Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Recover from a cyber incident

When things do go wrong

Version 1.0 | May 13 2024

Mailservers are offline. Important data can no longer be accessed. To make matters worse, the backups are also encrypted. It is just one of the scenarios that you could be faced with. Should something like this happen, you want to ensure that your business returns to business as usual as soon as possible.

The ability to recover from cyber incidents is a prerequisite for digital resilience. But recovery includes more than just backing up data. Knowing what to protect, the resources needed and how to carry out and practise your recovery operations is essential.

In this guide, the National Cyber Security Centre (NCSC) explains the importance of recovery, how to implement it, and what measures can be taken to effectively recover from cyber incidents.

Background

Approximately 1 in 5 organisations experience a cyber incident resulting in damage or downtime every year. [1] Vulnerabilities in software, human error, but also disasters, pandemics or power outages can lead to unexpected events and even disruptive incidents or crises.

Recovering from a cyber incident can be complicated and time-consuming. Recovering from ransomware, for instance, can take days, if not weeks. Moreover, recovery operations are not always carried out flawlessly.

It often turns out that recovery is not practiced enough or backups cannot be restored properly[2]. The longer the recovery time and more complicated the recovery operation, the greater the impact on business operations. This can cost money and may damage your reputation. In the worst case, it can even lead to bankruptcy.

In the event of a cyber incident, your organisation's ability to recover effectively is critical in order to continue your services[3]. What recovery means and how to implement it, is explained in this guide. We will look at what exactly recovery is, how to organise and implement it, and what measures you can take to effectively recover from cyber incidents.

Target group

Chief Information Officers, Chief Information Security Officers, Business Continuity Managers, Risk Managers and Crisis Managers.

Partners

This basic guide is the result of a collaboration between ASML, De Volksbank, Nederlandse Vereniging van Banken, Rabobank, Triodos Bank and the AIVD.

1 Cybersecuritymonitor 2022. In 2021, approximately 14% of organisations experienced a cyber incident with an internal cause and 7% experienced an external attack.

2 Gartner Global Security and Risk Management Governance Survey 2021.

3 See also the TNO report: Herstelvermogen binnen IT-infrastructuren.

Cyber incidents can have significant impact

Cyber incidents disrupt the availability, integrity or confidentiality of information systems and data. If it affects critical products and/or services and their associated business processes, you want to have a recovery plan in place to get back to normal as quickly as possible.

Recovery from what?

In this guide, cyber incidents are defined as incidents that disrupt IT systems and prevent the delivery of critical products, services and processes. In such cases, it may mean that organisational objectives can no longer be achieved, resulting in damage. It is then important to be able to fall back on plans, procedures and agreements so the recovery operation can be started and carried out in the best possible way.

Recovery plan

It is important that your organisation has a recovery plan in place before a disruptive cyber incident hits your business. But how do you make such a plan? In the following steps, we list the tools you need to build up your recovery capacity.

Step 1: Knowing what to protect

It is impossible to fully protect your organisation against every form of interruption or cyber threat. It is therefore wise to identify and prioritise potential threats and their impact on your products and services at an early stage. You can do so by conducting a Business Impact Analysis (BIA).

The BIA is a prerequisite for effective Business Continuity Management (BCM)[4]. The BIA helps you to understand your interests that need to be protected[5]. A BIA enables you to map the critical products, services and processes together with the owners and persons responsible. This also includes any supporting assets (software, hardware, people, suppliers and data). This helps you to understand which products, services and processes are critical to how you operate and what is required to keep them running.

The following 4 steps will help you prepare for the BIA:

1. **Identify your interests**

   A BIA starts by distinguishing between critical and non-critical products, services and business processes, and the assets required for their operation. Also consider suppliers, IT service providers and the dependencies between them[6]. This concerns the entire supply chain for which you are the data owner. For each service or product, you indicate the impact of a potential asset failure on the continuity of the service or product and therefore the organisation. Think of the financial impact, operational disruption, legal and regulatory sanctions, reputational damage or health risks and safety (or other business goals).

2. **Conduct a threat analysis**

   Now that the critical products, services and processes are mapped, the next step is to consider which threats are relevant to your organisation. These could include attacks by cyber criminals, but also threats such as internet outages, power cuts or flood damage. In a threat analysis, you identify for each threat how likely it is to manifest, what processes it may affect, and what impact it will have[7].

