December 2019

CYBER SECURITY FOR THE BOARD OF DIRECTORS

Recommendations to strengthen Cyber Security Competences

Board Leadership Society
Center for Cybercompetences

KROMANN REUMERT

CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND
FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

CONTENTS

CONTACT

Board Leadership Society
Center for Cybercompetences

Tom Jacobsgaard
CEO
Email: tj@bestyrelsesforeningen.dk

Marianne Philip
Chairman of the Board
Email: mp@kromannreumert.com

Troels Ørting Jørgensen
Chairman of the Advisory Board
Email: toe@bestyrelsesforeningen.dk

Kirsten Hede
Project manager - Cyber
Email: khe@bestyrelsesforeningen.dk

1. Introduction

These recommendations have been prepared as part of the project “Strengthening of strategic cyber competences in Danish companies”. The purpose of the project is to increase awareness of cyber risks and to strengthen cyber security competences in Danish Boards and Executive Management, including in small and medium-sized companies.

The project is supported by the Danish Industry Foundation, as part of the effort to turn cyber security into a competitive advantage for corporations and society at large.

The project is managed by the Board Leadership Society of Denmark in collaboration with a group of partners, including Copenhagen Business School (CBS), CBS Board Education, the University of Aalborg (AAU), World Economic Forum, Dubex, EY, IBM, PwC, Centre for Cyber Security (CFCS), and Kromann Reumert.

2. Cyber competences in the Board of Directors

Risk management is at the core of any business decision. The more digital products and infrastructure become, the more vulnerable the companies are to cyber attacks. Today, cyber attacks are among the most critical business risks facing corporations. A cyber attack may damage the profit, customer relations, and the reputation of a company. Accordingly, it is crucial to focus on cyber and information security in the board room.

Board members need cyber competencies. Not just to manage business risks but also to turn cyber security into a competitive advantage and an enabler for the product development and growth.

It is the responsibility of the Board of Directors (the"Board") to oversee the company's risks effectively, among others to protect and generate revenue in the Company they are responsible for.

However, many boards lack sufficient knowledge and competences to be able to address cyber risks appropriately.

Risk management includes understanding, identifying, measuring, reporting, monitoring, and managing risk. Risk cannot be eliminated, but by applying a systematic approach to risk management, the risks may be contained. This may allow the board to prioritise resources more efficiently.

To assess if the board of directors possess adequate cyber competencies, each board member must consider: "Do I understand the company's cyber risks landscape, and do we have a cyber strategy?"

The purpose of this publication is to help board members work with the cyber strategy and to act as a tool when they interact with executive management about cyber security risks.

Board members need cyber competences to:

- ✔ Protect the assets, business processes, and customers.
- ✔ Generate growth and utilize business opportunities in the digital era.
- ✔ Set the company's risk profile and propensity to invest.
- ✔ Comply with the directors' liability.

3. Selected types of cyber attacks

Cyber attacks are driven by different intentions and methods. Some attacks aim at stealing data or spying. Other attacks aim at stealing money. Some attacks are simple while others are advanced. Cyber attacks may be performed by organized criminals, sovereign states, amateurs, insiders, and competitors. A successful attack may ultimately shut down the business.

Cyber attack is generally defined as an attempt to disrupt or gain unauthorized access to data, systems, digital networks or digital services. A successful attack may paralyse the entire business and take substantial time to restore. Two of the most common cyber attacks today are phishing emails and CEO fraud (e.g. targeting board members). These attacks can cause great damage. The specific risk exposure of a company depends on its industry, most valuable assets and vulnerabilities, and must be assessed on a case-by-case basis.

