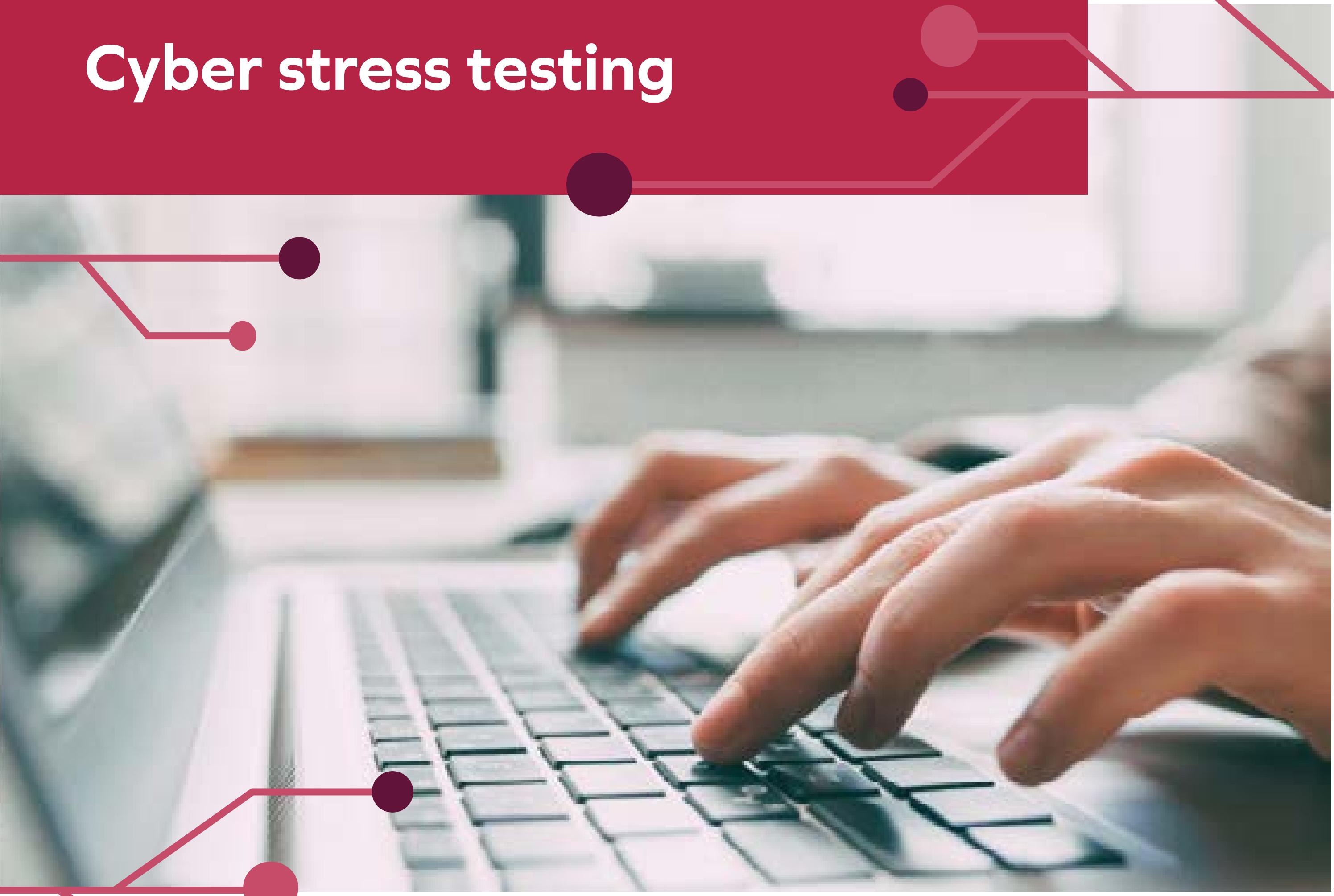
Cyber stress testing



Danish Financial Supervisory Authority

DANISH FINANCIAL
SUPERVISORY AUTHORITY

Indholdsfortegnelse

1. Summary

As the first financial supervisory authority in the EU, the Danish Financial Supervisory Authority (the Danish FSA) has developed and tested a new method, cyber stress testing, to investigate and, on this basis, strengthen the financial sector's ability to manage extensive, long-term ICT disruptions. This has been done in collaboration with seven institutions that are essential and important for the financial infrastructure. Danmarks Nationalbank, the central bank of Denmark, has been an advisory partner. The initiative is inspired by the Bank of England, which is a pioneer in the work of strengthening the operational resilience of the financial sector, among other things by means of cyber stress testing.

