SECURE DIGITALISATION TOOLKIT FOR BUSINESS LEADERS

NATIONAL EMERGENCY SUPPLY ORGANIZATION
DIGIPOOL

NATIONAL EMERGENCY SUPPLY ORGANIZATION
DIGIPOOL

Overview of security of supply

The Finnish model is based on co-operation between the administration and the business community.

In a networked society, preparedness requires extensive collaboration among authorities, businesses, and industry organisations.

State and municipal authorities have the statutory duty to undertake measures, such as preparedness plans, to guarantee the continuity of their critical operations amid disruptions and emergencies. Enterprises do not usually have such a statutory duty; the continuity management activities undertaken by enterprises are determined by business requirements, contractual obligations toward customers, and risk management.

Together with the sectors and pools of the National Emergency Supply Organisation (NESO), the National Emergency Supply Agency (NESA) is tasked with integrating the objectives and interests of both society and the business community.

New perspectives are required by globalisation, a networked economy, and technological developments

Finland has many characteristics that are advantageous for the efforts to maintain national security of supply.
Among these are abundant natural resources, good food production capacity, advanced welfare and education systems, and a well-functioning infrastructure.

Our national economy is increasingly integrated with the global economy. Globalisation, the networked economy, and technological developments may present new hazards. For this reason, the methodology and tools of preparedness are constantly being developed. In the 2000s, material preparedness was supplemented with an equally important component: operational continuity management, an activity designed to ensure continuity in the operations of organisations and networks that provide critical infrastructure and services.

Publisher:
NESO Digipool

This document is based on the work and results of a Digipool project #Strategia22

Publisher: NESO Digipool
Images: GettyImages and Colourbox
Layout: LM Someco Oy
Publishing year.: 2022
ISBN: 978-952-7470-19-0

Contents

SAFE DIGITALISATION TOOLKIT FOR BUSINESS MANAGERS

In recent years, not only the trade and industry but also society as a whole have invested extensively in digital solutions. The excitement about development has been so high that people have sometimes forgotten that they should also take care of digital security. Cyber and overall security should, however, always be a part of new projects from the start, and organisations should develop their own cyber culture systematically.

A company's digitalisation solutions should focus first on their strategic grounds, understanding the overall operational picture better, as well as the operating methods and processes. Only then comes the time to find out what kind of digital technology and services the company needs. Once these factors are thoroughly understood and implemented, there is an opportunity to grow the business, increase the investors' trust and generate added value and growth for the owners.

The amount of cyber crime and worldwide costs are growing rapidly, which is due to the reduced cost of carrying out attacks and the increased need for protection. During the pandemic, the number of digital devices has increased significantly, and they are used in more and more locations. At the same time, the core functions of companies are becoming more dependent on digital systems.

In digital security, the aim is to guarantee the safety of an electronic and networked society. This means identifying and preventing threats and preparing for the impact of disturbances in electronic and networked systems on the critical functions of society. Digital security includes (in accordance with the framework of the public administration) risk management and handling, management of the continuity of operations and preparedness, information security and data protection as well as cyber security.

The safety of digital solutions must be a central goal of the top management, because in the end, the management is responsible for everything that happens in the company. Digital security must be managed throughout the organisation consistently and in a centralised manner. The business units must be assigned clear duties and responsibilities for implementing their own digital security. The top management must prioritise digital and cyber security as a part of a business unit's own core functions.[1] Along with the business, the development debt of digitalisation that accumulates between the developing functions and systems as well as their cyber security must be monitored.

Finland is constantly targeted by cyber espionage, and this will not subside even over a long period of time. Cyber espionage is used, for instance, to acquire product development

information and data critical to the operation of companies. In Finland, private companies in particular, but also higher education institutions and research institutes, are targets of spying for this kind of information. The more digitalised a society becomes, the greater the damage that can be done by changing data or preventing access to it. The biggest threat of cyber influence is currently related to financially motivated cyber crime,[2] such as using ransomware to demand ransom.

For companies, the risk brought by digitalisation is now everywhere. Many companies are still facing the challenge of including cyber security as a proactive part of their strategy, operation and culture, and seeing it as more of an opportunity than a threat. The fundamental reason is twofold: 1) Cyber security is treated as a technological challenge and administrative work, and 2) most heads of digital and cyber security do not participate in the strategic decision-making of the company. Today, managers must be able to integrate security into the operation of the whole company, react to threats rapidly and influence other managers[3]. A credible security culture that updates continuously must be developed for the company. In addition, digital and cyber security must be a permanent item on the agenda of the board of directors and the management team.

The top management of the company must be committed to cyber security and responsible for developing it. In Finland, section 8 of the Limited Liability Companies Act (2006/624) states: "The management of the company shall act with due care and promote the interests of the company." In addition to this, from the perspective of information security, obligations on the operation of companies are imposed by the regulations of the GDPR of the European Union, which also guides the commitment of corporate management to implementing data protection and information security through sanctions.

Risk management is an essential part of the safety of digitalisation. Digital and cyber risks are a part of the high-level strategic and business risks that should be treated as a single whole, not separate concerns[4]. Digital and cyber risks are like any other significant business risks that may affect strategy, finances and technological choices. The management and protection of business chains, partnership agreements and cyber insurance also need to be taken into account in implementing the business model, if necessary.

All companies should keep the continuity of the business, protecting the brand, compliance with the requirements and growth in mind when building their strategy. The business context guides the strategic choices; you should think about factors such as pressure due to regulations, susceptibility to risk and what the customers value.

Because digital and cyber security cannot function in a vacuum, business managers must encourage the right stakeholders to cooperate closely with each other – ecosystem thinking is the key. Even though organisations need digital skills, such as online security, threat intelligence and reacting to incidents, they should not be used as a yardstick for digital managers. Technical capabilities must also be valued in digital and cyber leaders, but the heads of business units themselves must play the key role in decisions related to technology and risk management in addition to the business strategy[5].

The recent cyber attacks have made many digital and cyber security challenges even clearer than they were before. One of the observations is that the safety of companies is just as dependent on the worldwide digital ecosystem as it is on just the actions of the companies and organisations close to it. High cyber security 'hygiene' – maintaining digital protection, its tightness and thoroughness – is of crucial importance. To maintain uniformly high cyber hygiene throughout the whole company, new investments and partners included, transparency and open communications are needed[6]. The board of directors and operative management of the company must have an up-to-date cyber operational picture that enables proactive measures, as well as a comprehensive idea of the level of digital and cyber security of the company. Management of digital and cyber security on the strategic level is highlighted.

This toolkit by the Digipool has been created for business managers to make the comprehensive management of digital and cyber security easier on the level of the company's board of directors and management team. The starting point of drawing up the content has been management through strategy and ensuring the continuity of the company's operations.