It is estimated that…

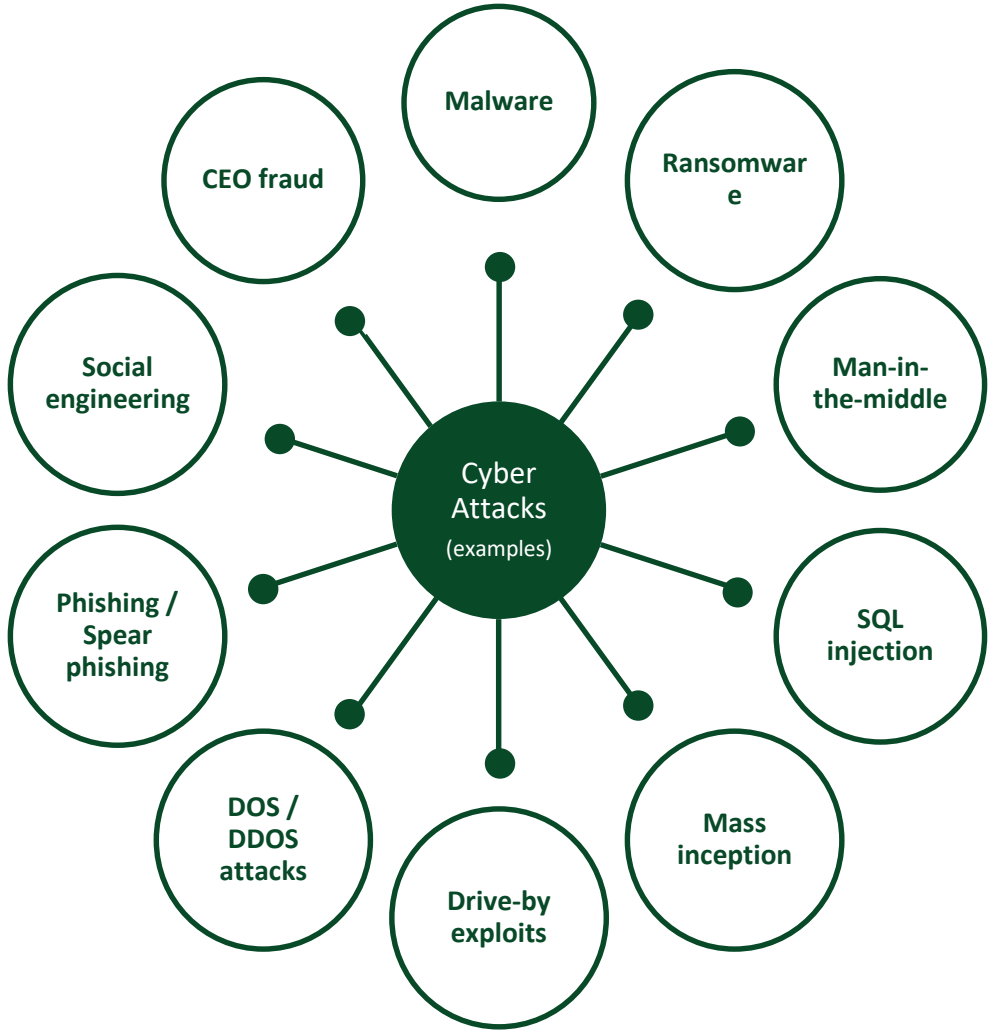
- **9** out of **10** companies have been hacked.
- Between **500** and **1000** targeted hacker attacks occurs on a daily basis in Denmark.
- **+100.000** Danish PCs are infected with potentially damaging virus.

Source: CSIS Security Group

Top exposed industries include…

- Finance and insurance
- Utilities
- Healthcare
- Transportation
- Consulting
- Retail
- Manufacturing

Sources: IBM X-Force Cyber Security Intelligence Index 2019; Drooms Top 5 Industries at Risk 2019



The figure shows examples of different types of cyber attacks and methods. Terms and concepts are further explained in the glossary in Appendix 1.

4. Themes for a cyber strategy

Cyber security is more than IT. Cyber security also concerns governance, management, tools, processes and people. Ultimately, the board of directors remains liable for the company's risk and security level. Accordingly, cyber security needs to be an important topic on the board's agenda. The cyber threat is real and all companies must have a strategy to address it.

The overall objective of a cyber strategy is to implement 5 basic functions of a cyber security framework: The ability to **Identify**, **Protect**, **Detect** and **Respond** to cyber incidents and the ability to **Recover** affected systems, data etc. On this basis the board may structure its cyber strategy into the six (6) themes shown in the table to the right. Each theme is summarised in an overall recommendation (see section 5), and is further detailed in a number of "toolboxes" with key considerations for the board (see section 6, pages 8-14 below).

5 objectives of a cyber strategy

1. **Identify** assets, vulnerabilities, threats etc.
2. **Protect** the company by appropriate measures
3. **Detect** if/when a cyber security event occurs.
4. **Respond** to a detected cyber security incident.
5. **Recover** capabilities and services affected.

6 KEY THEMES FOR A CYBER STRATEGY

Theme	General
1. **Risk assessment and vulnerabilities**	The Board has insight into the company's vulnerabilities, threats, impact of potential attacks, and the probability of their occurrence.
2. **Risk appetite and strategy**	The Board sets the company's risk appetite based on the company's business objectives, risk profile, and costs/investments.
3. **Plans, processes, and contingency**	The Board monitors the implementation of cyber security measures through tested contingency plans and processes, including covering the 5 themes: Identify Protect, Detect, Respond and Recover.
4. **Reporting and control**	The Board receives regular and relevant reporting and has implemented cyber security into its annual wheel.
5. **Culture and people**	The Board leads the way in adopting a positive security culture and ensuring awareness programs for employees, directors etc.
6. **Competencies and organisation**	The Board and the Executive Management possess adequate technical competences and experience to understand, assess, and address cyber security risks.