What is a cyber stress test?

A cyber stress test is an analytical tool for testing the capacity of firms to manage a severe, but plausible cyber scenario that causes a significant disruption to the firm's ICT services. This means that the test is about the capacity to ensure the continued delivery of critical business services as well as the capacity to recover normal ICT services. This is critical as an ICT disruption could have severe negative impact on the affected institution and its customers. Furthermore, a severe ICT disruption has the potential to affect the financial and operational stability of the financial system.

The test is a desktop exercise which takes place over a longer period of time. The test takes as its analytical starting point that the cyber defenses of the institution have failed. This means that testing the institution's capacity to prevent and detect a cyber-attack is out of scope in a cyber stress test.

The new tool complements institutions' and authorities' other work to strengthen operational resilience, i.e. the ability to respond and recover after a disruption so that critical functions are maintained despite the disruption.

More than ever, it is necessary to be prepared to manage extensive, long-term ICT disruptions. The dependency on ICT is high and increasing, and so is the threat of disruptions, including from cyber-attacks.

The Danish FSA's first cyber stress test has resulted in valuable learning points for all participating institutions and the Danish FSA. At the same time, it has strengthened the common understanding of challenges and opportunities in managing extensive ICT disruptions.

Against this background, the Danish FSA recommends cyber stress testing as a method for investigating and strengthening operational resilience for the financial sector and for authorities and critical institutions in other sectors as well.

The Danish FSA is currently developing the next cyber stress test in cooperation with Danmarks Nationalbanken. Whereas the first test focused on the individual institutions' management of an extensive disruption, the aim of the next test is to examine how such a disruption is managed across institutions and at sector level.

2. Introduction

As the first financial supervisory authority in the EU, the Danish Financial Supervisory Authority (the DFSA) has developed and applied a new methodology, cyber stress testing, to test – and on that basis strengthen – the financial sector's ability to manage an extensive, long-term ICT disruption. The DFSA has developed and tested the method together with seven firms that are essential and important to the financial infrastructure in Denmark. The central bank of Denmark (Danmarks Nationalbank) has acted as a sparring partner.

A cyber stress test examines the ability of organisations to manage cyber-attacks and other extensive, long-term ICT disruptions once the incident has occurred. The test is carried out as a desktop exercise over a prolonged period of time and is based on a specific, but fictitious ICT disruption scenario. The new tool supplements firms' and authorities' other initiatives to strengthen operational resilience, i.e. the ability to withstand attacks and restore ICT services after a disruption to ensure that critical functions are maintained despite the disruption.

Cyber stress testing is an investigation of the entire firm. Because when ICT system breakdown, the task is not only to restore the systems as effectively as possible. It is just as much a matter of ensuring that the firm's critical functions can continue until normal ICT services work again. This applies regardless of whether the disruption affects customers' online banking solution or the bank's ability to carry out payment transactions or trade in securities. And last, but not least, the crisis must be managed so that customers and other stakeholders do not lose confidence in the firm.

It is more important than ever to be prepared to manage extensive, long-term ICT disruptions. This is due to the fact that the level of dependency on ICT is high and increasing and so is the threat of attacks. Recently, the Danish Centre for Cyber Security (CFCS) has called on authorities and firms essential to society to revisit and, if necessary, strengthen their cyber contingency planning. This is because the threat level of destructive cyber-attacks against infrastructure that is essential to society has been raised from low to medium.

The Danish FSA has completed the first round of cyber stress testing. The test provided all the participating firms and the Danish FSA with relevant learning points and also strengthened the shared understanding of challenges and possibilities to manage extensive, long-term ICT disruptions. In addition, there were individual learning points for all the participants. Finally, the test confirmed to the participants that testing contingency management across business and ICT is essential to being sufficiently prepared for the time when a disruption may occur.

