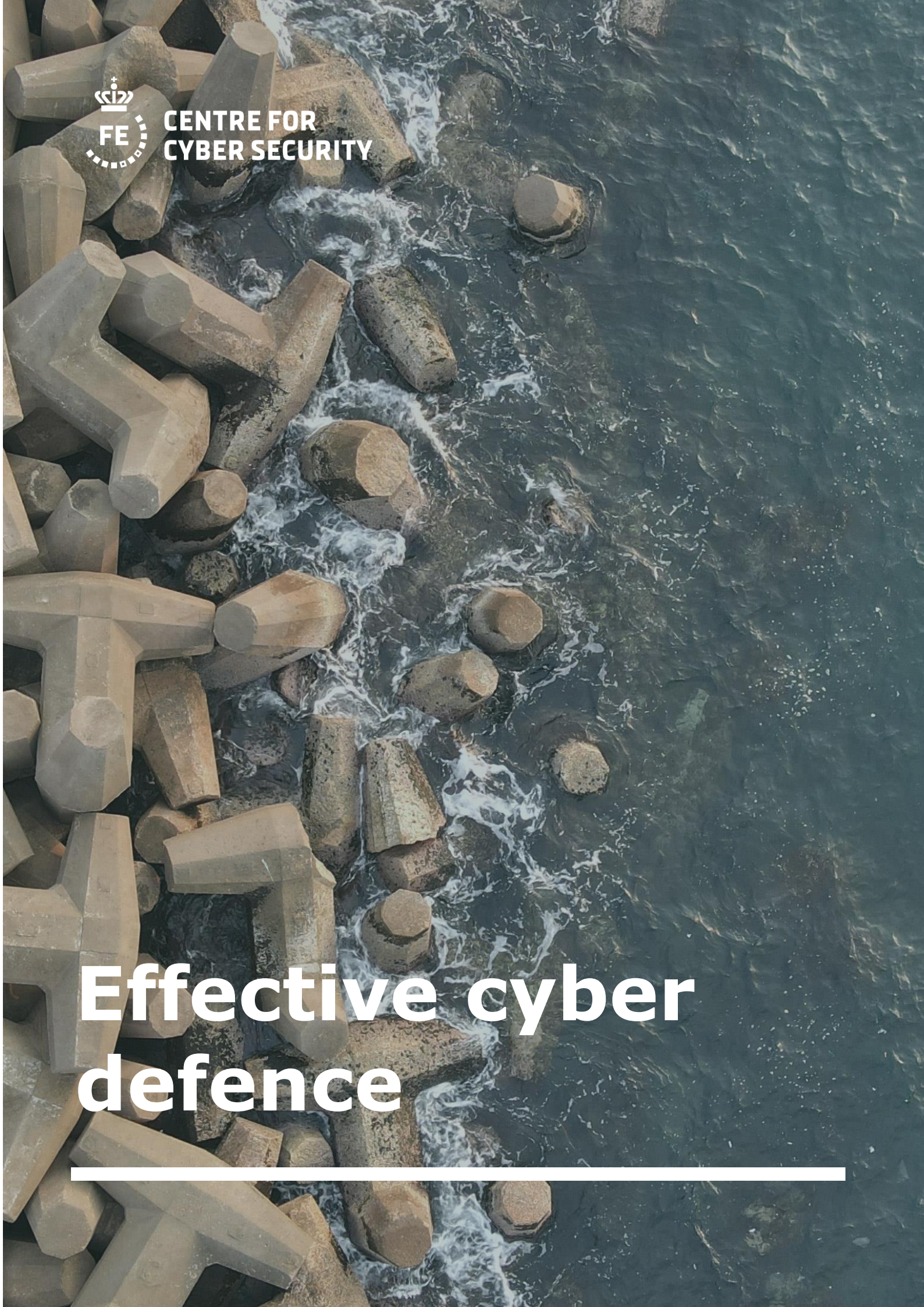

CENTRE FOR
CYBER SECURITY
Effective cyber defence

Table of contents

CENTRE FOR CYBER SECURITY

Kastellet 30
2100 København Ø
Tel: + 45 3332 5580
Email: cfcs@cfcs.dk

Front page illustration: Evgeniy Pavlovski/Shutterstock
4th edition, October 2023.