5. Recommendations for the board

Strategy

Execution

People

1. Risk assessment and vulnerabilities

It is recommended that

- at least twice a year, the Board receives and reviews an updated cyber risk assessment based on the company's most valuable assets, technology landscape, primary vulnerabilities, probable threats, potential losses from cyber attacks, and recommendations for (further) investments.

2. Risk appetite and strategy

It is recommended that

- at least once a year, the Board sets the company's risk appetite within cyber security taking into consideration e.g. the company's business objectives, digitalisation strategy, risk profile, current IT security budget, and willingness to invest.

3. Plans, processes, and contingency

It is recommended that

- the Board oversees that cyber security risks are addressed in the company's policies and processes for IT and physical security as well as digital behaviour.
- the Board oversees that the company has contingency plans and communication plans to address critical incidents (anything from cyber attacks to power outages) and that these plans are tested on a regular basis.

4. Reporting and control

It is recommended that

- the Board implements cyber security as a permanent part of its annual wheel and has cyber security on the agenda of each board meeting (see example in Appendix 2).
- prior to each board meeting, the board receives relevant reporting from the Management, such as updated risk assessment, test results, security incident, findings from audits, security budget, insurance coverage, outcome of awareness activities, recommended actions and investments, etc.

5. Culture and people

It is recommended that

- the company maintains a training programme for members of the board and executive management as well as employees in relation to security and awareness training.
- the Board leads the way in adapting a positive cyber security culture in the company.

6. Competences and organisation

It is recommended that

- at least one Board member has cyber expertise and experience and acquires insight into the company's technology and security landscape.
- the company's security organisation (or function) is anchored at a management level reporting directly to the board of directors.

6. Toolbox

Theme 1 – Risk assessment and vulnerabilities

In order to manage cyber risks and prepare a cyber strategy, the board needs to have adequate insight in to the general technology landscape of the company, its most valuable assets, primary vulnerabilities, probable threats, and the potential consequences of a cyber attack.

Although Boards are used to risk management, few boards feel comfortable in assessing and addressing cyber risks.

However, as with other business risks, a robust risk assessment remains essential in order to identify, analyse and evaluate cyber risks.

The list in right table may help assess whether the board receives sufficient information in order to understand and assess the potential cyber risks facing the company.

At least twice a year, the Board should receive an updated risk assessment from the executive management describing, e.g.:-

1) Most important assets and systems
2) Consequences of leaks or unavailability
3) Primary vulnerabilities
4) Threats (prioritised) and probabilities
5) Plan for risk management and further investments

The Board can also take inspiration from World Economic Forum's Board Cyber Risk Framework and Cyber Resilience Tools (reference in Appendix 4).

According to PwC 2019 Annual Corporate Directors Survey less than 40% of the surveyed leaders responded that their board of directors understands the cyber risks of the company.

Key considerations in the board room

Values and system landscape

- What are the most important values of the company? It can be tangible assets (e.g. systems), intellectual assets (e.g. data and IP) and reputation.
- Where is the most important data and information of the company stored (e.g. cloud, at an external supplier, inside or outside Denmark)?
- Which IT systems and services are the most critical?
- Who are the most important suppliers and partners of the company?
- Which control and security systems have been implemented by the company (e.g. supervision, AI-based access codes, multi-factor authentication)?
- Are these records regularly maintained – and by whom?

Consequences of a security incident

- What does it mean to the business if important values are changed, stolen, leaked, or if critical systems or other IT services are inaccessible for a shorter or longer period of time?

Vulnerabilities

- Where is the company most exposed to security breaches (vulnerabilities can be systems and programmes e.g. Active Directory, processes lacking or not being complied with, a lack of awareness among employees etc.)?
- Is access to data and networks limited adequately (the risks increases as more people gain access)?
- Is the level of security regularly tested, e.g. through "red team"-attacks, firewall audits, vulnerability scans, penetration tests, GAP analyses etc.?

Threat picture and probability

- Who are the likely attackers?
- What is their objective (e.g. steal money, IP, information, digital identity)?
- Which tools/techniques do they use to achieve the above objective (e.g. phishing, drive-by exploits, social engineering, DDoS, malware etc.)?
- How likely are these threats in the light of the company's vulnerabilities?

Plan for risk management and investment

- What is the company's risk management and investment plan?

6. Toolbox

Theme 2 – Risk appetite and strategy

At least once a year, the Board should set the company's risk appetite within cyber security as part of the overall cyber strategy understood as the risk the Board is willing to accept in order to achieve the company's strategic objectives.

The risk appetite is the link between the company's strategic objectives and its operations.

Among others, the risk appetite is determined considering the company's business objectives, risk exposure, and expected costs relating to further investments in a higher level of security.

The risk appetite may be set as a general objective (e.g. ensuring a "low risk" of abuse for data leaks, or maintaining a minimum level of security during outsourcing).