Against this background, the Danish FSA recommends cyber stress testing as a method to investigate and strengthen operational resilience for the financial sector as well as for authorities and organisations essential to society in other sectors.

The Danish FSA is currently developing the next round of cyber stress testing in collaboration with Danmarks Nationalbank. While the first round focused on the individual firms' management of an extensive, long-term ICT disruption, the purpose of the next round is to investigate how such a disruption is managed across actors in the sector and to identify the consequences of disruptions at sector level.

Purpose of this report

The following section gives a brief introduction to what a cyber stress test is and what it can show. Five key learning themes from the first test are described. The five themes give rise to questions that other financial firms which did not participate in the test and authorities and firms essential to society in other sectors may ask about their cyber contingency planning.

3. Why conduct cyber stress testing?

The financial sector is dependent on ICT. Without ICT, there is no banking: No digital payments, no stock trading, no account transfers. The financial infrastructure is critical to society, and it is built on ICT.

The threat level requires robust cyber security contigency planning

The current developments in the threat landscape necessitate that financial firms and other organisations essential to society do what they can to be prepared to manage cyber-attacks.

The CFCS released a new threat assessment in June 2024, raising the threat level of destructive cyber-attacks from low to medium. The Danish Defence Intelligence Service (FE) and the Danish Security and Intelligence Service (PET) believe that som nations states likely to have become more willing to accept risk in relation to using hybrid measures against European NATO member countries. The CFCS assesses that this willingness to accept risk also includes destructive cyber-attacks. The raised threat level applies to Denmark as a whole. If a nation state decides to launch destructive cyber-attacks on Denmark, the targets are likely to be selected from a wide range of organisations in sectors essential to society. Consequently, the CFCS calls on authorities and firms essential to society to revisit and, if necessary, strengthen their cyber contingency planning.

The CFCS defines destructive cyber-attacks as attacks in which the expected effect could be bodily injury, material damage to physical objects or the destruction of data or software so that they cannot be used without significant restore. For example, this may include so-called wiper attacks in which the victim's data is deleted or overwritten.

The CFCS now estimates that the threat level of destructive cyber-attacks is medium. In addition, the level of cyber-crime threats against the Danish financial sector is very high. According to the CFCS, cyber-crime may disrupt the availability of services provided by the Danish financial sector. In addition, the CFCS sees a development in ransomware attacks where hackers not only encrypt data but also steal data from their victims to blackmail them further.

Financial firms must be ready to manage many different types of advanced attacks, including from attackers aiming to destroy infrastructure and attackers aiming to make threats to obtain money or aiming to steal money.

ICT disruptions may have serious consequences

An extensive, long-term ICT disruption may have serious consequences for a financial firm and its customers. However, even if only one firm was affected from the outset, such a disruption would, however, also affect other financial firms either directly or through derived effects. If, for example, one bank is unable to carry out payment transactions, other banks and their customers will very soon be needing the money from such transactions. The consequences of an extensive, long-term disruption may also worsen and spread if customers and other stakeholders lose confidence in the firm under attack. A loss of confidence even has the potential to spread to other firms regardless of whether they are themselves directly affected by the disruption.

In a worst-case scenario, what starts as an ICT disruption, may develop and result in systemic financial consequences due to financial, operational or reputational effects.

The digital dependency, the threat level and the potential consequences of extensive, long-term ICT disruptions mean that there is a need to strengthen operational resilience. It must be ensured that the firms are able to manage a disruption in a manner so that the consequences are manageable for the citizens and so that there is less risk of society coming to a halt as a result of an attack.

Focus on operational resilience

Generally, there is an increased focus on strengthening operational resilience. For example, Danmarks Nationalbank, the European Systemic Risk Council (ESRB) and the Basel Committee focus on the risk of systemic implications of operational disruptions and on how financial firms' operational resilience can be strengthened.

Specifically, the ESRB considers cyber stress testing to be an important measure to strengthen operational resilience. The Danish FSA's cyber stress testing is inspired by similar testing carried out by the Bank of England, which has pioneered the area. Since 2019, the Bank of England has conducted two cyber stress tests and is currently conducting a third test. At the beginning of 2024, the Single Supervisory Mechanism (SSM) under the European Central Bank initiated its first round of cyber stress testing, which comprised 109 financial firms under its supervision.