Introduction

The cyber threat is a constant concern for Danish public authorities and private companies. In short, it is a matter of when, not if, an organization falls victim to a cyber attack. ”Effective cyber defence” is a guide that contains six steps that organizations can take to establish basic cyber defences. By following these steps, organizations can prevent many of the cyber attacks they encounter on a daily basis, and effectively mitigate successful attacks.

6 steps for an effective cyber defence

1) The management's toolbox
2) Helpful technical measures
3) Conduct is key
4) Detect your enemy
5) Be prepared!
6) Spot the gaps in your cyber defence

Cyber security vigilance at the executive level is the cornerstone of an effective cyber defence. The top management has to govern cyber and information security by continuously supporting, prioritizing and following up on security objectives and strategies with the same vigilance as applied to other business matters, for example finance and HR. Ensuring an effective cyber defence is not a one-time project but rather a continuous process that requires constant evaluation and optimization. This applies to all six steps in this guide. Consequently, the top management has to ensure continuous follow-ups and improvement.

We recommend that Danish organizations use international standards and best practices as a starting point. In Denmark, the following cyber security frameworks are often used: ISO 27001, NIST Cybersecurity Framework, SANS and CIS 18. Compliance with standards and best practices creates a foundation for establishing set and repeatable processes that improve cyber and information security within organizations.

Target audience

”Effective cyber defence” is intended for all public authorities and private companies with complex IT systems and may also be useful to anyone interested in good cyber and information security practices. This guide is directed primarily at top management, and cyber and information security staff.

Public authorities and private companies may be obligated to comply with specific cyber and information security requirements. Such requirements may entail following a particular standard, for example ISO 27001, or implementing specific technical measures such as ”The technical minimum requirements for government authorities”.

”Effective cyber defence” does not replace such requirements, and this guide should be read in the context of these requirements.

Step 1: **The management's toolbox**

An effective cyber defence is anchored in top management. In essence, it is about the top management overseeing cyber and information security on an equal footing with areas such as finance, HR, development and research. Similarly, the handling of personal information has become an area that requires top management oversight. Even the very best intentions regarding an effective cyber defence will fail without anchoring at the top management level.

It is important for a leader to understand the cyber threat. It is equally important to realize that this threat is an underlying condition for all Danish organizations. The top management must take ownership of the organization's cyber and information security objectives and strategies. The policies, procedures and guidelines used to manage cyber and information security within the entire organization must reflect these objectives and strategies.

The top management must prioritize the establishment of repeatable processes designed to support the organization's cyber and information security strategy. Without established and documented processes, there is a risk of managing cyber and information security risks on an ad hoc basis with an over dependency on few key personnel. The top management must ensure that the established processes are regularly controlled and improved in order to ensure their efficiency.

There is also an important cyber and information security aspect to consider when organizations develop and implement new infrastructure, systems and applications. The top management must ensure that fixed processes are in place in which cyber and information security is a guiding principle.

In general, the top management must prioritize and oversee cyber and information security across the organization. In this context, it is important for the top management to ensure that the right skills are available, either on-premise or off-premise in the form of external consultants or advisers.

The formulation of objectives and strategies, prioritization of resources, establishment of repeatable processes and regular follow-ups are the management's most important tools when overseeing cyber and information security.

We recommend that the top management asks itself eight questions and asks its organization sixteen questions. The answers to these questions will give the top management an idea of how the organization manages cyber and information security.

Good questions are important tools

The answers to the following questions can give the top management an indication of whether, and to what extent, appropriate security measures are in place. The top management and the rest of the organization should be able to answer the questions within each category. The sequence of the questions does not reflect any prioritization of the questions.

