TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber security and the responsibilities of boards

Traficom publications
2/2020

Table of contents

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland
ISBN 978-952-311-465-4
ISSN 2669-8757

Introduction

Corporations have become increasingly dependent on digital services and systems. Simultaneously, they face an increasing swarm of cyber threats. A well-designed cyber security solution can help shield company's operations and ensure that it will be able to utilise the benefits provided by digital technology in every domain of its business. The key mission of any corporate board is to promote the things that will be of benefit to the company. This is why its members must also possess an adequate level of understanding of the nature of cyber security and the associated risks to the company's business.

The purpose of this guide

This guide will provide you with the tools that a company's board of directors needs as well as the necessary support for improving the cyber security of your organisation. This guide does not focus on any individual technological solutions as such, but it rather has been designed to help the members of board to ask the right key questions from company's heads and staff.

This guide is meant specifically for the board members of large and medium-sized organisations, but the people responsible for cyber security, in a company of any size, can use it as an everyday cyber security tool too. In practice, this guide can be useful to companies of all sizes and in every area of business.

The structure of this guide

This guide presents a general introduction to cyber security, and its individual chapters focus on various thematic aspects from the perspective of both the board and the organisation at large. The parts of this guide:

- explain what cyber security is and why it should be taken seriously
- provide operating models that can be used by boards and organisations
- present the key questions that a board can review within its organisation.

Chapter 2 contains an introduction to cyber security and some examples of the most common types of threats. Chapter 3 provides guidance on how to assess your organisation's current state. Chapters 4, 5 and 6 focus on risk management, understanding the threats that an organisation may face, and the responsibilities and processes used to promote cyber security. Chapters 7, 8 and 9 present the operating models that a board can use to promote the enforcement and development of cyber security within its organisation. Chapters 10 and 11 focus on collaboration and how one can plan for various crises.

The end of the guide includes appendices that describe the key legislative texts and official responsibilities related to cyber security.

This guide has been prepared by the National Cyber Security Centre of the Finnish Transport and Communications Agency and the Digipool of the National Emergency Supply Agency. Anne Berner, Satu Koskinen, Harri Pynnä, Tuija Soanjärvi and Juhani Strömberg provided their comments for the draft version of this guide. This guide is based on the Cyber Security Toolkit for Boards, which is published by the NCSC-UK.

For more information and guidance on cyber security, see the website of the National Cyber Security Centre of the Finnish Transport and Communications Agency: https://www.kyberturvallisuuskeskus.fi/en/

PART I

What is cyber security?

Cyber security remains a fairly new and undefined concept. In practice, it refers to the new types of security-related challenges that have affected organisations and society at large as digitalisation has progressed. In this guide, cyber security refers to the measures that an organisation can use to protect its critical business systems, software, devices and data communications networks against any cyber threats.

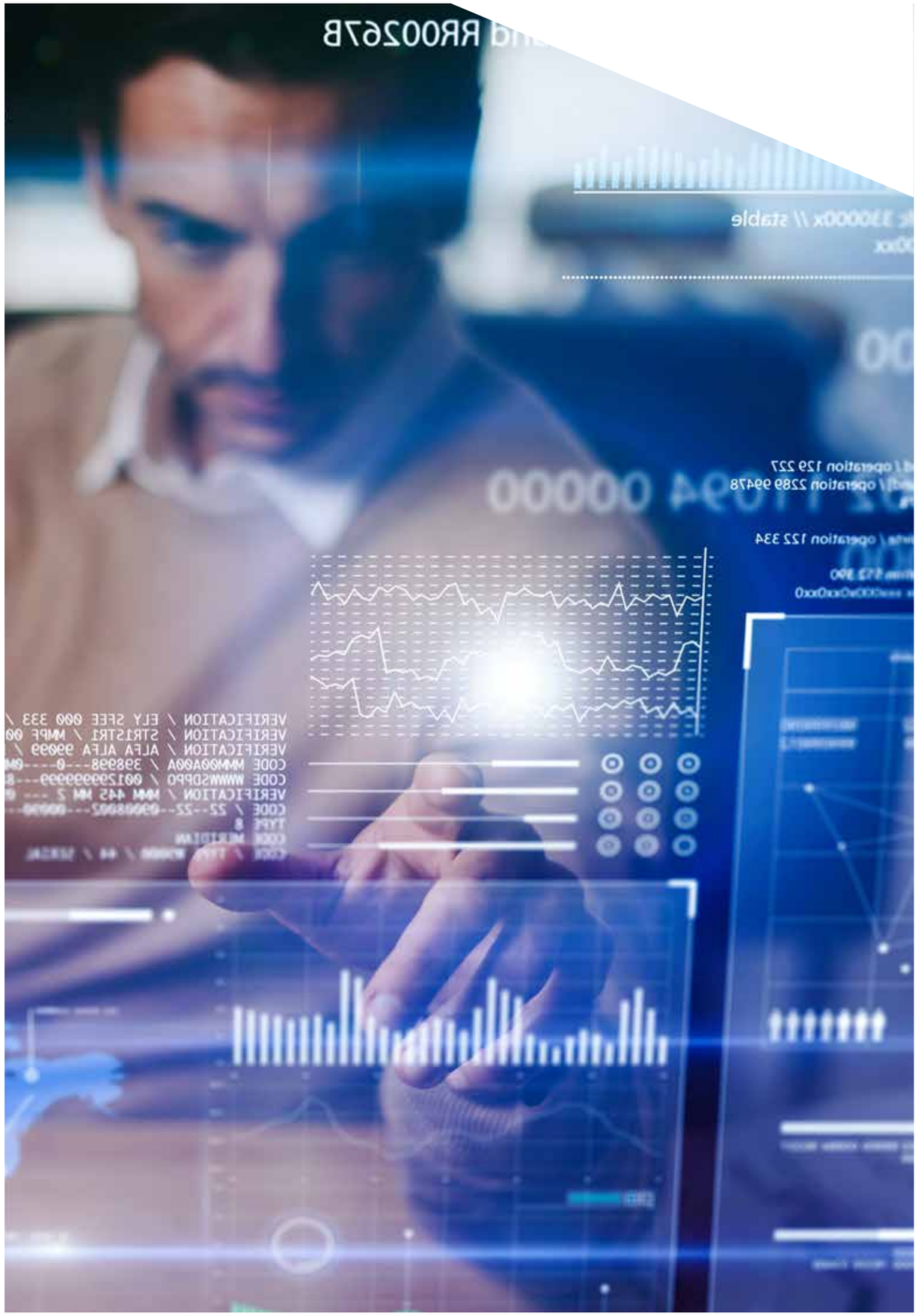
Cyber threats are harmful events or processes that can affect an organisation's operations, finances, data and, at worst, the continuity of its business.

Examples of cyber threats

Phishing

The objective of phishing is to gain access to user ID and password pairs or other data that is valuable to a user or organisation, such as payment card data. For example, users can be tricked into visiting a scam internet page that resembles the actual login page of a service that

An example of an Office 365 phishing email



they use. Once the user enters their data into the scam site, the data ends up in criminal hands. This data can then be used in many ways depending on the criminals' motives and the organisational roles or duties of the person whose data has been compromised.

Usually, the goal of the perpetrators of this type of crime is to gain access to as many email IDs as possible. After this, they can log in to the accounts and search for keywords that are related to invoices and billing activities. Based on this information, they can create fake invoices that utilise the information and contexts presented in the actual invoices that they have gained access to.

The affected account can also be used to create new phishing emails that are then sent to the victim's contacts. Stolen user IDs, on the other hand, can be used for corporate espionage. Data processing-related activities can also expose victims to reputational and regulatory risks.

Phishing scams are especially common in Microsoft Office 365 environments. It is a very popular service in Finland, and not all organisations understand its security mechanisms well enough.

Several hundreds of Finnish organisations have fallen prey to Microsoft Office 365-related phishing scams. The damages caused by phishing crimes amount to several millions of euros.

As a board member, you will be privy to all kinds of data that could be of interest to criminals. This is why you may end up being targeted by cyber criminals. For example, an attacker may attempt to ascertain your user IDs and passwords or impersonate you in an email. After this, they can send a scam email to your organisation's financial unit and direct them to pay a forged invoice.

Example 1

Algol Oy, which specialises in technical trade, became the victim of a shrewd Office 365 hack. Based on log details, the unknown thief was traced to Sweden, where they managed to break in to the company's email system. From there, the thief sent forged yet suitably believable order confirmation and payment detail emails to the company's financial department. The result of this scam was a 140,000-euro transfer that was sent to the scammer's bank account. These losses could have been far greater if the scammer's bank in Hong Kong had not prevented another payment from going through.