4. What is a cyber stress test

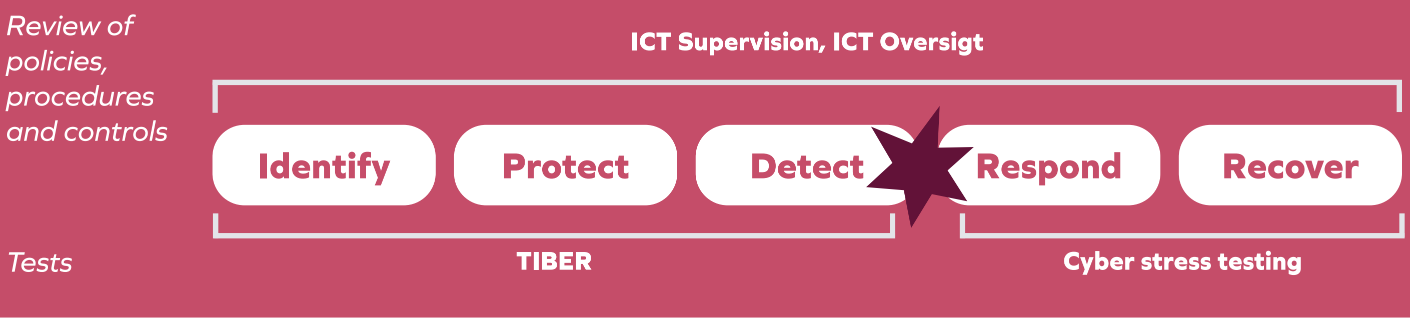
A cyber stress test is an analytical tool that tests an organisation's ability to manage an extensive, long-term ICT disruption, which means that IT systems supporting key business functions fail in whole or in part.

The first cyber stress test was conducted as a learning exercise for both firms and authorities, and the method is still being developed.

Not testing cyber defences but testing the ability to manage a disruption

A cyber stress test is conducted on the basis of a scenario in which an firm's cyber defences have failed. Thus, the test is not a test of the firm's ability to defend itself, but a test of its ability to manage the consequences of an attack as shown in **figure 1** below.

Figure 1. What is tested in a cyber stress test?


Review of policies, procedures and controls
ICT Supervision, ICT Oversigt
Identify
Protect
Detect
Respond
Recover
Tests
TIBER
Cyber stress testing

How is a cyber stress test carried out?

A cyber stress test is carried out as a desktop exercise on the basis of a fictitious ICT disruption scenario. The purpose of the test is to stress the firms beyond "normal" incident management that is already being tested regularly in tests as well as live. Therefore, the disruption which the firms are subjected to in the test must be extensive and long-term – and something that they have not experienced before.

When the test commences, the participating firms will receive the disruption scenario. Regardless of firms' cyber defences, the test does not allow a participating firm to answer that they would be able to prevent the attack. The disruption is the basic condition of the test.

The firms must answer how they manage the fictitious scenario based on a number of questions within the following main areas:

- How and to what extent can the firm maintain critical business functions that are affected by the disruption?
- How and how quickly can the firm restore normal ICT operations?
- How does the firm manage its reputation during the crisis?

The firms will have a prolonged period of time to account for how they will manage the scenario. So, the test is not carried out in real time, and it is not a crisis management exercise. Instead, the firms have the opportunity to think their management of the disruption through and discuss it with third-party providers etc.

The answers given by the firms will then be analysed together with material such as business continuity plans, ICT recovery plans and communication plans to identify learning points and good practice for the individual organisation and across participants.

The Danish FSA's first round of cyber stress testing

The Danish FSA's first cyber stress test was conducted in 2023. It focused particularly on retail payments since it is an area critical to society with immediate implications for the everyday lives of citizens. A total of seven firms participated in the test. Four SIFIs (Danske Bank, Jyske Bank, Nykredit and Sydbank) and three data centres that provide ICT services to the participating SIFIs (JN Data, BEC and Bankdata).

The test was divided into three phases, and the firms were requested to submit responses after each phase, which lasted about a month. Thus, the firms had time to prepare a thorough response. During the process, the phasing was also used to validate that the scenario worked as intended and that there was a shared understanding of the scenario.