The risk appetite may also be quantifiable (e.g. a minimum availability on critical systems or a prohibition against storing sensitive data outside of Denmark).

Board members must be careful not to underestimate cyber risks, as that may lead to a distorted view of the actual risk appetite.

The Board can take inspiration from the list to the right when determining the risk appetite based on the company's risk assessment.

According to Deloitte Cyber Risk Landscape Report 2019, 50% of the surveyed leaders thought that their company could go back to 'business as usual' in a couple of days. More than 1/3 thought that it would take only one day. Smaller companies were most optimistic.

Key considerations in the board room

Strategy

- What are the general strategy and business objectives of the company?
- What is the digitization strategy of the company?

Risk exposure

- What is key in executive managements risk assessment (see '*Risk assessment and vulnerabilities*' in Theme 1), including in which areas are the company most vulnerable to attacks, what is the probability of an attack against the company in such areas, and what are the potential consequences of an attack, e.g. economic, societal and to the reputation.
- Does the company have critical infrastructure or is it otherwise subject to regulatory requirements that affect the risk appetite?
- Is the company about to invest in new technology and services (such as more IoT and cloud) that changes the risk exposure and require new security investments?
- Does the company have legacy systems (i.e. older systems that need replacing)?
- If so, does the company have a plan for phasing out or isolation of programmes and operating systems that are no longer supported or updated?

Costs

- What is the budget for cyber and information security?
- What is the company's security level and budget compared to other companies?
- What are the potential costs related to investments in security upgrade?

Risk appetite

- On the basis of an overall assessment, what is the company's tolerance for taking on cyber risks, including the tolerance value for the individual risks, e.g. risk type, product type, customers, strategy, objectives etc.?

Allocation

- Is the risk appetite implemented as a framework in the internal policies of the company, e.g. for operational risks, compliance risks, market risks, liquidity risks, insurance risks, outsourcing, etc.?

6. Toolbox

Theme 3 – Plans, processes, and contingency

The question is no longer ‘if’ a company will experience a successful cyber attack, it is a matter of ‘when’. Accordingly, all companies must have tested contingency plans in place and the board should inquire about tested plans and processes for preventing and reacting to cyber security incidents.

Even if the company already has security policies and contingency plans, such policies and plans may not take into account how the company actually identify, protects, detects and respond to a security incident and restores systems and services after an attack.

Security incidents can be costly in terms of root cause analysis, recovery actions, operating loss, compensation to customers, etc. Thus, it is important to have documented and tested policies, processes, and contingency plans in which the employees are trained in order to effectively prevent and respond to an attack.

The Board can take inspiration from the list to the right to determine if the company has in place an appropriate level of security and contingency, e.g. based on recognised standards.

If the company does not comply with an international standard or a security framework, it may be considered using e.g. ISO27001, which is an international standard for information security that has been mandatory to apply by Danish public authorities since 2014.

According to PwC 2019 Annual Corporate Directors Survey 53 % of the surveyed responded that the board felt confident in the company’s plan for managing security

Key considerations in the board room

Processes and policies

- Does the company have written IT security policies actively supported by the Executive Management and taught to the employees? E.g. policies on how often the IT security level must be tested/upgraded (such as policies suggesting that firewall audits must be performed monthly or that new applications must go through code review before being deployed), behavioural policies for employees, suppliers, customers etc.
- Is security made an integral part of the business processes of the company?

Contingency plans

- Are there any plans for system and data recovery (Disaster Recovery Plans and Technical Recovery Plans)?
- Are there any plans for how the business can continue in case of a lack of access to systems, programmes and data (Business Continuity Plans and IT Service Continuity Plans)?
- Do the plans describe who should be involved in the event of a crisis, e.g. communication, finance, management, legal, response team, and/or IT experts?
- Do the plans describe who the business can continue in the event of a crisis?
- Does the company have an agreement with external advisors or specialists that may be contacted to support the internal teams?
- Do the plans have procedures for orientation and escalation, e.g. when must the Board of Directors be briefed?
- What are the procedures for communicating with the authorities, e.g. police, supervising authority, the Danish Business Authority (virk.dk)?
- When and how does the company plan to inform other stakeholders, e.g. suppliers or individuals whose personal data has been compromised?
- Will the plans be rehearsed and tested regularly?
- What has been the result of recent tests, and has it led to any improvements?
- Will the plans be adjusted in the light of attacks that have occurred to other companies?

6. Toolbox

Theme 4 – Reporting and control

The Board shall receive understandable and measurable reporting on cyber threats, -risks, and -incidents in order to oversee the company's cybersecurity and to perform supervision and security control.

Adequate and relevant reporting is paramount, as the board cannot fulfil its supervisory task without understanding the company's potential threats and risks.