Example 2

The Office 365 cloud service used by a Finnish financial corporation was broken into with the help of a phishing scam. Two of the company's employees were sent an email that contained a link to a phishing site. The scammer then monitored the company's email traffic for several months and set up new email forwarding rules without anyone in the company noticing. This prevented the company from determining how long its emails had been monitored or what types of data had been leaked from it.

In addition, the scammers had also attempted to add new invoices to the company's payment transactions, which, had they been paid, would have transferred the funds to the scammers' bank accounts. The invoices utilised the information available in the company's other emails to make them look as authentic as possible.

Malware

Malware is computer software that is used to cause unwanted events in computer systems or their parts. Usually, malware is spread through email attachments, websites infected with malware, and vulnerable servers. Some malware may be almost harmless, but an increasing number of malware applications have been used to cause serious harm.

One recent example of a worldwide malware phenomena is Big Game Hunting. The term refers to a scenario where a criminal targets especially lucrative and cash-rich organisations.

In this type of attack, the criminal penetrates the systems used by an organisation and infects its network. After this, the criminal will initiate an encrypting ransomware program that will slow down and hinder the organisation's operations or even paralyse them. Finally, the criminal will ask for a ransom in return for decrypting the organisation's files. As the name of the attack suggests, the attacker will aim to find any targets that have plenty of funds at their disposal. A company that has a large number of users or customers can also make for an attractive target.

Example 3

The National Cyber Security Centre is aware of numerous cases in Finland where ransomware infections have caused significant financial harm to organisations. These damages were caused by the interruptions to the companies' business activities and the time spent returning their IT systems back to operational condition. At least one Finnish company was forced to fold its business operations in their entirety, as rebuilding the ICT infrastructure that the ransomware software destroyed would have proven far too costly.

DoS attacks

DoS (Denial of Service) attacks have become an everyday occurrence on the internet, and thousands of them are committed in Finland every year. In a DoS attack, a server is bombarded with maliciously generated traffic. The objective is to paralyse some specific service or information system. Oftentimes the target of the attack will be the public website of some organisation or a service used by its customers. DoS attacks usually last for as long as they have an impact on the operations of the attacker's intended target. The effects of the attack usually cease once the DoS attack has been prevented and the affected service has been returned back to operational condition. However, in such situations the attacker often simply changes their target and continues their attack against another service belonging to the same organisation.

Most cyber threats are not targeted against any individual organisations. At its core, cybercrime is a fairly opportunistic form of crime. The usual objective of such activities is to discover any weaknesses in an organisation's systems and processes that could be used for criminal purposes. Cybercrime is often international in scope and largely automated in nature. Like most criminals, cyber criminals are usually only interested in quick monetary gains.

Most cyber threats are not targeted against any individual organisations.

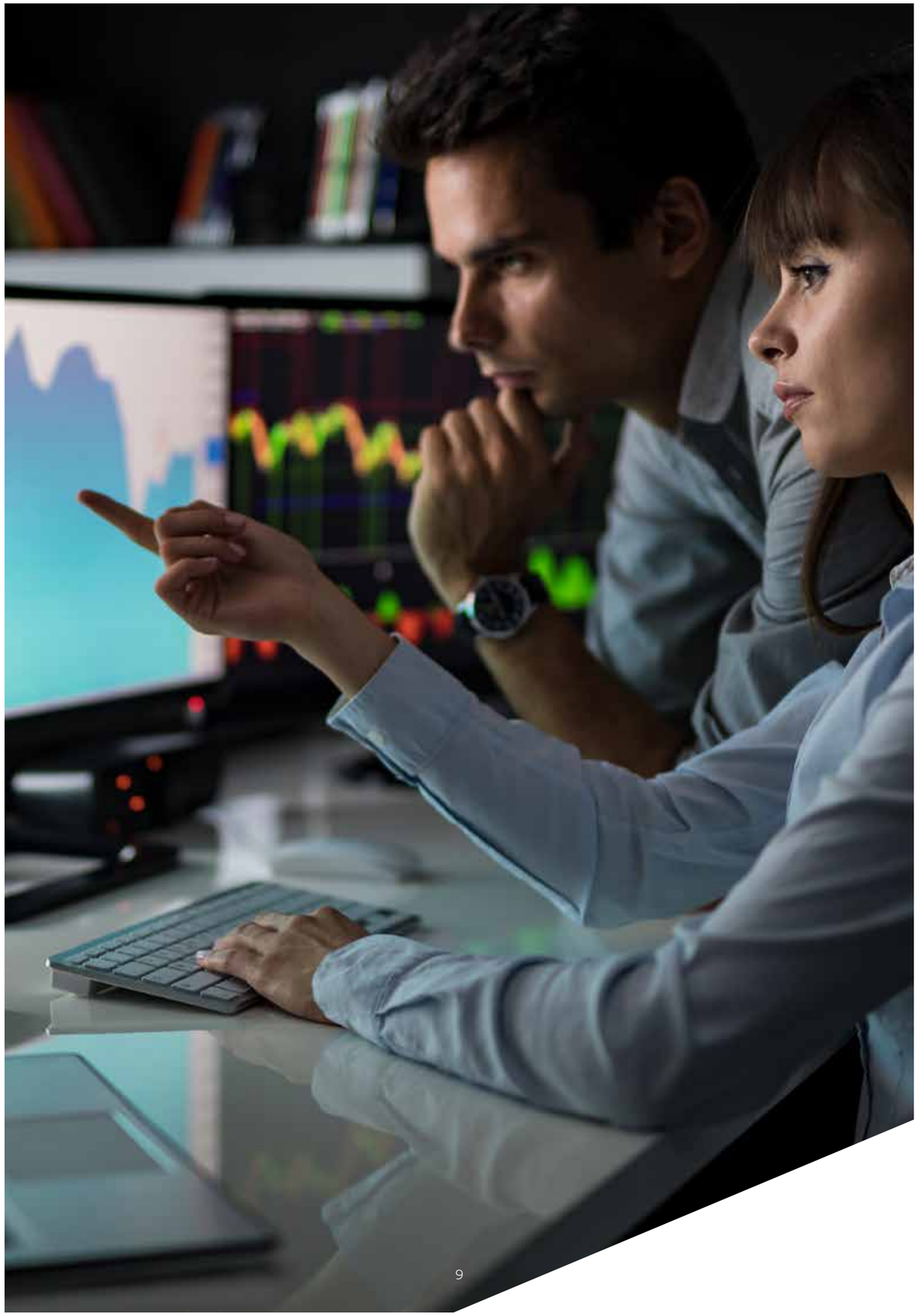
And, on top of it all, a significant number of cyber attacks are implemented using the simplest tools. These include various types of scam emails that are used to harvest an organisation's user IDs and passwords. This is why you can improve the cyber security practices used by your organisation with the help of fairly simple methods, such as training your staff on how to identify any would-be scams.

Organisations must develop their cyber security practices in a diligent and risk-oriented manner. The required measures may be both technical and non-technical in nature. The duty of every board is to ensure that the organisation that it serves is suitably well-versed in the necessary cyber security practices. The management of said organisation, on the other hand, must be aware of the necessary factors and information that will allow it to make the best and most effective decisions.

Example 4

From the perspective of internet networks, most DoS attacks will seem like normal online traffic, and only the target of the attack can truly determine whether it is really being attacked. DoS attacks cannot be prevented in their entirety, so organisations should prepare for them in advance and determine the best methods for preventing them with their internet service providers. Your organisation could also end up as a collateral victim of a DoS attack if, for example, an attack is targeted against the hosting service used by the intended target.

Several Finnish organisations are targeted by DoS attacks every day, and the risk of such attacks must be included in your risk assessment. If the services provided by your organisation need to be available online on a 24/7 basis, you must also have a plan for DoS attacks. In addition, you should prepare for them well in advance.



PART II

Assessing the situation of your organisation

Your organisation must assess which parts of its technical environment (systems, data, services and networks) are the most critical for ensuring the success of its goals. In addition, your organisation must be aware of the parts that actually comprise its technical environment.

Your organisation should define the parts of your technical environment that are the most critical for achieving your business objectives.

What can the board do?

Assess key issues

Much like with business risks, an organisation can never remove every single cyber security risk that it may face. However, the organisation's board must ensure that, first and foremost, the parts that are key for the organisation's business objectives have been protected.

The board must also assess the risks that the organisation may face on a wider scale. For example, an organisation's management and board may be aware that a specific partner is vital for the organisation and that endangering the data of said partner could prove catastrophic for the organisation's finances and reputation. The parties responsible for an organisation's cyber security must always be informed of these types of risks.

The board, management and experts of an organisation must always communicate with one another, as the organisation's management and board may be aware of certain business factors that the organisation's technical experts do not know. An example of this type of information is the order in which an organisation's partnerships have been ranked. The technical experts, on the other hand, may be aware of the prerequisites necessary for achieving the organisation's key goals. This type of information includes the systems or data that the organisation's partners depend on.