In the first part of the scenario, bank customers saw incorrect amounts being deposited on and withdrawn from their accounts. The reason was unclear. The task was therefore to find the cause, to have the error corrected and to decide how to manage payments and communication to customers etc., while it was uncertain what was going on. The second part of the scenario was a supply chain attack. In the scenario, a third-party provider of critical IT operations was under attack. In the scenario, the Danish FSA had decided that it should take the provider about a week to develop a solution that made the systems work again. This meant that key functions at the affected bank were unavailable for at least seven days without the firms being able to restore the systems themselves.

It is relevant to test many different scenarios. The above scenario was selected for the first round of testing because it included various critical business functions, different types of disruptions and a prolonged duration.

Some of the firms chose to simulate a real crisis by conducting a large number of meetings in the firms' various internal and external contingency forums to discuss how the firms would manage the attack. In the test responses, the firms then described their analyses of the situation and what actions they would take on the basis of their current contingency plans and other setups. In this way, the cyber stress test is a demanding but at the same time a highly practical test form.

The Danish FSA initiated the test, but it was widely developed in collaboration with the participating firms and with input from the Danmarks Nationalbank. For example, the attack scenario was prepared on the basis of inputs from the participants to ensure that the scenario was relevant to them. During the test, the participants were also given the opportunity to provide feedback and ask questions so that the test could be adjusted in the process. The Danish FSA has had a very good collaboration with the participating firms, which contributed constructively to obtaining great learning from the test.

5. What does a cyber stress test cover?

The key learning themes from the Danish FSA's first round of cyber testing are described below in the form of the following:

- General questions that can be used to establish organisations' ability to manage extensive, long-term ICT disruptions
- Specific learning points from the Danish FSA's first round of cyber stress testing

1. How long will it take to restore normal IT operations?

In a cyber stress test, one of the key questions is how long it will take to restore normal ICT operations in the specific disruption scenario. This is important to know because the duration of the disruption is essential to the other initiatives – to what extent are contingency plans or even alternative ICT operations required? What communication measures are required? And what about customer service?

The threat landscape means that it is necessary to prepare for prolonged IT disruptions and new types of disruptions. If, for example, a firm is affected as a result of attacks on a third-party provider, the risk exists that the firm depends on the provider attacked in order to restore its own systems. If a firm experiences an extensive ransomware attack, restore is a complex and lengthy process in which it must be ensured, for instance, that the attackers have been removed from the data and systems before restore can commence. Firms that have been affected in real attacks experienced that it took weeks to restore ICT operations and sometimes even longer. And in light of the development in the threat landscape, unprecedented disruptions are also plausible.

Learning points from the first round of cyber stress testing: Restore may take a long time.

The second part of the disruption scenario in the cyber stress test was designed so that the firms experienced, among other things, a large-scale disruption lasting about a week. This means that the duration of the ICT disruption was dictated to the firms participating in the test. The test did not allow the firms to restore their normal ICT operations themselves because the disruption was due to a security breach at a third-party provider.

The first learning taken from this scenario was that firms are not always fully in control of the duration of the restore of their systems. The firms may, among other things, rely on critical components from third-party providers to maintain important business operations.

It is important to identify such dependencies in advance. And to analyse the main types of disruption scenarios that could affect an firm and how long it will take to restore operations. This is a prerequisite for taking measures to shorten the duration of the restore if it turns out to be too long. It is also a prerequisite for ensuring that the preparation of continuity plans, crisis communication etc. is calibrated to the expected duration of the disruption, also in extreme but plausible scenarios.

Secondly, the test showed that the actual restore – despite external dependencies in some cases – can be planned in advance to ensure that the duration of the restore is as short as possible. It is important to ensure that there are plans in place for all relevant main types of disruption scenarios because there is a big difference between what it takes to restore operations in the different types of scenarios. In the event of, for example, a fire at a data centre, restore may typically take place at a mirrored data centre. However, in the event of, for example, a ransomware attack where data is encrypted, it will not be possible to switch to another data centre with mirrored data because this data will also be encrypted. In this case, other measures will be necessary.