On behalf of the #STRATEGIA22 project

Digipool

FOUNDATION FOR THE TOOLKIT FOR BUSINESS MANAGERS

Strategic digital and cyber management can be defined by following the general principles of strategic management. They can be crystallised in ten sections that form the foundation pillars on which strategic digital management must be built. They show that digital and cyber security must be included in the agenda of the top management and it must be an integral part of the everyday management of every company and organisation.

The responsibility cannot be divided, and the management must have a sufficient ability to read the risks related to digitalisation at every moment. This does not mean that everyone must be a technical expert, but a comprehensive situational awareness creates good preconditions for management and making decisions at the right time.

Investing in digital and cyber management is sure to pay for itself in the form of better competitiveness and the job satisfaction of the personnel. We can solve less than half of the growing digital and cyber security challenges with technology. Humans enter the spotlight; responsible employers invest in the expertise and digital skills that all of us need in our everyday lives, too.

The foundation pillars[7] of strategic cyber management that form the basis of this work can be grouped into four sections:

I. Leadership

1. Comprehensive and reliable digital and cyber situational awareness by the top management
2. A credible and reliable digital and cyber analysis and risk management system
3. Strategic cyber management concept as a part of the business strategy

II. Resourcing

4. Correctly proportioned resourcing for digital and cyber security
5. Correct and innovative technology choices and their functionality

III. Continuity management

6. Comprehensive and up-to-date preparedness and a continuity management plan
7. Well-trained and practiced crisis management organisation as well as a crisis communications plan

IV. Digital culture

8. The core processes and operating methods meet the requirements of business development and the operating environment
9. Appropriate digital and cyber skills and expertise of the whole personnel
10. A flexible and developing digital and cyber culture, approved by the top management

The management team of a company, typically together with the CEO, is tasked with preparing the company's strategy, business plans, budget and other issues to be decided by the board of directors. In addition, the management team usually decides and processes the operative matters most important to the company. The duties of the management team can be defined in more detail in the management team's rules of procedure.

In expanding the business and continuity management, identifying the role of digital security in implementing the strategy plays a central role. In general, the strategy tells how the company expands its markets or maintains the market share

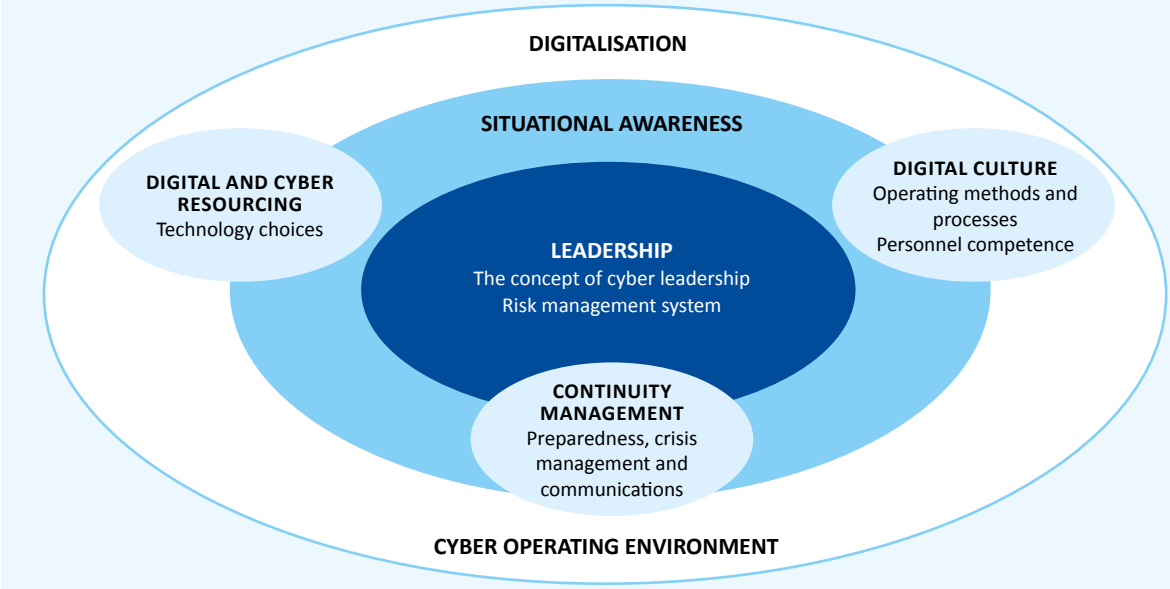


Figure 1. The four aspects of digitalisation management and the foundation pillars of security

and competitive assets it has achieved, including its partners, as well as the product and service development in addition to potential company acquisitions and the company's own expertise. The company's different industries and business functions should be reviewed at least from the perspectives of sales and marketing, communications, financial management, production and services, stakeholders and customer relationships, risks and continuity management as well as development.

The CEO selects the members of the management team. Here it would be beneficial for more than one person to have expertise related to digitalisation security. The task of a separately appointed digital manager can be used as an intermediate stage until all members of the management team have gained sufficient skills in digital security. Because the management team is responsible for the issue as a whole, responsibilities can be divided based on competence by function or business area. Figure 2 shows possible ways of dividing the responsibilities.