An organisation's most important business factors are vital to its success. They may be valuable simply because the organisation would not be able to function without them. Endangering an organisation's business factors may also expose it to reputational or financial harm. These types of factors include:

- the personal data that an organisation is in possession of
- an organisation's intellectual property rights
- public websites
- industrial control systems
- the user and access systems used for internal networks.

What can your organisation do?

Assessing the initial situation

Assessing your initial situation is important, as it will allow you to determine the security measures that your organisation needs and which of them it will be able to implement. The following details are especially important for this process:

- which of your systems are interconnected
- who has access to specific data
- who owns which network or service.

Collecting all of this information will allow you to, for example, update any vulnerable systems and protect your organisation from attacks. This information may also be needed whenever you need to react to an attack. This way, you will be able to assess the type of damage that an attacker could inflict or the effects that any corrective measures could have.

Understanding your environment in its entirety may prove to be challenging, especially if the networks and systems used by your organisation have grown organically over time. But understanding even just the basics, such as the systems that are used in your organisation's networks, will help you initiate the necessary measures.

Defining critical technical resources

Your organisation should define the parts of your technical environment that are the most vital for achieving your business objectives. For example, your organisation may place special emphasis on taking care of long-term customer relationships. You can support this objective by, for example, using your cyber security measures to protect your customer data, ensure the functionality of your order-delivery system, and secure the availability of your organisation's website.

Collaborating with service providers and partners

Most organisations have service providers or partners from which they receive, distribute or deliver information, systems or services. Every organisation must include these external service providers and partners in their risk management practices. One key method for achieving this is to agree on any cyber security-related obligations and rights with your partners.

Think about the following questions

Do we, as an organisation, understand how our technical systems, processes or resources promote the realisation of our objectives?

The following questions will help you define these dependencies:

- What are the critical technical resources without which our organisation would not survive?
- What obligations must we fulfil (e.g. legal or contractual obligations)?
- What are the things that we do not want to happen and how could these come about?
- Does our organisation employ a process that will identify the important systems, data and services and monitor their functionality and security?

Has our organisation communicated its most important objectives in a clear manner and have we ensured that these priorities are also used to guide our cyber security measures?

- Your cyber security measures must support your organisation's strategy. Your guidelines for cyber security, such as your strategy or policy for cyber security, must also be able to safeguard your organisation's strategic objectives.

PART III

Risk management and cyber security

Many organisations conduct risk assessments purely for the purposes of satisfying specific requirements. These include the following:

- obligations related to external factors, such as regulatory requirements
- customer demands
- legislative requirements.

However, if your assessments are based on these factors alone, your risk management processes may end up amounting to ticking the necessary boxes on a checklist. In such situations, an organisation may think that it is able to manage the risks it could face, even though it has only acted in the manner required by specific processes.

Compliance and security are not the same thing. They may overlap, but one can comply with general security requirements while still using weak security practices. Good risk management goes beyond mere compliance.

Good risk management goes beyond mere compliance.

What can the board do?

Include cyber security in your organisation's risk management processes

Cyber risks must become a part of your organisation's everyday risk management practices. When you place cyber risks in a separate category or classify them as mere 'technological risks', you make it harder to identify the impact that they may have. At the same time, it may become harder to identify how your organisation's other risks could affect its cyber security.

Your cyber security measures must support and promote your business by helping you manage the risks related to your use of digital technology. However, they should never prevent or hinder the processes that are key to your business or result in any excessive costs.

Never measure your success by how much you have mitigated your risk level

It can also be difficult to measure the success of your measures. Typically, the success of your cyber security policy is defined by how seamless your operations are. This, however, is difficult to measure, as a disturbance can also be related to matters beyond your organisation's cyber security measures.

Risk assessments typically present some estimate of a risk's likelihood and effects (e.g. large - medium - small). You may feel tempted to utilise these types of assessment methods for measuring the success of your policies. However, you should remember that these types of assessments may only measure a fraction of the measures that an organisation has implemented. This is because cyber risks are influenced by external factors, such as software vulnerabilities, that can change rapidly and are often beyond a single organisation's control.

Some examples of the indicators that can be used to assess different measures are presented in more detail in the chapter 'Implement the necessary measures'.

What can your organisation do?

Apply the same risk management principles to cyber risk management as you would with any other types of risks. However, please keep in mind that cyber security solutions and technologies develop at a rapid pace, and if you are not careful, you may end up utilising outdated methods when assessing your cyber risks. We recommend assessing cyber risks at more frequent intervals than other risks.

Cyber security is still a fairly new term with many different definitions. It may be the case that your organisation does not have the same level of understanding of cyber risks than what it does of the risks to its financial performance or the occupational safety of its staff. Your organisation may also lack a knowledge base that it can use to assess its cyber risks. These factors should be taken into account when evaluating the reliability of your cyber risk assessments – especially in such circumstances where the results of these are compared directly with "traditional" risk assessments.

Think about the following questions

Does your organisation employ a process that can be used to ensure that its decision-makers are provided with the most comprehensive information possible?

- This process must focus primarily on ensuring that your organisation's decision-makers can utilise the best possible information that is available to them at the time. These decision-makers include your board, management and other employees in your organisation. Both the board and the implementer of the measure must be provided with as much understandable information as possible to support the decision-making process.
- This is why all risk assessment results must be parsed according to their significance. Most of the time, qualitative results are better than numerical scores that have been generated using some set of arbitrary figures and multipliers.

Does your organisation employ a process where the assessment of cyber risks is linked to the assessment of business risks?

- Do you assess your cyber risks as part of your business decision process, or as part of any other decisions for that matter?

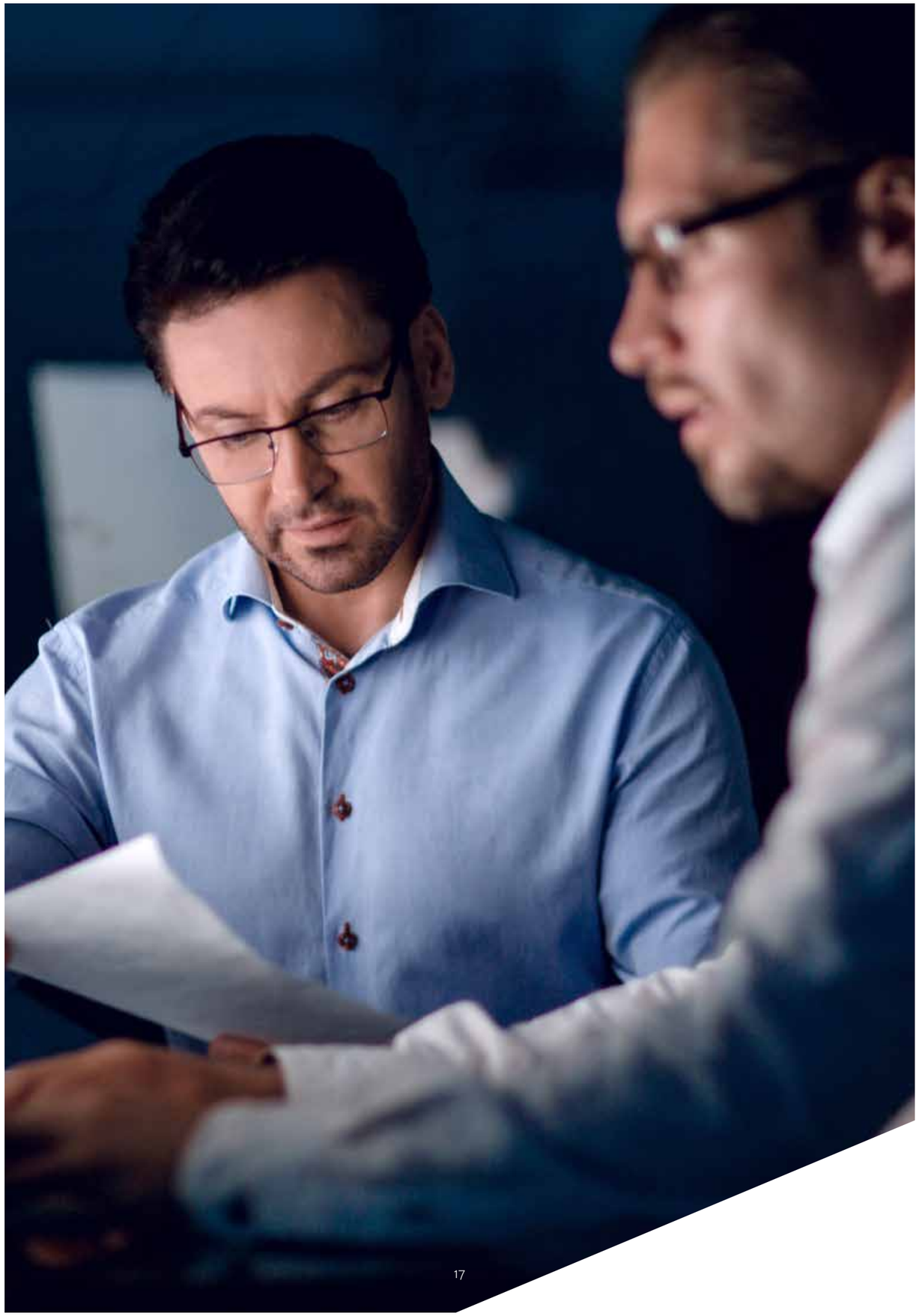
Does your organisation utilise an efficient and appropriate approach for managing its cyber risks?