2. How can critical business functions be maintained without IT operations?

A cyber stress test also illustrates whether a firm has adequate business continuity plans in place that can be used to maintain critical business functions. Does the firm know, for example, which payments are critical and when they fall due? Are there any plans for how payments must be made when normal ICT operations are down? And for how long is it possible to continue using the continuity plans? Did the plans prove useful and adequate in tests?

Cyber stress testing may also give rise to considerations as to whether the firms can strengthen their ICT service continuity, i.e. whether they, in addition to their manual continuity plans, could beforehand look into the availability of alternative minimum ICT operations or whether these could be developed with a short period of time. In this way, the test can help identify whether the contingency planning can and should be optimised.

Learning points from the first round of cyber stress testing: Preparation is essential.

It became clear during the prolonged ICT disruption in the cyber stress test that it is essential that the business contingency plans prepared by the firms match the expected duration of the firm's restore of normal ICT operations after an extreme but plausible disruption scenario. They must also match the main types of disruptions identified. For example, it will typically be relevant that contingency plans cover if the IT systems do not work. They must also cover if the disruption consists of incorrect central information in the systems, for example because it has been manipulated or if confidential information has been leaked.

The test also showed that it is important that the plans have been tested and are applicable in practice. For example, it is essential that it be ensured that critical data used in a contingency plan is in fact available during a disruption. And in a sufficiently updated version.

Finally, the test showed that it is important that the firms have established in advance which functions are critical to both the firm itself and its customers and which functions the firm can manage in various disruption scenarios and for how long.

In an extremely stressed scenario, it is essential that the firms have made preparations so as to maintain critical functions to a sufficient degree and thus also to maintain the confidence of their customers and other stakeholders.

In all probability, it will not be possible to prepare for the exact disruption that actually occurs. Both in this and other areas, it is therefore important to work with main scenarios rather than (too) many detailed scenarios to ensure the applicability of scenarios and plans.

In all circumstances: The better prepared a firm is, the more options are available to it when a disruption actually takes place.

3. Does the firm have an overview of the consequences of a disruption - also over time?

A cyber stress test offers specific insight into what the consequences are if normal ICT operations are disrupted for a long time. And in situations where multiple critical business functions are affected at the same time. What perhaps is a source of irritation on day 1 may be a serious deficiency on day 5. It may be easier to do without some functions for a long time or easier to do without them at some times than at others. The cyber stress test shows whether the firm understands the effects, consequences and costs of disruptions over time well enough to be able to scale the continuity plans and the other crisis management measures to an adequate level.

Moreover, the cyber stress test offers authorities insight into firms' expectations for the development in consequences over time. And thus also an increased understanding of when and how a disruption in operations may develop into having systemic consequences. This knowledge can be used to plan and prioritise regulatory measures in the future so as to manage systemic effects in the best possible way.

Learning points from the first round of cyber stress testing: The consequences develop over time.

The relatively long duration of the disruption showed that the consequences of a disruption develop over time. For example, changes must be expected in how and to what extent customers contact a bank experiencing an ICT disruption on day 1 and, for instance, day 5, respectively.

It is therefore important to have considered in advance what the effects will be in different main scenarios over time. At the same time, it is important that firms not only assess the consequences (e.g. a financial loss or a loss of reputation) in cost intervals, but also consider what would actually happen, who would be affected and how. In this way, an informed basis is created for preparing sufficiently for how to manage the consequences.

4. Does communication form an integral part of contigency planning and crisis management

In a cyber stress test, firms must address how they intend to communicate internally and externally, including to both customers and the general public during a prolonged disruption. The test illustrates whether the planned communication supports the contingency plans and crisis management in general. For example, is it clear to customers what to do? How many customers are expected to contact the firms to get help with what is not working as usual? Or just to ask what is going on? How many resources does customer service need to help customers? And how will the firm manage publicity in both traditional and social media?

Learning points from the first round of cyber stress testing: Communication is essential if an firm is unable to provide the services it normally provides.

The firms were also asked how they would manage communication during the disruption. That is communications to customers, the general public and other stakeholders. And on different platforms, including social media.