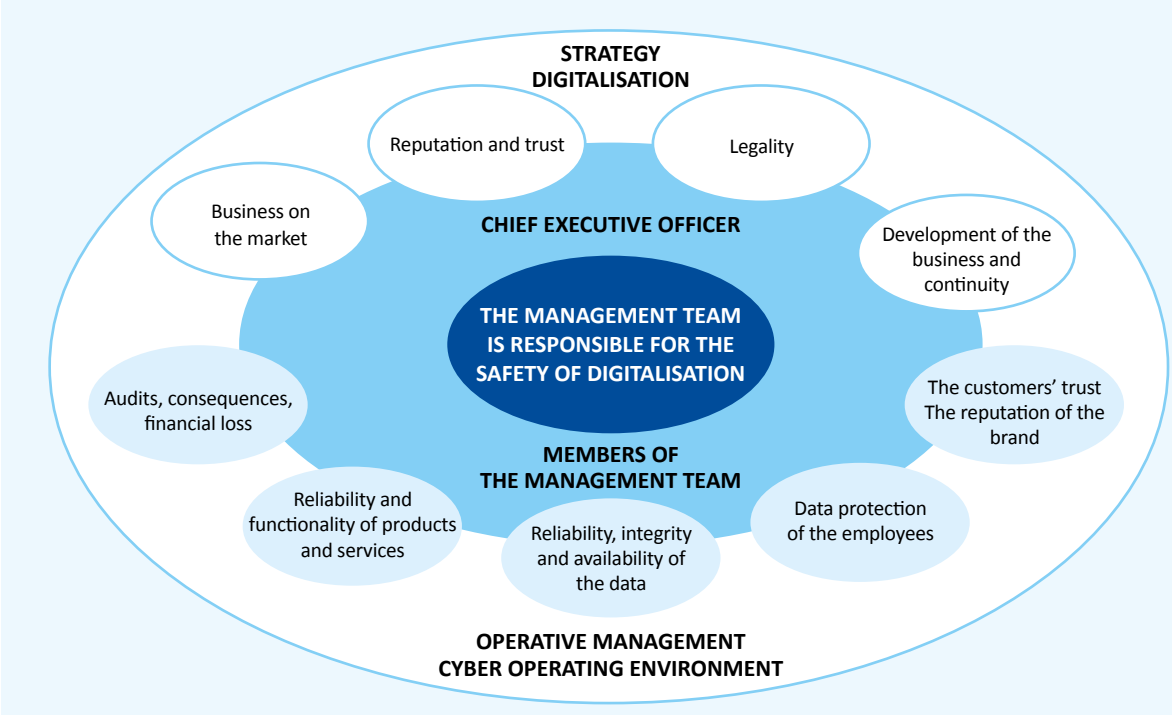


Figure 2. An example of division of responsibilities by topic in the management team

CYBER SECURITY TOOLKIT ON ONE PAGE

LEADERSHIP

1. Comprehensive and reliable digital and cyber situational awareness by the top management

The operative management is responsible for reporting a comprehensible assessment of the digital and cyber risks, threats and ramifications to the board of directors as a permanent item on the agenda of board meetings.

2. A credible and reliable digital and cyber analysis and risk management system

The board ensures that the management includes resilience and cyber risk assessment in the business strategy and the company's overall risk management and takes it into account in budgeting as well as the development debt created in the allocation of resources.

3. Strategic cyber management concept as a part of the business strategy

The board ensures that the different parts of the company cooperate internally to assess whether they have detected similar threats and to coordinate reactions or implement joint monitoring measures for the centralised processing and management of the risk. Annually, the board specifies and measures the risk tolerance of the business in relation to the cyber resilience and ensures that it is in accordance with the company's strategy and willingness to take risks.

RESOURCING

4. Correctly proportioned resourcing for digital and cyber security

The board can understand the impact of digital and cyber security risks and how they can differ in relation to the company's different goals in balancing the operative costs/impact of risks and digital security measures. The benefits of digital and cyber security investments have been scaled.

5. Correct and innovative digital technology choices and their functionality

The digitalisation goals have been defined in the company's strategy (e.g. the level of digitalisation). Before setting the goals, the different technologies that support development have been reviewed, after which goals for utilising them with respect to business and administration have been specified.

CONTINUATION MANAGEMENT

6. Digital preparedness and continuity management plan

The board ensures that the management supports the manager in charge of resilience or digital and cyber security by drawing up, implementing, testing and improving recovery plans continuously. They must be harmonised for all business areas of the company, which requires monitoring performance and regular reporting to the board.

7. Well-trained and practiced crisis management organisation as well as crisis communications

The members of the board and the management team receive a digital and cyber security orientation when they accept the position, and they receive regular updates on recent threats and incidents. They participate in training in accordance with the plan.

DIGICULTURE

8. Core processes and operating methods that meet the requirements

The core processes and operating methods meet the requirements of business development and the operating environment.

9. Appropriate digital and cyber skills and expertise of the whole personnel

The skills required for reaching the company's goals and managing the risks have been specified. A training programme ensures regular maintenance of the skills and knowledge, taking account of the requirements set by the changing operating environment. The level of training is assessed in regular exercises.

10. A flexible and developing digital and cyber culture

Together, the board and the management team ensure that the company has and develops a good digital and cyber culture, consisting of the operating methods related to digitalisation, work morale, joint rules and conditions and the ways employees interact with each other.

ACTION CARDS FOR THE BUSINESS MANAGER

The card consists of two sections: the first includes questions that guide you through the topic, followed by the second section that includes a list of the measures that the company management should at least take into account in the strategic management and steering of digitalisation.

The publication "Advancing Cyber Resilience Principles and Tools for Boards" by the World Economic Forum has been used in drawing up the action cards.

Card 1: Comprehensive and reliable digital and cyber situational awareness by the top management

Guiding questions

- Does the company use a process that ensures that the board of directors and the management team receive comprehensive information on digital security to support the decision-making?
- Has the board of directors assigned responsibilities to the right people in the company so that the digital and cyber security and its progress can be managed in accordance with the digitalisation goals?
- How is the development of digitalisation security monitored and maintained?

Task list, to be confirmed

- The company has a clear operating model for how to utilise the three different levels of the operational picture effectively (the levels: strategic, risk management and operative).
- The board of directors receives the necessary shareholder, regulatory, customer and other external social perspectives so that they can put the digital and cyber risks into the correct proportion.
- The business functions have been prioritised taking account of the support for critical national infrastructure or other national interests that meet the requirements set by society.
- The company understands how the technical systems, processes or resources promote the achievement of goals and create a competitive advantage.
- The named responsible manager has access to the board of directors and the management team as well as the sufficient authority, mastery of the topic, experience and resources to carry out their duties.
- The board of directors ensures that an independent official digital and cyber security review is carried out on the organisation annually.

Card 2: A credible and reliable digital and cyber analysis and risk management system

Guiding questions

- Do the members of the board of directors and the management team receive regular updates on the company's digital and cyber maturity, vulnerability to risk, the risk situation as well as the implementation situation?
- Is the level of digitalisation and cyber security reporting to the board of directors correct, and does it reflect the current and potential future situation in relation to strategy, its implementation and the business?
- How do the board of directors and the management team define the strategy concerning the company's ability to survive and the related risks/risk level?

Task list, to be confirmed

- The company has a process in which the assessment of risks related to digitalisation and cyber security has been linked as a part of the business risk assessment.
- The level of risk reporting to the board of directors is correct and provides information on both the current and the future situation.
- The board of directors recognises the actual impact of digital and cyber risks with regard to the business, such as disruptions in the business or the effect on reputation or the quality of the product/service.
- The company is able to manage digital and cyber security related to the planned business or changes made to the technology.
- The company's activities are assessed or audited internally and externally.
- The company is certified in order to promote competitive advantage and demonstrate responsibility.
- The company informs its personnel and contracting parties about risks and their consequences.

Card 3: Strategic cyber management concept as a part of the business strategy

Guiding questions

- Do the different parts of the company cooperate internally (e.g. with other business units) to assess whether they have detected similar threats and to coordinate the reaction or to implement joint monitoring measures to process and manage the risk in a centralised manner?
- Is the board of directors satisfied that the company is able to manage effectively the cyber security vulnerabilities and the required updates that may result from its business or planned changes to the technology?