The Board should make cyber reporting an integral part of its annual wheel. An example of how this can be done is shown in Appendix 2.

The specific reporting the board should receive and how often is partly dependent on the individual company.

There is no standard reporting for cyber security, as opposed to e.g. financial reporting, why cyber reports tend to become more subjective.

It is important that the Board requests to receive consistent reporting on cyber and that the board receives sufficient information and data to understand the reporting and how it matches the general cyber strategy.

The Board can take inspiration from the list to the right in order to assess if the board receives adequate information.

According to PwC 2019 Annual Corporate Directors Survey 66 % of the surveyed responded that the board receives meaningful reporting on the field of cyber.

Key considerations in the board room

Reporting

- Does the Board receive reporting on the company's cyber security from the executive board after set intervals, e.g. concerning:
  - Top 5-10 most important cyber risks and most recent progress/trends
  - Results from tests of contingency plans and critical systems
  - Security incidents and consequences thereof
  - Status of implantation of security measures
  - Any derogations from the risk tolerances laid down by the Executive Management

  Results from internal and external audits
  Security budget and market comparison
  Insurance and the costs/losses they cover in a cyber attack
  Recommendations for improvements and investments related to this

Annual Wheel

- Has the board implemented cyber security as a permanent part of an annual wheel that ensures continuous observation and control as a regular part of the board's work, and ensures proper reporting in time?
- An example of an annual wheel with cyber activities is shown in Appendix 2.

Audit (on security)

- Does the company have certified auditors that prepares statements in relation to IT security, e.g. ISAE3402 or ISAE3000?
- Does the company require its customers or suppliers to have these statements prepared?

  Are there findings from these audits, and if so, a plan for repair?

Controlling Authorities

- Is the company in an industry or sector that requires continuous dialogue and expectation reconciliation with national authorities (e.g. companies providing critical infrastructure)?
- Does the company have a process of storing and reviewing data for any supervisory visits?

6. Toolbox

Theme 5 – Culture and people

Strategies and plans are important, but if they are not adhered to by management and employees, you are back to where you started. Employees are one of the most important sources to ensure a high level of security, as a security incident may be caused by a single inattentive employee.

There is a need for training and awareness programmes for employees in Danish companies, both in terms of sharing knowledge, increasing knowledge and changing behaviour.

The explosive growth of phishing emails, malware and ransomware targeting management and employees not only places great demands on the company's security measures but also to digital behaviour.

It may seem trivial, but for hackers it is much easier to get in via (bad) IT habits than having to hack in via the 'digital front door'.

There is a need for the Board to take the lead in supporting a culture in the company where security can be discussed openly, where employees can report mistakes and security breaches and learn from one's mistakes.

Work on awareness can take place at different levels, e.g. in terms of sharing knowledge internally, raising awareness/knowledge and changing behaviour.

The list on the right can be used as inspiration when discussing and challenging the executive management regarding the digital behaviour.

According to PwC 2019 Cybercrime Survey the unconscious actions of the employees/insiders constitute the biggest cyber threat. 54 % of the surveyed stated that the company actually did test its employees in awareness training etc.

Key considerations in the board room

Education, training and awareness

- Is there a training programme for Board Members, Executive management and employees to continuously receive cybersecurity and awareness training, including training in crisis management and disaster recovery?
- Is there a training programme for Members of the Board, the Executive Management and employees to receive ongoing education in cyber risks, e.g. through participation in external events, conferences and seminars focusing on cyber risk, cybercrime, and trends and developments within the company's industry?

Key people

- Does the company conduct background checks on key people when hiring?
- Do key people receive targeted education and training in cyber security?
  Is there any specific cyber security awareness program for key people or people with critical functions, e.g. a travel policy in relation to specific countries or a social media policy, BYOD (bring your own device)?

Culture and knowledge sharing

- Is there a cross-organization collaboration where knowledge is shared?
- Does the company encourage its technical specialists to exchange knowledge and experience with employees from similar organizations to take advantage of the 'wisdom of the crowd' with regards to prevention?
- Does the IT responsible use his/her network and partnership to strengthen knowledge and competences within cyber?
- Does management support a positive security culture, e.g. by continuously informing about the cybersecurity strategy, the current threats, and how the company is protected?

6. Toolbox

Theme 6 – Competences and organisation

Board members are expected to be capable of understand and addressing key issues in relation to cyber security and to participate in discussions on the topic with the executive board.

The Board does not need to know cyber and information security in every detail, but at least one member should have insight in the company's technology and security landscape and be able to discuss the issue on equal footing with the executive management.

Cyber and information security is too important and complex to leave the understanding to only a few, and IT is too critical and the risk too great for the Board not to stay updated on the issue.

The Board is ultimately responsible for ensuring that the right competences are present in the board and in the company – regardless of delegation and outsourcing.