Your board and the other actors in your organisation must be able to present your process within the span of a few minutes and in a clear and simple manner, for example with the help of the following information:

- How are risks escalated?
- What is the threshold for the board's participation in decisions concerning risks?
- How often are risks assessed?
- Who is responsible for which risks?
- Who is responsible for the risk assessment process and for evaluating its appropriateness?

Have your board and management clearly defined how your organisation manages risks

- Are your risk reporting processes easy to understand?
- Have you assessed and compared the different types of risks that you may face? Have you communicated the significance of these different risks to the rest of your organisation? For example, an organisation may accept the risk that its email service may occasionally be out of order for a day, but it can never accept the risk of any personal data being leaked from its databases.
- Have you taken cumulative risks into account? How will your organisation respond if two or more risks occur at the same time?



PART IV

What are the threats to our organisation?

When you understand the threats that your organisation and partners face, you can also determine the cyber security measures and investments that you need. Every organisation must make a conscious decision on which threats it will aim to shield itself from, otherwise it may end up trying to defend itself from every possible threat. This in turn can lead to the adoption of inefficient measures.

What can the board do?

Understand the threat you face

When a board understands the true nature of the cyber threats it may face, it can make conscious decisions on how to act. A key part of this process is understanding what drives attackers: Why would they be interested in your organisation in particular? Of course, it is always possible that an attacker is solely motivated by the fact that your organisation has vulnerable computers that are connected to the internet, which the attacker can use for their criminal activities.

Make sure that your organisation is collaborating with others when it comes to your security

Your partners and peer organisations are often good sources of information concerning any threats or best protection practices. By developing your collaborative and information exchange practices, you can significantly improve your ability to shield yourself from cyber threats. Do not think of it as a risk to your competitive edge: shared information can benefit everyone involved.

Assess your risks

By mapping out the most significant risks and possible attackers that you may face, you will be able to make better decisions on which threats your organisation should focus on.

Continuous dialogue between your organisation's management, board and experts will help you prioritise the threats you may face and the precautions you need to take. Your experts understand the technical nature of the threats you could face. The board, on the other hand, is more aware of the factors that could make your organisation into a lucrative target for attackers. In addition, it is vital that you always discuss any such decision in advance that could have a significant effect on your organisation's threat profile. This way your technical experts will have enough time to implement the necessary precautions for shielding your operations.

The National Cyber Security Centre recommends that all organisations actively exchange information with one another. The Centre is responsible for maintaining sector-specific Information Sharing and Analysis Centres (ISACs) that serve this very purpose. Make sure that your organisation is an active participant in any information exchange groups that focus on cyber security, for example by participating in the ISAC of your sector or in some other information exchange-oriented group. For more information on ISAC activities, see the following page: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management

What can your organisation do?

Do not underestimate untargeted attacks

In an untargeted attack, the attacker seeks to impact thousands of potential victims at a time instead of a single target. In such situations, the attacker will usually employ an automated and generally available tool to, for example, scan public websites or other services for any vulnerable systems or services. Once one has been found, the same tool will automatically exploit this vulnerability to hack into the system, for example. The effects of this type of mass-scale attack can be as devastating as in a targeted attack. However, a good level of cyber security will help shield your systems from most untargeted attacks.

Obtain good situation awareness information and use it

To make decisions that will help guide your operations, you will need situational awareness information that focuses on cyber security. There are several operators on the market who can provide you with this information. Their selections vary from general annual reports to technical papers that focus on individual malware applications. The National Cyber Security Centre is one such operator that produces an annual report on the general status of cyber security in Finland https://www.kyberturvallisuuskeskus.fi/en/

Think about the following questions

Which threats are the most significant for your organisation and why?

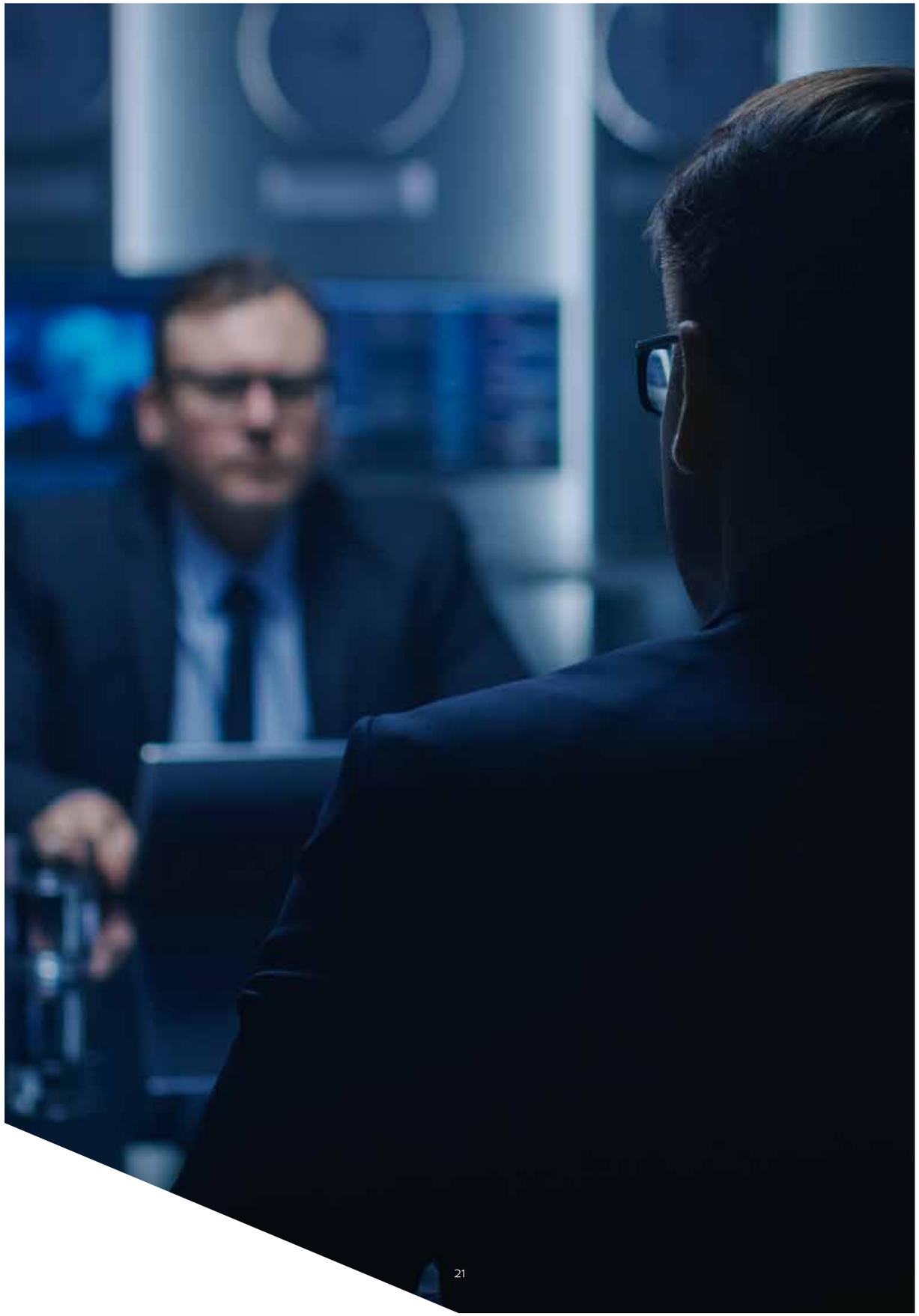
In your assessment:

- define the possible effects of the threats and the likelihood that they will target your organisation
- define the types of risks that your organisation is willing to tolerate
- utilise the knowledge that your organisation has gained from any previous attacks that it has faced.

How can our organisation stay informed of any new cyber threats?

Your organisation can:

- look for evidence of any attacks in its system log files, if such exist
- utilise different situation awareness products (e.g. the situation awareness products provided by the National Cyber Security Centre)
- participate in information exchange activities (e.g. in an ISAC)
- adopt measures that it can use to distribute information internally on key cyber threats.