8 questions that the top management should ask itself

1. Have we identified data and information that support critical business activities?
2. What are the consequences for the business, if data or information that support critical business activities is unavailable, manipulated or leaked?
3. Are we convinced that there is adequate protection of our information against known threats?
4. Have we defined the cyber and information security objectives, strategies and policies that we are actively prioritizing and pursuing?
5. Do we have a security organization anchored at top management level?
6. Do we receive regular reporting on the status of our cyber and information security strategies and objectives?
7. Have we considered our organization’s security risk appetite?
8. Do we understand that we as members of the top management are obvious targets of cyber attacks (for example of CEO fraud and spear phishing)?

16 questions that top managements should ask their organizations

1) Which IT systems support our business critical activities?
2) Where do we store our most important data and information?
3) How do we keep ourselves updated on the cyber threat landscape and on the techniques used, among others, in cyber espionage and cybercrime?
4) How do we defend against cyber attacks such as phishing attacks and CEO fraud?
5) Are we obligated to comply with external cyber and information security requirements (for example standards or technical measures)?
6) Which methods do we use to control access to IT systems, data and information?
7) Which special precautions do we take when travelling?
8) How do we ensure that IT systems, computers and phones are updated?
9) How do we ensure the use of strong passwords to gain access to IT systems, computers and phones?
10) How do we supervise the use of user accounts with privileged rights?
11) Do we have the skills and resources needed to implement our cyber and information security strategies and objectives?
12) How do we educate our employees on cyber and information security practices?
13) Do we encourage relevant staff members to share cyber security knowledge and experience with staff members from other organizations?
14) When did we last test the effectiveness of our crisis management?
15) Do we regularly carry out internal cyber and information security controls, audits or revisions?
16) How do we ensure that business partners and suppliers protect data and information that we share with them?

The answers to these questions will enable the top management to identify areas that need increased focus and attention. In this way, the questions serve as a tool to help the top management oversee cyber and information security in the organization.

You can find further guidance on how to understand and answer these questions at sikkerdigital.dk, where a number of guides, templates, etc. are freely available to public authorities, private companies and citizens.

Step 2: **Helpful technical measures**

Implementation of appropriate technical measures can significantly reduce the risk of falling victim to a cyber attack. The appropriate technical measures can also make it easier to detect and mitigate cyber attacks that have breached cyber defences. We recommend that organizations give high priority to the implementation of technical measures in their cyber security efforts.

We have compiled a list of ten areas (see the following page) where organizations should prioritize the implementation of technical measures. The list is not set in order of importance but outlines steps that organizations are advised to adopt as part of their effective cyber defence.

Typically, an organization's IT department or external consultants will be responsible for implementation of technical measures in the organization's IT environments. It is essential that the IT department or the external consultants adopt a systematic approach to the implementation and continuous maintenance of the technical measures. We recommend that organizations follow standards and best practices such as ITIL and CIS 18 to ensure systematic implementation, documentation and continuous maintenance.

Organizations that have outsourced their IT operations must ensure that the supplier does in fact implement the appropriate technical measures. We recommend that organizations require their suppliers to provide regular reporting on both the organizations' IT environments and the suppliers' own IT environment, as a weakness in the supplier's own IT infrastructure may result in damage to the organization's IT systems. We have published a guide on information security in customer-supplier relationships which describes some of the issues to address in connection with the use of IT suppliers (CFCS & DIGST, *Cybersikkerhed i leverandørforhold*, 2022). Our guide on the use of cloud solutions (CFCS & DIGST, *Vejledning i anvendelse af cloudservices*, 2020) deals with issues relating to cloud sourcing.

Technical measures act as a bulwark against cyber attacks – in other words, they help ensure an effective cyber defence. However, technical measures alone will not suffice. Employee behaviour is equally important as a solid line of defence against cyber attacks.

The implementation of even basic technical measures requires the right technical skills. Consequently, it is vital that the relevant staff in the organization understand these measures and are able to implement them. If this is not the case, then it is up to the top management to prioritize and ensure access to such skills, for example by use of external consultants or advisers.