Until the right competences are present, the Board must ensure that both the Board, Executive Management and the organisation have access to the necessary competences and resources in the field of cyber – if necessary, through agreements with external partners and specialists.

The Board can take inspiration from the list to the right in order to assess whether the right competences and division of roles are in place.

According to PwC 2019 Annual Corporate Directors Survey 36 % of the surveyed responded that the board had sufficient competences in the field of cyber.

Key considerations in the board room

The Board of Directors

- Does at least one member of the board have competences and experience with cyber and information security, e.g. cyber security and risk assessment processes, supplier management, security requirements etc.?
- Is cyber security a permanent subject on the agenda of the board meetings?
- Does the board stay updated on cyber threats and actors threatening the company, their methods and their motivation?
- Does the board actively participate in discussions about cyber security?
- Does the board receive ongoing training and education in cyber security matters?
- Is the board aware that it itself may be an obvious target for cyber attacks (e.g. CEO fraud)?

The Executive Management

- Does the company have a security organisation firmly anchored at the executive level, e.g. CEO, CFO or CIO?
- Does this function report directly to the board or through another process of reporting?

The organisation

- How is the responsibility for cyber and information security otherwise allocated in the organisation (person/function)?
- Should other business units be involved in the work with cyber security, e.g. head of departments of product/service development?
- Who does this security function report to?
- Have sufficient resources with adequate technical competences been allocated to handle the task?

External

- Does the company have the right technical competences inhouse or does it need external assistance?
- Does the Board need help with the supervisory task, e.g. from advisors or a committee?
- Would the Board benefit from getting external experts to present trends and best practices in order to provide cyber security with an extra perspective.

Appendix 1. Glossary – examples of selected terms and key concepts within cyber security

Botnet: A botnet is a network of compromised computers controlled by a third party. A botnet is created when computers with internet access are infected with malware, after which the person who controls the botnet can use it to perform DDoS attacks, phishing attacks (spam), distribute malware, mine bitcoins, etc.

CEO fraud: CEO fraud involves the duping of business information or paying money by pretending to be a CEO of the company. Often uses (spear)phishing techniques (such as email) and social engineering.

DDoS-attack: Short for Distributed Denial of Service and is an overload attack. Hackers exploit compromised computers (a botnet) to generate unusually large amounts of data traffic against a website (web server) or a network, leaving the website or network unavailable for legitimate traffic during the attack.

Drive-by exploits: An expression that indicates that the affected company was not the target of the campaign, but was hit by accident.

Malware: Malware means malicious software and is a term for computer programs that do malicious, harmful, or unwanted things on the devices on which they are installed. The term covers all categories of malicious programs including viruses and worms such as spyware, ransomware, botnets and Trojans. Antivirus programs usually fight not only viruses, but several different types of malware.

Man-in-the-middle: Attacks where a malicious device or person is located between two devices, for example, between the user and the router. This allows the intermediary to access all data send by the user.

Mass interception: Massive monitoring of telecommunications and internet activity, for example through logging of internet sessions. Performed by states, but can also by the use of extensive networks of surveillance programmes be used by IT criminals to collect huge amounts of behavioural data.

Phishing/spear phishing: Phishing is an attempt via social engineering to manipulate a person to in good faith forward personal information or click on infected files or links to fake websites. Phishing emails are often widely sent to many recipients. Spear phishing is particularly distinguished by targeting the individual recipient and applying social engineering techniques. Emails are typically designed to make them seem particularly relevant, compelling and trustworthy to the recipient, e.g. to use names, person-specific information or relevant files discovered by prior reconnaissance.

Ransomware-attacks: In a ransomware attack, data and systems on the victim's computer are held hostage as they are encrypted and thereby become inaccessible. The person responsible for the attack typically requires a ransom in the form of cryptocurrency (such as Bitcoin), to allow access to data again. Commonly, the person responsible for the attack will install malware using phishing emails. Most ransomware attacks succeed because the user is cheated to click on a link or attachment in an email, but ransomware attacks can also be done via text messages or advertising banners on a website. There are many variants of ransomware. Targeted ransomware attacks try to hit e.g. administrative networks in specific companies and authorities.

