Thomas Dauner, Lukas Kastler
Daniel Rommel, Moritz Krenmayr

Prof. Schäffter
ISMS

CRITIS Information Security Policy

Index

1. Introduction

Critical infrastructures are services and institutional structures and facilities of a vital importance to a nation’s economy and sociality. Their failure would result in high supply shortages, significant disruption of public safety and security or other very dramatic consequences. They are essential for everybody’s life. Critical infrastructures mean for example hospitals, electricity, water supply and other basic services.

Critical infrastructures have special legal requirements. In Germany, the “IT-Sicherheitsgesetz” declares, that critical infrastructures have to be secured. There are many statements about these security measures.

In our critical infrastructure case study, we designed a security policy for a hospital.

2. Business goals of the hospital

The main business goals of the hospital are patient treatment, improving patient service, quality of care and hospital growth.

Our customers are patients. We provide live saving measures and general healthcare for those patients. With treating the patients we can earn money.
It’s our goal to improve the patient service quality and the quality of care consistently. This is done by using the newest technologies like surgery robots, intelligent healthcare devices and modern research facilities and techniques. Those connected devices rely on a good IT architecture.

3 CIA analysis & assets

Asset	C	I	A	Explanation of assets
Patient				
Patient records	9	9	5	Patient specific data. This data needs to be confidential and integer.
Patient treatment	3	9	10	The treatment a patient receives need to be very available and integer.
Medical devices	1	9	9	The medical devices need to work very integer and need to be very available.
Hospital				
Research	7	9	3	The research & development needs to be very confident and integer.
Hospital finances	8	8	4	The finances of the hospital need to be confident and integer.
Management data	9	9	5	The data of the hospital like employee data, shift plans, etc. need to be very confidential and integer.
IT				
Servers	4	8	8	The servers need to be very integer and available. The servers control the processes in the hospital. The data needs to be confidential -> patient records/management data.
Computers	4	8	8	The computers need to be very integer and available. The computers are used for patient treatment by nurses and for management. The data needs to be confidential -> patient records/management data.
Medical (device) software	4	9	9	The medical device software needs to be integer and available.
Management software	4	9	9	The management software needs to be integer and available.

3.1 Explanation to the CIA analysis

The CIA analysis shows, that the 3 segments of the hospital (patient, hospital, IT) need different requirements:

For the patient, the integrity and the availability of his treatment is really important because the patient should always have access to his treatment and the treatment based on his data should be correct.

For the hospital the integrity and confidentiality are very important otherwise treatments based on wrong research results could lead to horrible situations. It is also necessary to secure our confidentiality for hospital matters to secure our payments or employee data.

For the IT, a high amount of integrity and availability is needed. Because without a working IT network, a hospital won't be able to treat patients as needed.

4 Example statements for the overall security policy (cf. ISO27k2, A5.1.1)

Definitions:

Information security for this hospital means, that our critical infrastructure works as expected. To fulfill our business goals like patient treatment, improving patient service, quality of care and hospital growth, we need a reliable, secure and working IT infrastructure.

Based on our CIA analysis, there are different requirements for different kinds of assets. Those requirements are declared at topic "3.1 Explanation of the CIA analysis".

The main objective of information security is, to ensure that the business targets of the different business units can be reached.

Principles:

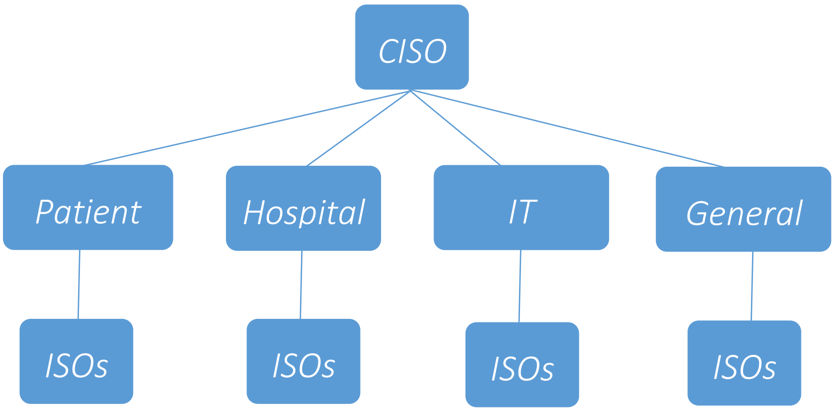
To ensure information security many different principles are used.