No.	Area and measures	Description
1	Keep operating systems and applications updated	All software, including operating systems, applications and firmware on clients, mobile devices, servers, network equipment, etc. must be updated when new versions or security updates are released from the supplier. The update must follow a fixed process that helps ensure that potential compatibility issues or inadequacies are uncovered before the update is transferred to the production environment. Deadlines are set as to how fast security updates should be commissioned after their release.
2	Segment networks and limit traffic between segments	The organization's internal networks should be physically or logically divided into network segments, allowing a unit (clients, mobile devices, servers or network equipment) to be placed in a segment in accordance with its use and sensitivity. The network traffic between individual network segments must be limited to only that which is required and, if possible, be protected and monitored.
3	Protect clients with antivirus programmes and firewalls	All clients must be protected by an antivirus solution and a locally installed firewall.
4	Control user accounts and rights	Creation, use and closure of user accounts must take place based on a senior management approved process. The granting of rights, including privileged rights, must only take place based on work-related requirements. These rights must be continuously reviewed, updated and approved in relation to potential changes in roles and responsibility. Privileged rights to clients, applications and systems must be granted on a "need to have" basis.
5	Use secure passwords and multi-factor authentication	Access to any account must be protected by use of secure passwords and, if possible, be supplemented with multi-factor authentication. Access to accounts with privileged rights must be protected with multi-factor authentication, including accounts that are used in connection with remote access to organization systems.
6	Conduct backup of data and configurations and test recovery	Backup of data from business critical IT systems must be conducted. Backup must always be conducted in accordance with organization policies that consider the consequences to an organization if data in the production environment is lost. Configurations and systems, which are necessary to recover following a major security incident, must also be included in the backup. Regular testing must be undertaken to ensure that the backup contents are complete and that data and configurations can be loaded from backup. A copy must be kept offline.
7	Establish logging of anomalies and security incidents	Logging of key systems must be enabled, including successful and failed login attempts. Logging of configuration changes and access to sensitive data or systems must also be logged. Logs should be kept separately and with limited access and be regularly reviewed. Logs must be kept for an adequate period of time.
8	Protect remote access to systems	Remote access to organization systems must be protected with multi-factor authentication. The integrity of the communication must be protected by encryption, for example by use of HTTPS or a VPN service.
9	Encrypt data on clients and mobile devices as well as communication over other networks	Data on clients and in particular portable clients used outside the organization must be protected by full disk encryption. Similarly, data on mobile devices should be protected with encryption and possibly administered at an MDM (Mobil Device Management) platform, which also allows remote deletion. All communication with organization systems over other networks outside organizational control must be encrypted.
10	Compile a list of approved applications (whitelisting)	Installation and closure of applications on organization clients must be limited to the pre-approved applications authorized for use in the organization.

Step 3: **Conduct is key**

Employee behaviour and skills play an active and critical part in an effective cyber defence. International surveys estimate that the majority of breaches can be attributed to the human factor[1].

Most employees are recruited based on their expertise within the organization's core business, not their cyber and information security knowledge and awareness. Changing behaviour and habits generally requires a lot of effort on the part of the individual employee, especially when it comes to making adjustments outside their main work function. The organization should consider this factor when working to establish a good security culture.

Five essential phases in creating a good security culture
We recommend that the organization's top management calls for and initiates the following security enhancing activities in order to facilitate the desired security behaviour:

It is important that the organization knows which security behavioural challenges it is facing and addresses these challenges from a behavioural perspective.

The nature of any given behaviour initiative depends on the problem identified in the target group. Posters, newsletters and information meetings can be a good place to start introducing basic security awareness. However, such initiatives are seldom enough to change security behaviour. To achieve lasting change in security behaviour, initiatives must therefore aim to tackle the identified security behaviour problems through a customized course of action. For example, an identified security behaviour problem could be "persistence" – which is to say that the target group has difficulties in maintaining the security choices in the long term due to lack of motivation or because the desired security behaviour is not compatible with other objectives. In this context, a course of action to improve security behaviour could be reducing barriers, including reducing the number of times that employees have to click to make sound security choices. Another course of action could be the introduction of a systematic feedback regime when making good security choices such as real-time feedback when reporting phishing emails.