Task list, to be confirmed

- The factors resulting from a change in the operating environment are identified and taken into account with regard to the company's own business and safety.
- Proven and standardised operating methods that promote the security of the business are used.
- Technologies that take advantage of business development are selected and managed on a justified basis.
- The comprehensive construction of cyber security is taken into account, requiring measures on the company's strategic, operative and technical/tactical level.

Card 4: Correctly proportioned resourcing for digital and cyber security

Guiding questions

- How large of a share of the annual operating costs are used for the company's continuity management, and how does this compare with the self-determined objectives, the norms of the field or the industry average?
- Does the company have a targeted budget for digitalisation and security, and who/which parties own(s) it?
- Does the company have other budgets that promote the continuity of the company's business and safety?

Task list, to be confirmed

- The company has a process for drawing up an overall budget that takes the impact of digitalisation security into account.
- The company is able to understand the effects of digital and cyber security risks and how they can differ in relation with the company's different goals in balancing the operative costs/effects of risks and cyber security measures.
- If cyber security insurance is used, its costs must be taken into account.
- The benefits of investments in digitalisation and its security have been scaled.

Card 5: Correct and innovative digital technology choices and monitoring their functionality

Guiding questions

- Has the company strategy defined the goals of utilising digital and cyber technology with regard to the business and the management of the company?
- Does the company have a process for assessing digital resilience with third parties that can control information or technology resources?

Task list, to be confirmed

- The goals of digitalisation have been specified (e.g. the company's level of digitalisation). Before setting the goals, different kinds of technologies, their opportunities as well as cyber threats and other risks related to their use must be reviewed (e.g. platform services, cloud services, the possibilities of artificial intelligence, 5G, the industrial internet, etc.)
- The business processes, administrative processes as well as products and services subject to digitalisation have been specified.
- The company has defined the parts of the IT environment that are critical to reaching the business objectives.
- The company has a plan for using different technologies in developing activities and their implementation.
- It has been verified that the technology selected supports the development of the business in a digital and cyber secure manner.
- The security and partnership agreements that correspond to the analysis mentioned above have been drawn up.
- The steering processes produce a strategy, risk management, an operating environment analysis and resources for the company and implement change management.
- Administrative processes support the company's decision-making and communications at a level higher than the other processes.

Card 6: Comprehensive and up-to-date preparedness and continuity management planning

Guiding questions

- Does the company use business continuity plans and recovery plans including communications, combating information security attacks and disruptions?
- How have the digital systems been protected? (e.g. technical solutions)
- How has the safety been verified? (e.g. auditing, penetration testing)

Task list, to be confirmed

- The company's management team is responsible for these plans.
- The plans include sufficient and diverse representation by the management to ensure that key perspectives and needs are taken into account (e.g. legislation, sales and marketing, media relations, administrative relations, relationships with the investors, premises management, corporate security, etc.)
- A person has been appointed as responsible for statutory and regulatory requirements (understanding them) in the different jurisdictions, in which the company operates globally, and the way these requirements are included in the plans.

Card 7: Well-trained and practiced crisis management organisation as well as a crisis communications plan

Guiding questions

- Do the members of the board of directors or the management team receive sufficient orientation training in digitalisation and cyber security when they accept the new position?
- Does the company have a regular training and exercise programme used to update their skills and knowledge regarding the latest security incidents?
- Does the management inform the board of directors of potential physical, functional, human-related, legal and/or reputation damage that could be caused by a cyber incident?
- Does the management notify the board of directors about the current industry-specific threats/threat models/trends/measures, including risks related to third parties (e.g. suppliers)?
- How is the public content managed so that they do not create threat factors towards the company?

Task list, to be confirmed

- The company's operating model and tasks are approved by the board of directors.
- The crisis management organisation is trained and exercises regularly focused on topics based on risk analysis, for instance.
- The organisation has a plan for exercises and further training.
- The activities are budgeted.
- The company has communicated the organisation's most important goals clearly and ensured that these priorities also guide the digital and cyber security measures.
- The company has an internal and external communications plan.
- The communications roles are named and the parties taking care of the duties have been trained.
- The company communicates regularly over different channels.
- Reputation management is taken into account in the communications plan.

Card 8: Appropriate digital and cyber skills and expertise of the whole personnel

Guiding questions

- Will the company's new employees receive sufficient orientation training in the company's digitalisation and its security?
- Does the company have a regular training and exercise programme used to update their skills and knowledge regarding the latest threats and trends (development of situational awareness)?

Task list, to be confirmed

- The skills needed to reach the company's goals and manage the risks have been specified.
- The capabilities and skill levels required by the work tasks have been defined as a basis for planning the training.
- Employees must be provided resilience-related skills in accordance with their duties.
- A training programme ensures regular maintenance of the skills and knowledge, taking account of the requirements set by the changing operating environment.
- The training programme includes the company's operating models for continuity as well as operating models for exceptional circumstances and the use of technologies.
- The level of training is assessed in regular exercises.

Card 9: Core processes and operating methods that meet the requirements for developing the business

Guiding questions

- Does the company have a process and operating methods in use for developing business that can also be used to identify information or technology resources?
- Have the company's core processes been specified with regard to the business and the company management?
- Have the key partners/outsourcing/subcontractors/contracting parties been identified?
- What has been agreed concerning information security, continuity management and security agreements in the outsourcing agreements?
- How is the customer information managed with regard to the company's own reputation and the customer/stakeholder?

Task list, to be confirmed

- The company's business goals guide the functions of the business process.
- The operational processes have developed so that they are safe in order to implement the products and services produced for the customers.
- The support processes enable operational processes with the help of human resources, systems or accounting, for example.
- Corporate acquisitions and the related cyber risks are managed. (Cyber Due Diligence in significant cases, if data and/or systems are transferred along with the acquisition.)

Card 10: A flexible and developing digital and cyber culture

Guiding questions

- Has it been ensured that the employees feel that they can influence the company's digitalisation and cyber security and that they have the opportunity to bring up shortcomings related to them?
- Are the members of the board of directors and the management team committed to decisions on digital and cyber security, do they personally comply with them and do they bring up inefficient practices in cooperation with the employees?
- Has it been ensured that the organisation talks openly and positively to the personnel on why digital and cyber security is important?

Task list, to be confirmed

- A good safety culture in the company consists of the operating methods related to digitalisation, work morale, joint rules and conditions and the ways employees interact with each other.
- The changes brought by digitalisation and cyber security have been processed amicably, covering the joint goals, work tasks and areas of responsibility as well as the rules and operating methods.
- The personnel of the company know how and to whom to report problems or incidents. They also feel that they are encouraged to report.
- The personnel are not afraid of negative consequences when reporting problems or incidents.
- The personnel feel that they can question operating models constructively; the skills, abilities and creativity of the personnel are utilised.
- The views of the personnel are actually used in the change and planning of digital and cyber security practices.
- The personnel understand the importance of digital and cyber security and their importance to the organisation. A learning and developing work community is taken into account; smooth cooperation and being active are encouraged.
- Instead of failures, the reporting and internal communications focus on successes (for instance, the number of people who reported phishing messages is stated instead of the number of those who fell for them).
- Time for social interaction is provided.