CIA analysis helps defining targets and priorities for information security. CIA means confidentiality, integrity and availability.
Risk management is needed to determine the probability and potential damage of a possible attack.
Access control means control of physical access to buildings and rooms like doors and locks and virtual access to IT infrastructure like password protection and access rights.
A **BCM** (business continuity management) is needed to define rules and processes for handling deviations and exceptions to ensure the business continuity.
A **clean desk** principle is needed. No important, confidential data should be left in rooms or offices.
A **need-to-do-principle** is used to give different groups of persons specific access/use rights. Everybody gets those rights that he/she needs to fulfil his job. But not more rights than needed are given.

Responsibilities:

CISO (chief information security officer):
The CISO is responsible to create a new business unit, which main part is the creation and improvement of an ISMS (information security management system). He is in charge to implement the ISO 27K family standards and keep those up to date. Those implementations need to be documented in policies, manuals and procedures structured from general to specific documents.

The CISO is in charge to employ ISOs referred to the following orgchart.



ISO (information security officer):
The CISO is the of the ISO. The ISO is in charge to do the tasks he gets from his CISO. He is helping in implementation of the ISO 27K family standards and documentation of those.

IT admin:
He is in charge for the maintenance of the IT infrastructure. He needs to implement the created policies and manuals to the IT system. He is in charge to keep the systems up-to-date, install important updates and refer to the ISOs and CISO in terms of problems.

Patients:
Patients need to follow the policy rules. They are in charge to inform a respective employee if there are problems or security breaks.

Employees:
The staff needs to follow the policy rules. They are in charge to inform the CISO if there are problems or security breaks.

Process for business continuity:

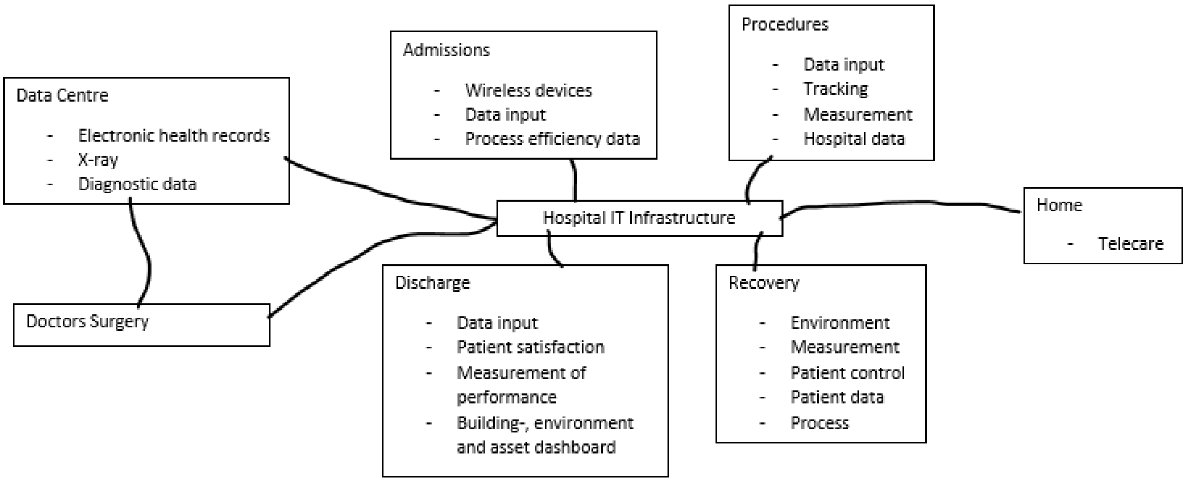
For any exceptions the responsible persons need to be informed. The CISO needs to be informed of every security breach.
The further exception handling is in the responsibility of the CISO. The CISO is in charge to set up a business continuity management (BCM) and a disaster recovery plan (DC) referred to ISO 27k.
It's needed to inform the respective authority if there is a security breach.