[1] https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/

Good security behaviour is not about knowledge, but about conduct.

It is crucial to build security behaviour initiatives on solid analytic work that identifies the causes of the behavioural problem. If not, efforts to change security behaviour will rarely be successful. Furthermore, it is essential that organizations test initiatives before a full-scale implementation. Tests will also identify any potential side effects. Organizations should make ethical considerations part of the development of any initiatives that intervene in human behaviour.

Optionally, organizations can gain further insight from our codex for running security test, which is available in Danish at digst.dk.

Finally, it is of course important for the organization to evaluate and follow-up on its security behaviour initiatives. In this way, the organization can adjust behaviour initiatives as needed and ensure continuous efforts to build a good security culture in the organization (CFCS & DIGST, *Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed,* 2021).

Step 4: **Detect your enemy**

An organization's ability to detect cyber attacks is dependent on its active use of monitoring to reveal abnormal activity patterns or other indications of potential cyber attacks. Cyber security monitoring is a key component of an effective cyber defence. Step 4 primarily deals with the policies, processes and procedures that must be in place in order for organizations to detect a cyber attack.

Monitoring
Before using monitoring as a means of detecting cyber attacks, organizations must identify their business-critical IT assets.

Firstly, organizations should ensure monitoring of business-critical IT assets and should monitor the appropriate aspects (parameters). To begin with, monitoring should be in place at all levels, from the network to application layers and on the organization's IT units. Be thorough when choosing the appropriate parameters for monitoring as monitoring of encrypted traffic, for instance, is not necessarily informative. Keep in mind that the term "security monitoring" often covers more aspects than typical operations monitoring of IT solutions.

Next, organizations should set up "alarms" that are triggered if any activity is observed that deviates from normal network activity or resembles known attack patterns, or if an activity threshold is exceeded, for instance too many rejected login attempts as a result of wrong password entries. In this respect, the occurrence of false alarms in the start-up phase is quite normal, as activities that register as anomalies are in fact part of the normal picture.

The organization itself can undertake monitoring; however, this requires specialist skills. For this reason, we recommend that organizations outsource monitoring when such skills are not available within the organization.

Examination of potential incidents
In order to expose the chain of events in a potential incident, the organization must decide how to integrate monitoring data into the organization's overall logging. We recommend centralizing collection and processing of selected monitoring data and logs from relevant network components. This may be undertaken either by the organization itself on-premise or off-premise by an external provider.

For more information on which types of logs that may be required when examining potential cyber incidents, see the CFCS guide: "Logging – part of a god cyber defence" (2023) at cfcs.dk.

The CFCS situation centre provides a 24-hour on-call service for reporting IT incidents.[2]

[2] https://www.cfcs.dk/da/om-os/netsikkerhedstjenesten/situationscenter/

Step 5: **Be prepared!**

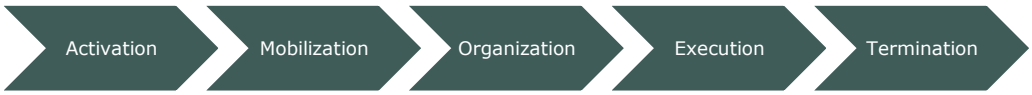
Regardless of the number of technical and organizational measures implemented and in spite of excellent in-house education programmes, it is only a matter of time before a cyber attack will hit your organization.

The lesson here is to have a strategy in place in case a cyber attack occurs and cripples parts of your organization. This includes cyber attacks on suppliers or business partners.

In relation to serious cyber incidents that cannot be addressed within the framework of normal operations, it is first and foremost important that organizations know when and how to activate their crisis management regime. The main goal of crisis management is to handle the unfolding crisis and to restore normal operation as quickly and effectively as possible. This is only possible if the crisis management team has the right members with the right skills. If such skills are not available in-house, we recommend assigning external members to the team.