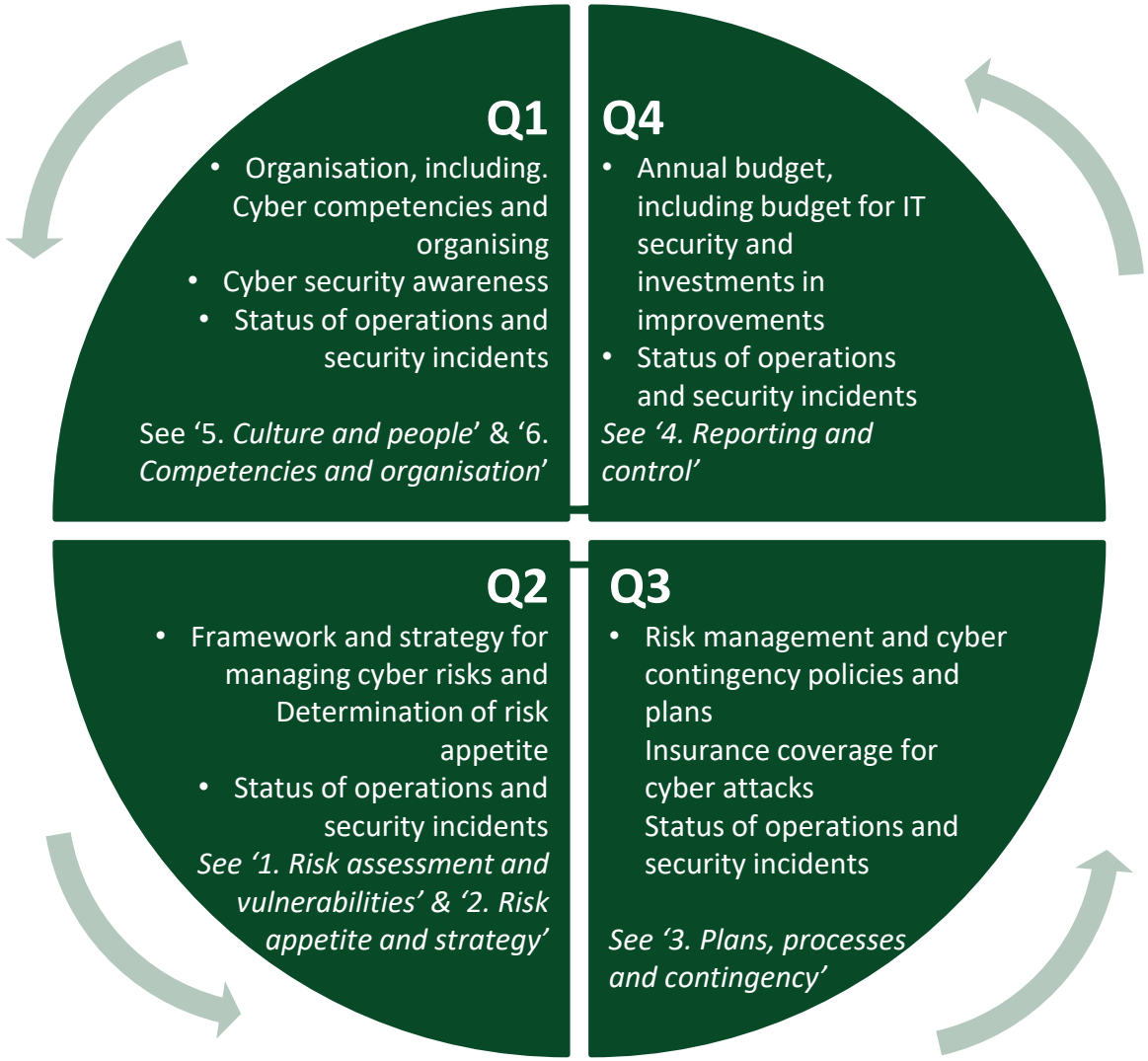
Social engineering:

An expression of exploiting social interactions and psychological tricks to trick a person or company into providing information, accessing systems or transferring money to them.

SQL injection: Attacks aimed at the database layer in software that exploits a vulnerability in handling input and database calls. The database call is manipulated through the input (typically using special characters) to achieve a different effect than the intended one - for example, to reveal who has administrator privileges.

There are various definitions of key concepts in cyber and information security. Selected concepts appear in this appendix.
More information can be found in CFCS's dynamic glossary: https://fe-ddis.dk/CFCS/PUBLIKATIONER/ORDFORKLARING/Pages/default.aspx

Appendix 2. Annual wheel – An example of the section relating to cyber matters



Appendix 3. Checklist of key cyber security issues for Boards

Summary of the questions in item 6, theme 1-6

1. Risk assessment and vulnerabilities

- ❑ What does it mean for the business if valuable assets are changed, stolen, or leaked, or if critical systems or other IT services are unavailable for a shorter or longer period of time?
- ❑ Who are the likely attackers, what are their goals, and what tools or techniques do they use to achieve these goals?
- ❑ In which areas is the company most vulnerable to cyber attacks (technology, people, processes, etc.) and how likely are cyber attacks in these areas?
- ❑ What is the company's current risk management plan, including investments?

2. Risk appetite and strategy

- ❑ How big is the company's cyber security budget?
- ❑ What is the company's level of cyber security and cyber security budget compared to other business areas - and to other companies?
- ❑ What are the potential costs associated with investing in a security level upgrade?
- ❑ Based on this, what is the company's risk tolerance relative to cyber risks?