Policies:

The CISO and her organization is in charge to create, implement and ongoing improve low level policies referred to ISO 5.1.1/27002 in particular for the following aspects: access control, information classification, physical and environmental security, end user policies, backup, information transfer, protection from malware, management of technical vulnerabilities, cryptographic controls, communications security, privacy and protection of personally identifiable information and supplier relationships.

The CISO is also in charge to implement CRITIS specific policies referred to ISO 5.1.1/27799.

5 IT architecture overview



6 Threats

6.1 Threat 1: Malware

Concrete attack:

A device gets infected by malware. The origin may be an infected device like a USB stick an attacker puts in a computer or an external attack through an email. The malware gets in the network and may infect other devices. The malware can cause different problems. For example it can stop devices from working or change their behavior. If the devices stop working, no patient treatment can be performed. Operations may be canceled. Emergency patients can no longer be treated. In worst case, many patients die. If the data on the servers get encrypted, a basic treatment of patients can be done. But the organization will be a big issue.

Sequence:

a) Attacker wants to attack the hospital
b) Attacker sends infected E-Mail to the hospital
c) Worker opens the email
d) Malware infects the network, servers and devices
e) Patients cannot be treated and may die

Risk reducing controls:

<u>Learning from information security incidents (A.16.1.6)</u>

Knowledge from analyzing previous attacks shall be used to reduce the likelihood or impact of future incidents.

Information security incidents should be monitored. Those gained information from the incidents should be used to identify future incidents or used in an awareness training, as example of what could happen, how to respond and how to avoid them.

-> Security gaps can be closed and prevent a new attack

<u>Responsibilities and procedures (A.16.1.1)</u>

Responsibilities and procedures shall be established to ensure orderly response to information security incidents.

Responsible persons (e.g. a CISO, different ISOs, …) for different tasks need to be named. Policies and procedures for security incidents need to be produced. Those persons need to report necessary actions in case of information security events.

-> Through the “need-to-know”-principle, the attacker cannot access all parts where higher access rights are needed

<u>Backup (A.12.3.1)</u>

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A backup policy should be established to define the organizations requirements for a backup for software systems. Regular backups need to be done. Those need to be stored and need to be available in case of data loss/failure. Those backups should be protected against unauthorized physical access and environmental threats.

-> The servers can be restored with a backup in case of infection with malware

6.2 Threat 2: Hacker

Concrete attack:

A hacker exploits the network and gains access to it. This may happen through many different ways. Physical access to the IT infrastructure, an email attachment with a Trojan, etc. The hacker gains access to the servers, data and infrastructure. He may steal some data or corrupt it. In worst case, he destroys the servers with a virus which could infect other devices. The main problems are, that in case of a data loss patients could not be treated. Operations need to be canceled. In case of a data corruption, patients could get a wrong therapy which can also lead to their death. When the hacker corrupts software for medical devices, he could kill the patients very easily without having physical access to them.

Sequence:

a) Attacker wants to steal data/destroy devices
b) Attacker gains access to network/physical access
c) Attacker elevates access rights in the network
d) Attacker destroys hardware/corrupts software/steals data
e) Attacker leave unrecognized
f) Patients cannot be treated or may die

Risk reducing controls:

Learning from information security incidents (A.16.1.6)

Knowledge from analyzing previous attacks shall be used to reduce the likelihood or impact of future incidents.

Information security incidents should be monitored. Those gained information from the incidents should be used to identify future incidents or used in an awareness training, as example of what could happen, how to respond and how to avoid them.

-> Security gaps can be closed and prevent a new attack

Responsibilities and procedures (A.16.1.1)

Responsibilities and procedures shall be established to ensure orderly response to information security incidents.

Responsible persons (e.g. a CISO, different ISOs, …) for different tasks need to be named. Policies and procedures for security incidents need to be produced. Those persons need to report necessary actions in case of information security events.