During a crisis, it is important that organizations take a broad approach to crisis management. Bearing this in mind, a crisis caused by a cyber incident cannot be reduced to a mere IT issue but will entail crisis management within IT as well as other domains such as communications and business.

Effective crisis management requires an operational response plan that is up-to-date, tested and approved by the management. We recommend creating a response plan that involves these five phases.



Activation
Organizations must determine the specific criteria that activate the crisis response, and identify who in the organization has the authority to activate and convene the crisis management team. It would be advantageous for organizations to bridge any gaps between the crisis response plan and existing IT incident management processes. There will often be a category of IT incidents called "major incidents" or "serious incidents". It is only when major IT incidents fall within the activation criteria that organizations should consider activating the crisis management regime.

Mobilization
When the crisis response plan is activated, the members of the crisis management team must be mobilized. A crisis response plan must include a description of how to mobilize and convene the crisis management team. The description should have sufficient details on how the members of the crisis management team are to be contacted and by whom, how quickly they are to convene and where. Weigh the possibility of whether team members should meet physically or virtually. If the team meets physically, communicate the necessary details – address, meeting room and any accessibility issues - clearly to the team members.

The Danish Agency for Digitisation has developed a basic emergency action plan template that organizations can fill in and use to provide the crisis management team with a quick overview of contact information, meeting places and first steps when responding to an incident.

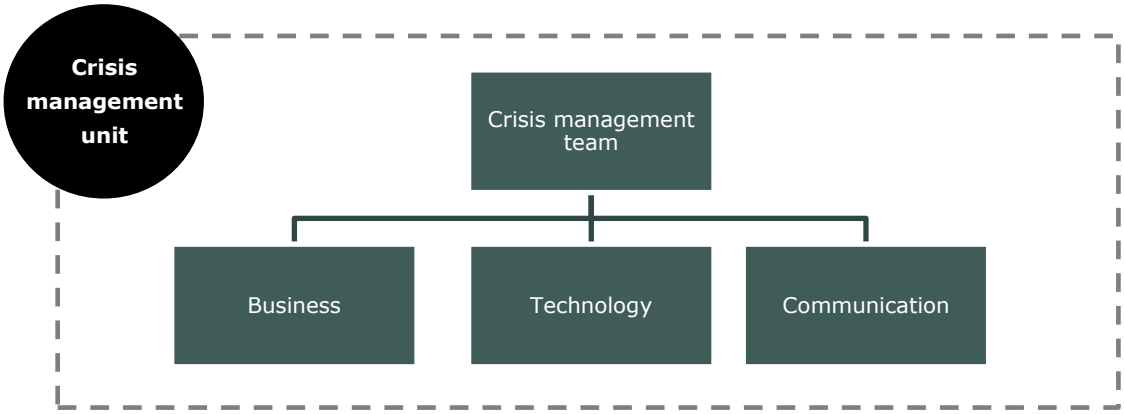
Basic emergency action plan templates can be found at: sikkerdigital.dk.(only available in Danish)

It may be relevant for some organizations to designate an alternative meeting location for their crisis management team. As a rule, we recommend that the crisis management team meets at the organization's place of business. However, if the team chooses to meet virtually, whether by video conference or chat forum, the platform must be easily accessible and known to all team members in advance. For more information on how to work safely on virtual meeting platforms, see the CFCS guide "Råd om sikkerhed på virtuelle mødeplatforme" at cfcs.dk (only available in Danish).

Organization

The crisis management team must include relevant representatives from across the organization. The team must be able to use extra resources and to make decisions that may have extensive implications for the organization. The representatives in the crisis management team must therefore have decision-making authority over financial and staff resources.

The organization of a crisis management unit depends on the organization's structure; however, organizations can use the model below as a template:



It is essential to staff the groups under the crisis management team with employees with in-depth knowledge in the respective areas. We recommend the inclusion of representatives from suppliers and business partners, who are part of the operations and critical business areas affected by the crisis.