PART V

Cyber security as part of your organisational objectives

Cyber security is a key element in the implementation of your organisation's objectives, and it is also being increasingly regarded as a competitiveness factor. This requires that your organisation believes in a culture of cyber security, invests in your cyber security practices and utilises the appropriate measures in its management.

What can the board do?

Cyber security is a factor that affects both the objectives and risks of an organisation

Cyber security has comprehensive effects to an organisation. Because of this, it should be part of organisation's risk management and decision-making practices, so that it can be properly managed. For example:

- Cyber security will most likely have an effect on an organisation's operative risks, as most organisations rely on the security of the digital services they use (email services, software suites, etc.).
- Cyber risks are linked to legal risks, such as contractual terms that protect a partner's business information or statutory requirements for specific data processing methods.
- Cyber risks can also become financial risks. Some examples of these include being deprived of your funds in an online scam or the losses caused by a cyber-attack-induced outage to the services you provide.
- When you employ a good level of cyber security, your organisation can take on calculated risks and fully utilise any new technologies that are available to you.

Your cyber security practices should be an intrinsic part of your organisation's activities. Achieving a good level of cyber security requires not only functional technical solutions but also personnel who are trained and fully committed to good information security practices.

Your organisation can prevent an attacker from gaining access to any sensitive data and ensure that only personnel who have a current and a verified need to do so, can access the data. In such cases, your organisation must make sure that:

- The technical solution uses to store said data is appropriate.
- The staff who process said data are trained in how the processing is to be done.

What can your organisation do?

Your cyber security practices affect your entire organisation – not just your information management unit. This is why your cyber security should never be the responsibility of a single individual. For example, a successful cyber attack can affect your online sales and contractual relationships or lead to legal or regulatory consequences. Your board must be knowledgeable enough to lead your organisation's cyber security policies.

Involve experts

Think about whether your board is provided with the information it needs on the cyber security of your organisation. It is vital that the person responsible for the cyber security of your organisation can easily communicate with your organisation's management and that all reporting on cyber security is arranged in a functional manner.

Think about the following questions

Do we understand how cyber security affects the responsibilities of the board and management? Focus on the following issues:

- Does the board have enough expertise to understand the significance of cyber security for the business and strategic objectives of our organisation?
- Who is responsible for monitoring our cyber security?
- Have we expressed in a clear enough manner the information that the board and management need on cyber security?

Who is currently responsible for our cyber security? This responsibility should have been given to an appointed person. Focus on the following issues:

- How does this person keep in touch with the board? Does this person report directly to the board or do they participate in some other type of reporting process? Does this encourage the board to actively participate in discussions concerning cyber security?
- What are the person's objectives and who sets them? Do these objectives promote cyber security in a manner that benefits the entire organisation?
- Is this person able to reach the necessary people for ensuring the efficiency of your cyber security? At its simplest, this means having enough people whose job it is to work on your cyber security. This can also refer to the other parts of your organisation, such as your HR and financial departments.

How can the board ensure that the cyber security solutions employed by our organisation are efficient enough? The board should check that:

- Your organisation has been provided with the appropriate technical security solutions and that the results of said solutions are reported to the board in an understandable manner.
- Every threat assessment and necessary precautionary solution should be checked regularly, and any precautions should be updated as necessary.

Does our organisation employ a process that will ensure that cyber risks are included in the list of risks to our business?

- Does your organisation utilise a process to mutually assess any specific operation-specific risks and impacts? Has your organisation made a decision on, for example, the use of personal devices, such as mobile phones, in work-related matters? This can increase efficiency and flexibility, but it can also decrease your organisation's insights into the cyber threats that it may be facing.

PART VI

Security culture

Organisations often focus on the technical aspects of cyber security without paying any attention to the needs and everyday work habits of their employees. This type of approach rarely leads to a successful outcome. If an official policy makes it harder or slower to work, people will often begin looking for shortcuts and unsanctioned work methods to circumvent these obstacles. It pays to understand that your staff will never commit to your cyber security objectives without a good security culture.

Some organisations consider their staff the "weak link" of their cyber security efforts. We must rid ourselves of this type of attitude.

What can the board do?

Lead by example

Your board and management can have a significant effect on how other people think about these issues. It might be that your upper management is not complying with your security practices and processes. They may also receive preferential treatment, such as access to devices that deviate from your organisation's IT policy. This could lead to a situation where the rest of your organisation will think that the rules are not meant to be followed, and that bypassing them could even be considered an appropriate course of action.

If the management and board members of an organisation do not comply with the organisation's practices, it is unlikely that anyone else will follow them either. If some practices are having an adverse effect on your organisation, they should be changed into something more functional.

Developing a new type of culture takes time and mutual effort. The attitude towards security that your board and management want will not spread automatically within your organisation.

What can your organisation do?

Place your staff at the centre of your security

Some organisations consider their staff the weak link of their cyber security efforts. We must rid ourselves of this type of attitude. Implementing an effective policy of cyber security requires balancing every single factor involved – and not just assuming that people will bend to every technological requirement. If your staff is circumventing your operating models, this may be a sign that your practices or processes need to be checked again.

A trained and well-honed staff plays a key role in the detection of any security deviations.

Your organisation must ensure that your staff is willing to report any threats and deviations they may have detected. In addition, your organisation must utilise a clear set of processes for reviewing these reports.

Towards a culture of openness

Make sure that your staff has been encouraged to discuss and report any concerns that they may have. At the same time, you must also ensure your staff that this will lead to the appropriate measures and that the process will not include any search for a guilty party. This will allow your staff to focus on developing the security of your organisation instead of having to focus on how to best protect themselves.

Think about the following questions

How can the members of a board and management provide an example?

- Make sure that your employees feel that they can have an effect on the safety of your organisation and that they have the tools to report any security-related concerns.
- Commit to the decisions concerning safety that you have already made, follow them, and highlight any inefficient practices together with your staff.
- Make sure that your organisation has an open and positive channel of communication with its employees regarding the importance of cyber security.

Does our organisation have a good security culture? Here are a few signs that may indicate that you have a good security culture:

- Your staff knows how and where to report about any concerns or deviations. They also feel that they are encouraged to submit reports.
- Your staff is not afraid of any negative consequences should they report about their concerns or any deviations.
- Your employees feel that they may question any existing operating models in a constructive way.
- The views of your staff are truly utilised when you shape your security practices.
- Your staff understands the importance of cyber security and what it means to your organisation.
- Instead of failures, your reports and internal communication channels focus on success stories (for example, a report can focus on the number of people who reported the phishing emails they received instead of the number of people who fell for them).

PART VII

Cyber security expertise

There is an increasing demand for cyber security experts, which has made it challenging to meet the hiring-related needs of many organisations. It is vital to recognize and to focus on the type of expertise that you will need now and in the future. This includes planning on how you will be able to acquire said expertise.

What can the board do?

Understand your organisation's current situation

Does your organisation have an information security manager or director? How about an information security group? Any persons in charge of incident management? If not, then should it?

This information will help you assess your organisation's level of cyber security competence. This information will also help you understand where the information that the board has received on your organisation's cyber security came from.

Your board should also think about its own level of expertise. Does your board feature enough expertise to ensure that it will be able to make the appropriate strategic decisions concerning your cyber security? Will your board be able to keep up with the latest technological advancements that will also present new challenges to your cyber security?

According to the Global Information Security Workforce Study, Europe will face a shortage of 350,000 cyber security experts by 2022.

What can your organisation do?

Formulate a plan

Your organisation must assess which types of cyber security expertise it needs. Cyber security covers a wide range of skills and areas, from data network security to risk and deviation management, just to name a few. First, you should focus on the skills that your organisation needs to reach its most crucial objectives and manage its most relevant risks. After this, you can assess which of these skills cannot be outsourced.

Define how quickly your organisation needs to acquire these skills. If your plan is to develop the expertise of your current staff, remember that attaining an adequate level of expertise will take time. Participating in a single course will not turn someone into an instant cyber security expert – you must allow your staff to develop their practical skills as well. If you need to quickly bring in a new level of expertise, the best solution may be to hire a consultant or an expert.

Think about the following questions

What sort of cyber security expertise does our organisation need and what type of expertise do we already have?

- What type of expertise does our organisation need to manage its cyber risks? Which tasks should we keep in-house and which should we outsource?
- What kind of expertise should every staff member in our organisation have on cyber security? How comprehensively and often should we train our staff on our security practices? And on the special threats that our organisation may be vulnerable against?

What kind of plan does our organisation have in place for the development of any missing areas of expertise?

- Who is responsible for the development of cyber security expertise? Is this development work based on a plan and who is/are responsible for its implementation?
- Where can we find the people we need? Do they work in our organisation or should we acquire the skills we need through outsourcing, for example?
- How can the board support this work?

Does the board have enough knowledge and expertise to make the right decisions on cyber security?

