWS_USPRX_CL68540-1

5: Interdependencies of Services

other critical infrastructure services and sectors that are connected and depend on one another:

- You need a working mobile phone or landline to call emergency services.
- Operational radio communication is necessary for organising police and ambulance crews.
- Police cars and ambulances need fuel, so we need working petrol stations.
- Card payment terminals need to work so that the fuel can be paid for.
- These terminals need a working banking information system and data communication network.
- A data communication network needs electricity to work.
- Eliminating electrical failures needs working telephone communications.
- An operating security company is needed to guarantee the physical security of sites.
- Sending alarm signals from sites needs a working data/voice telephony network.
- A boiler house needs gas (or the supply of a different type of fuel) to work.
- A water supply company needs electricity to work.
- Air traffic control needs various working information systems and a working connection with other air traffic control centres as well as between control centres and aircraft.
- Airfields depend on good maintenance of runways, working runway lights, security checks of passengers and baggage, aircraft fuelling and maintenance, etc.

5: Interdependencies of Services

- Communications networks need electricity and operational network components: telephone exchanges, network nodes, mobile communication masts, routers, communications channels, servers of different communications networks that provide specific services, settlement systems, software, etc.
- Power can be supplied when electricity generation, transmission networks and distribution networks are all working.

This list could go on and on as it does not list all the possible dependencies of a service.

As said above, most services need a power supply to function. We cannot get by without it. Or if we can, then for only a very short time. Organisations may have diesel generators, but they must be refilled with fuel. How big are the generators' fuel tanks? Can extra fuel be obtained from somewhere during a power cut? Can a petrol station give fuel from its tanks when there is no electricity?

The above demonstrates rather well that while most services depend on electricity and communications, they also depend on many other services and this makes the whole situation more complicated.

From a state perspective, a strong overview of dependencies is vital. If such an overview doesn't exist, it becomes very difficult to assess the scale and impact of different types of incidents. Every responsible ministry should have oversight of their governance area and draw up a list of state-level dependencies. At the country level, governments should appoint an agency to be responsible for emergency management. The same agency should have information on the dependencies in all critical infrastructure

5: Interdependencies of Services

sectors, cross-sectoral dependencies and cross-border dependencies.

Heavily CII-dependent states have more complex interdependencies and will need information systems to run almost everything. This means power supply becomes more important because information systems are bricks without electricity.

Lesson 5: Analyse and identify the interdependencies of services and their reliance upon power supplies.

Copyright IT Governance Ltd
Provided by IHS Markit under license with IT Governance Ltd
No reproduction or networking permitted without license from IHS

CHAPTER 6: VISUALISATION OF INFORMATION

*'The greatest value of a picture is when it forces us to notice what we never expected to see.'*⁹ – John Tukey

After implementing everything described in the previous chapters, we should have a list of critical services, descriptions of the services and service providers, and an analysis of the interdependence of services at a certain level. This has generated a lot of information that must be managed, changed or updated if necessary. A proper overview of it should also be created.

This can be done with a word processor, spreadsheet or database, but they are not the best methods as finding the data and getting a good overview of it in these formats will be difficult or even impossible.

It would be better to visualise this information somehow, which will reveal the connections that otherwise only a good data analyst could find. While it might be simpler for people who deal with the topic every day to understand these connections, this information must be comprehensible to people who do not, especially those who will be responsible for protecting critical infrastructure.

Data visualisation could be the solution to the aforementioned problems. Data visualisation is important at the levels of companies, sectors and the entire state. At the level of companies, it should support describing the

⁹ Tukey, John W. (1977). *Exploratory Data Analysis*. Pearson. ISBN 978-0201076165