As a crisis may be protracted, we recommend that practical issues such as catering, cleaning, etc. are included in the overall organization and planning.

Execution

Once the crisis management team has convened, it must ensure that the relevant staff functions are present and assign the relevant roles to team members. Then team needs to agree on meeting frequencies and the agenda for meetings. The purpose of the crisis meetings is to create situational awareness and to ensure that suitable measures are taken to handle the crisis as quickly as possible.

The summaries of each meeting should be distributed among the team members to ensure that members know their tasks leading to the next meeting.

We recommend that crisis team members follow the steps in the cycle above during the execution phase of the crisis response plan. The first step is to define and isolate the cause of the operational interruption. The second step is to remove and eradicate the cause of the interruption. The third step is to restore the affected systems and networks. This 3-step cycle can be repeated as required and scaled to fit the relevant system and network level.

In this phase, it is important to have access to adequate logs. The use of logs can help to assess the extent of the attack on the organization’s IT assets. Another essential factor at this phase is restoring relevant configurations and data using backups. A review of relevant logs and monitoring makes it possible to identify how far back in time restoration of data is needed to ensure that the data backup is consistent with the state of the data before the compromise occurred. We recommend that organizations with no in-house resources for forensics and remediation engage external consultants to handle these tasks.

Termination

After completing effective isolation, eradication and recovery, the crisis management team can disband and the organization can return to normal operations. However, the crisis management team must verify the following before demobilizing the team and reporting that the crisis is resolved:

- That the restoration of IT systems has been successfully completed, alternatively that a clear time-plan for the completion of restoration is in place.
- That relevant documentation related to the management of the crisis, from both the crisis management team and groups under the team, is secure, and that a timeframe has been set for completing the crisis report.
- That all crisis-related communication to internal and external stakeholders are concluded.

Finally, the crisis management team should schedule a follow-up meeting to run through the crisis report. The lessons learned during the crisis should give rise to tangible actions such as changing existing business procedures, implementing training courses or revising risk assessments and protection measures.

Step 6: **Spot the gaps in your cyber defence**

Cyber and information security is evolving rapidly. Organizations must therefore continuously look for gaps in their cyber defences. Yesterday's or today's cyber defences may not be adequate to stop tomorrow's cyber attacks.

A key element of an effective cyber defence is therefore an organization's on-going assessment of its existing security measures.

We recommend that organizations routinely assess the security measures and processes implemented to determine whether they do in fact have the desired effect and whether new measures or processes are required.

Different types of security assessments
There will be different methods for detecting gaps depending on the area assessed. For example, a technical assessment may include vulnerability scans and penetration testing (called "pen testing"). An assessment of the organization and its processes will typically be in the nature of internal control, audit or revision. An assessment of employee behaviour will typically be in the nature of evaluations or tests – for example phising tests.

To a large extent, organizations will be able to carry out certain types of assessments by themselves, for example internal control, inspections and internal audits. Other types of assessments will require the assistance of external partners such as certified auditors, accountants, IT experts, etc. In the context of technical assessments, it is advisable to run regular scans of key IT assets to detect known vulnerabilities, also called CVEs (Common Vulnerabilities and Exposures).

A range of tools is available to perform so-called vulnerability scans. As specialist skills are required to perform such scans, we recommend outsourcing vulnerability scanning if the relevant skills are not available in-house.

Organizations can also consider performing penetration tests. These tests simulate scenarios where a third party tries to break into the organization's network, components, systems and applications using the methods a criminal or a spy would apply. As is the case with vulnerability scanning, penetration testing requires specialized skills.

The top management must prioritize resources for regular assessments of the organization's cyber and information security. This includes ensuring that the required skills are available either in-house or through external consultants and partners.

No matter the type of assessment an organization performs, the application of its results is key.

It is important that management requests reporting of results on the effectiveness of implemented cyber security measures and processes. Cyber and information security management reports can, for example, be dealt with at executive or board meetings on an equal footing with reports regarding finance, research and development, etc.