- Does the board adequately understand the cyber security decisions that are made in our organisation?
- If not, then how could the members of the board improve their understanding?
    - You can start by reading the introduction to part 2: “What is cyber security?” in this guide. Many operators also provide training sessions on cyber security that have been designed specifically for board members.

How can we ensure that we have the right staff who will be able to solve our future cyber security challenges?

- Are we receiving the information we need on our organisation's cyber security-related expertise and recruitment needs?
- Are we focusing on a versatile selection of recruitment channels?

PART VIII

Monitoring your measures

Implementing even the simplest measures can help alleviate the likelihood or impact of any deviations.

What can the board do?

Take a few minutes to familiarise yourselves with the latest technological advancements

By having a basic understanding of cyber security, you will be able to ask the right questions that will then allow the members of your board to determine your organisation's true maturity in cyber security. You can begin by discussing your current cyber security measures with the experts in your organisation. The questions below will provide you with a general idea of the types of questions you should ask.

What can your organisation do?

Begin with the basics of cyber security

Many attackers use the same types of publicly available applications and methods, most of which are preventable with a basic level of cyber security controls. Several frameworks exist for determining the basic-level controls of good cyber security practices. These include, for example, the ISO/IEC 27000 information security standards and the NIST (National Institute of Standards and Technology) Cybersecurity Framework. In 2020, the National Cyber Security Centre will publish a set of national assessment indicators that an organisation can use to evaluate the maturity of its cyber security practices.

Tailor your measures according to your key risks

Basic-level cyber security controls will help prevent the most common cyber attacks. Once you have defined and achieved your basic starting level, you should implement the necessary measures for managing your top-priority risks. These measures must be tailored to your organisation's business objectives, technical environment and threat profile (shielding yourself from specific threats and/or attackers).

A multilayer information security architecture can help an organisation prepare for situations where an individual area may fail or an attacker gains access to a single layer, since the attack will be halted by the following layer of security. Organisations should focus implementing several different measures at once that, when used together, will help alleviate the impact of any cyber threats. Once an organisation has defined its objectives for cyber security, it can focus on adding enough protective layers to the most important parts of its operations.

The National Cyber Security Centre's HAVARO system can detect and warn organisations about any serious information security violations. These include, for example, information security threats that could affect an organisation's finances, the data in its possession, or the continuity of its business activities. For more information on the HAVARO system, visit https://www.kyberturvallisuuskeskus.fi/en/havaro-service

Remember to also shield yourself from internal threats

Your security measures should not stop at the border between your organisation and the internet. Any good security practice will always be based on the assumption that an attacker could penetrate your organisation's internal network at any time. By securing your internal network, or intranet, you will be able to minimise the damage that an attacker could cause.

One key practice for achieving this is identity and access management. The most common methods include efficient user access management and segmenting your organisation's network into different parts. By being able to quickly detect any outside parties in your system, you will be able to minimise the potential damage that an attacker could cause. The collection and monitoring of log data are crucial for the detection of these types of adverse activities.

These measures will also help limit any internal threats. This refers to any persons who have been granted access to your systems but who still intend to cause harm to your organisation. This type of threat can vary from an unsanctioned action committed by an individual employee to systematic corporate espionage.

Check and assess your measures

Good cyber security focuses on continuous action that includes the availability of information that is both correct and sufficient, decisions that are based on knowledge, and the measures used to alleviate risks. Your organisation must assess and adapt its protective measures to the changes in your organisation and its threat profile. This is why it is vital that you also have the correct tools at your disposal to assess the effectiveness of the measures that your organisation has implemented.

The effectiveness of your measures can be assessed in various ways, for example by testing the security of your networks and services (so-called penetration testing) or by judging the functionality of your processes. You can also combine internal assessment measures with external assessments.

By involving your staff, you can gain a better understanding of the effectiveness of the measures that have been implemented in your organisation. This will also provide you with valuable information on how you could improve your practices or processes. With the help of various instruments and indicators, you will be able to detect the areas in your organisation that need to be changed or developed further.

Think about the following questions

How does our organisation ensure the efficiency of its measures?

To achieve this, your organisation can utilise the following example measures:

- Penetration testing by an outside organisation and the development measures implemented on the basis of its results.
- The automated testing of all security measures, logging all network activities, and monitoring said logs.
- Assessing any implemented measures with the appropriate frameworks. This assessment can be conducted either internally or by an independent consultant. Some examples of applicable frameworks include the ISO/IEC 27002 standard, the NIST Cybersecurity Framework, and the national assessment indicators provided by the National Cyber Security Centre.
- By ensuring that any threat assessments and cyber security-related focus areas are checked regularly and the appropriate security measures are updated whenever necessary.
- By ensuring that the focus areas for cyber security measures are matched with the risks that have been defined and emphasised by the board.

What measures has our organisation implemented to minimise any potential damages that could be caused by an attack?

Make sure that your organisation has considered at least the following questions:

- How are your users and devices verified and how are they granted access rights?
- How will you be able to detect any intruders in your network?
- Have your organisation's networks been separated from one another so that a potential attacker cannot use one device or network area to access your organisation's other network areas?

How is our organisation protected from phishing attacks?

- We filter or block any incoming phishing emails.
- We ensure that all outside mail is marked as such.
- We prevent attackers from forging any company emails.
- We help our staff identify any suspicious emails and report them.

How does our organisation monitor how the access rights of any technical user accounts are used?

- We apply the principle of minimum access in the creation of staff accounts.
- We limit the impact of any attacks by monitoring all authorised user accounts.

What measures does our organisation use to ensure that our software and devices remain up-to-date?

- We have defined the processes that will help us detect, classify and correct any available vulnerabilities in our technical environment.
- We have prepared end-of-life plans for any devices and software that are no longer supported.
- Our network architecture has been designed to minimise the damages that an attacker could cause.
- We utilise third-party or cloud services whenever appropriate and focus on the areas that we can influence the most.

How have we implemented our user identification and system and data access policies?

- Our organisation complies with good password practices.
- Our organisation utilises two-factor authentication whenever possible.

PART IX

Collaboration

Cyber security is a key issue whenever you collaborate with any service providers or partners. This is because:

- You increase the number of external attack routes as you increase the number of connections and services at your disposal. If one of them is endangered, you may also endanger your entire organisation.
- Your organisation may serve as a penetration route to another organisation that you are providing your services to.
- Someone may attempt to penetrate your organisation through a service provider you use.
- Your organisation may process data that is sensitive in nature or valuable to your partners.

What can the board do?

Include cyber security in the decisions you make

All organisations interact with at least one other organisation. These relationships often include access to the partner organisation's systems, networks or data. Check that the following three issues have been taken into account:

1. Do not provide any attackers with a route that they can use to penetrate your organisation.
2. Every partner and service provider that you work with must process your organisation's sensitive data in an appropriate and secure manner.
3. Every product or service that you purchase must comply with your cyber security practices.

You must take your cyber security practices into account whenever you make a decision that concerns a new relationship or partnership. This includes any decisions that you have made on service providers, suppliers, fusions, acquisitions and partners. Even with your old relationships, you should check that any cyber security-related obligations and responsibilities still remain up-to-date.

What can your organisation do?

Define the level of security that you expect from your service providers and partners and inform them of these requirements in a clear and unambiguous manner.

Check the arrangements that you have made with your current service providers and make sure that the related security requirements have been taken into account. If your organisation is a service provider, you must also meet the security requirements set by your clients.

Make sure that your security requirements are reasonable, proportionate and that they match your estimated risk scenarios. Remember to also take the current state of your service providers into account and provide them with enough time to make any necessary improvements.

Ask for guarantees

From the outset, you must include provisions on security in every agreement that you sign. Your organisation must be able to trust that the agreed security requirements have been met. This can be verified with, for example, tests, inspections or standard-related compliance measures. You should also go through your cyber security maintenance and incident management processes together with your partners.

Remember to consider the consequences of a situation where your service provider is compromised.

Regardless of your security agreements or partners' level of cyber security, your partners will most likely be compromised at some point. Plan the security of your networks, systems and data with this assumption in mind. This type of scenario should also be taken into account in any agreements that focus on security. How will your partners be expected to act? For example, will they be required to report any deviations to your organisation?

Think about the following questions

How can your organisation limit the risks that come with sharing your data, systems and connections with other organisations?

Check that the following have been taken into account:

- Your organisation must understand its service providers well, and it must also be aware of the data and systems that they have access to. In addition, you need to have a process in place that is used to grant and revoke access privileges.
- Clearly define your expectations of how your partners should protect your organisation's data and how they may use your systems.
- From the outset, include provisions on cyber security in every agreement that you sign.

Do the following:

- If your supply chain includes a substantial number of companies, negotiate with your most important service providers on the processes that will guide their subcontracting activities and their reporting obligations to you.
- Select organisations that can demonstrate the safety and security of their activities.
- Minimise the level of access that other organisations have to your services as well as the amount of data that you exchange with them.
- Authenticate and verify any users from your subcontractors before granting them any access rights.