Attachment 1:

CONCEPTS

1. Digitalisation, cyber security

In digitalisation, data and information technology are used to change operations or enable new ones. For example, when the tax return filled in by taxpayers was replaced by the pre-completed tax return compiled by the tax authority, this involved digitalisation.

Cyber security means securing the confidentiality, integrity and availability of data, equipment, networks, software and users in cooperation between users and administrators.

2. Operational picture and situational awareness

The company's awareness and understanding of the operating environment is a precondition of management measures taken at the right time and used to ensure the success of business activities even when the cyber operating environment changes. A cyber operational picture can be generated for the planning and implementation of business; its contents and the need for it vary greatly between different operators and levels of management, which means that it is not possible to give an unambiguous definition of a cyber operational picture that would suit all situations and companies of all sizes.

A cyber operational picture does not consist only of the technical operational picture. At its best, the cyber operational picture can combine threat information and the overall situation successfully in addition to the technical information. The most important element, however, is the person who can compile the data into a clear whole and draw sensible conclusions based on it.

Levels of operational picture, importance of the operational picture

1. Strategic operational picture
   Makes it possible to increase and maintain the situational awareness of the company management.

2. Operational picture of digital and cyber risks
   Enables risk-based decision-making and management.
   Offers a foundation for continuity planning and the continuity of the business.

3. Operative picture
   Basis for daily and crisis management.

Sources of the operational picture: Commercial analysis and image services, networks of the ICT service partners, own sensor networks, situational picture services of the National Cyber Security Centre Finland as well as SOC services.

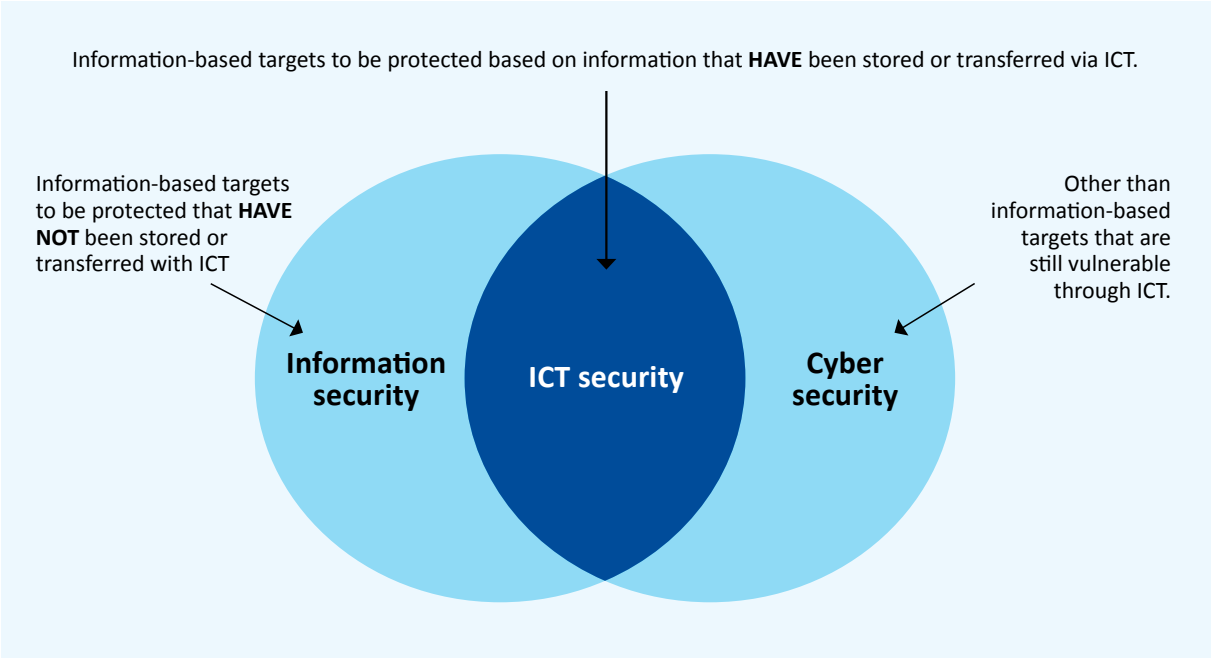


Figure: Definition of information security, ICT security and cyber security

Cyber operating environment

A company's cyber operating environment changes constantly. The operating environment can be described by three different types:

- a turbulent environment, in which there are a great many changes and the predictability is poor; the situation is chaotic

- a dynamic environment, in which a large number of changes occur, but these changes are more or less predictable based on previous events and experiences

- a stable environment, in which only few changes occur and they can be predicted based on previous experiences.

3. Leadership

Strategic management of cyber security

The strategic management of cyber security means identifying and setting goals derived from securing the digital operating environment, coordinating activity and preparedness as well as leading the management of extensive disturbances[8]. The figure below shows the general principles of cyber security management.

The responsibility of the board of directors

According to the Limited Liability Companies Act, the board of directors takes care of the management of the company and the appropriate organisation of activities (overall authority). As a part of good governance, the board of directors is responsible for monitoring the digital and cyber risks and resilience related to digitalisation. The board can assign primary monitoring activities to an existing committee (such as an inspection or risk committee). An assessment must be made to determine if the current board members have the necessary skills, knowledge and experience for the effective management and monitoring of digitalisation, and whether the lack of knowledge requires appointing new members to the board.