-> Through the “need-to-know”-principle, the attacker cannot access all parts where higher access rights are needed

Backup (A.12.3.1)

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A backup policy should be established to define the organizations requirements for a backup for software systems. Regular backups need to be done. Those need to be stored and need to be available in case of data loss/failure. Those backups should be protected against unauthorized physical access and environmental threats.

-> The servers can be restored with a backup in case of corrupted data

Physical entry controls (A.11.1.2)

Secure area shall be protected by appropriate entry controls to ensure that only authorized personal are allowed to access.

The date and time of entry and leaving of each visitor should be recorded. Every employee, contractors and external parties should wear some form of visible identification, e.g. ID-cards/passports. Special areas with confidential information can only be accessed by authorized

personal using an access control with e.g. 2-factor authentication.
-> Attacker cannot gain physical access to servers/devices which prevent the physical attack

6.3 Threat 3: Electrical black out

Concrete attack:

There are different reasons, why an electrical blackout can occur. There may be some heavy weathers which destroy the electrical infrastructure leading to the hospital. The electrical infrastructure inside the hospital can get damaged due to a catastrophe or a sabotage. In case of an electrical blackout, after a short time the emergency generators should start and produce electricity. In this case, the basic electrical system can be used to do basic lifesaving treatment. Unnecessary operations may be canceled. Patients may not get the best treatment due to missing electricity for less important treatments. In case of a sabotage, the emergency generators may not start. In this case, the whole hospital is without electricity. No operations can be done, no machines can be used for treatment. In this case, many patients could die.

Sequence:

f) Heavy weather occurs
g) Electrical infrastructure get destroyed
h) Electrical devices in the hospital work no longer
i) Patients cannot be treated as needed
j) Patients die

Risk reducing controls:

<u>Supporting utilities (A.11.2.2)</u>
Equipment shall be protected from disruption caused by failures by supporting utilities. Supporting utilities should be inspected and tested regularly to ensure they are proper functioning and if necessary be alarmed to detect malfunctions. Supporting utilities are emergency devices to provide electricity, water,… in case of a malfunction of the main systems. Those need to be installed. In case of the hospital, the main aspect are emergency generators to provide electricity in case of an electrical black out. Those emergency generators need to be protected from unauthorized access to prevent sabotage and need to be tested and checked regularly.
-> The electrical devices in the hospital are working even in blackout

<u>Physical entry controls (A.11.1.2)</u>
Secure area shall be protected by appropriate entry controls to ensure that only authorized personal are allowed to access.
The date and time of entry and leaving of each visitor should be recorded. Every employee, contractors and external parties should wear some form of visible identification, e.g. ID-cards/passports. Special areas with confidential information can only be accessed by authorized personal using an access control with e.g. 2-factor authentication.
-> Attacker cannot gain physical access to servers/devices which prevent a physical attack

6.4 Threat 4: Sabotage

Concrete attack:

A person who wants to do a sabotage gains physical access or access via the network to the critical devices or areas. The person uses an infected USB stick or an exploit to gain access and improve their access rights in the network. Then the person can destroy or corrupt critical devices. The person also can corrupt or destroy critical devices through physical access. For example the person can destroy cables to the servers or steal hard drives.

Sequence:

k) Attacker wants to sabotage devices
l) Attacker gains access to network/physical access
m) Attacker elevates access rights in the network
n) Attacker destroys hardware/corrupts software
o) Attacker leave unrecognized
p) Patients cannot be treated and may die

Risk reducing controls:

Learning from information security incidents (A.16.1.6)

Knowledge from analyzing previous attacks shall be used to reduce the likelihood or impact of future incidents.

Information security incidents should be monitored. Those gained information from the incidents should be used to identify future incidents or used in an awareness training, as example of what could happen, how to respond and how to avoid them.

-> Security gaps can be closed and prevent a new attack

Responsibilities and procedures (A.16.1.1)

Responsibilities and procedures shall be established to ensure orderly response to information security incidents.

Responsible persons (e.g. a CISO, different ISOs, …) for different tasks need to be named. Policies and procedures for security incidents need to be produced. Those persons need to report necessary actions in case of information security events.