How does our organisation ensure that cyber security is taken into account in all business decisions?

- Check that your security practices are included in your organisation's culture and strategy.
- Make sure that your security policies are always taken deliberately into account in all decisions concerning procurements, fusions and acquisitions.

As a service provider, can our organisation be certain that it is compliant with the necessary security requirements?

- If your organisation provides services to other organisations, your risks are that much greater. Make sure that your organisation is ready to respond to any situation where the customer data that is in your possession has been compromised.

Does our organisation have a well-defined set of terms on the use of service providers? And have we informed the people in our organisation about these terms?

Have the following issues been clearly defined in the strategy and guidelines concerning service providers and procurements?

- What risks is your organisation ready to accept when it uses service providers? For example, the reputational risks caused by exceptional circumstances may be smaller when the responsibility for said circumstances falls to the service provider. However, your financial risk may remain the same even if a service provider is not present.
- What does your organisation expect when it comes to the security practices of your service providers? How much more are you willing to pay for a better level of security?

PART X

When your worst scenario comes true

Security breaches can have a significant effect on your organisation's finances, productivity and reputation. A small deviation can also turn into a cyber security incident that will have a widespread effect on the operations of your entire organisation. You can limit your potential damages by preparing in advance so that you will be able to detect and quickly react to any breaches. This, in turn, will help alleviate the financial and operational effects that a breach could have on your business.

The National Cyber Security Centre wants to assist all Finnish organisations that have become the targets of security breaches. The Centre's contact information is available on the back page of this guide.

What can the board do?

Make sure that your organisation has a plan

Most Finnish organisations have no plan in place for how they will act during a security breach or a serious incident that has been caused by a breach. Make sure that your organisation has a plan for any security breaches or serious incidents.

Understand the role you play in the management of security breaches

I Especially during wide-ranging incidents, the decision-making capabilities of individuals and organisations can often diminish greatly. This is why everyone must be aware of the role they play and their organisation's mode of operation in advance.

The board must make it clear when it expects to be informed of a security breach.

- At what point should the board be informed of the breach?
- And how severe must the breach be before it crosses the reporting threshold?

Participate in exercises

The best way to test an organisation's processes and roles is to practice the management of cyber security incidents. If a person's duties include participating in the management of any real incidents, they should also practice these skills. Participating in exercises together with your staff can help highlight any problems that are related to, for example, your decision-making processes. You can think of an exercise as a crisis situation whose timing and effects are chosen entirely by you. Learning from these situations is extremely valuable. With the help of exercises, you can practice what you have learned without having to face an actual crisis that could harm the operations of your organisation.

Promote a "no-blame" culture

The purpose of a post-security breach analysis is to decrease the likelihood and effects of said breach in the future. The most important point is to be honest and objective about what has happened. This can be done in an organisation whose culture does not focus on placing any blame. Your board should also note that most regulations, such as the General Data Protection Regulation of the EU, lay the responsibility for any security breaches on to the organisation instead of the individual. This is why the board, as a governing body, is ultimately responsible for all deviations in the cyber security of its organisation.

What can your organisation do?

Find out what a security breach looks like

One of the most commonly overlooked issues is the ability to determine what constitutes a security breach. There are two aspects to this:

- how is an event or deviation detected to begin with?
- at what point does an event or deviation become a security breach?
- at what point will said breach become such a serious incident that the situation will require adopting an operating model that deviates from the usual process?

HOW ARE EVENTS DETECTED?

By monitoring, we mean observing the data or logs collected from your networks or systems for the purposes of detecting any such deviations that could indicate that harmful activities are taking place. Even if you do not have any monitoring mechanisms in place, it is still important to collect system and log data, as these can be used to investigate any deviations and create new security measures.

WHEN DOES AN EVENT BECOME A SECURITY BREACH?

This is not always entirely clear. An organisation may attempt to collect as much information as possible for the assessment of an "event", but it most likely will not have a general idea of what has happened. It is often the case that investigating and reacting to an event can cause additional costs. If the event is serious, it can even affect the organisation's reputation and productivity. It is for this reason that your organisation must define in advance who has the authority to decide how you will react to an event and the threshold values for these decisions.

In addition, you must plan for how you will limit the impact caused to your partners or customers in case the cyber security of your organisation is compromised. When should they be notified? What measures can you adopt to limit the damage done to them?

You will also need to think about how your organisation will respond if the cyber security of a service provider you use is compromised. Your organisation may not be able to influence how your service provider will react to the security breach. What can your organisation do on its own to limit any potential effects?

WHAT IS A SECURITY BREACH?

A security breach is a breach that focuses on the security of a system or service. Usually it represents one of the following:

- an intrusion or attempted intrusion of a system and/or data
- the unauthorised use of a system dsigned for the processing or storage of data

- any modifications to a system's firmware, software or devices that are done without the permission of the system's owner
- the intentional disruption and/or obstruction of a service.

Utilise the information that you already have

The information you collect on the threats you face and your technical environment can help you in two very important ways:

- They provide information on the effects of a breach. If an attacker manages to access a device, what other areas could they access? Could the attacker gain access to any critical parts of your organisation?
- They help define the necessary procedures. If an attacker has gained access to a specific network, could that network be isolated? If it can be isolated, what effects will this have on your organisation's operations?

Implement preventive measures

You should implement measures that will help you limit the damage that an attack can cause. These types of measures include:

- preventing any attackers who have penetrated your organisation's network from proceeding
- limiting the effects of an attack in advance – for example, by making backups of your data to limit the impact of any ransomware.

Much like with any other preventive measures, these must also focus on protecting the most important areas of your organisation.

Formulate a plan for managing any security breaches and cyber security incidents caused by these

In addition to your technical solutions, your plan must cover the following areas:

- humans and processes, such as the media and how you communicate with your customers and stakeholders
- submitting reports to the National Cyber Security Centre
- reporting to regulators
- reporting crimes to the police.

It may be beneficial to create a specific plan for the most common types of deviations so that you will all know the measures that your organisation is supposed to implement. Do not forget to practice!

Past experiences

Most organisations neglect to make any security breach assessments after the breach is over. However, the breach that you have experienced may provide valuable information on the cyber security of your organisation. For example:

1. The threat to your organisation
   - Who committed the attack? Was it targeted?
   - Was the attack conducted in the manner that you expected?
   - Did the attack focus on the areas that you had anticipated?
2. The effectiveness of your protective measures
   - What did your protective measures protect?
   - What did they not protect?
   - Could they be improved?
3. The effectiveness of the measures used to react to the breach
   - What should have been done differently?
   - Did your measures help limit the effects of the attack?
   - Did they make something worse or hinder certain areas?

The National Cyber Security Centre supports organisations that want to arrange exercises. With the help of our services, an organisation can start its own exercise activities or ask for our experts' help in planning the contents of any existing exercise programmes. For more information on exercises, see https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

Think about the following questions

Does our organisation have a incident management plan in place?
How can we ensure the efficiency of our plan?

Your plan must include at least the following:

- Key internal and external contact information.
- Clear escalation paths (for example to upper management) and predefined processes for critical decisions.
- A clear division of responsibility and a clause that states whether this applies to regular working hours or if it is always valid.
- A general flow chart or process description for the entire lifespan of an event and security breach.
- Instructions on regulatory requirements – for example, when a security breach must be reported and to whom.

Do the people in our organisation know where they can ask for help if they spot a security breach?

- Does your organisation have a contact information list on its key people?
- Is this contact information available to the right people even in situations where access to your information systems has been blocked?

As an organisation, can we learn from security breaches and near-incidents?

- Does your organisation keep any records of what you have learned and experienced?
- Are the operations of your organisation developed on the basis of these?

How is our organisation informed of the security breaches it has been subjected to?

This question involves two aspects: Which factors can help highlight a security breach? And how can you distribute this information within your organisation? Your organisation should take note of the following matters when considering the information that could be gained from any possible security breaches:

- How does your organisation monitor critical data (e.g. personal data) that should never be compromised, lost or altered?
- Who checks your log files? Do these people have enough training to identify any abnormal activities?
- How can your staff report any suspicious activities?
- Are your thresholds for alerts set to the right level? Are they low enough so that the right warning can be given in case any deviations are detected? Or are they high enough so that the people who process these are not burdened with meaningless information?

Your organisation should take note of the following matters when considering the internal distribution of information concerning security breaches:

- What is a security breach?
- Who has the authority to decide whether a situation can be considered as a security breach?
- Who needs to receive more detailed information on the security breach?
- Has the board given clear instructions on the threshold after which it must be informed of a security breach?

Does the board know who is responsible for leading the response to a security breach and who has the authority to make decisions?