Responsibility of the CEO

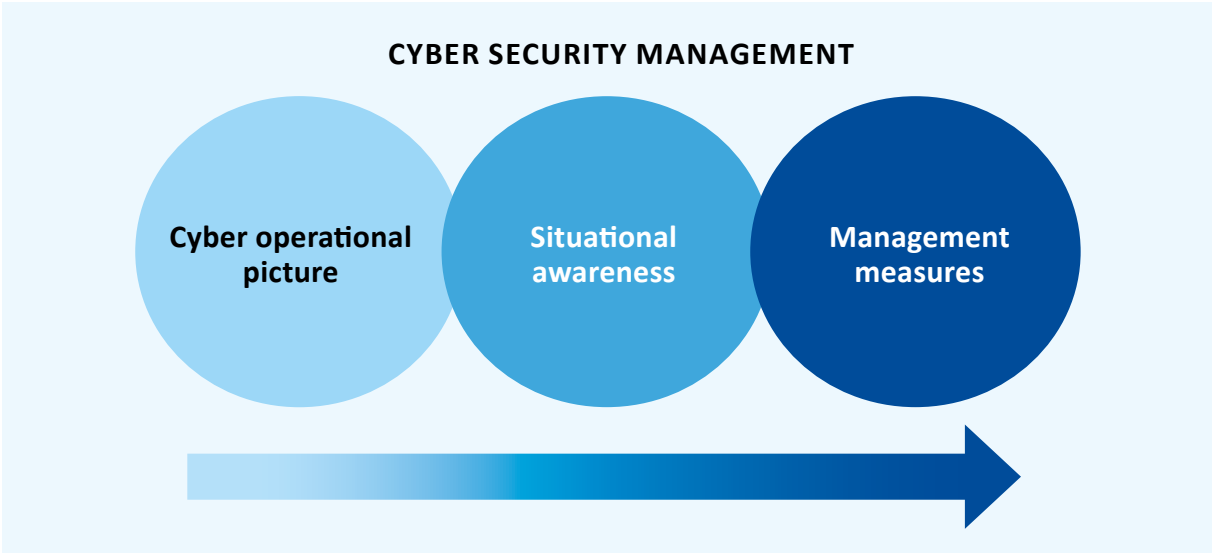
The CEO takes care of the day-to-day management of the company in accordance with the orders and instructions issued by the board of directors. The CEO must provide the Board and its members with the information needed to handle the Board's duties.

Duties of the management team in connection with digitalisation security

1. Keeping their own and the company's situational awareness (operational picture) up to date.
2. Ensuring that the digitalisation and cyber security management plan (incidents, risks) exists.
3. Understanding the role(s) involved in managing incidents with respect to their own areas of responsibility.
4. Participating in exercises.
5. Promoting a good safety culture.

Communications strategy

The communications strategy supports the realisation of the organisation's top level strategy goals; it includes the same values, target groups and objectives and also takes account of the organisation's challenges and operating environment. Choices are made based on these factors; what issues or products we want to bring into the awareness of our target groups, what kind of messages, language and channels we use and who acts as the spokesperson for communications in practice. The communications strategy includes the fundaments and operating methods of crisis communications.



4. Strategy

Strategy is a plan linked to long-term activities that the organisation develops and follows in order to improve the production of products and services, taking the threats and opportunities of the operating environment into account. The aim of the strategy on the competitive market is to gain a competitive advantage in relation to competitors. Each company has its own starting point for strategy.

Strategic planning of digital and cyber security must be used to ensure that the top management of the company understands how technologies assist in reaching the business goals and what kind of resilience the organisation has when it comes to losses due to technology and its activities. This is a way to ensure the commitment of the company management to taking digital and cyber security into account in the strategy[9].

Risk management

The board of directors ensures that the company management combines resilience and the assessment of digital and cyber risks with the overall business strategy and the company's risk management as a whole, as well as the allocation of budgeting and resources.

5. Objectives

Resilience, tolerance

The ability of the company's organisation, personnel, system, information network, measures and process to tolerate the consequences of an interruption or disturbance of the business and continue their activities at an acceptable minimum level. (ISO 2007)

Continuity management

A business continuity management system safeguards the ability of the organisation and company to continue its activities during a disruption. It helps with identifying the vulnerable aspects of the activity and makes it possible to assess the effects of threats as well as plan and implement operating methods in case of disruptions. The standard ISO 22301 can be used to build and implement a business continuity management system. The standard specifies requirements for the implementation, maintenance and improvement of the management system. The requirements are suitable for organisations of all types and sizes or parts of organisations, both in the private and the public sector. (ISO 22301)

Competitive advantage – generating value

Competitive advantage refers to a company having a relative advantage compared to its existing and potential competitors with regard to an ability, operating method or other factor affecting the success of its business. The most successful companies recognise the business opportunities offered by digital technology and also take advantage of them actively (e.g. mobile and social technology, analytics). Companies that take strategic advantage of digitalisation usually succeed financially and generate value for the company.

Assessing the cost-effectiveness of digital and cyber security

Assessment of the cost-effectiveness of digital and cyber security is based on risk assessments as well as functional indicators. Risk assessments include assessing every significant risk from the perspective of digital security, too, by describing the probability and impact of the risk as well as the effects of protective measures on the risk quantitatively. The goal is to target investments in digital and cyber security to combat critical risks based on the risk analysis. Functional indicators can be used to measure goals that generate benefits that cannot be assessed in euros.[10] For instance, the loss of the customers' trust that would result in the customers moving to competitors can be assessed. Losses due to incidents can be divided into the following types: financial losses, operational impact, impact on the customers and impact on the personnel.

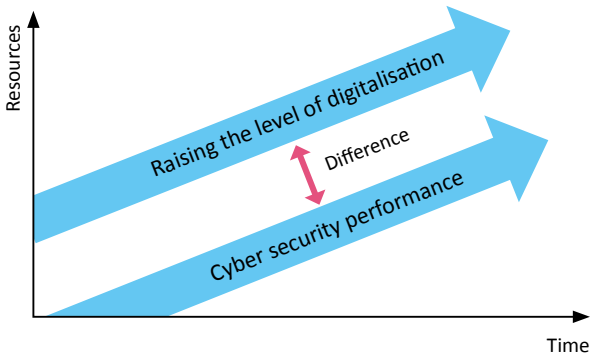
6. Effectiveness

Level of digitalisation

The level of digitalisation is usually understood to mean the availability and rate of utilisation of digital services in the selected service areas. The level is determined by using indicators such as the amount and rate of utilisation with regard to different applications.

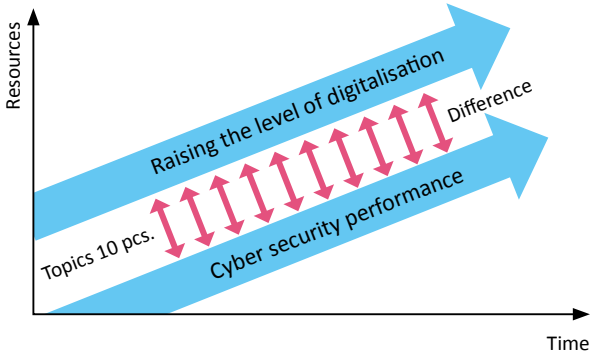
Development debt

A company's digitalisation development debt consists of the difference between the increase of digitalisation and the related cyber security capability, measured in time. If the difference is reduced over time, the company achieves better relative cyber security. If the difference increases, however, cyber security will not be able to match the development of digitalisation. An increase of the difference requires investments in the growth of security.