-> Through the “need-to-know”-principle, the attacker cannot access all parts where higher access rights are needed

Backup (A.12.3.1)

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A backup policy should be established to define the organizations requirements for a backup for software systems. Regular backups need to be done. Those need to be stored and need to be available in case of data loss/failure. Those backups should be protected against unauthorized physical access and environmental threats.

-> The servers can be restored with a backup in case of corrupted data

Physical entry controls (A.11.1.2)

Secure area shall be protected by appropriate entry controls to ensure that only authorized personal are allowed to access.

The date and time of entry and leaving of each visitor should be recorded. Every employee, contractors and external parties should wear some form of visible identification, e.g. ID-cards/passports. Special areas with confidential information can only be accessed by authorized personal using an access control with e.g. 2-factor authentication.

-> Attacker cannot enter server room to do sabotage

6.5 Threat 5: Ransomware

Concrete Attack:

The system gets infected by a ransomware. The origin can be an e-mail or the visit on a faulty website. This program can encrypt the data or lock the access to the whole system. The attacker can demand ransom to release the system or decrypt the data. It's also possible that the ransomware infect other external or internal systems and organizations via the system from the hospital.

Sequence:

a) Attacker wants to attack the hospital
b) Attacker sends infected E-Mail to the hospital
c) Worker opens the email
d) Ransomware infects the network, servers and devices
e) Servers and data get encrypted
f) Patients cannot be treated and may die

Risk reducing controls:

Learning from information security incidents (A.16.1.6)

Knowledge from analyzing previous attacks shall be used to reduce the likelihood or impact of future incidents.

Information security incidents should be monitored. Those gained information from the incidents should be used to identify future incidents or used in an awareness training, as example of what could happen, how to respond and how to avoid them.

-> Security gaps can be closed and prevent a new attack

Responsibilities and procedures (A.16.1.1)

Responsibilities and procedures shall be established to ensure orderly response to information security incidents.

Responsible persons (e.g. a CISO, different ISOs, …) for different tasks need to be named. Policies and procedures for security incidents need to be produced. Those persons need to report necessary actions in case of information security events.

-> Through the “need-to-know”-principle, the ransomware cannot access all parts where higher access rights are needed

Backup (A.12.3.1)

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

A backup policy should be established to define the organizations requirements for a backup for software systems. Regular backups need to be done. Those need to be stored and need to be available in case of data loss/failure. Those backups should be protected against unauthorized physical access and environmental threats.

-> The servers can be restored with a backup in case of encryption through ransomware

7 Risk matrix

Probability/ *Potential damage*	*Very low*	*low*	*medium*	*high*
high			T3	T1,T2,T5
medium			T4	
low				
Very low				

7.1 Explanation to risk matrix

Threat 1: Malware
A malware attack has a very high probability and a very high potential damage. Malware is since many years the top highest IT security risk.[1] Such an attack is easy to perform via the internet and can cause very much damage, because it can infect the whole system.

Threat: Hacker
A hacker attack has a very high probability and very high potential damage. Hacker attacks are easy to perform from all over the world. Hospitals store a lot of user specific and high confidential data. So for identity theft and other crimes, hacker attacks on hospitals are very effective and cause a lot potential damage if the hacker changes software or data unrecognized.

Threat: Electrical blackout
An electrical blackout is likely, but not very likely to happen. The damage could be very high. Temporary blackouts happen often, but most of the time, they are quite short. But even 10 Minutes without electricity can cause lives (e.g. an intense care patient with external ventilators).

Threat 4: Sabotage
A sabotage is not the most likely attack to happen, but it is possible. Also the damage depends on what device or infrastructure gets sabotaged. But in most cases, the sabotage affects a specific device or part of the infrastructure and not the whole system. So the damage is about medium but depends on the attack.

Threat 5: Ransomware
A ransomware attack has a very high probability and a very high potential damage. Ransomware is since many years one of top highest IT security risk. Such an attack is easy to perform via the internet and can cause very much damage, because it can infect the whole system. Often, the system cannot be decrypted and need to be installed completely new. Maybe even the backups can be infected.

[1] CSI Annual Computer Crime and Security Survey, 2010/11