3. **Establish the maximum tolerable period of disruption**

   The business determines the Maximum Tolerable Period of Disruption (MTPD) for each of its products, services and underlying processes. After what period of time (hours, days, weeks) is a product or service delivery failure truly critical?

[4] The Digital Trust Center has drawn up a risk analysis step-by-step planv for entrepreneurs. This is useful for when a BIA is less appropriate. However, the underlying principles are the same.

[5] The Business Impact Analysis includes not only cyber incidents, but also other potential disruptions to business continuity, so it is not just about IT.

[6] For more information, see the NCSC publication 'Dealing with risks in the supply chain' and make use of the 'Cybercheck'.

[7] For more information, see the NCSC factsheet 'Risk management: the value of information as point of departure'. And for more information on digital threats, see the NCSC's weblog: Digitale aanvalstechnieken, leer je tegenstander kennen!

In order to do this, it is necessary to know how long it takes to recover from an incident to an acceptable level at which the continuity of the product or service can be guaranteed. This can be quantified with the Recovery Time Objective (RTO). If it turns out that full or partial recovery from a cyber incident takes longer than the RTO prescribes, this could mean that the MTPD is exceeded and potentially serious damage is caused.

Tailor-made solution

The recovery plan is a tailor-made solution. For smaller organisations, it may be sufficient to have call lists of their IT suppliers and a summary of agreements with them on how to recover from a cyber incident[8]. For organisations with complex IT environments, a more comprehensive plan is required.

It is necessary to facilitate the discussion between business and IT (and suppliers) at this stage to identify and remove barriers. In some cases, you may also need to consider the maximum amount of data loss you can tolerate. This amount is quantified by the Recovery Point Objective (RPO). If data is not backed up frequently enough, a cyber incident could result in the loss of data. If this data loss becomes too great, it could also cause damage to your organisation.
The MTPD, RTO and RPO help you to understand your recovery capability requirements. It is important to involve your suppliers and IT service providers in this step as well. They have essential information that will help determine your MTPD, RTO and RPO.

4. **Prioritise your critical products and services**
   You can then start to prioritise based on the risks, impact of potential disruptions and maximum downtime.
   - Distinguish between critical and non-critical products, services and processes.
   - Determine what the crown jewels are and which IT assets are associated with them.
   - Rank the processes according to their impact on your operations. RTO and RPO should be at the top of the list.

Step 2: Develop a recovery plan

With the information obtained from the BIA, you have the tools to build the recovery plan (also known as the (IT) Disaster Recovery Plan).

A recovery plan is a document – or part of a business continuity plan – that includes policies and procedures that describe how to quickly resume operations after a cyber incident. The recovery plan is essentially a step-by-step guide used during a cyber incident to recover effectively and quickly.

Make sure the recovery plan is always ready and up to date. A recovery plan or playbook (see below) may contain sensitive data. Think about how you can protect your plans and keep them available at all times. One solution is to store the plans on encrypted laptops, or use well-secured remote locations separate from your own network.

In any case, a recovery plan describes:

- **Activation, implementation and termination**

  Describe who can initiate the plan and define when the recovery plan should be activated, who should perform it and when the recovery operation should end.
  Describe which decisions may be taken within each role (e.g. who is responsible for pulling the plug?). As a general rule, the authority to activate, implement and terminate the recovery plan rests with senior management. They can form a recovery management team in which strategic decisions are made.

- **Roles and responsibilities**

  The recovery plan describes who is on the recovery team, their roles (network team, application team, server team, communications team) and, also relevant, their contact details. A notification list or call tree is essential in this respect. You may also want to consider suppliers and IT service providers

[8] For more information, see the web page of the Digital Trust Center: Afspraken maken met een IT-leverancier.

and their contact details here. Describe what their role is in the recovery process and what agreements (SLAs) and contracts are relevant.
Discuss what your business continuity requirements are and the efforts you expect suppliers to make to align your recovery time with your BIA requirements. Think in advance about who has what responsibilities in the recovery process and describe these in the recovery plan.