Applying assessment results

Organizations must use the results of an assessment to prepare a prioritized plan for minimizing the security gaps. In this respect, it is essential that the plan ultimately gains top management approval. As is the case with other business areas, the prioritization of the different elements of the plan should be in accordance with the organization's risk appetite.

Some organizations have a dedicated security organization with top management representation, while others have assigned such matters to the board. The top management's involvement in the prioritization is vital as the management must manage and prioritize the organization's cyber and information security based on the organization's risk appetite.

Regular and systematic assessments, whether internal control, audits, tests or revisions, are one of the key tools for managing cyber and information security in organizations and subsequently for an effective cyber defence.

References

- Australian Cyber Security Center (AU). (2023). *Essential Eight Explained*. *https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained*
- Canadian Centre for Cyber Security (CA). (2021). *Top 10 IT Security Actions to Protect Internet Connected Networks and Information.* *https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089*
- Center for Internet Security. (2021). *CIS Controls V8.* *https://www.cisecurity.org/controls/v8_pre*
- Infosecurity Magazine. (2021). *90% of UK Data Breaches Due to Human Error in 2019.* *https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/*
- National Cyber Security Center (UK). (2021). *10 steps to Cyber Security.* *https://www.ncsc.gov.uk/collection/10-steps*
- National Cyber Security Center (UK). (2023). *Board Toolkit v2.* *https://www.ncsc.gov.uk/collection/board-toolkit*
- National Security Agency (US). (2018). *NSA'S Top Ten Cybersecurity Mitigation Strategies.* *https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf*
- Nasjonal sikkerhetsmyndighet (NO). (2022). *Fem effektive tiltak mot dataangrep*. *https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/5tiltak*
- OECD. (2019). *Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit.* *https://www.oecd.org/regreform/tools-and-ethics-for-applied-behavioural-insights-the-basic-toolkit-9ea76a8f-en.htm*

Further reading (mainly in Danish)

- Bestyrelsesforeningen. (2021). *Cybersikkerhed for bestyrelser.* https://bestyrelsesforeningen.dk/vejledninger-og-anbefalinger/

- Center for Cybersikkerhed. (2023). *Cybertruslen mod Danmark.* https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/

- Center for Cybersikkerhed. (2021). *Råd om sikkerhed på virtuelle mødeplatforme.* https://www.cfcs.dk/da/forebyggelse/vejledninger/distancearbejde/rad-om-sikkerhed-pa-virtuelle-modeplatforme/Digitaliseringsstyrelsen og Center for *

- Center for Cybersikkerhed. (2021). *Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed.* https://www.cfcs.dk/da/forebyggelse/vejledninger/vejledning-metode-til-at-arbejde-med-adfardsindsatser/

- Center for Cybersikkerhed, Digitaliseringsstyrelsen, KL m.fl. (2021). *Kodeks for gennemførelse af sikkerhedstests.* https://digst.dk/media/23689/kodeks_for_sikkerhedstest_2021_digst.pdf

- Center for Cybersikkerhed. (2023). *Logning – en del af et godt cyberforsvar.* https://www.cfcs.dk/da/forebyggelse/vejledninger/logning/

- Center for Cybersikkerhed. (2022). *Phishing – beskyt organisationen mod phishingangreb.* https://www.cfcs.dk/da/forebyggelse/vejledninger/phishing/

- Center for Cybersikkerhed og Digitaliseringsstyrelsen. (2022). *Cybersikkerhed i leverandørforhold.* https://www.cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

- Center for Cybersikkerhed. (2022). *Reducer risikoen for falske mails.* https://www.cfcs.dk/da/forebyggelse/vejledninger/reducer-risikoen-for-falske-mails/

- Digitaliseringsstyrelsen og Center for Cybersikkerhed. (2020). *Vejledning i anvendelse af cloudservices.* https://digst.dk/data/vejledning-til-anvendelse-af-cloudservices/

- Digitaliseringsstyrelsen. (2019). *Miniberedskabsplan.* https://sikkerdigital.dk/myndighed/iso-27001-implementering/beredskabsstyring/implementering