Development debt assessment

The development debt can be assessed by using the pillar model presented above, for example. Each pillar is assessed on a scale of 0–5 (0=the best result) and the points are added together. The smaller the sum, the lower the development debt. After several temporally sequential assessments, the direction of the difference can be calculated. Based on this, the management team can allocate the company's resources more accurately in the necessary direction in order to promote security. The benefits of digitalisation will not materialise if the development debt is too high.



7. Business continuity management

Continuity plan and implementation

The board of directors ensures that the management supports the manager in charge of resilience/digital and cyber security by drawing up, implementing, testing and continuously improving the continuity plans. They must be harmonised in all business areas of the company. This requires that the CEO (or the named responsible manager) monitors the performance and reports on it regularly to the board of directors.

Exercises

The board of directors confirms and the management team personally participates in accordance with their roles in exercises related to the company's digital and cyber security. The management team reports the observations and proposals for changes to the board of directors.

Attachment 2:

RECOMMENDED ACTIONS FOR DIFFERENT TYPES OF COMPANIES

TYPE	1	2	3	4
SIZE	Micro company–SME	Micro company–SME	Corporate group–large company	Corporate group–large company
ENVIRONMENT	Stable/dynamic	Turbulent/dynamic	Stable	Dynamic/turbulent
LEVEL OF DIGITALISATION	Low	High	Low	High
PRODUCT TYPE	According to the competition on the market	Individual products, stable services	Standard products or services, mass-market products	Customer-specific products or services
1. Comprehensive and reliable digital and cyber situational awareness by the top management	Measures are taken logically based on the joint operational picture.			
2. A credible and reliable digital and cyber analysis and risk management system	The management of digital and cyber risks is specified for the whole organisation.	The management of digital and cyber risks is monitored systematically and developed continuously as a part of the risk management of the whole organisation.	The management of digital and cyber risks is monitored systematically and developed continuously as a part of the risk management of the whole organisation.	The digital and cyber risk management strategy is a part of the general risk management strategy.
3. Strategic cyber management concept as a part of the business strategy	The concept has been drawn up as a part of the business strategy.			
4. Correctly proportioned resourcing for digital and cyber security	The resourcing of critical services is planned for all critical resources throughout the whole organisation.	The resourcing of critical services is organised under the monitoring of the management and in connection with society consistently throughout the whole organisation.	The resourcing of critical services is organised under the monitoring of the management and in connection with society consistently throughout the whole organisation.	The top management is responsible for ensuring sufficient resources for providing critical services, and the authorisations for decision-making have been implemented appropriately and effectively.
5. Correct and innovative technology choices and their functionality	The choices support digitalisation and ensure that they are cyber safe and functional.			
6. Comprehensive and up-to-date preparedness and a continuity management plan	Continuity planning is specified for the whole organisation.	Continuity planning is carried out systematically and developed on a risk-oriented basis.	Continuity planning is carried out systematically and developed on a risk-oriented basis.	The organisation regularly trains for recovery from different kinds of incidents, disturbances and accidents and improves the plans based on the training exercises.
7. Well-trained and practiced crisis management organisation as well as a crisis communications plan	The skill and knowledge requirements on security personnel have been specified consistently for the whole organisation. The collection and sharing of digital and cyber security data has been planned for the whole organisation and stakeholders.	The security personnel, assessments and training programmes are being developed regularly. Digital and cyber security data are collected, analysed and shared consistently throughout the whole organisation and with stakeholders.	The security personnel, assessments and training programmes are being developed regularly. Digital and cyber security data are collected, analysed and shared consistently throughout the whole organisation and with stakeholders.	Through training and exercise activities, the management and security personnel receive advance instruction in cyber security incidents and scenarios, including serious ones. Relationships with internal and external operators are maintained for collecting and sharing information on cyber security, threats and vulnerabilities with the aim of reducing risks and strengthening the ability to function.
8. Core processes and operating methods that meet the requirements	The company's core processes and operating methods meet the requirements of business development and the operating environment. They have been implemented and they are being maintained when the business or the operating environment changes.			
9. Appropriate digital and cyber skills and expertise of the whole personnel	The skill and knowledge requirements of personnel have been specified consistently for the whole organisation.	Personnel, assessments and training programmes are developed regularly.	Personnel, assessments and training programmes are developed regularly.	With training and exercise activities, the personnel receive an orientation in security incidents in advance, and their skills and knowledge are maintained.
10. A flexible and developing digital and cyber culture, approved by the top management	The management of the company fully supports the development of the culture.			

Attachment 3:

EXAMPLES OF INSTRUCTIONS OR GUIDES INTENDED FOR THE USE OF THE COMPANY

Cyber security and the responsibilities of boards, Traficom publications 2/2020.
(The guide is based on the publication “Cyber Security Toolkit for Boards” by NCSC-UK)

Pienyritysten kyberturvallisuusopas (Cyber security guide for small companies), National Cyber Security Centre, Traficom publications 228/2020. (The guide is based on the material “Small Business Cyber Security Guide” produced by the Australian Cyber Security Centre.)

Advancing Cyber Resilience Principles and Tools for Boards, World Economic Forum 2017.

Cyber Security Toolkit for Boards, National Cyber Security Centre, UK.

SFS (2021) ISO/IEC 27000 Tietoturvallisuuden standardisarja (Information Security Management), https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

Katakri 2020 – Information Security Audit Tool for Authorities. Traficom publications 232/2020.

Kybermittari - Cybermeter. https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

SOURCES

1 Boone, A. (2017). Cyber-security must be a C-suite priority. Computer Fraud & Security, 2017(2), 13–15.

2 National security overview 2021, Finnish Security and Intelligence Service. https://supo.fi/en/cyber-threats.

3, 5 Matthew Doan (2019). Companies need to rethink what cybersecurity leadership is? Boston Consulting Group, https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is.

4 Cybergovernance and the Role of the Board: An Interview with Kaiser Permanente's George DeCesare. (2018), https://www.bcg.com/en-nor/publications/2018/cybergovernance-role-board-interview-kaiser-permanente-george-decesare.

6 Ayman Al Issa, Tucker Bailey, Jim Boehm and David Weinstein (2021). Enterprise cybersecurity: Aligning third parties and supply chains. McKinsey, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/enterprise-cybersecurity-aligning-third-parties-and-supply-chains.

7 Aapo Cederberg, Strategic cyber leadership is needed to address current security challenges. Cyberwatch Magazine 2021/3.

8 Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen, Strategic management of cyber security in Finland, March 2018, Publications of the Government´s analysis, assessment and research activities 28/2018.

9 Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

10 Digitaalisen turvallisuuden kustannusvaikuttavuusarviointi julkisessa hallinnossa (Cost-effectiveness assessment of digital security in public administration), study report, 1 June 2020, Ministry of Finance.

Literature used in the work

Accenture, Cyber Threat Intelligence Report 2021,
https://www.accenture.com/fi-en/insights/security/cyber-threat-intelligence-report-2021.