- **Playbooks**
  A good recovery plan is action-oriented and can guide the recovery team during a cyber incident. Playbooks can be added to the recovery plan. Based on BIA's threat analysis, these are concise descriptions of scenarios and how to recover from them, step by step.
  For example, consider scenarios such as ransomware[9], DDoS attack[10], interruption due to power failure[11], fire, leakage, etc. Bear in mind that, in practice, cyber incidents almost never fit neatly into a playbook.
- **Communication plan and alternate location**
  - Describe how you will communicate with various stakeholders during a cyber incident. See the "Reporting an incident" section under Communication and Coordination.
  - Provide alternative communication channels and alternate locations (if possible), e.g. in case the internet or mobile telephony fails ('out of band communications').
- **Systems and applications inventory**
  - Include an overview of all systems and applications and their interdependencies, suppliers, etc.
  - Rank them according to their impact on your business.
- **Network descriptions and diagrams**
  Include network descriptions and diagrams so you can understand your network and its interdependencies. The challenge here is to keep these regularly up to date. This needs to be secured in a process.
- **Back-up strategy**
  A backup strategy is necessary in case a cyber incident affects the availability, integrity or confidentiality of data. Our recommendation is to base your backup strategy on the BIA threat analysis. After all, a server room flooded by water requires a different type of backup than a ransomware attack. A proper backup strategy therefore takes into account the various threats and the underlying RTOs and RPOs of the affected processes.
  Considerations regarding backup media (snapshots, hard disk, cloud), locations (onsite, offsite, offline), types of backups (full, incremental, differential) and retention periods will ultimately depend on risk, cost, regulatory requirements and preferences[12]. Also consider the ability to replace hardware (switches, servers, etc.) and back up system and network configurations (virtual machines, config files).
  Finally, it is a good idea to check what agreements (SLAs) you have with IT suppliers for systems and applications that are not in-house.

Step 3: Practise, test and train the recovery

Even if you have everything written down, this in itself is still not enough. Recovery operations are proving difficult in practice and one of the main reasons for this is that the plans have not been sufficiently practised, tested and trained. Practising the recovery plan and underlying scenarios reveals whether the recovery capability is in line with the requirements to restore business processes in time. Practice ensures that the people implementing the recovery plan also learn how to work effectively as a team.

[9] For more information, see the web page of the Digital Trust Center: Afspraken maken met een IT-leverancier.

[10] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten

[11] See the playbook interruption resulting from power failure created by the Information Security Service (Informatiebeveiligingsdienst (IBD)).

[12] A good example of a backup strategy is the 3-2-1 strategy. For more information please consult DTC's web page: Een back-up strategie opstellen.

Practice can take various forms. Think of a tabletop exercise, an exercise with live recovery, etc[13].

Regular testing and restoring of backups is also essential. This shows whether the backups are able to restore the data to the desired point in time (RPO), the result (data integrity), the quality and how long it takes to do so (RTO). Based on these tests, assess whether the backup strategy needs to be tightened up.

Finally, there is the issue of regular staff training. They need to familiarise themselves with their role in the recovery team, learn the processes, understand the recovery procedures and gain practical experience in recovery operations.

Communication and coordination

Effective communication and coordination are essential during a cyber incident. A cyber incident can have a significant impact on an organisation. It can also cause unrest among customers, suppliers and other stakeholders, resulting in reputational damage[14]. A communication plan, as described above, is needed because you can think through many considerations in advance.

- **Work on your culture**

  Cyber incident recovery is a job carried out by people. People need to feel that they can safely report an incident and that they can contribute to its recovery. Allowing people to make mistakes is essential to achieving this.

- **Internal communication**

  If part of the business is down, it is not just the business that is affected. Employees will have questions about how to get back to work, or expectations about how long the disruption will last. Designated employees will also have to take action to contribute to the recovery or continuation of the business.

  It is our recommendation to communicate as openly and, above all, as factually as possible so the right expectations are set and any noise is removed. At the same time, remember that internal communication is also external communication. So fine-tune what is being shared, who is sharing it and what the message is. Communicate what you know, as well as what you do not know (yet).

- **External communication**

  Customers, suppliers and other stakeholders may also suffer damage or inconvenience as a result of a cyber incident that manifested at your organisation. They may depend on your product or service, or be directly affected by a similar cyber incident. It is therefore important to provide prompt, transparent and factual information about the incident to preserve the relationship. In doing so, do not forget to provide clear options on how to act.