3. Plans, processes, and contingency

- ❑ Does the company have documented IT security policies that are actively supported by the management and that the employees are trained in?
- ❑ Does the company have contingency and communication plans in place to handle cyber security incidents?
- ❑ Do the plans describe how the business can quickly resume work after an unplanned incident, who needs to be involved in the event of a critical incident, and how affected systems and services are recovered?
- ❑ Are the plans being tested and rehearsed regularly?
- ❑ What are the results of the recent tests, and has this led to any changes?
- ❑ Are the plans adjusted in light of security incidents that have hit other companies?
- ❑ Does the company have agreements in place with external specialists who can be called in to support the internal teams in the event of a security incident?

4. Reporting and control

- ❑ Does the Board receive reports on the company's cyber security (risk assessments, investments, recommendations, etc.) from the Executive Management at regular intervals?
- ❑ Has the board implemented cyber security as a permanent part of an annual wheel?

5. Culture and people

- ❑ Is there a training and education program for Members of the Board of Directors, the Executive Management, and employees to receive cyber security and awareness training on an ongoing basis, including crisis management and disaster recovery?
- ❑ Is there a collaboration across the organization where knowledge is shared?
- ❑ Does the company encourage its technical specialists to share knowledge and experience with specialists from other organisations?
- ❑ Does the Board lead by example to help promote a healthy cyber security culture?

6. Competences and organisation

- ❑ Do at least one permanent board member have technical or security expertise? If not, does the Board seek advise on cyber security issues, e.g. from external consultants or a committee?
- ❑ Is cyber security a regular item on the agenda of board meetings?
- ❑ Does the Board actively engage in cyber security discussions?
- ❑ Is the Board aware that its members are obvious target for cyber attacks?
- ❑ Where is the responsibility for cyber security placed in the organisation (person(s) or function(s))?
- ❑ Who are these person(s) or function(s) reporting to?
- ❑ Are sufficient resources with the right technical skills allocated to carry out the tasks related to cyber security?
- ❑ Does the company have access inhouse to the right technical skills or is there a need to procure external assistance?

Appendix 4. References and background material

Centre for Cyber Security	> Cyberforsvar der virker: (https://fe-ddis.dk/cfcs/publikationer/Documents/Cyberforsvar%20der%20virker%20-%202017_110117.pdf) > CFCS: Ordforklaringer: (https://fe-ddis.dk/CFCS/PUBLIKATIONER/ORDFORKLARING/Pages/default.aspx) > CFCS: Cybertruslen mod Danmark: (https://fe-ddis.dk/cfcs/publikationer/trusselsvurderinger/Pages/default.aspx)
Deloitte	> Cyber Risk Landscape Report 2019: (https://cyber.deloitte.dk/artikler/artikler-it-sikkerhed/cyber-risk-landscape-report-2019/)
The Agency for Digitisation	> Sikkerdigital.dk (https://sikkerdigital.dk/virksomhed/) > Vejledning i it-risikostyring og vurdering: (https://sikkerdigital.dk/media/10382/vejledning-it-risikostyring-og-vurdering.pdf)
The Danish Business Authority	> Styrket digital sikkerhed i virksomhederne: (https://erhvervsstyrelsen.dk/styrket-it-sikkerhed-i-virksomhederne)
IBM	> IBM X-Force Threat Intelligence Index 2019 (https://www.ibm.com/security/data-breach/threat-intelligence)
Industriens Fond	> Projekt for Styrkelse af Strategiske Cyberkompetencer: (https://www.industriensfond.dk/Styrkelse-af-Strategiske-Cyberkompetencer)
National Cyber Security Centre (UK)	> Board Toolkit (https://s3.eu-west-1.amazonaws.com/ncsc-content/files/board_toolkit_final.pdf)
PwC	> Hvordan kan din bestyrelse være effektiv i håndteringen af cyberrisici? (https://www.pwc.dk/da/nyt/publikationer/bestyrelseshaandbogen-2019/bestyrelse-haandteringen-af-cyberrisici.html) > 2018 Global State of Information Security: (https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html) > 2019 Annual Corporate Directors Survey: (https://www.pwc.com/us/en/services/governance-insights-center/assets/pwc-2019-annual-corporate-directors-survey-full-report-v2.pdf.pdf) > 2019 Cybercrime Survey: https://www.pwc.dk/da/publikationer/2019/11/cybercrime-survey-2019.html
World Economic Forum	> Advancing Cyber Resilience Principles and Tools for Boards: (http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf) > Ten Ways the C-Suite Can Protect their Company against Cyberattack: (https://www.weforum.org/press/2019/10/ten-ways-the-c-suite-can-protect-their-company-against-cyberattack/)