Alashi S. A., Badi D. H. (2020) The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations, Department of Information Science, King Abdulaziz University, Jeddah, Saudi Arabia.

Andrews, K. R. (1997). A reader in the resource-based perspective. Foss, N. J. (ed.), (pp. 52–59).
New York, NY, United States: Oxford University Press.

Deloitte, Yritysvastuu alihankintaketjun vastuullisuus (Corporate responsibility, responsibility of the subcontracting chain), https://www2.deloitte.com/fi/fi/pages/risk/articles/yritysvastuu-alihankintaketjun-vastuullisuus.html

Fujitsu, Customer-first security: What it is and best practices for success,
Fu-jistu_Customer_First_Security_Whitepaper123.pdf, fujitsu.com.

Garcia-Granados, F (2020) Cybersecurity Knowledge Requirements for Strategic Level Decision Makers, Conference Paper, Tallinn University of Technology.

Hill, A & Hill, T (2009) Manufacturing operations strategy. Palgrave Macmillan.

Leena Hiltunen, Metodina kyselytutkimus, University of Jyväskylä, 2009.

IBM, IBM Security Strategy, Risk and Compliance Services, https://www.ibm.com/downloads/cas/GKN51N92

Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

Johnson, G., Scholes, K. & Whittington, R. (2008). Exploring corporate strategy (8th ed.). Harlow; Munich: Prentice Hall Financial Times.

National Security Authority NSA, Katakri 2020 – Information Security Audit Tool for Authorities, Traficom publications, ISSN 2669-8757, online publication.

Kim, J. (2017). Cyber-security in government: reducing the risk. Computer Fraud & Security, 2017(7), 8–11.

KPMG, Kyberturva kohtaa fyysisen maailman turvallisuuden, 2021, https://home.kpmg/fi/fi/blogs/home/posts/2021/05/kyberturva-kohtaa-fyysisen-maailman-turvallisuuden.html, and https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut/teknologiakonsultointi/tietoturva.html

National Cyber Security Centre, Cyber security and the responsibilities of boards, (original version: Cyber Security Toolkit for Boards, NCSC, 2019, ncsc.gov.uk), National Cyber Security Centre 2/2020, kyberturvallisuuskeskus.fi

National Cyber Security Centre, Pienyritysten kyberturvallisuusopas (Cyber security guide for small companies), Traficom publications 228/2020. (The guide is based on the material “Small Business Cyber Security Guide” produced by the Australian Cyber Security Centre.)

Kasey Panetta, 5 Security Questions Your Board Will Inevitably Ask, Gartner 12 June 2020 a, the report itself: Sam Olyaei and Jeffrey Wheatman, 19 July 2019, https://www.gartner.com smarterwithgartner/5-security-questions-board-will-definitely-ask/

Kasey Panetta, The 15-Minute, 7-Slide Security Presentation for Your Board of Directors, Gardner 18 June 2020 b, https://www.gartner.com/smarterwithgartner/the-15-minute-7-slide-security-presentation-for-your-board-of-directors

Posthumus, S., von Solms, R. (2004). A framework for the governance of information security. Computers & Security, Volume 23, Issue 8, 2004, 638–646.

SFS (2021) ISO/IEC 27000 Tietoturvallisuuden standardisarja (Information Security Management), https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

von Solms, B. (2001). Corporate Governance and Information Security. Computers & Security, Volume 20, Issue 3, 2001, 215–218.

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371–376.

Jussi Tammelin, Tietoturvastrategia ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa, University of Jyväskylä, 2021, master’s thesis.

TietoEVRY, An Introduction to Cybersecurity, https://www.tietoevry.com/en/services/Cybersecurity/cybersecurity-guidebook

Jiri Vidgren, Kyberturvallisuus yritysstrategiassa, 2019, University of Jyväskylä, Information Systems Science, bachelor’s thesis.

IBM, IBM Security Strategy, Risk and Compliance Services, https://www.ibm.com/downloads/cas/GKN51N92

Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

Johnson, G., Scholes, K. & Whittington, R. (2008). Exploring corporate strategy (8. ed.). Harlow; Munich: Prentice Hall Financial Times.

Kansallinen turvallisuusviranomainen, Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille, Traficomin julkaisusarja, ISSN 2669-8757, verkkojulkaisu.

Kim, J. (2017). Cyber-security in government: reducing the risk. Computer Fraud & Security, 2017(7), 8–11.

KPMG, Kyberturva kohtaa fyysisen maailman turvallisuuden, 2021, https://home.kpmg/fi/fi/blogs/home/posts/2021/05/kyberturva-kohtaa-fyysisen-maailman-turvallisuuden.html, sekä https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut/teknologiakonsultointi/tietoturva.html

Kyberturvallisuuskeskus, Kyberturvallisuus ja yrityksen hallituksen vastuu, (alkuperäinen Cyber Security Toolkit for Boards, NCSC, 2019, ncsc.gov.uk), Kyberturvallisuuskeskus 2/2020, kyberturvallisuuskeskus.fi

Kyberturvallisuuskeskus, Pienyritysten kyberturvallisuusopas, Traficomin julkaisuja 228/2020. (Opas perustuu Australian kyberturvallisuusviranomaisen tuottamaan materiaaliin Small Business Cyber Security Guide.)

Kasey Panetta, 5 Security Questions Your Board Will Inevitably Ask, Gandner 12.6.2020a, varsinainen raportti Sam Olyaei ja Jeffrey Wheatman, 19.7.2019, https://www.gartner.com/smarterwithgartner/5-security-questions-board-will-definitely-ask/

Kasey Panetta, The 15-Minute, 7-Slide Security Presentation for Your Board of Directors, Gardner 18.6.2020b, https://www.gartner.com/smarterwithgartner/the-15-minute-7-slide-security-presentation-for-your-board-of-directors

Posthumus, S., von Solms, R. (2004). A framework for the governance of information security. Computers & Security, Volume 23, Issue 8, 2004, 638-646.

SFS (2021) ISO/IEC 27000 Tietoturvallisuuden standardisarja, https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

von Solms, B. (2001). Corporate Governance and Information Security. Computers & Security, Volume 20, Issue 3, 2001, 215-218.

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371–376.

Jussi Tammelin, Tietoturvastrategian ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa, Jyväskylän yliopisto, 2021, pro gradu.

TietoEVRY, An Introduction to Cybersecurity, https://www.tietoevry.com/en/services/Cybersecurity/cybersecurity-guidebook

Jiri Vidgren, Kyberturvallisuus yritysstrategiassa, 2019, Jyväskylän yliopisto, Tietojärjestelmätiede, kandidaatintutkielma.

NATIONAL EMERGENCY
SUPPLY ORGANIZATION
DIGIPOOL