  An important precondition for open communication is to think, well in advance, about the target groups you need to approach, always focusing on legal requirements, information needs, interests, and reputation-related risks. You should also be aware of any legal implications of the communication. This requires careful consideration with legal and communication teams.

- **Coordinate the recovery**

  Coordination of the recovery operation is required to ensure that recovery is properly timed. A recovery that is too early or too late may be ineffective or may get in the way of resolving a cyber incident. Acting too soon, for example, can have an impact on forensic evidence and the chain-of-custody.

  Coordination between internal and external stakeholders such as Managed (Security) Service Providers (MSSPs), system owners, developers or government agencies is important to ensure a smooth and flawless recovery. And a practical point: organise facilities support (space, stationery, secretarial support, etc.).

[13] Every two years, the NCSC organises the ISIDOOR exercise, in which the National Digital Crisis Plan is put into practice (see web page: Isidoor NCSC for more information).

[14] See also the NCSC publication Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten [Key points for crisis management and communication during digital incidents].

– **Report the incident**
In some cases you are obligated to report the cyber incident. Vital and essential service providers have a duty to report serious cyber incidents to the NCSC[15]. In the case of criminal offences, a report can be made to the police[16] and in the case of a data breach, to the Dutch DPA (Autoriteit Persoonsgegevens)[17]. If the involvement of a state actor is suspected, the General Intelligence and Security Service (AIVD) can be contacted[18].

Continuous learning and improving

We can learn from cyber incidents. Once the rubble has been cleared, the incident resolved and business processes resumed, it is time to consider what lessons can be learned.

– **Reporting**
It may seem like an open door, but in the chaos of a cyber incident, it can be easily forgotten: the reporting process. In order to learn from a cyber incident, it is necessary to report on the recovery process. Make sure that decisions and activities of the recovery team, management team, response team, correspondence with external parties (IT suppliers) are accurately and unambiguously recorded.
A useful tool for organising reporting can be the OODA-loop. OODA stands for Observe, Orient, Decide (in Dutch referred to as BOB). Also take into consideration the duration of the work in order to establish a timeline. We prefer to designate one person who is responsible for recording for each team involved.

– **Evaluate**
In the immediate aftermath of a cyber incident, an evaluation can help to identify the first lessons learned. This can be painful, especially if (human) errors have been made. So also keep an eye out for the things that went well. This encourages the willingness to learn. An initial assessment often reveals more about the cause and damage of the cyber incident, and what activities made the response and recovery easier or harder. Make sure that the points for improvement that emerge from the evaluation are clearly invested and that their progress is monitored.

- **Recovery information**
Reporting and evaluation(s) help to understand the duration and quality of the recovery work carried out. This information can be converted into recovery information or metrics[19]. Recovery information can be useful to enhance the quality of recovery. Take for example the time it took to restore a malware-infected server, or the time it took to restore backups. Other information, such as the cost of a cyber incident (legal, hardware, software, labour, etc.) or the frequency of certain cyber incidents in a year, can also be useful in planning your organisation's recovery.

- **Improve**
Put the lessons learned into action by comparing them to the interests, threats, RTOs, RPOs and priorities identified in the BIA. Are they still accurate or do they need updating? Do we have the right resources or do we need additional investment? The lessons learnt are of crucial importance in answering these questions. When lessons are integrated, practised and tested, a cycle of improvement is created.

[15] You can file a report on the NCSC's website: Wbni-melding.

[16] See the website of the police: aangifte of melding doen

[17] See APB's website: datalek melden.

[18] See the AIVD's website: contact.

[19] You can find examples in the MITRE report: Cyber Resiliency Metrics.

Conclusion

It is not always possible to prevent cyber incidents. And when it does happen, you want to be able to recover from the incident as swiftly and as effectively as possible. Recovery requires an understanding of what needs to be protected, the creation of recovery plans and the regular practice of these plans. In the event of a cyber incident, communication and co-ordination are key to success. Informing those affected, both internally and externally, and letting them know what to expect helps limit damage and false expectations. Finally, recovering from a cyber incident means learning from what went right and what went wrong. The lessons you learn from this will help you become even more resilient.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

May 2024