The test demonstrated clearly that all of the participants were very aware that successful communication during a crisis is essential to maintain confidence in a firm. It is important that the communication has been coordinated between the relevant parties and on different media platforms to be successful. For example, when and how it is announced that a cyber attack has occurred – if that is the case. It is also important that the communication supports

other initiatives, including contingency plans. If the contingency plan, for example, assumes that affected customers are able to contact the firm, it is essential that the customers are notified and that the capacity available to manage inquiries is adequate.
Preparation and advance testing of communication efforts are a key factor given the extreme time pressure during a crisis. This applies at several levels: **Strategy** – what will the firm communicate when? **Coordination** – who should the messages and their timing be coordinated with both in advance and underway? **Specific plans and messages** – pre-fabricated and agreed messages for main scenarios to avoid starting from scratch, while 'things are out of control'.

The test also highlighted that social media mean that it is much more difficult to manage the narrative during a crisis than it used to be. Everyone – dissatisfied and frightened customers, influencers with an agenda of their own, internet trolls, etc. – has access to social media. And once something has been written on social media, it is extremely difficult to erase. Regardless of whether it is true or not. This new reality must be considered in communication strategies and plans for successful initiatives so that confidence is maintained.

5. Is the firm's contigency planning sufficiently coordinated?

Ultimately, cyber stress testing focuses on developing a comprehensive set of contingency plans in which the business, ICT and communications are connected and support one another. An ICT department is unable to manage an extensive, long-term ICT disruption alone. The ICT department can see to it that normal ICT operations are restored as soon as possible. However, it is the business-oriented departments rather than the ICT department that can activate the business continuity plans and thus ensure, among other things, that an affected bank's customers can still pay for goods in stores even though the bank's ICT systems are down. The communication department can ensure that customers and the media are informed of what is happening and what to do. Finally, it requires joint efforts to ensure that ICT operations restoration, business continuity plans and communication are coordinated – also with an firm's executive management. In a cyber stress test, the total initiatives in a specific scenario are stressed to the extreme in order to shed light on what can be improved.

Learning points from the first round of cyber stress testing: Coordination is a prerequisite for managing extensive, long-term ICT disruptions.

As mentioned above, the test concerned firms' management of the disruption in various key action areas.

The test demonstrated clearly that effective management requires coordination, including with external parties, such as providers. This applies at several levels. For example, restoring specific IT systems typically requires that the underlying IT – servers, networks etc. – is restored first. This applies also to communication. For example, if one firm provides information to the general public about the cause of a disruption, other affected firms cannot choose to wait.

It is therefore essential that coordination has been planned in advance and that it has been tested that everything works. This applies internally at the firms between business, ICT and communication, and it applies between relevant parties, such as providers.

Finally, the management of extensive, long-term ICT disruptions must be embedded in an firm's full management team. This is a prerequisite for adequate coordination between parties.

6. Systemic focus in the next round of cyber stress testing

The first round of cyber stress testing focused on the individual firm's management of an extensive, long-term ICT disruptions. It provided both participants and authorities with significant learning.

As described above, an extensive, long-term ICT disruption would in reality also affect other firms very quickly. Such a disruption would also be managed in cooperation between several parties, both other financial firms and the authorities. If a situation is sufficiently serious, the crisis response plan of the FSOR (the Financial Sector Forum for Operational Resilience) will be activated.

FSOR and FSOR's crisis response plan: The FSOR is a public-private collaboration forum in the financial sector initiated and operated by Danmarks Nationalbank. The objective of the FSOR is to enhance operational resilience across the sector, including the resilience to cyber attacks. The FSOR has prepared a crisis response plan at the sectoral level supplementing its members' own crisis response plans and the national crisis management under the National Operative Staff (NOST). The crisis response plan will be activated in the event of serious operational disruption that has the potential to affect financial stability.

The Danish FSA will conduct another round of cyber stress testing. The purpose will be to investigate how an extensive, long-term ICT disruption is managed across parties in the sector and to identify the consequences at the sectoral level. As the test will focus on the financial system as a whole and the consequences at the sectoral level, it will be conducted in close collaboration with Danmarks Nationalbank, whose responsibility, among other things, is to ensure financial stability.

The test will be based on a disruption scenario affecting firms across the financial sector. This will, among other things, give additional insights into which tools available to firms and authorities are useful for managing operational disruptions and how they are best put to use.

The test is being planned and is scheduled for completion in 2025.