This depends on how your organisation has been structured. The related authorisations may belong to the members of your board, the managing director, some other director, or they could have been distributed among the different duties and tasks in your organisation. To the extent that it is possible to do so, check the following in your organisation:

- Who can make decisions and on which issues? If possible, avoid specifying any individual persons in your instructions. Instead, assign the responsibility to the task or function at hand.
- Create backup plans for situations where the specified decision-makers are not available.
- Hone the functionality of your organisation's decision-making proces.s

Appendix I

Key legislation

Act on Electronic Communications Services (917/2014)

The key piece of regulation on digital communications in Finland is the Act on Electronic Communications Services (917/2014). The Act contains provisions on matters related to e.g. information security and the security of confidential communication channels. The Act applies to telecommunications operators, communications providers, corporate or association subscribers and domain name registrars. For most Finnish organisations, the key parts of this Act are the provisions concerning corporate subscribers. The term 'corporate or association subscriber' means an undertaking or organisation which subscribes to a communications service or an added value service and which processes users' messages, traffic data or location data in its communications network. This means that a corporate or association subscriber can be, for example, a business operator, cooperative, limited liability company, association, educational institute or state agency. For example, a corporate or association subscriber can be a business that acquires and provides phone and broadband connections to its employees and WLAN connections to the persons visiting its offices. The obligations of corporate or association subscribers concerning functionality, information security, and security of confidential communications are specified specifically in parts VI and X of the Act.

The EU Directive on network and information security (NIS Directive))

The EU Directive on network and information security aims to ensure a high level of security in the networks and information systems used throughout the European Union. The Directive contains provisions on information security obligations and disruption reporting practices.
The Directive mandates that key service providers and some specific digital service providers must: maintain a comprehensive level of network and information security-related risk management; manage the continuity of their services during incidents; and that they must report about any security deviations to the responsible authorities in case the deviation could hinder or even threaten the continuity of their operations.
The obligations in the Directive are directed towards the fields that are vital for the functionality of society. In Finland, these obligations have entered into force through sector-specific legislation, and their compliance is monitored by the authorities responsible for each sector.

- Transport - Traficom
- Energy supply - Energy Authority
- Healthcare - Valvira
- The finance sector - Finnish Financial Supervisory Authority
- The infrastructure of the finance sector - Finnish Financial Supervisory Authority
- Water supply - ELY Centres
- Digital infrastructure - Traficom
- Digital services - Traficom

General Data Protection Regulation of the EU

The General Data Protection Regulation of the EU (GDPR) sets the requirements concerning the collection, storage and management of personal data by companies and organisations. These requirements apply to both European organisations that process personal data within the EU and organisations outside the EU that process the personal data of EU residents. The GDPR applies if a company processes personal data and is located in the EU. This is done irrespective of where the data itself is processed or if the company is located outside the EU but processes personal data that is related to the provision of goods or services to people within the EU, or a company monitors the behaviour of individuals within the EU.

Data Protection Act (1050/2018)

The Data Protection Act specifies and supplements the GDPR. The Act applies to the processing of personal data in general. As it has been designed to specify and supplement the GDPR, the Act does not form an independent and comprehensive set of regulations, and is instead meant to be applied in conjunction with the GDPR.

The Criminal Code of Finland (39/1889)

The Criminal Code of Finland does not contain the term cybercrime, and cybercrimes are instead typically classified as technical or information network crimes. These are specified in detail in chapter 38 of the Criminal Code. In addition, the other chapters of the Criminal Code contain provisions on other crimes related to cybercrime. For example, provisions on business secret violations and misuses are presented in chapter 30 of the Criminal Code, which focuses on business offences.

Appendix II

Finnish authorities

Obligations of the Finnish Transport and Communications Agency's National Cyber Security Centre

The National Cyber Security Centre, which operates under the Finnish Transport and Communications Agency Traficom, is the national authority responsible for information security. Its areas of responsibility include the following:

- collecting information on security breaches and any related threats
- providing information on information security matters and the functionality of communication networks and communication services;
- investigating any information security incidents and related threats that target network services, communication services and added value services
- monitoring and guiding the information security and preparedness of telecommunications operators
- the inspection and approval of systems and networks
- monitoring the obligations related to the privacy of digital communications

Private individuals, companies and other organisations can submit confidential reports to the National Cyber Security Centre on the security breaches or attempted security breaches that they have encountered, such as suspected malware attacks, phishing attempts or DoS attacks. Based on the reports it receives, the National Cyber Security Centre can, whenever necessary, offer to assist in the assessment and investigation of the security breach and to coordinate the necessary measures.

To report a security breach to the National Cyber Security Centre, send an email to cert@traficom.fi or click the "Report incidents" button the Centre's website: https://www.kyberturvallisuuskeskus.fi/en.

For more information on the National Cyber Security Centre, visit https://www.kyberturvallisuuskeskus.fi/en

Police

As a general rule, the competent authority in the prevention, investigation and prosecution of cybercrime is the police in collaboration with other law enforcement authorities. Finnish Customs and the Finnish Border Guard investigate the crimes that fall under their jurisdiction, and, in connection with these, they also investigate crimes that involve networks and technology. The majority of cybercrimes are investigated by local police departments. Every police department includes a unit that specialises in the processing and analysis of digital evidence. The national police helpline is +358 295 419 800 (weekdays, 8 am – 4.15 pm) / neuvontapalvelu@poliisi.fi

The National Bureau of Investigation (NBI) is a national unit that operates throughout Finland. The NBI includes a unit that specialises in the preliminary investigation of cybercrime, the Cybercrime Centre, which focuses mainly on more widespread, international crimes committed on information networks. You can request the NBI to investigate a criminal matter, but the investigation may be transferred to a local police department at the NBI's discretion. The NBI's switchboard can be reached at +358 295 480 141 (Mon-Fri, 8 am – 4.15 pm).

In addition to these, you can report an offence or cybercrime online at https://www.poliisi.fi/crimes/reporting_an_offence_online or https://www.poliisi.fi/nettip. The Net Tip is a forum where you can report even the smallest cyber security incidents that do not otherwise meet the criteria of a crime.

Finnish Security Intelligence Service

The Finnish Security Intelligence Service (SUPO) is a security and intelligence agency that investigates and prevents any threats to national security. In addition, it produces security intelligence for the heads of the Finnish state and other authorities to support them in their decision-making processes.

One key mission of SUPO is to reveal and prevent foreign espionage in Finnish information networks and the damage that could be caused. Cyberespionage targets not only state actors, but corporations as well. SUPO's counter-cyberespionage activities are conducted in collaboration with both national and international partners. Along with the authorities, SUPO also collaborates with Finnish businesses.

SUPO's objective is to prevent cyberespionage with the help of stakeholder collaboration activities that are designed to increase popular awareness, for example by providing training to companies that maintain critical infrastructures or are responsible for the security of the nation's supplies.

The SUPO switchboard can be reached at +358 295 48013 and by email at suojelupoliisi@supo.fi.

Office of the Data Protection Ombudsman

The Data Protection Ombudsman is the national supervisory authority who is responsible for monitoring compliance with data protection legislation. The Data Protection Ombudsman's tasks include e.g. monitoring compliance with data protection legislation and other laws concerning the processing of personal data, increasing popular awareness concerning the risks, rules, protective measures, obligations and rights related to the processing of personal data, and for conducting investigations and inspections as well as for imposing the administrative penalties for any violations of the GDPR.

You can submit a data breach notification to the Data Protection Ombudsman at https://tietosuoja.fi/en/data-breach-notification

National Emergency Supply Agency and its pools

The National Emergency Supply Agency (NESA) operates under the Ministry of Economic Affairs and Employment. Its task is to handle the planning and operative measures that are related to the maintenance and development of Finland's emergency supplies. NESA's tasks include helping businesses and state actors work together for their preparedness measures, manage the state's emergency supplies and reserve and compulsory stockpiles, ensure the functionality of any necessary technical systems, and secure the production of critical goods and services, as well as to monitor international developments and maintain communications with foreign officials and agencies.

The pools, which are organs that operate under Finnish enterprises, are responsible for operative preparedness activities. Their task is to operate together with the leading companies in each field and monitor, investigate, plan and prepare the measures necessary for the development of the supply-related security of their respective fields. The Digipool is a communication organ that operates between the field of technology and information networks and state authorities, and its activities involve the companies in the field as well as various authorities. The pool includes significant actors who work in the technology service sector, software and device vendors, information security companies, and telecommunications operators. The most important officials who are involved in the pool are the Ministry of Finance, Traficom, Defence Command and the NESA.

For more information about cyber security, please contact us via:
cert@traficom.fi

Finnish Transport and Communications Agency Traficom

National Cyber Security Centre Finland

PO Box 320, FI-00059 TRAFICOM
tel. +358 (0)29 534 5000

traficom.fi

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre