Swedish Civil Contingencies Agency

Co-financed by the Connecting Europe Facility of the European Union

Cyber attacks on essential information systems

25 recommendations for enhanced protection against cyber attacks

Cyber attacks on essential information systems
– 25 recommendations for enhanced protection against cyber attacks

Photo cover: Adobe Stock
Printing: By Wind
Production: Advant

Publication number: MSB2395 – September 2024
ISBN: 978-91-7927-524-2

Preface

At the beginning of 2023, the number of attempted cyber attacks against government agencies and operators of essential services increased sharply. The vast majority of these were denial-of-service attacks that, according to social media statements, were supposedly carried out in response to the "Quran burnings". Combined with the deteriorating security situation, the importance of resilience to cyber attacks has never been more important.

This report assesses the cyber threat landscape targeting government agencies and OES/DSPs and the consequences of cyber attacks. I would like to take this opportunity to express my appreciation to the organisations that report IT incidents to the Swedish Civil Contingencies Agency (MSB). Your commitment increases our understanding of your challenges, while providing MSB with the conditions to develop relevant support according to the needs.

The report shows that many cyber attacks are relatively unsophisticated but that they often nonetheless "succeed" in negatively impacting organisations. This indicates shortcomings and a need to improve security measures. Supply chain incidents, where a cyber attack affects or spreads to many organisations at the same time, can lead to major consequences for society. It is therefore particularly important that all organisations review the security of their supply chains. A fundamental prerequisite for the improvement work is that the management teams of the organisations get involved and provide resources where necessary.

Effective protection reduces the likelihood of being subjected to cyber attacks, but unfortunately, there are times when the protection is not enough. It is therefore crucial for an organisation to practice incident management on a regular basis. Good communication and routines for incident management are particularly important when the service or information system is outsourced and the organisation consequently does not have control over it.

Lastly, I would like to emphasise that the only way to head off a malicious actor is to systematically work on the whole based on risks from an all-hazards approach. My hope is that this report inspires greater study so that your organisation works proactively with protection to be able to withstand attempted cyber attacks and thereby contribute to society's resilience.

Stockholm, 17 January 2024

Åke Holmgren

Director of Cyber Security and
Secure Communications Department
Swedish Civil Contingencies Agency

Innehåll

Glossary

The concepts central to the understanding of the report are presented here. See *Appendix 1* for a more in-depth presentation of the concepts used in the report to analyse IT incidents resulting from malicious activity.

Actual incident: an event where the affected organisation is harmed or prevented from benefit, or where another organisation is unlawfully benefited or prevented from being harmed (see Annex 1 for a more in-depth description).

All-hazards approach: an approach seeking to assess all risks to something to be protected, and analysing all possible causes of a risk being actualised.

Artificial intelligence (AI): AI can be described as a set of technologies that, with the support of large amounts of computing power and data, with varying degrees of independence, can identify patterns and connections and calculate probability. Unlike ordinary programs, AI algorithms can be used to solve problems that there is no clear solution to. Examples of AI technologies include machine learning and deep learning. Machine learning uses algorithms that "learn" based on training data to conduct statistical reasoning and thereby perform tasks. Deep learning can be described as a more advanced form of machine learning that uses artificial neural networks to learn how to perform more complex tasks over time with less human intervention. One technology that has developed rapidly in recent years is generative AI. Generative AI includes models that learn based on training data to produce new content, including text, images and sound.

Attempted cyber attack: an attack attempt that meets the legality and practice criteria but does not meet the incident criterion, i.e. it did not result in an event that negatively impacted the confidentiality, integrity or availability of the attacked IT environment. These criteria are explained on page 23.

Availability: an aspect of information security meaning, in brief, that information is accessible when requested by authorised persons.

Change management: a systematic and structured method and process aimed at enabling changes to an organisation's objectives, processes or technologies in an efficient, controlled and low-risk manner.[1]

1. The concept has more specific definitions within certain IT related frameworks for the management and development of IT systems.

Component: the constituent part of a mechanism.

Confidentiality: an aspect of information security that, in brief, means that only authorised persons can access information.

Continuity management: a systematic and structured method and process to document and plan the organisation's operations in order to maintain a tolerable level regardless of the disruption it is subjected to.

Cyber attack: a malicious act that meets the conditions of legality, practice, consequence and intent as explained on page 23.

Deficiency: the lack of something that could lead to, or contribute to, a success.

Disruption: A consequence of an incident that means that an essential or digital service cannot be provided in the manner intended.

Digital supply chain: services and infrastructures that deliver or enable the delivery of digital products used to establish, maintain, develop or restore an organisation's information management and information systems.

Identity and access management: identity and access management means that organisations work to ensure that only authorised users and information systems have access to the IT environment. The organisation must design its access management in such a way that every digital identity does not have more access to information and information systems than it needs.

Incident: an undesirable event that has occurred. In incident reporting, causes are classified according to human threats (both antagonistic threats, in the form of attacks, and non-antagonistic threats, in the form of mistakes), technical threats (in the form of system failures) or natural threats (such as weather phenomena, earthquakes, solar storms, etc.).

Incident management: a systematic and structured method and process for identifying, documenting, analysing and resolving incidents.

Information system: systems for collecting, storing, processing and distributing information for a given purpose.

Integrity: An aspect of information security that means, in short, that information can be trusted to be correct and not manipulated or destroyed.

IT environment: a collective set of information systems used to process information for which the organisation is responsible. The IT environment includes both information systems that are managed internally and those that are outsourced.

Mechanism: a combination of components that, in interaction and together with a trigger, can cause a particular event to occur.

Monodependence: An organisation has a monodependency on, for example, a service when it is dependent on that service and no alternative services are available should the service in question cease to exist.

NIS regulations: Collective name for the law (SFS 2018:1174), the ordinance (SFS 2018:1175) and the authority regulations adopted in Sweden to implement the NIS Directive (EU) 2016/1148.

Obstacle: something that prevents, or contributes to prevent, a success.

OES/DSP: Operators of Essential Services (OES) and Digital Service Providers (DSP) that provide essential and digital services covered by the NIS regulations.

Opportunity: The lack of something that prevents, or helps prevent, a success.

Protection: Something that prevents, or helps prevent, an incident.

Risk: A possible undesirable event.

Security event: Type of incident. An event where a threat arises, a protection ceases/vulnerability arises, a success factor ceases/deficiencies arise or obstacles arise (see Annex 1 for a more in-depth presentation).

Success: a desired event that has occurred.

Success factor: something that leads to, or contributes to, a success.

Threat: something that causes, or contributes to cause, an incident.

Trigger: Something that can be added to a mechanism so that a certain event is caused.

Vulnerability: The absence of something that prevents, or helps prevent, an incident.

Summary

Summary

2023 began with an extensive number of denial-of-service attacks. Meanwhile, attempted cyber attacks usually represent less than one fifth of the total number of IT incidents reported to MSB. Based on identified challenges, recommendations have been developed for how an organisation can strengthen its protection against attempted cyber attacks, and minimise harm if an incident still occurs. Organisations that work systematically and risk based with an all-hazards approach are best equipped.

This report presents the cyber threat landscape against government agencies and operators of essential services based on IT incident reports received by MSB from April 2019 to September 2023. From an all-hazards approach, it is important to point out that the number of attempted cyber attacks constitutes less than one fifth of the total number of IT incidents reported to MSB until 2022. Other causes of IT incidents include mistakes, system errors or natural threats. Of the total 1,542 incidents reported during the time period, 16 percent were attempted cyber attacks. Government agencies account for most of the reported IT incidents, although their share is decreasing over time.

The number of reported attempted cyber attacks has decreased over time, but increased in 2023. The increase consists of an abnormally large number of reported denial-of-service attacks at the beginning of 2023. The denial-of-service attacks in question were described in the media and on various chat groups to be backlash to the "Quran burnings". Accordingly, although the number of attempted cyber attacks increased, it should be understood as a temporary peak rather than part of a trend with a constantly increasing number of attempted cyber attacks against government agencies and OES/DSPs.

The analysis of the attempted cyber attacks shows that 53 percent of the IT incidents describe a security event that resulted in actual impact on an organisation's operations. The remaining attempted cyber attacks are deemed to have failed or had such limited consequences that they did not achieve an organisation impact.

Many of the cyber attacks that have resulted in an impact have been carried out using less sophisticated methods. This suggests that the security work in organisations needs to be strengthened, but also that with relatively limited improvements better security can be achieved.

Cyber attacks can have serious consequences for those affected. The recovery period can be both long and expensive. If the information system affected maintains essential services, it can in the worst case entail a risk to life and health. Furthermore, if others depend the information system, many organisations and citizens can be affected. In addition, many organisations operate in complex ecosystems of digital supply chains and rarely have full control over their own IT environment. Monodependencies in the digital supply chains can lead to particularly difficult challenges. MSB's analysis highlights the importance of mapping organisations supply chains and planning alternative working methods should something occur in a service that the organisation is dependent on in order to continue operations.

In uncertain times, it is crucial that organisations allocate resources to review relevant protective measures to implement and practice. This in order to strengthen their protection against attempted cyber attacks, but also to minimise harm if the organisation is nonetheless affected. Based on the analysis of the cyber threat landscape and conclusions from previous reports, MSB has identified six specific problem areas where organisations face major challenges, namely:

- systematic approaches in the security work,
- incident and continuity management,
- employee knowledge,
- identity and access management,
- change management,
- digital supply chains.

Based on these problem areas, 25 recommendations have been formulated. The recommendations are addressed to decision-makers, operational developers and strategists in IT departments, but also to security units and operational support, as well as CISOs and others responsible for the information and cyber security work.

Conclusions and recommendations

Conclusions and recommendations

The current security situation is serious. Systematic and risk-based information and cyber security work with planning, implementation, follow-up and practice of preventive security measures is important to protect against attempted cyber attacks. MSB has developed recommendations for how an organisation can strengthen its protection against cyber attacks, and minimise harm if an attack occurs nonetheless.

Based on the IT incident reporting and previous reports, MSB has identified six problem areas where organisations have special challenges when it comes to improving their security measures against attempted cyber attacks. The recommendations presented are based on these challenges.

There may be other relevant problem areas that should be addressed. However, this report focuses on the areas which have been deemed relevant based on challenges described in the IT incident reports or identified as important within other reports and studies conducted by MSB.

The problem areas that many organisations need to manage better are:

- **Systematic approaches in security work:** Systematic and risk-based information and cyber security work with an all-hazards approach is central to preventing and managing IT incidents. In order to improve their resilience to attempted cyber attacks, it is crucial that organisations have the basic conditions required. MSB notes that many organisations in public administration lack a management that gets involved in security issues, systematic working methods and provide resources to carry out the preventive work. MSB has repeatedly highlighted this fundamental problem in previous reports.
- **Incident and continuity management:** A particular challenge for organisations is to manage cyber incidents, caused by a cyber attack, before it has consequences that affect the organisation. During an ongoing attack, there is often a lack of preparedness, skills and capabilities to respond effectively. Organisations may also lack clear common guidelines, rules and procedures, as well as functional communication structures to manage IT incidents resulting from a cyber attack. There is also a lack of practiced procedures to preserve key assets, as well as business continuity plans for alternative ways of working if, for example, information systems that are normally used are unavailable.

- **Employee knowledge:** Phishing and weak passwords are often cited in the IT incident reporting as the reason a malicious actor gains initial access to an organization's information systems. Today's malicious actors may have sophisticated tools at their disposal to produce convincing and complex password and phishing attacks, which are difficult for employees to identify, posing a challenge for organisations. Employees who lack knowledge of threats and vulnerabilities are also more likely to choose weak passwords or reuse the same password, which malicious actors can actively exploit. There are many databases with leaked credentials that a malicious actor can use to see if the employee reuses their passwords or uses a simple system. Organisations may also lack access to technical tools to detect weak passwords or to force employees to choose stronger passwords.
- **Identity and access management**: Vulnerabilities within the organisation can arise in the context of poor identity and access management. One explanation for some of these challenges could be that many organisations have relatively high personnel turnover, and continuous changes in their operations, which in turn could make it more difficult for organisations to manage to prevent access-related IT incidents. This may lead to vulnerabilities arising when, for example, employees who should have remained unauthorised are given access to sensitive information systems or file areas. Inadequate procedures for deactivating legacy user accounts can also benefit the malicious actor.
- **Change management:** It is common for organisations to have built their information systems and their IT environment in such a way that there are challenges and uncertainties in implementing updates. Organisations may lack clear change management procedures and it may take a long time before known vulnerabilities are addressed. Specialised expertise may also be needed to implement the change safely. Not infrequently, there is also a risk that the change causes compatibility problems with other information systems. Organisations may also lack a test environment similar to the production environment, which entails challenges in ensuring that new software and other updates do not cause problems before they are installed in the production environment. Overall, this means that many organisations leave vulnerabilities unaddressed for too long. Organisations that regularly scan for vulnerabilities often find old and serious vulnerabilities. Some of the more high-profile cyber attacks in recent years, such as WannaCry [2], have been possible thanks to unpatched vulnerabilities.
- **Digital supply chains:** Digital supply chains are a natural part of the modern digital ecosystem. Using specialised solutions is cost effective but not risk-free. Maintaining the security of one's IT environment can be a challenge when the organisation lacks transparency in its underlying supply chains and their security. Obtaining information from suppliers about ongoing or past attempted cyber attacks is a challenge for many organisations. Another challenge organisations face is if there is only one or a few providers of a particular service that meet one's quality requirements or are compatible with one's working methods. This in turn leads to monodependencies, where an organisation is dependent on a service and there are no alternative services to use if the service in use is discontinued.

2. WannaCry is an extortion software that targets computers with the Microsoft Windows operating system. In May 2017, WannaCry infected more than an estimated 200,000 computers in 150 countries.

These recommendations are intended to support organisations in their efforts to prioritise security measures, to strengthen protection against cyber attacks and to minimise harm if the organisation is nonetheless affected. The chapter *Cyber threat landscape* presents the IT incident reports with attempted cyber attacks as the underlying cause and the chapter *Challenges in security work* presents the challenges that form the basis of the specific recommendations.

The only way to stay ahead of a malicious actor is to continuously work with a systematic and risk-based approach. MSB's guides are useful to consult in support of this work:

- guidance on security measures in information systems[3],
- basic security in cyber-physical systems[4], and
- increased security in industrial information and control systems[5].

3. MSB. *Vägledning säkerhetsåtgärder i informationssystem [Guidance on security measures in information systems]*, https://www.informationssakerhet.se/stod--vagledning/saker-hantering-av-information2/Vagledning_sakerhetsatgarder_i_informationssystem/ (Downloaded 11/2023).

4. MSB. *Grundläggande säkerhet i cyberfysiska system [Basic security in cyber-physical systems]*, https://rib.msb.se/filer/pdf/29983.pdf (Downloaded 11/2023).

5. MSB. *Ökad säkerhet i industriella informations- och styrsystem* [*Increased security in industrial information and control systems]*, https://rib.msb.se/filer/pdf/29984.pdf (Downloaded 11/2023).

Recommendations to management:

1. Improve the organisation's security culture by setting clear goals and expectations for security, regularly communicating the importance of security, encouraging employees to report security events and improvement proposals, and serving as a role model.
2. Work systematically and risk based and allocate the necessary resources based on the risk analysis.
3. Invest in training to improve the skills and awareness among employees.
4. Invest and participate in cyber security crisis exercises.
5. Regularly take stock of the potential challenges that slow down the security work and use the *Cyber Security Checkup* to identify security gaps.

Recommendations to personnel responsible for information and cyber security:

Incident and continuity management	Employee knowledge	Identity and access management	Change management	Digital supply chains
6. Actively look for signs of malicious activity and use services or technical tools to detect cyber attacks early.	10. Regularly train employees to be able to resist social engineering, use strong passwords and handle them securely.	14. Take stock and identify all access permissions from different information systems.	18. Ensure that personnel with the right competence implement changes.	22. Introduce clear clauses in procurements regarding an information obligation from suppliers in the event of IT incidents.
7. Introduce processes to easily report and follow up security events.	11. Use multifactor authentication.	15. Make sure that only authorised users and information systems have access.	19. Regularly map information systems and establish a test environment that mimics the production environment as far as possible and test changes before they are introduced into production.	23. Review and document dependencies in the information systems of the organisation, especially with regard to external suppliers.
8. Plan and practice for cyber attacks.	12. Mark external e-mails and use technical tools to filter out e-mails with malicious links or attachments.	16. Introduce processes to regularly review permissions.	20. Update the organisation's critical information systems that are exposed to the Internet when new vulnerabilities are discovered.	24. Plan and implement your own processes for managing IT incidents occurred at a supplier.
9. Introduce and practice continuity plans, for example, communication during a cyber crisis.	13. Use technical tools to regularly review the use of weak, leaked or stolen passwords.	17. Use automated identity and access management for planning and verification of changing organisational needs.	21. Base the vulnerability analysis on information about new vulnerabilities, security updates, general guidelines and recommendations to increase resilience through external surveillance.[6]	25. Introduce alternative working methods in case of a supplier incident affecting a service the organisation depends on in order to continue its operations.

6. For example, by regularly visiting MSB's websites.

About the report

About the report

This report provides an overall picture of attempted cyber attacks against government agencies and OES/DSPs and their consequences. Recommendations have been developed based on the challenges identified when analysing the cyber threat landscape and conclusions from previous MSB reports. This report is the third part in a series of thematic reports.[7]

The chapter *Cyber threat landscape* is based on the IT incident reports received by MSB. With the information MSB receives preventative measures, based on the organisations needs, can be developed. Some organisations have reporting obligations because the activities carried out are considered particularly critical for our society. Reporting requirements vary depending on the regulation an organisation is affected by. The organisations that are required to report IT incidents to MSB are national government agencies[8] and providers of essential[9] and digital services[10] (OES/DSPs). Reporting obligations will be extended to more organisations and sectors when the NIS 2 Directive enters into force.[11]

The report is based on the IT incident reports received by MSB between April 2019 and September 2023. Unfortunately, many of the received incident reports lack detailed descriptions of the chain of events. In general, this could mean that some problems or needs that should have been included in the report are missing. In addition to these IT incidents, publicly known IT incidents were also analysed to exemplify the challenges and consequences that attacks can entail.

---

7. The first was: *Digital supply chains under threat: 50 recommendations to strengthen societal security*, https://rib.msb.se/filer/pdf/29829.pdf. The other was: *Threats and opportunities in change management: 20 recommendations for improving information security during changes,* https://rib.msb.se/filer/pdf/30193.pdf.

8. MSB. *Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter [The Swedish Civil Contingencies Agency's regulations on reporting IT incidents for government agencies]* (MSBFS 2020:8) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-8-foreskrifter-om-rapportering-av-it-incidenter-for-statliga-myndigheter.pdf.

9. MSB. *Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster [The Swedish Civil Contingencies Agency's regulations on incident reporting for operators of essential services]* (MSBFS 2018:9) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs2018_9.pdf.

10. MSB. *Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av digitala tjänster [The Swedish Civil Contingencies Agency's regulations on incident reporting for digital service providers]* (MSBFS 2018:10) https://www.msb.se/siteassets/dokument/regler/ forfattningar/msbfs2018_10.pdf.

11. EU. *The NIS 2 Directive* (EU 2022/2555) https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX-:32022L2555&qid=1701943333306.

The below account of the cyber attack on Kalix Municipality gives an idea of how a cyber attack can affect an essential actor's information systems.

On the night before Thursday 16 December 2021, Kalix Municipality suffered a serious service outage. It was soon clear that the municipality was subjected to a ransomware attack where a malicious actor encrypted and locked the municipality's information systems. The malicious actor demanded a ransom in order to restore the information. The cyber attack ultimately impacted a large part of the municipality's services, including home healthcare, home care, schools and libraries.[12,13]

The attack meant that the municipality was unable to use computers, phones or e-mail and instead was forced to work with pen and paper. This forced a complete change in the working methods for home care and home healthcare, for example. The employees were no longer able to access the schedules, medical records and medicine lists that were in the information systems. The work became time-consuming and required employees to use whiteboards for scheduling, among other things. They also had to flip through physical binders with decisions on approved interventions to ensure that all users received the right support. In order to keep the municipality's 1900 employees from going without their Christmas salary, the November salary was paid instead of the December salary. It was not only the municipality of Kalix that was affected, but also suppliers, partners and residents, who could not communicate with the municipality through the normal communication channels.

It would take until mid-January 2022 before most information systems functioned again, and even longer before everything returned to normal for the municipality. The cost of restoring the systems and at the same time upgrading IT security was estimated to amount to SEK 2.5 million.[14] It is unclear what the total cost of the incident was, but it was probably significantly higher. Kalix Municipality never paid a ransom, but instead promoted compliance with MSB's recommendations not to pay[15] and handling of IT incidents.[16,17]

12. Stahle, Nils. *It-attacken mot Kalix kommun – detta har hänt [The IT attack on Kalix Municipality – what happened]*. SVT. 2021-12-17. https://www.svt.se/nyheter/ lokalt/norrbotten/it-attacken-mot-kalix-kommun-detta-har-hant (downloaded 08/2023).

13. Warne, Karin. *Så ledde Kalix IT-chef arbetet under hackerattacken [How the Kalix IT manager led the work during the hacker attack]*. Vision. 2022-05-06. https://vision.se/ chefenifokus/arkiv/2022/nr2/sa-ledde-kalix-it-chef-arbetet-under-hackerattacken/ (downloaded 08/2023).

14. Svenska dagbladet. *It-attacken mot Kalix har kostat 2,5 miljoner [The IT attack on Kalix cost SEK 2.5 million]*. 2022-01-14. https://www.svd.se/a/ JxG1k4/notan-for-attacken-i-kalix-2-5-miljoner-kronor (downloaded 05/2023).

15. MSB. *Metoder som används vid cyberangrepp – Betalning till angriparna [Methods used in cyber attacks – Payment to the malicious actors]*, https://www.msb.se/sv/ amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/metoder-som-an- vands-vid-cyberangrepp/ (Downloaded 10/2023).

16. MSB. *Råd och stöd [Advice and support]*, https://www.cert.se/rad-och-stod/ (Downloaded 10/2023).

17. Hannu, Filip. *Lärdomen efter it-attacken i Kalix: Följ checklistan och lägg pengar på det [Lessons learned from the IT attack in Kalix: Follow the checklist and spend money on it].* SVT. 2022-05-22. https://www.svt.se/nyheter/lokalt/norrbotten/kommundirektorens-lardom-efter-attacken- folj-checklistan-och-lagg-pengar-pa-det (downloaded 08/2023).

The disruptions that arose as a result of the cyber attack on Kalix Municipality impacted users, citizens and other organisations. The risk of more than one organisation and its information systems being affected is growing as organisations are increasingly shifting their activities to a digital environment.

This report has been produced to increase the understanding of the cyber threat landscape targeting government agencies and operators of essential services, and to highlight the challenges that organisations have in their security work and which preventive measures should be prioritised.

Like previous thematic reports, parts of MSB's analysis model are included for those who want to do their own systematic analyses of IT incidents related to cyber attacks.

The report is produced with the support of funding from the EU's Connecting Europe Facility and is primarily addressed to decision-makers, operations developers and strategists in IT departments, but also security functions and operational support, as well as CISOs and others responsible for the information and cyber security work.

Malicious cyber activity

Malicious cyber activity

Digitalisation has entailed major benefits to society, but also means that malicious actors can use cyber attacks as a tool to achieve both short- and long-term goals. Understanding how cyber attacks can be structured, and the underlying aims, can contribute to the ability of organisations to counter cyber threats.

Over the years, cyberattacks have come to be defined in different ways. The different definitions have emerged as threats arising in cyberspace have become a concern for several different types of actors, with different views on what constitutes a threat and what information is worth protecting. In this report, a cyber attack is understood as an attempted cyber attack that has affected the IT environment. Cyber attacks are carried out as one, or a series of, interaction(s) between the *malicious actor* and the *target*. The target of the cyber attack can be an individual or an organisation. In order to qualify as a cyber attack, the interaction between the malicious actor and the target must meet four criteria. The interaction must be something that:

1. the malicious actor does not have the right to do to the target *(the legality criterion)*,
2. entails an exchange of information that results in an interaction, configuration, installation/saving, uninstallation/deletion or overloading in any of the target's information systems, or in information systems that the target uses *(the practice criterion)*,
3. results in at least one undesirable consequence for the target in terms of confidentiality, integrity or availability in the target's information system, in information systems used by the target, or information contained in such information systems *(the incident criterion)*,
4. the malicious actor acts with malicious intent *(the intent criterion)*, meaning that the malicious actor acts to:
    a. cause harm to the target, or to others through the target,
    b. prevent benefit to/for the target, or at others through the target,
    c. provide benefit to the malicious actor or others that the malicious actor supports,
    d. prevent harm to the malicious actor or others that the malicious actor supports.

The *legality criterion* is met when the malicious actor lacks a legal right to carry out an action in the scope of the interaction. Technical security solutions for access control and authentication should be used to restrict unauthorized users from accessing or making changes to information systems. However, if the

components of the information system lack adequate protection, there may be several ways for a malicious actor to access, alter or block access to information without a legal right to do so. In some cases, malicious actors can also discover ways to circumvent the protections that exist. The cases where the threat comes from within one's own organisation or where the malicious actor managed to obtain valid login information in another way, and thereby has technical access, are examples of scenarios where the malicious actor has technical permission, but lacks the legal right to access. The legality criterion allows for a distinction between a cyber attack and, for example, a penetration test.

The practice criterion is met when the interaction between the malicious actor and the target consists of one or more events. An event within this context means that the malicious actor's actions must, within the scope of the interaction, have resulted in something ending, arising or changing within the target's IT environment. For example, the event may consist of the installation of malware, the deletion of digital information assets, the copying of information or the reconfiguration of IT components. A delimitation of the term *cyber attack* could mean that it only includes interactions that occur in cyberspace. In this way, physical sabotage of information systems and network infrastructure is not counted as a cyber attack. MSB delimits the term cyber attack so that events in the physical environment, such as power outages and fires (even if they were deliberately caused), are not counted in the cyber attacks statistics.

The *incident criterion* is met when the interaction between the malicious actor and the target results in one or more incidents in the target's information system. In order to be understood as a cyber attack, the event must have caused an *IT environment impact*. In this context, an IT environment impact may consist of the availability, integrity or confidentiality of an information system or related infrastructure being compromised, altered or terminated. A cyber attack may, for example, result in information assets or information systems becoming unavailable to the target or becoming available to an unauthorised party. The impact criterion means that events that have arisen in connection with the interaction between the malicious actor and the target, but that did not result in any negative impact on the target, are not considered a cyber attack in this context. Such a course of events should instead be understood as a *failed* attempted cyber attack.

The *intent criterion* is met when the malicious actor carries out an interaction with malicious intent. In the section below on the *Aim of the malicious actor*, it is clarified that the malicious actor may have several overriding motives for carrying out the cyber attack. Regardless of the aim, a malicious intent is fundamental for an interaction that fulfils the other criteria to be classified as a cyber attack rather than a mistake. This is because IT incidents that arise as a consequence of a mistake, both due to ignorance or negligence, can in practice result in the same kinds of courses of events as an attack. If an individual who does not have permission configures an IT component resulting in parts of an information system becoming unavailable, but at the same time has no malicious intent, the act constitutes a mistake and not a cyber attack.

The difference between attempted cyber attacks and IT incidents

MSB makes a distinction between cyber attacks and IT incidents. An incident is defined in this report an undesirable event that has occurred. In the event of an IT incident, the undesirable consists of the effects that have occurred in terms of confidentiality, integrity or availability (the incident criterion).

Attempted cyber attacks, mistakes, system errors and natural events are all possible causes of IT incidents.

Appying this logic, it is the unavailability of the web service that is the IT incident. The reason why the web service is not available is a denial-of-service attack, a misconfiguration during change work, a power outage or something else.

By applying such a distinction, it becomes possible to, for example, compare the number of times a web service becomes unavailable, and for how long, due to cyber attacks with the number of times the same web service becomes unavailable due to other reasons. By making this comparison, the most frequent and most serious sources of error can be identified and managed.

Aim of the malicious actor

The malicious actor always has an aim in carrying out a cyber attack on the target. The malicious actor's overall aim determines both what type of actor may be a potential target for the attack and what types of attack methods the malicious actor will use to achieve the goal. As previously mentioned, the target can be an individual or organisation. If the malicious actor's aim is to harm a state or benefit another state, several organisations that contribute to the functioning of society in one way or another may be targets for the malicious actor.

The target of the cyber attack is not necessarily who the malicious actor primarily wants to impact. There are also situations where an actor can become a target for an attack because the malicious actor wants to impact users of the target's services. In this report, this is understood to mean that the malicious actor intends to impact others *via* the target. When the malicious actor's aim is to influence the public, essential societal services can be potential targets.

According to the intent criterion, it is possible to divide the intent of the cyber attack into different typical cases. It may involve:

Preventing benefit **for the target or among others via the target.** Preventing benefit means stopping or delaying certain activity or production. A malicious actor who wishes to prevent benefit works according to the goal that the organisation that constitutes the target should not be able to use information systems and other IT components that enable certain activity or production. This can be about making it difficult or impossible for the organisation to use central information systems, and thereby impact the entire organisation, or individual services. A malicious actor's aim may also conceivably be to prevent benefit for other individuals, organisations or states *via* the target of the attack. If the aim is to prevent

communication for the public, the target of the attack could be a telecom operator, for example. Examples of methods that the malicious actor could use in order to prevent benefit include denial-of-service attacks that make it difficult or impossible to transmit legitimate data traffic to and from affected network components.

Causing harm **to the target or to others via the target.** A malicious actor who wishes to cause harm to the target may, for example, work to destroy critical information assets or functionality or to disclose sensitive information assets. The harm the malicious actor intends to cause can be both material and intangible. For example, a malicious actor's aim could be to cause both financial loss or human physical and mental suffering. The malicious actor may also intend to cause harm to an individual, organisation or state via the target of the attack. If the malicious actor's aim is to cause harm to society as a whole, this may mean that essential services become targets for the attack. Cyber attacks can be carried out, for example, in order to sow distrust among users of an attacked service, as well as the provider of the service. It should be noted that a cyber attack that only prevents benefit for the target, can lead to harm being caused to other organisations and to the general public in the next stage. If, for example, the malicious actor succeeds in temporarily disabling the production of an electricity producer by carrying out a cyber attack, it can cause harm to both the public and the organisations that depend on the electricity supply. Methods that the malicious actor could use to cause harm include malware such as so-called "wiperware" that, when executed, delete information assets in the infected information system.

Causing benefit **to the malicious actor or others the malicious actor supports.** A malicious actor who intends to benefit himself will carry out cyber attacks to amplify his own ability or prosperity. This may involve extracting sensitive information assets from the target or making money. It may also involve cyber attacks carried out with the aim of incorporating parts of the targeted IT environment in the malicious actor's own production. A malicious actor who intends to provide benefit to someone the malicious actor supports at the expense of the target may conduct intelligence gathering that could benefit that party. Examples of attack methods that malicious actor can use in order to provide benefit to himself or someone he supports is installing spyware or a program for cryptomining[18] within the target's IT environment that can be used to extract sensitive information or mine cryptocurrency. Ransomware is also used for this purpose. The malicious actor demands a ransom from the target in exchange for encryption keys that can decrypt information assets that the malicious actor has encrypted.

Preventing harm **to the malicious actor or others the malicious actor supports.** A malicious actor who wants to prevent the counterparty from causing harm to the malicious actor, or others that the malicious actor supports, will work according to the goal of negatively impacting information systems or information assets that could be used for this purpose. Actors who become targets for these kinds of attacks have an ability to act in such a way that can cause harm. This may, for example, involve institutions working with law enforcement or news publishing.

18. Both spyware and cryptominers are examples of malware. Spyware can be used to transfer information about, for example, user activity from the target to the malicious actor. Cryptominers can be installed on the victim's computer in order to use its processing power to mine cryptocurrency.

If the malicious actor supports a state actor or an armed group, it could also involve taking out or disrupting offensive military capability. Attack methods that the malicious actor might use in order to prevent harm often correlate with methods that could be used to prevent benefit or cause harm to a target. A malicious actor who wants to prevent the publication of certain information could, for example, install wiperware within the target's information system to proactively delete information that has been identified as malicious.

Types of malicious actors

When reference is made to different types of actors that carry out cyber attacks, the more organised groups are usually referred to. These include everything from "hacktivists" and cyber criminals to state actors and state-sponsored groups. What they all have in common is that they have the ability to carry out cyber attacks far from their own geographical home base through the global reach of the internet.

The overall aim of the attack can be economically, ideologically, politically or geostrategically motivated and supports the malicious relationship developed by the attacker towards the target.

Malicious cyber threats

Based on the description of cyber attacks and malicious intent (the malicious actor's aim) above, it is possible to describe the concept of cyber threats. A *threat* is defined in this report as something that causes, or contributes to, an incident. A *cyber threat* is a threat that in some way interacts with an information system and can cause an incident in such an information system. Based on the reasoning presented in the previous two sections, the definition of threats can be narrowed and framed to characterise cyber threats as follows:

A cyber threat is a threat that can be used to fulfil the *practice criterion* and *incident criterion* in the description of a cyber attack above. In other words, a cyber threat is something that through, or by contributing to, interaction with, configuration of, installation/saving in, uninstallation/deletion from or overloading of an information system (the *practice criterion*) causes, or contributes to causing, an undesirable consequence in terms of confidentiality, integrity or availability in an organisation's information system, or in information systems used by the organisation, or information contained in such information systems (the *incident criterion*), unless measures are taken to stop such an effect.

Based on the previous section's reasoning, a *malicious cyber threat* can be understood as a cyber threat that is used or can be expected to be used by a malicious actor with malicious intent.

Sometimes one talks about advanced or qualified cyber threats. One way of understanding advanced cyber threats is as a subset of such phenomena that fit within the proposed definition of cyber threats above. A first way to delineate such cyber threats is to set an additional condition that such cyber threats, unless measures are taken to stop them, cause *actual incidents*[19]. An actual incident is defined in this report as an undesirable event that has occurred where:

1. *Harm caused* to the organisation, or to other organisations in conflict with the organisation's interests.
2. *Harm prevented* for the organisation's competitors, or for other organisations in conflict with the organisation's interests.
3. *Benefit prevented* for the organisation, or for other organisations in conflict with the organisation's interests.
4. *Benefit caused* for the organisation's competitors, or other organisations in conflict with the organisation's interests.

Another way of delimiting the subset is to set a condition that advanced cyber threats must have an ability to overcome any countermeasures deployed against them. Both in terms of discovery and in terms of handling. There are three ways of neutralising a phenomenon that constitutes a threat: causing the phenomenon that constitutes the threat to cease to exist (deletion), changing the phenomenon that constitutes the threat so that it no longer has threatening properties (modification) and blocking the threat so that what is threatened cannot be affected by the threat.

Based on the above, an *advanced cyber* threat could thus be defined as:

1. a cyber threat that causes, or contributes to, an actual incident,
2. that has protection against attempts to detect, delete or modify it, and
3. that has functions that render the protection set up to block the cyber threat completely or partially ineffective.

Execution of cyber attacks

There are many different approaches[20] and their sophistication varies greatly depending on the techniques and resources used for the specific attack attempt. Mass mails of spam containing malicious links and denial-of-service attacks can, for example, be said to constitute relatively unsophisticated methods, but at the same time, these vary in design and scale, and consequently potential impact. In some cyber attacks, the malicious actor focuses primarily on monitoring and accessing information without necessarily destroying or changing it. These attacks can take place surreptitiously and without, the target under attack, detecting it. Alternatively, it may take time before the attack is detected. Other cyber attacks

19. Type of incident. An event where benefit is prevented or harm is caused to the affected organisation or benefit is caused or harm is prevented for one of the organisation's competitors (see Annex 1 for a more in-depth account).

20. MSB, *Metoder som används vid cyberangrepp [Methods used in cyber attacks]*, https://www.msb.se/sv/amnesomraden/informations- sakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/metoder-som-anvands-vid-cyberangrepp/ (Downloaded 11/2023).

are more directly tangible and are therefore often discovered at an earlier stage. This includes attacks whose overriding purpose is to generate attention.

The aim of the attack determines whether the malicious actor attempts to gain and escalate access to the IT environment or uses other methods to affect the IT environment's functionality. More sophisticated cyber attacks often begin with an intrusion into the target's IT environment. The intrusion attempt may consist of a number of components[21] or steps, where, for example, an intrusion attempt (simplified) often includes the following:

1. initial access,
2. persistence,
3. lateral movement,
4. goal fulfilment.

Initial access is used by the malicious actor to try to enter an organisation network and information system. The malicious actor can use different intrusion methods such as phishing, the use of compromised authentication data or supply chain attacks.[22] This phase may also include reconnaissance and other preparatory activities aimed at revealing *how* an intrusion can be carried out against the target.

Once the malicious actor has access, he tries to *persist* in order to maintain access in the event of reboots, changed credentials, and other interruptions that could cut off their access. This can be done, for example, through changes to access, action or configuration or by replacing legitimate code such as startup code.[23] This can also be done by taking over several user accounts.

Lateral movement, i.e. when the malicious actor moves deeper into information systems or IT environments, can be implemented by taking advantage of system weaknesses, incorrect configurations or vulnerabilities. The malicious actor can also install his own remote access tools or use legitimate references with built-in network and operating system tools which may be difficult to detect for the target.[24, 25] When executing malware, several methods are often used together to achieve a broader goal. For example, remote access tools can be used to run a "PowerShell" script[26] to explore a network and steal data. The malicious actor can also try to escalate the privileges of the accounts the malicious actor controls, or by taking control of administrator accounts, for example.

---

21. Components can be described in varying degrees of detail. MITRE is an example of a framework for describing cyber attacks, https://attack.mitre.org/.

22. Mitre. *Initial Access*. 2018-10-17 (updated 2019-07-19). https://attack.mitre.org/tactics/TA0001/ (downloaded 06/2023).

23. Mitre. *Persistence*. 2018-10-17 (updated 2019-07-19). https://attack.mitre.org/tactics/TA0003/ (downloaded 06/2023).

24. Mitre. *Privilege Escalation*. 2018-10-17 (updated 2021-01-06). https://attack.mitre.org/tactics/TA0004/ (downloaded 06/2023).

25. Mitre. *Lateral Movement*. 2018-10-17 (updated 2019-07-19). https://attack.mitre.org/tactics/TA0008/ (downloaded 06/2023).

26. A PowerShell script is an unformatted text file that contains one or more PowerShell commands. PowerShell is a command line interface and a script language used for automation.

In order to *achieve the goal*, the malicious actor is almost always required to first explore the network and information systems in order to find his target. With unprivileged access, the malicious actor can enter, but usually higher permissions are required to be able to continue. As part of achieving the goal, the malicious actor can use different methods to try to affect information and the confidentiality, integrity and availability of information systems. See below examples of an attack where the malicious actor persisted, moved laterally and encrypted files and locked out employees from their computers. Given an assumption that it was carried out by criminals seeking profits, the overriding aim was to cause benefit for the malicious actor. As the malicious actor was not paid, the aim of the attack was not achieved and thus goal fulfilment was not achieved, even if the impact of the attack was extensive.

The attack on Norsk Hydro – an expensive story that affected 350,000 employees

- **Type:** Ransomware attack
- **Actual incident:** Benefit prevented, harm caused

On the morning of 19 March 2019, thousands of employees at Norsk Hydro, one of the world's largest aluminium manufacturers, were met with a screen notice that announced that the information systems had been encrypted and could be restored in exchange for a considerable ransom. Some employees could not log into their computers at all[27]. In order to prevent the spread of the virus, the multinational company was forced to stop certain activities, while others had to be managed through manual work processes.[28] Investigators were soon able to establish that the ransomware virus that was executed in the information systems was a malware called *LockerGoga*.[27]

How the malicious actors initially gained access to Norsk Hydro's information system is unknown. However, it is clear that the malicious actors initially targeted individual account users with lower level permissions so that, once inside the system, they could prepare to access users at a higher administrator level. Once access had been obtained to domain administrators, the malware was executed, encrypting files and locking employees out of their computers.[29]

27. Cohen, Gary. *Throwback Attack: Norsk Hydro gets hit by LockerGoga ransomware*. Industrial Cybersecurity Pulse. 2021-05-21. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-norsk-hydro-gets-hit-by-lockergoga-ransomware/ (downloaded 9/2023).

28. Austin, Patrick Lucas. *This Company Was Hit With a Devastating Ransomware Attack –But Instead of Giving In, It Rebuilt Everything.* Time. 2021-06-14. https://time.com/6080293/norsk-hydro-ransomware-attack/ (downloaded 9/2023).

29. Greenberg, Andy. *A Guide to LockerGoga, the Ransomware Crippling Industrial Firms*. Wired. 2019-03-25. https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/ (downloaded 9/2023).

Despite early crisis management efforts, LockerGoga caused significant harm. The attack affected all of Norsk Hydro's 350,000 employees and the company was forced to move to working with pen and paper for three weeks. A lack of knowledge regarding manual production processes meant that the company had to bring in formerly employed pensioners with experience in paper-based work. In parallel, Norsk Hydro, which never paid the ransom demanded by the malicious actors, examined and restored tens of thousands of harmed computers and servers. In some cases, it took three months to restore the information systems.[30] The total cost of lost income and damage-mitigation measures is deemed to have ended up at between NOK 300 and 350 million.[31] Norsk Hydro's openness about the attack, such as in the form of daily press conferences, is believed to have contributed to preventing the company from falling heavily on the stock market.[32]

The "successful" cyber attack

A cyber attack can be seen as "successful" from the malicious actor's point of view if the aim of the attack is achieved. *Table 1* describes how the goal is achieved based on the aim of the malicious actor to *cause harm or prevent benefit* at the target or others via the target, or by *causing benefit* or *preventing harm* to itself, or to others on whose behalf the malicious actor carries out the attack.

The major challenge regarding the categorisation of the effect of a cyber attack is that information about the effects or impact of the cyber attack are rarely available or public for various reasons. This means that certain assumptions must be made, which entails a certain degree of uncertainty and subjectivity.

30. Cohen, Gary. *Throwback Attack: Norsk Hydro gets hit by LockerGoga ransomware*. Industrial Cybersecurity Pulse. 2021-05-21. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-norsk-hydro-gets-hit-by-lockergoga-ransomware/ (downloaded 9/2023).

31. Affärsvärlden. *Så slog cyberangreppet mot Norsk Hydros resultat [How the cyber attack struck Norsk Hydro's earnings].* 2019-06-05. https://www.affarsvarlden.se/artikel/sa-slog-cyberangreppet-mot-norsk-hydros-resultat-6961055 (downloaded 9/2023).

32. Austin, Patrick Lucas. *This Company Was Hit With a Devastating Ransomware Attack–But Instead of Giving In, It Rebuilt Everything.* Time. 2021-06-14. https://time.com/6080293/norsk-hydro-ransomware-attack/ (downloaded 9/2023).

Table 1. The malicious actor's goal achievement based on the aim and effect of causing harm or preventing benefit at the target, or providing benefit or preventing harm to himself.

Overriding objective Overall impact	**Causing harm** to the target attacked, or at others via the target attacked	**Preventing benefit** at the target attacked, or at others via the target attacked	**Causing benefit** to the malicious actor, or to others on behalf of whom the attack is carried out	**Preventing harm** to the malicious actor, or to others on behalf of whom the attack is carried out
Causing harm to the target attacked, or to others via the target attacked	Goal achievement	Impact, but not goal achievement	Impact, but not goal achievement	Impact, but not goal achievement
Preventing benefit at the target attacked, or others via the target attacked	Impact, but not goal achievement	Goal achievement	Impact, but not goal achievement	Impact, but not goal achievement
Causing benefit to the malicious actor, or others on behalf of whom the attack is carried out	Impact, but not goal achievement	Impact, but not goal achievement	Goal achievement	Impact, but not goal achievement
Preventing harm to the malicious actor, or others on behalf of whom the attack is carried out	Impact, but not goal achievement	Impact, but not goal achievement	Impact, but not goal achievement	Goal achievement
None	Failure	Failure	Failure	Failure

Based on the table, a *successful cyber attack* can be defined as a cyber attack where the *goal was achieved* and according to four categories:

1. **Successful reckless cyber attack:** All types of impact are allowed.
2. **Successful controlled cyber attack:** Only certain specific other types of impact are allowed.
3. **Successful restrained cyber attack:** Only a certain number of other types of impact are allowed.
4. **Successful precise cyber attack**: No other type of impact is allowed.

See below examples of an attack that could be categorised as a *successful reckless cyber attack*.

Russia's attack on Viasat's satellite-based KA-SAT network

- **Type:** Denial-of-service attack, malware
- **Actual incident:** Benefit prevented at the target, damage prevented for the attacker

In the initial phase of the full-scale Russian invasion of Ukraine, Russia launched a series of cyber attacks believed to have aimed to overwhelm Ukrainian defence capabilities. The attacks, aimed at authorities and critical infrastructure, were carried out by, among other things, executing malware in the form of wiperware. Russia's attack on the telecommunications company Viasat, whose satellite-based KA-SAT network provides tens of thousands of people and organisations in Ukraine and the rest of Europe with internet access, has been referred to as the most successful.[33]

On 24 February 2022, the hours before Russia began the full-scale invasion of Ukraine, Russian hackers targeted denial-of-service attacks on the network to which Viasat's satellite equipment was connected. By exploiting an incorrectly configured VPN in the network, the attackers subsequently installed wiperware (today known as *AcidRain*). The malware disabled many of the modems that communicate with Viasat's *KA-SAT* satellite, with extensive disruptions as a result.[34]

The attack on Viasat is believed to have hampered the Ukrainian defence's ability to lead and coordinate during the initial phase of the war.[35] In addition, thousands of Ukrainians were left without internet access. The impact also reached Central Europe, where over 500,000 broadband customers lost internet access – in some cases for up to two weeks.[36] The German energy company Enercon also lost the ability to control 5,800 wind turbines.[37]

33. Lewis, James Andrew. *Cyber War and Ukraine. Center for Strategic and International Studies*. 2022-06-16. https://www.csis.org/analysis/cyber-war-and-ukraine (downloaded 2023/08).

34. Poireault, Kevin. *Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites*. Infosecurity Magazine. 2023-05-09. https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack/ (downloaded 2023/08).

35. Svenska dagbladet. *EU: Ryssland bakom cyberattack mot satellit [Russia behind cyber attack on satellite]*. 2022-05-10. https://www.svd.se/a/ V9J77J/eu-ryssland-bakom-cyberattack-mot-satellit (downloaded 2023/08).

36. CyberPeace Institute. *Case Study: Viasat*. 2022-06. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (downloaded 2023/08).

37. Greig, Jonathan. *Viasat confirms report of wiper malware used in Ukraine cyberattack*. The Record. 2022-04-01. https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack (downloaded 2023/09).

About cyber warfare

Cyber attacks can and have been used as a method for achieving tactical and operational goals in both hybrid warfare and full-scale war. These attacks may, but must not, involve the cause of destruction. A cyber attack in armed conflict, whether offensive or defensive, can cause personal injury or death or prevent the benefit, harm or destruction of objects. Cyber means can also be used to locate targets that are then attacked by other means. In addition to cyber attacks, traditional weapons and combat methods can be used to physically destroy computers, disrupt or destroy networks, or to impact, mislead or even kill users.

Cyber attacks in warfare have been used by Russia as a part of the full-scale invasion of Ukraine. In the report *When war came close*[38] , MSB mapped out what kinds of attempted cyber attacks were made and their aims. The figure below illustrates the aims for which cyber attacks and physical attacks on networks, information systems and other IT infrastructure have been used to achieve short- and long-term goals.

Categorisation of attempted cyber-attacks targeting Ukraine	
Preventing benefit in Ukrainian society	**Causing harm in Ukrainian society**
• Disrupting or disabling an essential service. • Disrupting or disabling industry or other operations of importance to the country's economy. • Disrupting integration towards the EU and other countries in the "West".	• Corrupting functions within government and the business community. • Sowing distrust, fear and conflict. • Destroying expensive technical equipment or important information assets.
Preventing harm to the malicious actor or the malicious actor's client	**Causing benefit to the malicious actor or the malicious actor's client**
• Influencing the Ukrainian government in order to not make choices that are not in Russia's interest. • Limiting the country's ability to defend itself militarily. • Preventing unwanted disclosures in the media or on social media.	• Espionage. • Creating sympathies for Russia or Russian positions.

38. MSB, *When war came close: Annual Report – IT incident Reporting 2022*, https://www.msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022/ (downloaded 10/2023).

Consequences of cyber attacks

Consequences of cyber attacks

A cyber attack can entail serious consequences for the organisation affected. Furthermore, if the information system maintains essential services, it can also have serious consequences for society.

An incident is an undesirable event that has occurred. The cause of an IT incident can be divided into four overall categories[39]:

- *attacks* (malicious threats),
- *mistakes* (non-malicious threats),
- *system errors* (technical threats) and
- *natural events* (weather phenomena, earthquakes, solar storms, etc.).

All hazards approach

With the all hazards approach one strives to assess all the risks to something to be protected and analyses every possible cause of the realisation of a risk. The most common causes of reported IT incidents are mistakes (often in connection with updates to the IT environment) and system errors (which could often have been avoided through updates in the IT environment). So working based on the all hazards approach in order to maintain essential information systems is central.

Threats are something that causes, or contributes to, the occurrence of an undesirable event. It is when an undesirable event occurs that an incident arises. Incidents caused by cyber attacks often receive greater media attention compared to other IT incidents. However, in terms of consequences, it does not matter if it is an attack, mistake or system failure that for example causes a life support information system to stop functioning. If the system is not repaired or replaced, patients may die. The consequences here are the effects that occur if nothing is actively done to stop them. It is important to remember that the most common cause of IT incidents reported to MSB in 2022 was system errors, followed by mistakes and then attempted cyber attacks.[40]

39. Categorisation used by MSB for reported IT incidents.

40. MSB, *When war came close: Annual Report – IT incident Reporting 2022*, https://www.msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022/ (Downloaded 11/2023).

An IT incident caused by a cyber attack on information systems that maintain essential services can have serious consequences for the individual organisation affected, but also for individuals and society at large. This is depicted, for example, in the cyber attack on Kalix Municipality[41] and in the example below.

Cyber attack contributed to the inability to prevent a death

- **Type:** Ransomware attack
- **Actual incident:** Benefit prevented

On 10 September 2020, the University Hospital in Düsseldorf, Germany, was subjected to a cyber attack that locked the information systems used for communication and coordination of patients, among other things. The hard-pressed hospital was forced to cancel operations and cut its capacity in half.[42] When the hospital received an alarm on the same night about a seriously ill woman, the ambulance was referred to a hospital located an hour away, whereby the woman died in transit.[43] The tragic event has been described as the first death caused by a cyber attack.[42]

The malicious actors introduced the malware by exploiting a vulnerability at the hospital's network provider. When the vulnerability was fixed, the virus had already been planted in the information systems. The ransomware attack is believed to have actually been directed at the university with which the hospital was affiliated and, at the behest of the police, the malicious actors came to hand over the decryption keys without any ransom being paid.[42] However, the damage was already done and it would take two weeks before the hospital could reopen its emergency department, and more time before it returned to full capacity.[44] The malicious actors, who could not be identified, are suspected by German police for manslaughter.[45]

41. See the chapter *About the report*.

42. Eddy, Melissa; Perlroth, Nicole. *Cyber Attack Suspected in German Woman's death*. The New York Times. 2020-09-18. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (downloaded 9/2023).

43. Dobos, Lars. *Patient avled efter ransomware-attack mot sjukhus [Patient died after ransomware attack on hospital]*. Tech World. 2020-09-18. https://techworld.idg.se/2.2524/1.739684/avliden-ransomware-sjukhus (downloaded 9/2023).

44. Silomon, Jantje. The Düsseldorf Cyber Incident. Institute for Peace Research and Security Policy. 2020-09-30. https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident (downloaded 9/2023).

45. Tidy, Joe. *Police launch homicide inquiry after German hospital hack.* BBC. 2020-09-18. https://www.bbc.com/news/technology-54204356 (downloaded 9/2023).

Organisation impact

An IT incident that affects the integrity, availability or confidentiality of an IT environment can, regardless of the reason, have consequences outside of it. The IT incident can disrupt the day-to-day operations of organisations with consequences such as reduced productivity, reduced communication, impaired website performance or disruptions of services.

The IT incident may also involve costs in the form of repair and recovery of the harm caused to the organisation. Organisations can also receive legal sanctions if they do not comply with laws or regulations on data protection, for example. If the IT incident is made public or, for example, leads to some form of data leak, it can harm customer confidence and the value of the brand, or even mean that the organisation goes bankrupt as in the example of data breaches at the Finnish company Vastaamo.[46] The different consequences of an IT incident can in turn lead to different forms of additional work, stress and concerns among employees within the organisation and their customers.

In order to be able to manage ongoing and prevent future incidents more quickly, it is crucial that IT incidents are reported[47, 48] and that information is shared.

Categories of impact

Different taxonomies can be used to categorise the impact of IT incidents where, for example, research suggests that the impact or damage of a cyber attack can be divided into five main categories consisting of physical/digital damage, economic damage, psychological damage, damage to reputation or social and societal damage[49]. ENISA uses a similar taxonomy with five main categories.[50]

The Swedish emergency preparedness system is structured around the safeguarding of a number of social assets in need of protection. In the context of the NIS, three designated protected assets are particularly important. In the event of an IT incident involving an essential service, an assessment must be made if the disruption negatively affects human health, the users' finances and/or the users' confidence in the essential service. The impact on these protected assets is important in order to determine the severity of disruption of an essential service. It may be easier to have an idea of the impact on certain protected assets than others. For example, operators of essential services in healthcare can more easily assess whether people's health is negatively impacted by the disruption, but have more difficulty in determining the impact on the users' finances.

46. Data breaches at Vastaamo led to an international scandal.

47. Government agencies must report IT incidents that occur in the authority's information system or in services provided by the authority to another organisation. Read more about IT incident reporting for government agencies on MSB's website, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter/.

48. Both operators of essential services and digital service providers must report incidents to MSB. Read more about incident reporting for OES/DSPs on MSB's website, https://www.msb.se/sv/ amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/incidentrapportering-for-nis-leverantorer/.

49. Agrafiotis, Ioannis; Nurse, Jason R C; Goldsmith, Michael; Creese, Sadie; Upton, David.*A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate*. 2018. https://doi.org/10.1093/cybsec/tyy006 (downloaded 09/2023).

50. ENISA. *ENISA Threat Landscape 2022*. 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (downloaded 06/2023).

Psychological dimension of the attack

One thing that separates cyber attacks from IT incidents caused by other factors, such as mistakes or system errors, is how different actors react to the incident. A reaction is not a consequence per se and does not necessarily happen automatically.

A cyber attack can be said to have three categories of actors whose reactions are important. These actors are the *malicious actor*, the *target* and *third parties* (such as an organisation using a service provided by the target). In general, third parties become more concerned and inclined to act in sometimes less thought-out ways when it is confirmed that an IT incident has been caused by a cyber attack. One reason for this reaction is that information about the incident and how it affects or will affect third parties is often deficient. This in turn leads to organisations not knowing how to act or what security measures would need to be implemented if, for example, sensitive information about customers or information systems was disclosed.

An occurred IT incident caused by an attack means that the attack attempt has at least led to an impact or had an effect (see Table 1), and in the worst the case succeeded.This could mean that the malicious actor tries to conduct an attack again, either against the same target, or against someone else. It may also mean that the malicious actor has managed, through the target, to attack others as well and that they have not discovered it. Concern at third parties, based on insufficient information about what has happened or distrust of who conveys the information or the information itself, creates uncertainty about the impact of the attack. Rumours and erroneous speculation can then arise that lead to undesirable reactions.

When it comes to the target, the reaction can be more agitated and worried if it is a cyber attack, while at the same time there is the possibility to blame another party for the IT incident. If it is instead a matter of an IT incident that the target has accidentally caused itself, it becomes more difficult to place the blame elsewhere.

See below examples of the psychological impact a cyber attack can have on both patients and the organisation when sensitive and confidential information ends up in incorrect hands and could be used for extortion.

Data breaches at Vastaamo led to an international scandal

- **Type:** Data breach
- **Actual incident:** Benefit caused, damage caused

On 21 October 2020, the Finnish psychotherapy centre Vastaamo announced that they had been subjected to a data breach and extortion.[51] About 36,000 patients' confidential information had been stolen.[52] The information stolen from adults and juveniles constituted personal and sensitive materials, such as medical records, therapy notes, diagnoses and client data.[53] Several of the files were published on the "dark web".[54] Many of the patients also received blackmail e-mails where they were asked to pay EUR 200 to keep their information from being made public.[55]

In retrospect, it has emerged that Vastaamo was attacked twice, both in 2018 and 2019. Vastaamo's CEO, Ville Tapio, was thought to have been aware of the security deficiencies that existed in the information systems, which resulted in the Board requesting his resignation.[53] The case is seen as exceptional and legally complicated – especially due to the large number of victims. Even from the victim's point of view, the case has been complicated with uncertainties about what is happening and what they should do to get their rights heard.[56]

Vastaamo went bankrupt in 2021, only months after the data breach had been made public.[57] In total, more than 25,000 patients' reports of blackmail were reported to the Finnish police, making the case the largest criminal case in Finnish history. Its scope, but also its ruthlessness in the form of blackmail attempts targeting private individuals and minors, has made the event an international scandal.[55]

Societal impact

Today, many information systems constitute more than a support for organisations, they are a direct prerequisite for the operation's functionality. Development entails both great opportunities and risks. The risks to information systems that maintain essential services and other critical infrastructure are increasing due to the widespread use of systems that, for example, control and monitor industrial

51. Svenska Yle. *Dataintrånget mot Vastaamo: Det här har hänt och det här vet vi nu [The data breach against the Vastaamo: What happened and what we now know]*. 2022-10-28. https://svenska.yle.fi/a/7-1496439 (downloaded 07/2023).

52. Helsinki Times. *The Cyber attack that rocked the nation*. 2020-12-22. https://www.helsinkitimes.fi/columns/columns/331-david-kirp/18450-the-cyber-attack-that-rocked-the-nation.html (downloaded 07/2023).

53. Yle. *Vastaamo board fires CEO says he kept data breach secret for year and a half*. 2020-10-26. https://yle.fi/a/3-11614603 (downloaded 07/2023).

54. "Dark web" refers to those parts of the internet that are not intended or visible to the public. They are used for illegal business and other criminal activities, but not everything is necessarily illegal on the dark web.

55. The Guardian. 'Shocking' hack of psychotherapy records in Finland affects thousands. 2020-10-26. https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland (downloaded 07/2023).

56. Yle. *Åklagaren har väckt åtal i Vastaamofallet. Aleksanteri Kivimäki åtalas för bland annat grovt dataintrång och försök till grov utpressning. Åklagaren vill se ett sju år långt fängelsestraff [The prosecutor has filed charges in the Vastaamo case. Aleksanteri Kivimäki is charged with gross data breach and attempted gross extortion. The prosecutor wants to see a seven-year prison sentence],* https://svenska.yle.fi/a/7-10043734 (Downloaded 11/2023).

57. *Helsinki Times. Young Finnish man detained in absentia over data breach at Vastaamo*. 2022-10-31. https://www.helsinkitimes.fi/finland/finland-news/domestic/22438-young-finnish-man-detained-in-absentia-over-data-breach-at-vastaamo.html (downloaded 07/2023).

processes. Many of today's information systems also have dependencies that extend both within and between organisations. With digitalisation and the complex dependency chains that have emerged, IT incidents affecting several organisations have become more common. Consequently, society has a new kind of vulnerability.

An incident at an organisation that is part of a digital supply chain can have a much greater impact on society than an incident at an organisation that does not play an important role for others. Therefore, vulnerabilities of organisations and information systems included in digital supply chains are attractive to a malicious actor. A malicious actor can, for example, write software that scans the internet for vulnerable software at different organisations and then interacts with the software in a way that allows for an intrusion, spread of malware or other malicious activities. When many organisations both use the same internet-connected software, and lack protection that can block attacks through that software, many organisations can be affected at the same time. This, in turn, can lead to major societal impact. See below examples of how a cyber attack can have societal impact.

Ransomware attacks knocked out hundreds of miles of oil pipelines in the United States

- **Type:** Ransomware attack
- **Actual incident:** Benefit prevented

On 7 May 2021, the Colonial Pipeline, which accounts for almost half of the fuel supply in the eastern United States, discovered intrusions into its administrative IT environment that turned out to be a ransomware attack.[58] The Colonial Pipeline chose to shut down hundreds of miles of its oil pipelines. The functioning of the oil pipelines is based on digital solutions, such as in the form of pumps and sensors that monitor and control the flows, all of which are connected to a central system that is sensitive to cyber attacks.[59] In addition to locking computers and servers in the administrative IT environment, the attackers also stole a large amount of sensitive data that they threatened to leak if a ransom was not paid.[60] The attack has been called the largest cyber attack ever to affect the U.S. energy sector.[61]

The oil pipelines shut down caused major problems in the south-east of the United States where the fuel ran out completely in some places. The prices of petrol skyrocketed and many people also hoarded petrol.[58] As a result of the fuel shortage, an emergency was announced in a total of 17 states, a measure aimed, among other things, at increasing the alternative transport routes for oil and gas.[62] The closed oil pipelines also supplied several airports with fuel,

58. Cohen, Zachary; Sands, Geneva; Egan, Matt. *What we know about the pipeline ransomware attack: How it happened, who is responsible and more.* CNN. 2021-05-10. https://edition.cnn.com/2021/05/10/politics/colonial-ransomware-attack-explainer/index.html (downloaded 9/2023).

59. BBC. *Colonial Pipeline: US fuel firm resumes service after cyber-attack.* 2021-05-12. https://www.bbc.com/news/business-57090428 (downloaded 9/2023).

60. Robertson, Jordan; Turton, William. *Colonial Hackers Stole Data Thursday Ahead of Shutdown.* Bloomberg. 2021-05-09. https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown (downloaded 9/2023).

61. Höök, Peter. *Amerikanska Colonial Pipeline stänger oljeledningar efter ransomattack [U.S. Colonial Pipeline closes oil pipelines after ransomware attack].* Infrastrukturnyheter.se. 2021-05-12. https://www.infrastrukturnyheter.se/20210512/24691/amerikanska-colonial-pipeline-stanger-oljeledningar-efter-ransomattack (downloaded 9/2023).

62. Collier, Kevin. *Colonial pipeline hack claimed by Russian group DarkSide spurs emergency order from White House.* NBC News. 2022-05-10. https://www.nbcnews.com/tech/security/colonial-pipeline-hack-claimed-russian-group-darkside-spurs-emergency-rcna878 (downloaded 9/2023).

forcing several airlines to change and in some cases cancel planned flight routes.[63] The cyber attack is estimated to have cost the Colonial Pipeline $4.4 million. In reference to the major impact on American society, the company chose, as early as the day of the attack, to pay the ransom to the attackers.[64] However, it was only after six days that the closed oil pipelines could be put back into operation.[65]

Note: Payment to the attackers is a way to finance (and thus motivate continued) aggravated criminal activity and MSB strongly advises against doing so.[66]

Certain types of essential services are provided by several organisations, often in competition with each other. This means that if there is an interruption at a bank, for example, payments can be handled with the support of other banks. There is therefore redundancy in society when it is possible for more than one organisation to provide the same kind of service. Hence, to make payments impossible, a number of organisations must be unable to provide their services at the same time. It is especially in such situations that it can be said that a cyber attack has serious societal consequences.

The following three risks in digital supply chains that can lead to serious societal consequences have been identified:

1. when things that are not to be delivered in a digital supply chain are still delivered to many organisations at the same time whereby threats or obstacles arise in them,
2. when things that are to be delivered in a digital supply chain are not delivered to many organisations at the same time whereby deficiencies arise in them,
3. when many organisations have the same or similar internet-exposed and vulnerable mechanisms.

63. Josephs, Leslie. *Pipeline outage forces American Airlines to add stops to some long-haul flights, Southwest flies in fuel.* CNBC. 2021-05-10. https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html (downloaded 9/2023).

64. BBC. Colonial Pipeline boss confirms $4.4m ransom payment. 2021-05-19. https://www.bbc.com/news/business-57178503 (downloaded 9/2023).

65. Lyons, Kim. *Colonial Pipeline says operations back to normal following ransomware attack.* The Verge. 2021-05-15. https://www.theverge.com/2021/5/15/22437730/colonial-pipeline-normal-ransomware-attack-fuel (downloaded 9/2023).

66. MSB. *Methods used in cyber attacks, Ransomware, Payment to the malicious actors,* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/risker-och-sarbarheter-in-om-cybersakerhet-och-cyberfysiska-system/hot-och-metoder-inom-cybersakerhet/metoder-vid-cyberangrepp/ (downloaded 9/2023).

An example of an IT incident in a supply chain as a result of a cyber attack may be that malware enters the operator's or other organisations' information systems. Particularly serious consequences can arise in so-called monodependencies, i.e. when organisations depend on a service and there are no alternative services if the service ceases. See below examples of consequences of an IT incident at an operator of emergency medical alarms when their service stopped functioning and other service was missing for the users.

Attacks on OES/DSP caused disruptions to emergency medical alarms used by 100,000 people

- **Type:** Operation disruption due to breach
- **Actual incident:** Benefit prevented

Shortly after midnight on 23 March 2023, disruptions to emergency medical alarms arose that were used by in-home care services in municipalities throughout Sweden.[67] The disruptions meant that healthcare professionals did not receive a signal in the event of incoming alarms from the elderly or the sick.[68] All affected municipalities used the same emergency medical alarm provider, Careium, which also provided the IT environment in which alarms were passed on from healthcare providers.[69]

In the evening of 23 March, Careium noted that the disruption of the emergency medical alarms was caused by an attack.[70] The disruptions lasted over half a day and affected 100,000 people, in a total of 150 municipalities.[71] The lack of services that could replace the function of the emergency medical alarms exacerbated the impact of the attack, with consequences for people's lives and health. During the time that the alarms were inaccessible, several home services had to go up into states of readiness to ensure that patients were unharmed. The operations were forced to call in extra staff and work according to strict priority lists.[72]

Careium's investigation of the incident showed that it cannot be ruled out that an unauthorised person gained access to personal data in connection with the attack. The company's final assessment is that in such circumstances, access to a "very limited amount of information" is involved.[73]

67. Hannes, Forssell. SVT. *Trygghetslarmen fungerar igen efter cyberattack [Emergency medical alarms working again after cyber attack]*. https://www.svt.se/nyheter/ lokalt/dalarna/trygghetslarm-i-falun-ur-funktion (downloaded 8/2023).

68. Cision. *Careiums larmsystem i Sverige är återigen i drift [Careium's alarm system in Sweden is once again in operation]*. https://news.cision.com/se/careium/r/careiums-larmsystem-i-sverige-ar-aterigen-i-drift,c3739863 (downloaded 8/2023).

69. Careium. *Careiums larmsystem i Sverige är återigen i drift [Careium's alarm system in Sweden is once again in operation]*. https://www.careium.com/sv-se/tjanster/alla-tjanster/larmmottagning/ (downloaded 8/2023).

70. Cision. *Careiums larmsystem i Sverige är återigen i drift [Careium's alarm system in Sweden is once again in operation]*. https://news.cision.com/se/careium/r/careiums-larmsystem-i-sverige-ar-aterigen-i-drift,c3739863 (downloaded 8/2023).

71. Dagens samhälle. *It-attack slog ut 100 000 trygghetslarm [IT attack knocked out 100,000 security alerts]*. https://www.dagenssamhalle.se/samhal- le-och-valfard/digitalisering/it-attack-slog-ut-100-000-trygghetslarm/ (downloaded 8/2023).

72. Mjölby Municipality. *Nu fungerar trygghetslarmen som vanligt igen [Now the emergency medical alarms are working as usual again]*. https://www.mjolby.se/nyheter/nyheter/ 2023-03-23-uppdatering-nu-fungerar-larmen-igen---detta-efter-en-tillfallig-driftstorning-med-vara-trygghets-larm (downloaded 12/2023).

73. Careium. *Careium bistår fortsatt sina kunder med anledning av personuppgiftsincident enligt GDPR [Careium continues to assist its customers on the basis of a personal data incident according to GDPR]*. https://www.careium.com/sv-se/om-careium/future-of-care/uppdaterad-information-med-anledning-av-person-uppgiftsincidenten/ (downloaded 8/2023).

According to MSB's analysis of reported IT incidents, there are indications that organisations often lack digital alternatives if, for example, their IT service provider suffers from a prolonged outage. Such indications can be seen, for example, among OES/DSPs both in healthcare when it comes to emergency medical alarms, but also in the drinking water supply where the monitoring systems in facilities send sensor data over a telecom operator's network.

Resistant in essential information systems

For essential information systems to be resistant, they must be robust, resilient and redundant.

- **Robustness** is achieved by the organisation conducting systematic risk prevention and risk management work.
- **Resilience** is achieved by the organisation planning and practising both incident management and continuity management. Resilience can be enhanced through cooperation. Having access to spare parts and components is central to good resilience.
- **Redundancy** is achieved by having a functioning market where organisations can compete and where there is the possibility for more than one organisation to provide the same kind of service.

Cyber threat landscape

Cyber threat landscape

MSB receives over 300 IT incident reports from government agencies and OES/DSPs annually. About 30–50 of these describe attempted cyber attacks. Most reported cyber attacks have limited impact and have primarily been carried out using less sophisticated methods. IT incident reporting is an important source of information in MSB's work to develop needs-based support. Incident data contributes both to MSB's current situation assessment and to the long-term strategic analysis.

This chapter describes the cyber threat landscape against Swedish government agencies and OES/DSPs based on the IT incidents caused by attempted cyber attacks. The chapter is based on IT incident reports received by MSB from 1 April 2019 through 30 September 2023 and which reported an attempted cyber attack as the underlying cause.[74] The report is limited to the mentioned time period as reporting requirements for OES/DSPs came into effect in spring 2019.

Number of unreported cases

There are actors required to file reports who do not report IT incidents, including cyber attack attempts, to MSB. The number of unreported cases comprises at least two different phenomena, namely that:

- organisations do not report at all,
- organisations do not report everything they should report.

The hidden statistics are discernible, among other things, because:

- certain reporting organisations have never reported an IT incident to MSB,
- in supply chain incidents, reports are received from some, but not all, affected organisations with a reporting requirement.

74. MSB is providing an account of the cyber threat landscape based on the IT incident reporting. The problem areas clearly identified by the IT incident reporting have been included, and special problem areas have been highlighted. The fact that some organisations required to report do not report IT incidents, combined with the fact that many of the received incident reports lack detailed descriptions of the course of events is unfortunate. Overall, this risks limiting the understanding of the operational situation, as well as trends over time, and therefore means that certain problems or needs that should be addressed and managed are missed.

Although there are unreported cases, MSB believe that the IT incident reporting provides a good overview of the cyber threat landscape against government agencies and, in part, OES/DSPs in terms of the distribution of reported causes and consequences. Consequently, MSB assesses that the underlying data is adequate for extrapolation. However, reported incidents might not be representative for the entire population as OES/DSPs within some sectors reports remarkably few incidents. MSB takes this into account when analysing the material.

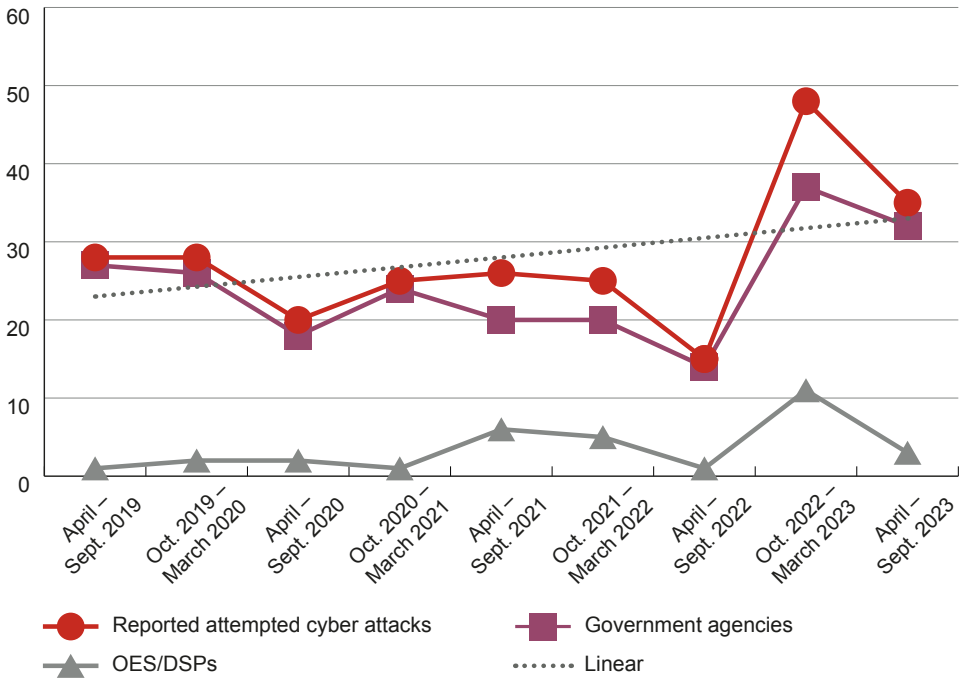
Between April 2019 to September 2023, MSB received a total of 1,542 IT incident reports. Of the total number of reports received, attempted cyber attacks are listed as the cause in 250 cases. This corresponds to 16 percent of the total number of reports received. In addition, another 41 reports describe malicious actions which do not meet previously defined criteria for being classified as an attempted cyber attack.[75]

Of the 250 attempted cyber attacks reported to MSB from April 2019 to September 2023, 87 percent have been received from government agencies and 13 percent from OES/DSPs. The notably large difference is due in part to the fact that the reporting threshold for the IT incident reporting obligation of OES/DSPs are higher than for government agencies.[76] This limits comparisons of the cyber threat landscape somewhat, but at the same time, the attempted cyber attacks that cause major impact are required to be reported by everyone and are thereby comparable. As described in more detail further down, 53 percent of reported attempted cyber attacks that are deemed to have resulted in some form of organisation impact.

75. In the chapter "Malicious cyber activity" in this report, four criteria are defined that the interaction between the malicious actor and the target must meet in order to be classified as a cyber attack. In accordance with these, 41 incident reports describing malicious activity have not been deemed to fall under the definition. Most of them constitute fraud carried out via email, but there are also cases of physical sabotage of IT components.

76. When NIS2 directive enters into force, the same requirements will be imposed on all organisations subject to reporting.

Figure 1. Number of attempted cyber attacks from April 2019 to September 2023



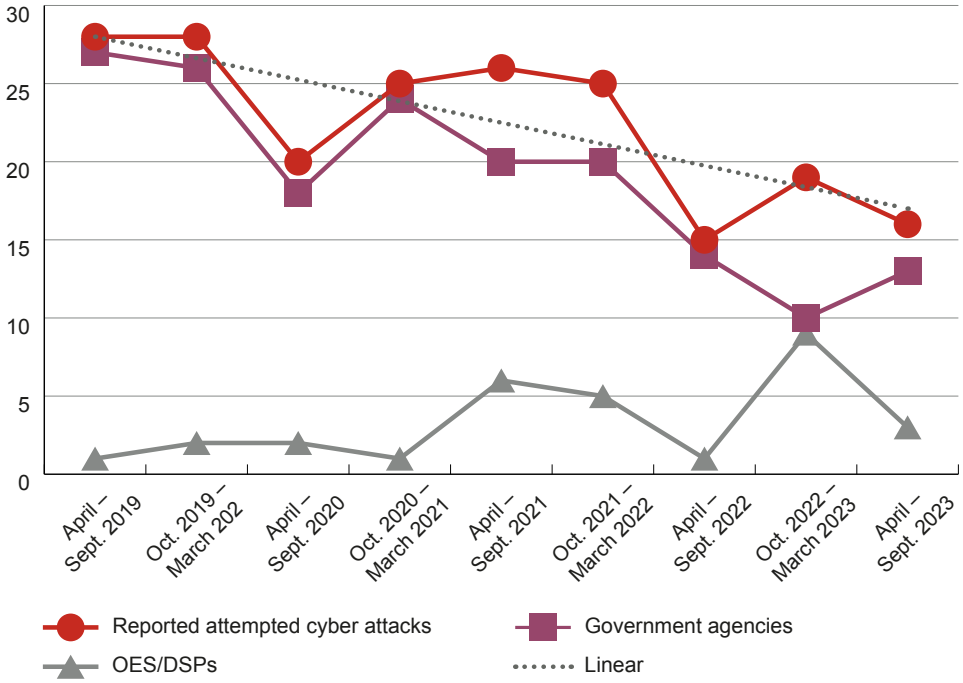
Line charts describing the total number of attempted cyber attacks reported by government agencies and OES/DSPs from 1 April 2019 to 30 September 2023. The chart includes a trend line that describes the development over time.

The frequency of reported attempted cyber attacks from both government agencies and OES/DSPs between April 2019 and September 2023 has been relatively stable. *Figure 1* shows that in most six-month periods, 20 to 30 cyber attacks were reported. However, the frequency has fluctuated more since 2021. The lowest number of attempted cyber attacks, 15 cases, was reported in the period April through September 2022. The highest number, 48 cases, was reported from October 2022 to March 2023.

A relatively large number of reports of denial-of-service attacks were received at the beginning of 2023. The attacks were forewarned on social media as backlash to the "Quran burnings" that were carried out in rounds during the period. The denial-of-service attacks therefore does not nessecarily represent a long-term trend of increased attempted cyber attacks against government agencies and OES/DSPs. On the other hand, it may be seen as likely that similar episodes of high activity will occur in the future as well.

It can also be seen that more cyber attacks were reported from both government agencies and OES/DSPs in the period October 2022 through March 2023. The denial-of-service attacks in particular received a lot of media attention and MSB has noted that more incidents, both concerning "successful" and "failed" denial-of-service attacks, were reported when the issue was highlighted and brought up at the societal level.

Figure 2. Development between April 2019 and September 2023 excluding externally triggered attempted cyber attacks



Line chart describing the number of attempted cyber attacks reported by government agencies and OES/DSPs excluding attack attempts deemed to be linked to an external "trigger phenomenon". An external trigger refers to a specific event or phenomenon in the physical world where something has happened that in turn can be shown to have served as a motive for acting maliciously against Sweden or Swedish interests. In order for an event to be counted as a trigger, a clear increase in the number of reported incidents caused by attacks should be observed in the statistics, and there should also be independent evidence indicating that the increase can be linked to the trigger phenomenon.

MSB has analysed all the received incident reports describing attempted cyber attacks during the time period and can only identify one phenomenon, the so-called "Quran burnings", that meets the above criteria. In the figure, denial-of-service attacks from the period 21 January to 4 May 2023 have been excluded. During that time period, four times as many denial-of-service attacks were reported as for the whole of 2022, i.e., far above normal.

Figure 2 presents all the reported attempted cyber attacks during the period, excluding the denial-of-service attacks that could be linked to backlash to the "Quran burnings". What remains is a representation of the normal situation provided by incident reporting.

In a comparison between *Figure 1* and *2*, a different picture is given of the frequency of reported attempted cyber attacks. The normal situation in *Figure 2* shows a reduced number of reported attempted cyber attacks over the entire measurement period. This can in part be explained by the total number of reported IT incidents having decreased during the same period. The OES/DSPs have indeed reported more attempted cyber attacks, but government agencies, which also account for the majority of the incidents reported, have contributed a gradually decreasing number of reports of attempted cyber attacks during the measurement period. That government agencies are reporting fewer attempted cyber attacks may be due to a combination of (i) a generally declining willingness to report, (ii) reduced propensity to report "failed" attack attempts (especially phishing attempts), (iii) better protection that led to fewer IT incidents and (iv) malicious actors increasingly regarded government agencies as low-priority targets over time.

Types of attempted cyber attacks

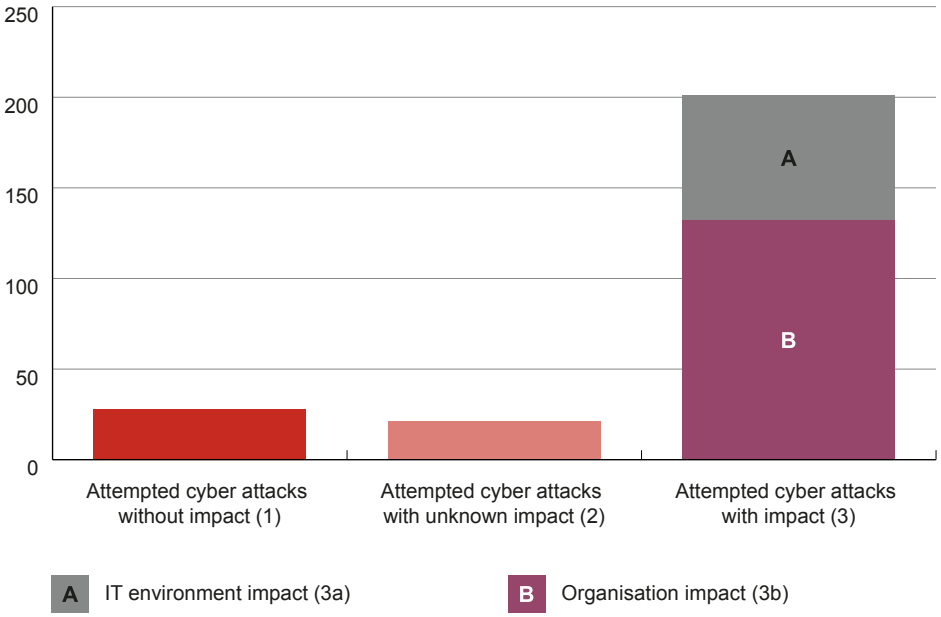
The attempted cyber attacks reported from organisations required to report have varied both regarding the method of execution and the degree of effectiveness. Some are completed cyber attacks that have had a major impact on the organisation's IT environment, and in turn the organisation at large, while other, unsuccessful attempts, have had no impact at all. The attempted cyber attacks analysed in the framework of this report can be divided into three broad categories:

1. Attempted cyber attacks *without impact*
   Attempted cyber attacks without impact include the attempted cyber attacks that have not resulted in any impact on the IT environment or information stored or processed in it. That the attempted cyber attack did not affect the IT environment or information in it means that it did not affect the confidentiality, integrity or availability within the IT environment. A total of about 11 percent, 28 cases, of the 250 reported attempted cyber attacks fall into this category.
2. Attempted cyber attacks *with unknown impact*
   Attempted cyber attacks with unknown impact include the reported attempted cyber attacks where it was not possible to discern, based on the submitted IT incident report, whether it had any impact on the IT environment or information stored or processed therein. In total, about 8 percent, 21 cases, of the 250 reported attempted cyber attacks fall into this category.
3. Cyber attacks *with impact*
   Cyber attacks with impact include the cyber attacks that affected the attacked IT environment, or information that is stored and or processed therein, and hence can be described as completed. The fact that the cyber attack affected the IT environment or information in it means that the confidentiality, integrity or availability of the IT environment or information has been affected. These incidents represent 80 percent, a total of 201 cases, of the reported attempted cyber attacks. Cyber attacks with an impact can be further divided into two related subcategories:
   a. Cyber attacks with an *IT environment impact*
   b. Cyber attacks with an *organisation impact*

Category I includes 34 percent of cases that have *only* resulted in IT environment impact. The IT environment impact refers to the fact that the cyber attack has resulted in undesirable consequences for the IT environment or information stored or processed in it. Category II includes the incidents that are deemed by MSB to have resulted in IT environment impact and an actual negative outcome for the affected organisation. This category also includes services provided by the organisation and used primarily by external users. Category II accounts for 66 percent of the 201 cyber attacks that had an IT environment impact. In other words, in terms of the total amount of attempted cyber attacks reported, 53 percent of the cases resulted in a disruption or other event that affected the organisation in an undesirable manner.

Figure 3 illustrates the distribution of reported attempted cyber attacks according to the categorisation.

Figure 3. Categories of attempted cyber attacks



Bar chart describing how many attempted cyber attacks (1) have no impact, (2) have unknown impact, and (3) have resulted in impact. Cyber attacks with an impact can be divided into those that have *only* resulted in IT environment impact and those that have resulted in IT environment impact *and* organisation impact.

Attempted cyber attacks without impact

MSB received 28 IT incident reports where the reporting organisation describes an occurred security event[77] without any impact on the organisation's IT environment. A security event may consist of a threat arising, a success factor ending, an obstacle arising or a protection ending. Security events that did not result in an incident within the IT environment usually constitute failed intrusion attempts where the malicious actor used methods such as phishing or systematic testing of different login information in order to access user accounts. The reporter often describes that phishing e-mails were sent to user accounts, but that no interaction took place, or that it was handled by established cybersecurity controls. The fact that attempts to access user accounts are reported to a greater extent than other ineffective cyber attacks may be assumed to be due to the fact that they are easier to detect. IT incident reports describing phishing attempts without impact were more common earlier in the analysed measurement period. This could be a sign that the tendency of government agencies to report these events has decreased.

77. A security event is an occurred undesirable event. It may be that a threat arises, a protection ceases/vulnerability arises, a success factor ceases/deficiencies arise or obstacles arise (see Annex 1 for a more in-depth presentation). It is only if the security event has affected the confidentiality, integrity or availability of the IT environment or information processed or stored therein that the security event constitutes an IT incident.

Attempted cyber attacks with unknown impact

21 reported cases lack a clear specification of whether the attempted cyber attack had any impact. As in the category of attempted cyber attacks without impact, an intrusion attempt is usually described, many of which consist of an initial phishing attempt. However, unlike the IT incident reports in the previous category, the outcome is not described, which makes it difficult to discern whether the attempted cyber attack was averted or not. In addition to phishing attempts, there are also other methods of data intrusion within this category. Among other things, there are cases where the reporter describes attempts to exploit vulnerabilities in code.

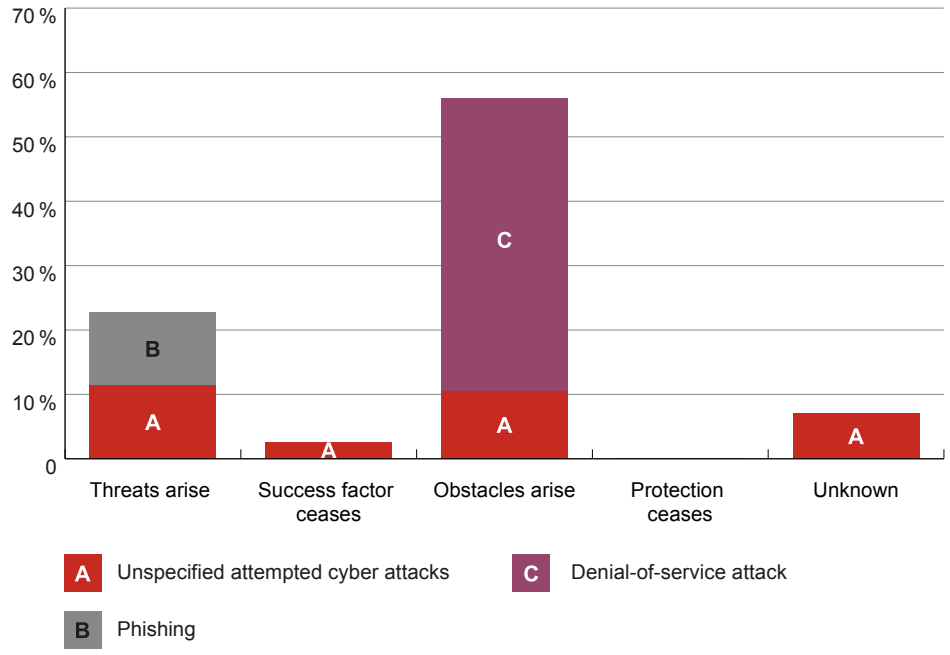
Cyber attacks with impact

A total of 201 cyber attacks are deemed to have affected the confidentiality, integrity or availability of the reporting organisation's IT environment or information stored or processed in it. Of these 201 cases, 132 cases also resulted in real impact on the organisation. Below is a presentation of what types of IT environment impact and organisation impact are described.

IT environment impact

The impact on the IT environment or information in it is presented in this report as types of security events within the IT environment. *Figure 4* presents the occurrence of different types of security events that arose in connection with the cyber attack.

Figure 4. Security events that affected the IT environment



Bar chart describing types of security events that arose in connection with a cyber attack. The diagrams include what percentage of these describe the methods of denial-of-service attacks and phishing.

A degradation or complete interruption in availability of functions or services is the most commonly reported impact. A total of 129 cases, 64 percent, consist of the cyber attacks that affected the IT environment or information in it because something was added to the IT environment in connection with the attack, which contributed to an *obstacle arising*. These incidents include events where something has been added, or a change has been made, that has blocked functionality or availability to information within one or more information systems. Most of these cases have not arisen as a consequence of a breach of the IT environment and the attacks have rarely affected the internal environment. Instead, it is the external access to the affected organisation's IT environment or information in it that has been affected. Denial-of-service attacks, when large amounts of data traffic are transmitted and thereby block access to servers and other network components, constitute the majority of the cyber attacks that result in an obstacle arising. Another occurring, but comparatively unusual case, is when the malicious actor installed malware. By using e.g. ransomware, the malicious actor has then actively prevented access to information assets by placing a layer of encryption "on top" of them.

The second most common type of case is that the incident caused a *threat to arise*, which was reported in 26 percent (52 cases) of the 201 cases where the cyber attack affected the IT environment or information in it. This category includes incidents that primarily affected the information systems' confidentiality, integrity or a combination of both. Unlike when an obstacle has arisen, these incidents are usually due to a breach of the IT environment. These are primarily incidents where, for example, one of the organisation's user accounts is hijacked and starts sending out spam messages or malicious content is added to websites belonging to or used by the organisation. Only a few describe that malware, which itself constitutes a threat, has been installed. Examples of malware described in the incident reports are backdoors and spyware. Several of the cases where accounts have been hijacked have resulted in an obstacle arising in the next stage. A common example is when the organization's domain gets blacklisted after a hijacked account starts sending large volumes of spam content. In 19 percent of the cases where a threat arises, the organisation has chosen to implement emergency shutdowns of affected servers and information systems as part of the incident management process.

Only 3 percent describe the occurrence of a security event where a *success factor has ended.* In an additional 6 percent, the occurrence of the security event was deemed to be unknown as the course of events was not reported in more detail in the IT incident report received. This includes cases where the organisation has described an organisation impact but not described the nature of the IT incident in more detail.The cessation of a success factor means that information, including functions, were removed or otherwise ceased to work. In this context, these events mean that malicious actors have removed information or deactivated functions used by users or information systems. Most of the cases deemed to belong to this category describe that information on websites has been manipulated or deleted. The fact that very few IT incidents fit within this category shows that it is unusual for organisations to describe incidents in which information has been deleted. Instead, it is far more common, that malicious actors either block access to information or use their own established access to information for their own purposes.

None of the reports describe malicious actions that resulted in the *cessation of protection* in connection with the malicious actor's removal or manipulation of established safeguards within the IT environment. On the other hand, 14 reporters (7 percent) inform that a protection was removed *before* the attempted cyber attack was carried out in connection with changes made by an employee or a supplier. Thus, 7 percent of the cyber attacks affecting the IT environment or information in it were preceded by changes affecting the IT environment. This either enabled the course of events or contributed to the consequences being more extensive. Examples of changes made include firewalls and denial-of-service protection being reconfigured or sensitive IT components mistakenly being connected to the internet in connection with major changes.

The IT incident reports in which the reporter describes that changes may have resulted in the cyber attack affecting the IT environment or information therein often include more detailed descriptions of the course of events than average. MSB assesses that mistakes made during changes are in reality likely to be exploited by malicious actors to a larger extent than can be seen in the IT incident reporting. Secure change management is an important part of the work to prevent and manage cyber attacks.

Who discovered the cyber attack attempt?

In 58 percent of IT incident reports where the question could be answered, it is reported that the attempted cyber attack was first discovered by the organisation's own staff. In 25 percent of cases the attack was first discovered by the organisation's technical detection system. The fact that it is more common for the IT incident to be discovered by employees indicates that many organisations do not have the ability to detect attacks until the attack attempt has been noted by employees.[78]

Based on the analysis, only three cases are deemed to have caused more than one type of security event. In these cases, it is both that a threat arose and that an obstacle arose within the IT environment. This is a result of installed malware being executed and spreading.

78. These percentages are based on the questions about the IT incident's discovery that are included in the current report form for government agencies (introduced in October 2020) and the report form for OES/DSPs. The question was answered in 154 out of a total of 168 IT incident reports in which the reporter used the current report form (92 percent).

When an obstacle has arisen that affected the IT environment or information in it, the average incident usually lasts for about 47 hours. However, the standard deviation is high and the median time is instead about 11 hours. During the time period that the incident is ongoing, access to certain IT components or information assets is partially or completely blocked. The average time of discovery, i.e., the time between the IT incident arising until it was discovered, was about 3 hours (median time about 2 minutes) and the average handling time, i.e., the time between the start of handling and the end of the IT incident, is 43 hours (median time 9 hours).[79]

In comparison, the average reported incident resulting from a cyber attack caused by a threat arising within the IT environment was ongoing on average for more than 218 hours, meaning more than five times as long as an IT incident resulting from the emergence of an obstacle. It should be noted that the median is 169 hours and that a few cases are raising the average a little. The average detection time was 131 hours (median time 64 hours) and average handling time was 87 hours (median time 15 hours).[80]

The large time difference between incidents where an obstacle and a threat arise is partly due to the fact that it may take longer to identify the threat, such as malware, if it has not resulted in any visible impact. Especially if the malicious actor actively tries to avoid detection. By comparison, the aim of blocking access to information for users and information systems is often for the attack to be detected. The time difference can also generally be attributed to the use of different attack methods. When a threat is introduced within the IT environment, the organisation needs to manage it in order for the threat to cease. While this is generally also the case when an obstacle arises, the majority of them consist of denial-of-service attacks, the effect of which ends when the network traffic subsides.

The fact that the average time for IT incidents where a threat or obstacle arises exceeds several days is serious. This may indicate a lack of preparedness and ability to manage the situation in a short time. The longer the handling time, the higher the risk that the organisation or a third party will be affected by the incident.

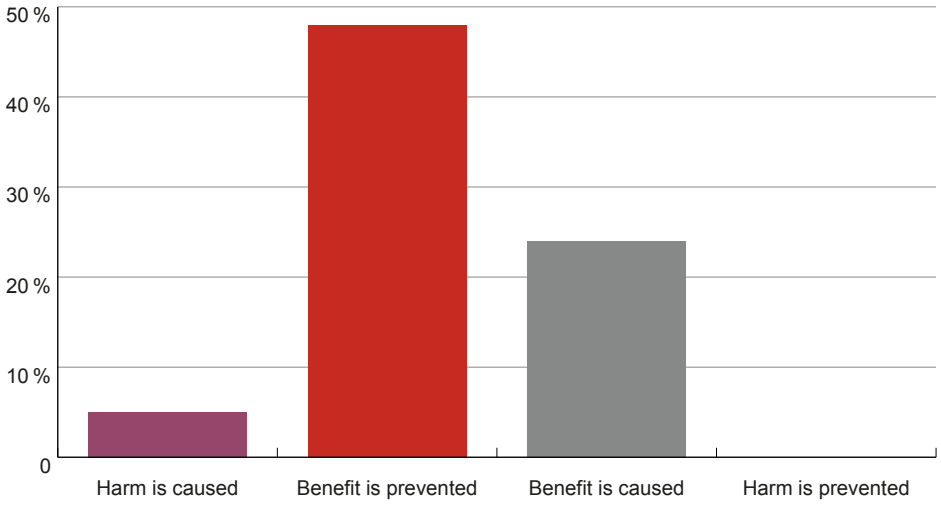
79. Time information is based on answered sub-questions about time included in the current report form for government agencies (introduced in October 2020) and the report form for OES/DSPs. A total of 168 attempted cyber attacks have been reported using these forms. The information is based on the incident reports in which the reporter has answered all the sub-questions about time in the report form. This includes time of incident, detection, disruption, initiated handling, the end of the incident and the end of the disruption. Reports in which the answer was incomplete have been excluded. As there is a high standard deviation, IT incidents that were ongoing for more than 1,000 hours were also excluded. The average and median of the category of obstacles arising is based on documentation from a total of 59 out of 103 IT incident reports that originate from the category in which the reporter used the current reporting form (57 percent).

80. Information for the average and median of the category threats arising is based on data from a total of ten of the 26 IT incident reports that originate from the category in which the reporter used the current reporting form (38 percent). The high drop-out is due, among other things, to the fact that many reporters do not know when the threat was introduced within the IT environment and thus cannot answer the question when the report was sent to MSB.

Organisation impact

66 percent (132 cases) of the incidents which has resulted impact on the IT environment has also had organisational impact. In cases where the IT incident resulted in an organisation impact, in addition to a security event, an *actual incident* has occured.[81] An actual incident may consist of benefit being prevented or harm being caused to the organisation or through the affected organisation, or that benefit was provided to or harm was prevented for the malicious actor. *Figure 5* below presents the percentages of each type of actual incident among reported cyber attacks with an organisation impact.

Figure 5. Actual incidents with an organisation impact



Horizontal bar chart describing the distribution of types of actual incidents. The diagram shows that *preventing benefit* is the most common actual incident that arises as a result of a cyber attack.

81. An event where the affected organisation is caused harm or prevented benefit, or where another organisation is unlawfully provided benefit or prevented harm (see Annex 1 for a more in-depth presentation).

The most common type of actual incident is that *benefit has been prevented* for the organisation or a third party. 48 percent of reported cyber attacks with impact have resulted in benefit being prevented (96 cases). Prevented benefit for an organisation is often a consequence of an obstacle arising (a security event) that affected the IT environment or information within it. In these cases, blocked functionality has led to the organisation or other stakeholders not being able to use services to their benefit. The most common scenario is that benefit was prevented in connection with the organisation's ability to communicate externally being negatively impacted. This includes cases where websites and related e-services as well as e-mail and VPN solutions became inaccessible to users over a prolonged period of time. In cases where the obstacle has affected a service or function that is time-critical, interruptions that have been ongoing for a very short time resulted in benefit being prevented. In several of these cases, benefit has been prevented for other organisations or the public as a consequence of the disruption.

The average disruption that occurred when benefit is prevented lasts for around 49 hours. However, the standard deviation is high and the median is equivalent to about 19 hours. During the period the disruption is ongoing, the affected service or information system is completely or partially inoperable periodically or constantly. The average detection time was 6 hours (median time 7 minutes) and the average handling time was about 45 hours (median time 9 hours).[82] That benefit is often prevented in connection with many cyber attacks shows that the organisations lack redundancy and indicates an obvious need to strengthen their own incident and continuity management.

82. Time information for averages and medians for the category of preventing benefit are based on data from a total of 41 of the 77 IT incident reports that originate from the category in which the reporter has used the current reporting form (53 percent).

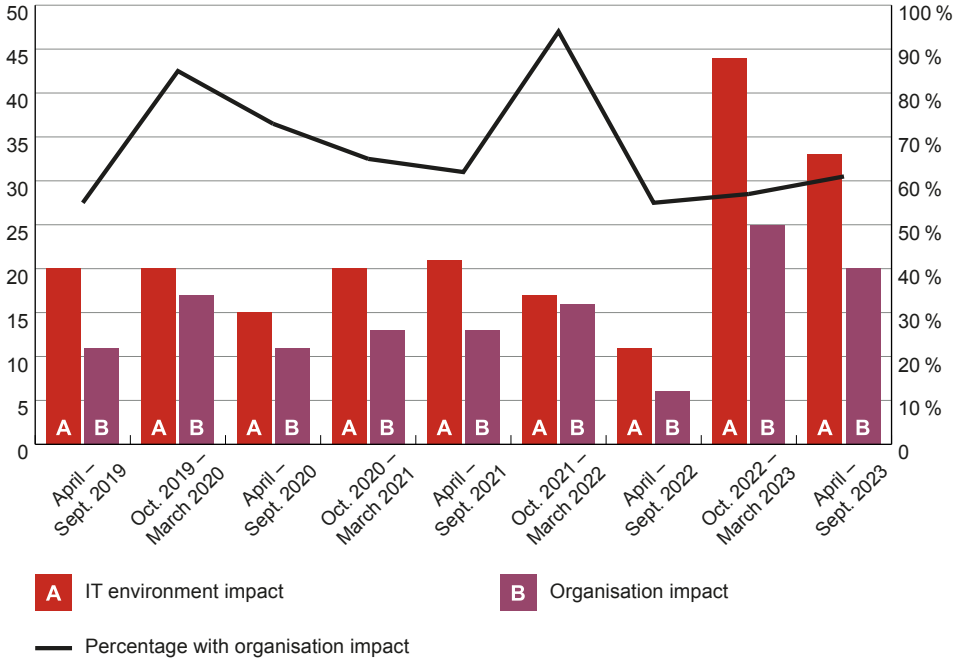
The second most common category, *benefit caused*, instead describes how the attack directly resulted in positive outcomes for the malicious actor, at the expense of the target or third party. The incidents resulting in benefit being provided to the malicious actor has occurred in 24 percent of the reported cyber attacks with impact (48 cases). This category primarily describes incidents where a malicious actor has managed to extract sensitive information from the organisation or managed to use the organisation's resources for their own purposes, for example by hijacking and using hijacked user accounts to spread spam or steal money. For example, one of the categorized reports describe how a malicious actor, following sucessfully hijacking an employee's account, changed the bank account to which the employee's salary should be paid. The fact that benefit is often provided in connection with user data and accounts being hijacked by malicious actors shows the importance of organisations working effectively with identity and access management in order to manage these risks.

Harm caused to the target or third parties has occurred in five percent of the reported cyber attacks with impact (ten cases). Harm being caused usually includes that the attack has had (significant) economic consequences. The incident reporters generally describe that a success factor ended in connection with the malicious actor deleting information and that the organisation was unable to restore the information lost. Unlike when benefit is prevented, it is unusual that harm is caused to the public or other organisations via the target of the attack.

In a total of 22 cases, the cyber attack is deemed to have caused impact that spans more than one category. In which case, the most common is that a malicious actor both provided benefit to himself, and prevented benefit for the organisation. This has been reported in 86 percent of these cases. These may, for example, involve cases where the malicious actor's spam mailings from hijacked accounts result in the organisation's domain being blacklisted or traffic to and from the organisation being otherwise blocked. Although the aim of the attack was not primarily to prevent benefit, it was nevertheless a consequence of the attack.

As shown in *Figure 6*, the percentage of cyber attacks that caused organisation impact has been relatively stable over time even though the number of reports received has increased in the past year. Around 60 percent of the reported attempted cyber attacks are deemed to have resulted in some form of organisation impact during the periods between April to September 2022 and April to September 2023.

Figure 6. Cyber attacks assessed to cause organisation impact during the period



Bar chart presenting the number of reported cyber attacks with IT environment impact and the IT incidents deemed to have resulted in organisation impact. The percentage of IT incidents resulting in organisation impact is presented separately.

Cyber attacks in digital supply chains

In MSB's report *Digital supply chains under threat*[83] from 2021, the agency describes the increasing dependence on complex digital supply chains as a phenomenon that increases the risk of extensive disruptions among organisations and society at large. Most reported supply chain incidents have been caused by system errors and mistakes, but a non-negligible number has also arisen as a result of cyber attacks.

Digital supply chains

A digital supply chain can be understood to be the services and infrastructures that deliver or enable the delivery of digital products used to establish, maintain, develop or restore an organisation's information management and information systems.

83. MSB, *Digital supply chains under threat: 50 recommendations to strengthen societal security* https://www.msb.se/sv/publikationer/digital-supply-chains-under-threat--50-recommendations-to-strengthen-societal-security/ (Downloaded 11/2023).

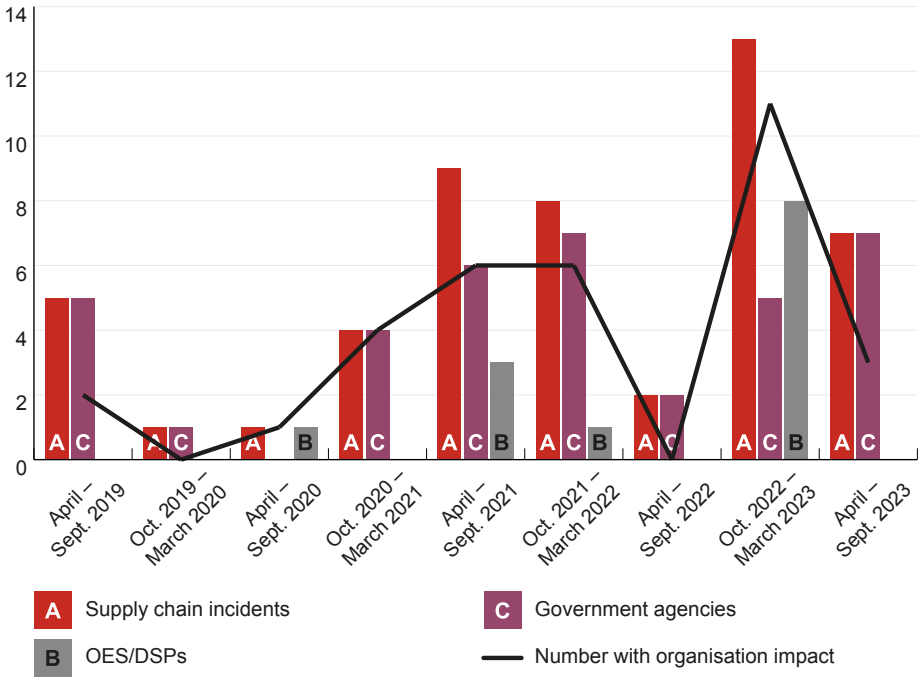
In 50 of the 250 attempted cyber attacks reported to MSB, a provider of the reporting organisation is reported to have been attacked. These may involve both providers of specific services or the organisation's IT operations. This means that supply chain incidents represent 20 percent of the total number of reported attempted cyber attacks. Supply chain incidents occur in more than 40 percent of the reports from OES/DSPs. The corresponding figure for government agencies is 17 percent. The difference could be due to the fact that OES/DSPs are more dependent on subcontractors or that they, to a greater extent, make use of the same suppliers. However, the distribution may also be a consequence of OES/DSPs primarily reporting IT incidents that caused major disruptions. This might indicate that supply chain incidents generally lead to more extensive disruptions. A small number of these reports refer to the same underlying provider and event.

44 of the supply chain incidents are deemed to have affected the IT environment of or information belonging to the reporting organisation and 33 are also deemed to have caused organisation impact. The most common thing is that benefit was prevented for reporting organisation in connection with the supplier's services experiencing disruptions or becoming completely unavailable. The supplier is often described as being subject to a denial-of-service attack, but there are also several cases where the service becomes unavailable in connection with a breach of the supplier's IT environment.

The organisations whose activities depend on services from a provider that is targeted by a cyber attack are at risk of suffering far-reaching consequences. On average, a disruption resulting from a cyber attack on a supplier lasts 18 hours. The median incident lasts for about 8 hours. The above time limits are based on a limited selection and thus relatively uncertain.[84] The fact that these incidents result in disruptions that have organisation impact and can last for a long time shows the importance of organisations reviewing their supplier relations and ensuring that redundancy and alternative working methods are available in the event of the failure of important services and other functions.

84. Time data for the average and median for the category of supply chain incidents are based on data from a total of 13 out of 44 IT incidents that originate from the category in which the reporter has used the current reporting form (30 percent). The high drop-out is assessed to be partly due to the fact that many reporting organisations have not received information about the scope of the IT incident from the affected operator at the time the report was sent to MSB.

Figure 7. Cyber attacks as a cause of supply chain incidents



Bar chart describing how many supply chain incidents were reported by government agencies and OES/DSPs between April 2019 and September 2023. The number of supply chain incidents with organisation impact per half-year is presented in a separate line.

Attack method: Denial-of-service attack

Denial-of-service attacks are an attack method used to prevent access to a service by, for example, overloading the service or the infrastructure on which the service is dependent. Such attacks can be carried out in several different ways, but most of the ones reported to MSB are "distributed denial-of-service" (DDoS) attacks.[85] DDoS attacks use, for example, botnets[86] to distribute and at the same time increase the amount of data traffic actively sent to affected IT components, blocking the access of legitimate traffic. The denial-of-service attacks reported by government agencies and OES/DSPs are often reported in a relatively large number over a limited period of time.

Because of a strong increase in the number of denial-of-service attacks since the beginning of 2023, these attacks constitute the most common attack method between April 2019 and September 2023. Denial-of-service attacks are often carried out in response to actions and events that the malicious actor, or the malicious actor's client, disapprove of or see a chance to exploit for his or her own purposes.

85. A DDoS attack, or Distributed denial-of-service attack, is a denial-of-service attack in which the malicious actor uses several different, often hijacked, units to send large amounts of data traffic to a server or other IT component in order to limit its ability to process legitimate incoming data traffic. The units that contribute to the attack are usually said to be part of a botnet.

86. The word botnet consists of the words "robot" and "network". Malicious actors use special Trojan viruses to break the security of several users' computers, take control of each computer and organise all the infected computers into a network of "bot" programs that the malicious actor can control remotely.

One telling example is the 50 denial-of-service attacks reported in connection with the "Quran burnings" in Sweden at the beginning of 2023.

Denial-of-service attacks in 2023

At the beginning of 2023, the number of denial-of-service attacks increased sharply. These attacks were announced in advance on social media as a reaction to a series of Koran burnings, the first of which was carried out on 21 January 2023.

For example, the group "Anonymous Sudan" wrote that Sweden and Swedish organisations would suffer retaliation for not preventing these happenings. The attacks were directed at both the public and private sectors. As is customary in cases of denial-of-service attacks, most had very limited impact. The events mostly received attention due to the reason for the attacks and the number of actors who were attacked.[87]

Throughout the period, a total of 105 IT incidents describing denial-of-service attacks as the underlying cause were reported. The attacks show great variation in execution techniques, volume and time span. Although denial-of-service attacks can render important services unavailable, the disruption usually lasts for a limited period of time. Even in cases where the attack lasts for a longer period of time, it is not usually a question of a constant outage, but rather of periods of longer response times interspersed with periods of a complete outage. When the attack has resulted in some kind of disruption, it is assessed to on average last for about 43 hours, off and on. Here, too, it should be noted that the median is nearly 11 hours and that a few cases bring up the average.[88] That the disruption persists over a longer period is believed to be due to the fact that more organisations restrict external access to the IT environment in order to avert the attack. The denial-of-service attacks comprise in some cases, several brief and recurring attacks, rather than an attack that is actively ongoing throughout the period described in the report.

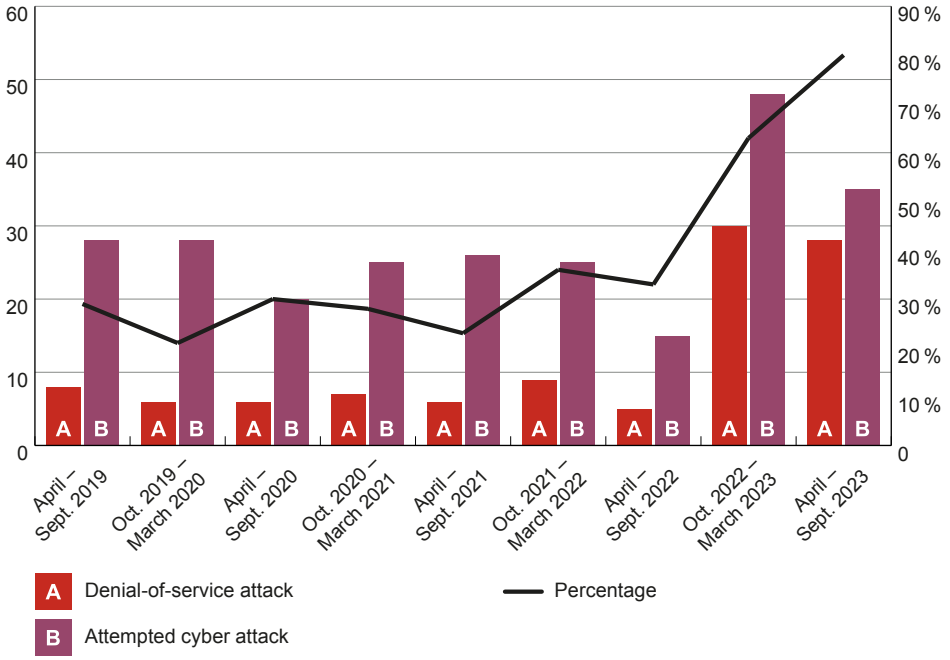
56 percent (59 cases) of all reported denial-of-service attacks are estimated to have caused that prevention of benefit in some way. In most cases, websites and associated e-services have become unavailable, or had long response times over a period of time. In 16 percent of the incident reports in question, the reporting organisation description of the incident suggests that an actual incident has not occurred, and the organisation has thus remained unaffected by the attack. In the remaining 27 percent, it is not possible to assess whether the IT incident results in organisation impact. When blocked functionality did not cause any organisation impact, it is usually because the organisation managed to compensate for the outage in a short time. It may also be that the outage did not result in benefit being prevented for the organisation, because it happened when users had no need for the service, for example on weekends or during the night.

87. Karin Lindström, *Fortsatta malicious actor mot svenska mål [Continued attacks on Swedish targets]*, 2023-02-20 https://computersweden.idg.se/ 2.2683/1.776492/overbelastningsmalicious actorna-fortsatter--expert-pekar-ut-ryska-killnet (Downloaded: 2023-10-28).

88. Time information for averages and medians for the category of denial-of-service attacks are based on data from a total of 58 of the 88 IT incident reports that originate from the category in which the reporter has used the current reporting form (66 percent).

Most denial-of-service attacks can be managed before they affect the IT environment of the target if the organisation has the right tools to do so. The fact that a majority of the denial-of-service attacks are, after all, deemed to result in disruptions that have an impact on the organisation shows that many organisations lack sufficient redundancy in their network infrastructure and technical solutions to both detect and avert denial-of-service attacks.

Figure 8. Reported denial-of-service attacks



Bar chart describing the number of denial-of-service attacks and the total number of attempted cyber attacks reported between 1 April 2019 and 30 September 2023. The denial-of-service attack percentage of the total number of cyber attacks reported during the period is reported in the line.

Attack method: Phishing

Phishing is the second most common method behind reported cyber attacks. This attack method is a form of social engineering where the victim is tricked into clicking on malicious links or other media, or is tricked into providing login information. Phishing can involve both mass mailings and targeted attacks designed to deceive a particular target group. During the period April 2019 to September 2023, a total of 45 cases of phishing were reported.[89]

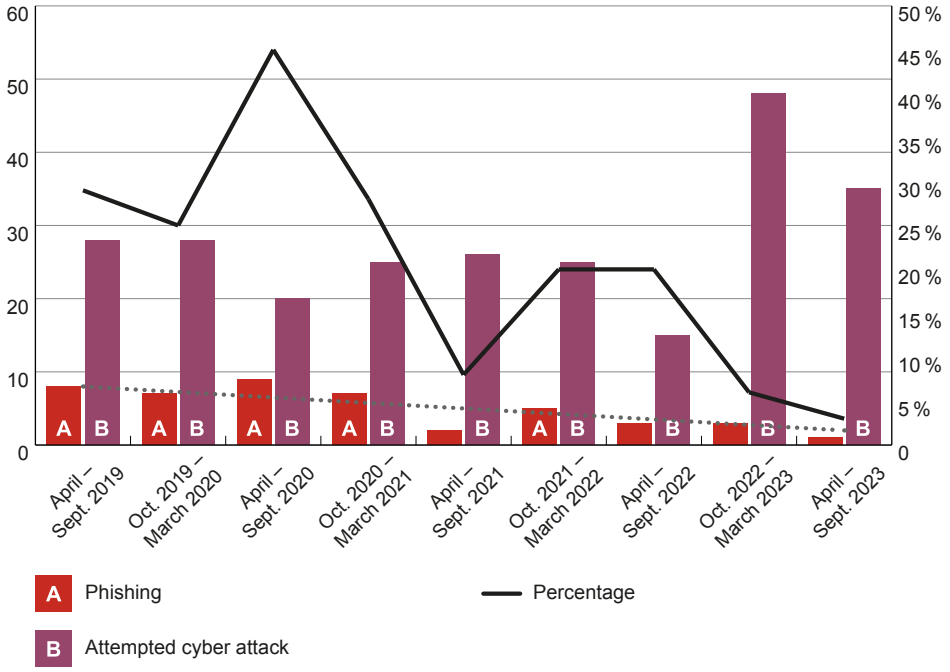
Phishing attempts reported to MSB often have either relatively limited consequences for the IT environment or they have completely failed. Only 44 percent of reported cases were assessed in this analysis to cause some form of organisation impact. The consequence of these cyber attacks is usually that a malicious actor gets access to user accounts and information of varying degrees of sensitivity.

89. Phishing is also a common component of many of the attacks excluded from the data set in this report because they do not meet the practice criterion described in the first chapter of this report. This includes e-mail fraud where malicious actors try to trick users into paying out a sum of money by spoofing e-mail addresses, for example.

However, in a limited number of cases, the attacks have led to availability disruptions in connection with malware being installed and spread within the organisation's IT environment. As previously mentioned, there are also cases where spam mailings from hijacked user accounts caused communication from the reporting organisation to be blocked.

The frequency of reported cases of phishing has decreased over time. This negative trend may be due to increased knowledge and caution among employees, but also to established safeguards becoming better at filtering out and isolating malicious content. Another explanation could be a decreasing tendency of government agencies, which account for the majority of reported phishing attempts, to report these events.

Figure 9. Reported phishing attempts



Bar chart describing the occurrence of phishing and the total number of reported attempted cyber attacks between 1 April 2019 and 30 September 2023. The phishing attempt percentage of the total number of attempted cyber attacks reported during the period is presented in a line.

Although phishing attempts are over-represented among attack attempts that fail, the fact that it remains the second most commonly observed attack method shows the importance of organisations taking measures both to prevent and manage the consequences of users' interactions with phishing messages.This includes both working to increase employees' knowledge of these methods and developing incident management processes aimed at limiting the consequences of a successful phishing attempt.

Challenges in security work

Challenges in security work

A systematic and risk-based cyber security work with planning, implementation, follow-up and practice of preventive security measures is important to protect against attempted cyber attacks. These security measures contribute to both increasing protection against IT incidents as a result of cyber attacks and minimising harm if the attack nevertheless occurs. This chapter presents some of the identified problem areas where organisations have challenges in their daily security work.

To be successful in the security work, working methods are required to continuously identify the organisation's security and improvement needs. There are many challenges and security work is often slow. For those organisations where the work is slow, it is particularly important to stop and review what can be done better.

In the work on this report, six specific problem areas have been identified that pose particular challenges for organisations regarding the work to strengthen protection against attempted cyber attacks. These areas are (I) systematic approaches in security work, (II) incident and continuity management, (III) identity and access management, (IV) employee knowledge, (V) change management and (VI) digital supply chains. There may be other relevant problem areas that should be addressed. However, this report focuses on the areas which have been deemed relevant based on challenges described in the IT incident reports or identified as important within other reports and studies conducted by MSB.

Systematic approaches in security work

In order to improve their resilience to cyber attacks, it is crucial that organisations have the basic conditions necessary to work systematically and risk-based with their information and cyber security.

Challenges

- Management commitment
- Lack of resources

A general challenge, where there is great potential for improvement, concerns the maintenance of the commitment to and a fundamental systematic approach in the security work. This requires strategic and long-term planning. There should be a security culture that is reflected in the organisation's ideas and

social behaviours where security thinking is in each employee's DNA. MSB sees that many organisations in public administration lack a management that gets involved in security issues.[90] When the management and managers of an organisation are involved in the security work, it is reflected in the employees' involvement.[91] Unfortunately, the opposite also applies, that is, if the management is less involved in security practices, the employees will imitate this risky behaviour.[92]

Resource shortages are another challenge in the prevention work for many organisations. [93] Resources are needed to find out what challenges the organisation has, to implement systematic and risk-based working methods, train and provide training to employees and to lead and coordinate the work. This also includes operating and managing the organisation's IT environment in a secure manner.

Management can promote a good security culture by setting clear goals and expectations for the security work. Furthermore, management should regularly communicate the importance of security, offer training and practice opportunities, encourage employees to report security events and improvement proposals, and lead by example by following the organisation's security procedures.

Incident and continuity management

In order to be able to manage IT incidents resulting from cyber attacks so that the impact on the organisation and its IT environment is minimised, working methods are needed for both incident and continuity management.

Challenges

- Handling cyber attacks early
- Good preparedness
  - Right competence
  - Common guidelines
  - Communication

In terms of the total number of attempted cyber attacks reported, 53 percent of the cases resulted in a disruption or other event that affected the organisation. The average disruption in connection with the prevention of benefit lasts about 49 hours. Time information for when obstacles and threats arise shows that organisations have difficulty handling the arising IT incident quickly and that in some cases (especially when a threat arises) it also takes a long time before the IT incident is discovered.[94]

90. MSB. *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen [The systematic information security efforts in public administration]*, Resultatredovisning Infosäkkollen [Results Report, Information Security Check] 2021. 2022. https://rib.msb.se/filer/pdf/30002.pdf (downloaded 09/2023).

91. See MSB's practice materials for *Övning – Informationssäkerhet för ledningen [Exercise – Information security for management]*, https://www.msb.se/sv/ publikationer/ovning--informationssakerhet-for-ledningen/.

92. Dhillon, Gurpreet. *Information Security: Text & Cases* (Second Edition). Burlington: Prospect Press, 2018.

93. MSB. *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen [The systematic information security efforts in public administration]*, Resultatredovisning Infosäkkollen [Results Report, Information Security Check] 2021. 2022. https://rib.msb.se/filer/pdf/30002.pdf (downloaded 09/2023).

94. The detection time is defined as the time between when the incident arises and its detection. The handling time is defined as the time between the start of the handling of the incident and the end of the incident.

This suggests that there is a need to strengthen the work on incident and continuity management at organisations.

Incident and continuity management

When a cyber attack is discovered, the organisation needs to handle it in accordance with its incident management procedures. This work includes documenting the incident, prioritising and assigning tasks to appropriate employees, and quickly finding solutions to minimise the consequences.

Continuity management is about ensuring that an organisation can continue its operations even in the occurence of unplanned events. The work includes identifying and managing risks in advance, documenting and planning to maintain its operations at a tolerable level no matter what disruption it is subjected to.

The challenges many organisations can face in their work on incident and continuity management include handling cyber attacks early on and having good preparedness. In order to have good preparedness, the right competence, common guidelines and well-functioning communication procedures are required both internally and externally.

Today, most attempted cyber attacks described in the IT incident reports are discovered and reported by employees[95]. Often, they are discovered in connection with a disruption, such as when the information systems have long response times or an information system completely ceases to work. This indicates that a cyber attack has not been handled before consequences have arisen. An explanation for this may be that organisations lack technical solutions to detect malware or breaches early on, for example. It may also be that the attack was discovered at an earlier stage but that those working on the handling of the attack do not have the right mandate or authority for the work to proceed quickly enough. Such mandates may include, for example, having the right to implement emergency measures such as an emergency shutdown in order to limit impact and avoid knock-on effects. Another explanation may be that there is a lack of effective working methods to report events out of the ordinary if employees suspect something is wrong, but are not absolutely certain.

The lack of good preparedness leads to a longer time to handle IT incidents resulting from a cyber attack and return to a normal situation. Preparations help to anticipate and manage the stress that a crisis can cause, whether it is cyber-related or not. In addition, stress and fatigue increase the risk of misunderstandings during an ongoing incident. In the first few hours, it is often difficult to know exactly what is happening, to determine causes of incidents, to identify the source or sources and to anticipate how the course of events will develop. The employees' ability to keep their cool, cooperate and quickly make the right decisions is based on them having practised. Employees who have practised can act faster to limit negative impact if an attack occurs.

95. See fact box *Who discovered the attempted cyber attack?* on page 52.

For good preparedness, organisations also need to have established working methods to preserve important assets, for example by taking backups and practising restoring them, and ensuring that there are continuity plans for alternative working methods if, for example, information systems that are normally used are unavailable.

Good preparedness also requires that the right competence is available at organisations. One of the challenges is that employees with the technical knowledge and experience needed to carry out the work needed in a cyber attack are not available.[96] This work may include, for example, analysing the attack, averting subsequent attacks or taking other steps to minimise further harm. Organisations that lack these resources themselves should consider agreeing with external parties specialising in the task, or making sure they have cyber insurance[97] that provides access to the right expertise and assistance in an incident.

A cyber attack often affects several parts of the organisation and may therefore need to be managed by employees who are not used to working together. In the event of an incident with a major impact on the organisation, the IT department may, for example, need to work closely with management, the communications, legal affairs and personnel departments and others concerned. If the groups practise together, a common terminology and working method can be developed not least for how the organisation communicates about the incident internally and externally so that the spread of rumours can be avoided. In the event of a cyber attack (or as a result of the actions the organisation is taking to respond to an ongoing cyber attack), the usual communication channels such as e-mail, internal chat and other tools may also stop working or otherwise be impacted, which makes both internal and external information dissemination more difficult.

The most common scenario in an attack is that benefit is prevented in connection with the organisation's ability to communicate externally being negatively impacted. This includes cases where websites and related e-services as well as e-mail and VPN solutions have become inaccessible to users over a prolonged period of time, or during a time-critical period when the organisation needed the service. Organisations need to have established plans for communication and information dissemination that can be used during an ongoing incident. These are important for employees as they provide information about how they should act and how to communicate externally.

96. Li, Yuchong; Liu, Qinghui. *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*. 2021. https://www.sciencedirect.com/science/article/pii/S2352484721007289 (downloaded 07/2023).

97. MSB advises against using cyber insurance instead of conducting systematic and risk-based information and cyber security work, but it can be a complement to such work.

Employee knowledge

In order to strengthen the resilience to attempted cyber attacks, it is important to regularly improve employees' knowledge of the different approaches used by antagonists.

Challenges

- Social engineering
- Use of weak, same and standard passwords
- Leaked passwords

The human factor is a challenge for the security work of every organisation. In the IT incident reporting to MSB, phishing and weak passwords are often used by the malicious actor to gain initial access to an organisation's information system. Similar observations have been made by the U.S. Cybersecurity and Infrastructure Security Agency (CISA).[98] Managing social engineering, the use of weak passwords, standard passwords, and leaked passwords constitute a special challenge for organisations.

Through various social engineering methods[99], employees can be tricked into carrying out actions that lead to a threat arising. For example, employees can be tricked into clicking on a link in their e-mail that leads to the installation of malware in the organisation's information system. The malware can be a wiperware or ransomware that in turn can lead to harm caused by the organisation's files being deleted or an obstacle arising if files or the information system is blocked. Today, malicious actors can use different tools to create increasingly convincing and complex variants of social engineering and it is difficult for employees to identify these threats.[100]

Both technical tools and training are needed to reduce the risks. Technical tools can to some extent be used against phishing by e-mail to filter out messages that contain malicious links or attachments. Training of employees can in turn contribute to an improved ability to identify social engineering or other techniques used.

In addition to phishing, weak passwords[101] are mentioned in the IT incident reports as the cause of how a malicious actor gains initial access to an organisation's information system. Weak passwords also make it easier for the malicious actor to consolidate their position and with lateral movement move deeper into the organisation's IT environment.[102] Furthermore, it is a problem if employees use the same password for several different services, if the standard password for

98. CISA (Cybersecurity and Infrastructure Security Agency, which is part of the Department of Homeland Security). *CISA Analysis: Fiscal Year 2022 Risk and Vulnerability Assessments*. 2023-06. https://www.cisa.gov/sites/default/files/2023-07/FY22-RVA-Analysis%20-%20Final_508c.pdf (downloaded 09/2023).

99. In IT security, social engineering are methods used by malicious actors to manipulate people into performing actions such as clicking on links, disclosing passwords or other confidential information.

100. CERT-SE wants to highlight this problem and has compiled proposed measures as well as general tips for everyone who handles e-mail, https://www.cert.se/2023/09/oka-motstandskraften-mot-bedraglig-e-post.

101. Weak passwords mean that a large part of the passwords can be guessed based on modified dictionaries or by trying a small number of very common passwords against a large number of account names.

102. Read more about this in the section *Execution of cyber attacks* in the chapter *Malicious cyber activity*.

an information system has not been changed or if the same password used at work is also used in various services that employees use privately. Organisations do not always have access to technical tools to detect the use of weak passwords or lack knowledge about how technology can be used to force employees to choose stronger passwords.

Stolen or leaked passwords can be posted by the malicious actors online so that they are either relatively freely available or can be purchased by other criminal actors. Organisations then need to have access to web services to identify if user information is available online and change passwords for those users whose data may be compromised. Two-factor authentication with some form of code generator can be advantageously used when logging in as a complement to name and password. Unfortunately, these solutions also have shortcomings because phones can be compromised, SIM cards copied and signals intercepted. The human factor also plays a role here as users can be tricked into giving up their names, passwords and one-time codes. With the help of a physical security key that replaces SMS codes and mobile apps for two-factor authentication, a greater level of security can be achieved.

Identity and access management

In order to ensure that only authorised users have access to the organisation's information system, working methods for identity and access management are needed.

Challenges

- A high level of activity means that the security work does not keep up.

The IT incident reports show that it is common for user accounts to be hijacked and then used to, e.g., send out spam messages or malicious content. One example describes that the malicious actor, after hijacking a user account, changed the bank account that the employee's salary is to be deposited into. In the IT incident reporting, attempted cyber attacks are also presented where a malicious actor systematically tests different login data against different services. Although these usually constitute failed intrusion attempts, malicious actors sometimes manage to get in. In addition, the reports show that security events occur in organisations that lead to vulnerabilities arising when, for example, unauthorised personnel are given access to information systems or file areas, or through legacy user accounts not being deactivated and then used for malicious purposes.[103]

103. See the section *Cyber attacks with impact*, in the chapter *Cyber threat landscape*.

Identity and access management

Identity and access management means that organisations work to ensure that only authorised users and information systems have access to the IT environment and design their identity and access management in such a way that every digital identity has no more access to information and information systems than it needs.

One potential explanation for some of these challenges could be that many organisations have relatively high personnel turnover, and continuous changes in their operations, which in turn could make it more difficult for organisations to prevent access-related IT incidents. There are many elements in the everyday activities that directly or indirectly affect identity and access management. It can be difficult in practice to ensure that only those who should have rights have them, and that they only have the rights they should have, when they should have them. Examples of aspects that challenge identity and access management are the introduction of new information systems, changes in and the phase-out of information systems, new hires, staff transfers within the organisation and termination of employment, and the handling of temporary staff or consultants.

An indication that the organisation works with identity and access management in an unsatisfactory manner may, for example, be that the organisation lacks established control of and documented working methods for the management of permissions. For example, deficiencies can be seen in the absence of logging and traceability, or that permissions remain long after an employee has quit.

Overall important steps in the work with permissions are the review and collection of all permissions from different information systems, which in itself can pose a challenge as permissions and operating processes can be changed in the course of the work. The next step is to create user groups based on roles, which have different tasks, in the information systems. Finally, decisions must be made as to what permission should be given to employees, consultants and whether these permissions are based on departmental or unit affiliations, and whether specific roles are needed. Then, documented working methods are needed to regularly review all the permissions.

An automated identity and access management can facilitate the planning and verification of the users' permissions and also make it possible to adjust the permissions in relation to the changing needs of the organisation. With automated permission analysis, discrepancies can also be flagged and it makes it easier for different parts of the organisation to approve or reject permission changes.

Change management

In order to be able to implement changes in information systems without introducing new vulnerabilities, working methods are required for change management.

Challenges

- Lack of competence
- Compatibility problems
- Time of restart
- Compromised update
- Functional test environment

Over time, IT incident reporting has shown that secure change management in information systems is a recurring problem area for many organisations.[104] In the IT incident reporting, it is noted that seven percent of the attack attempts that affected the organisation's IT environment took place in connection with or after a change was made in an information system[105]. An example of the change management having deficiencies may be that a firewall is deactivated in an update whereby a vulnerability arises that is exploited by a malicious actor.

Change management

Change management is a systematic and structured method and process that aims to enable changes in an organisation's objectives, processes or technologies in an effective, controlled and risk-minimised manner. Change management involves preparation for changes, implementation of changes and support for adaptation after changes have been implemented. Changes can be implemented as a result of new needs, requirements or objectives.

A change in an information system can also lead to the occurrence of a threat[106] arising. This can occur, for example, if an employee connects a hard drive to the internet during work on an update or by mistakenly making a file area containing sensitive information available via the internet.

Preventing change-related IT incidents can be made more difficult by, for example, competence deficiencies, compatibility problems, that the time for rebooting exceeds what the organisation can accept, possibly compromised updates and the lack of a sufficiently production-like functional test environment.

104. MSB, *Threats and Opportunities in Change Management*, https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/ (downloaded 07/2023).

105. The section on *Cyber attacks with impact*, in the chapter *Cyber threat landscape*. The percentage may seem small, but is partly attributable to the fact that only a limited number of the reports have detailed descriptions of what has happened. Excluding those reports that have incomplete or unclear descriptions, the percentage where this is a problem increases significantly.

106. In other words, a vulnerability arises. See *Annex 1* for more details on how basic concepts can be understood.

Several of the most high-profile attacks in recent years have been based on the fact that known vulnerabilities have been exploited. There have often been available updates or other change options available to provide the necessary protection, but the changes have not been made in a timely or correct manner.[107]

Operations-critical information systems that are exposed to the internet must always be updated when new vulnerabilities are discovered. However, it is common for organisations to have built and arranged their information systems so that there are major challenges and uncertainties in making changes. For example, specialist expertise may be needed to make a change in a secure manner, which may be unavailable. There may also be a risk that the change will cause compatibility problems with other information systems. The fear that the change will take too long or that the information system will not be able to be rebooted after the change may also be reasons why many people wait to make changes, including those that provide direct protection against a vulnerability. There may also be a perceived risk that an update will entail new vulnerabilities if, for example, it has been compromised.

Organisations may also lack working methods to ensure that software updates come from a reliable supplier. Such working methods may include, for example, that updates are received on a special server and that the supplier protects its files against manipulation using signing. Access to a test environment, which as far as possible mimics the production environment, where updates can be tested before they are introduced into the production environment, is a way of discovering and circumventing some of the challenges of change management. However, it can be a challenge in itself to successfully establish a functional test environment because the IT environment of organisations is often complex and changing.

Leaving known vulnerabilities unresolved may increase the likelihood that an attack attempt results in an IT incident. This is particularly true if the information system is connected to the internet. If the organisation is also part of a digital supply chain, the risk increases of more organisations or society being affected when an incident occurs. Regular analyses of risks in the IT environment of organisations that also include suppliers and their subcontractors are therefore important. The same applies to horizon scanning to access information on new vulnerabilities, newly developed safeguards, security updates, general guidelines and recommendations to increase resilience by, for example, reading weekly newsletters from CERT-SE[108]. MSB's report *Threats and opportunities in change management*[109] describes the importance of having functioning working methods for change management and recommendations for more secure changes in information systems.

---

107. MSB, *Threats and Opportunities in Change Management*, https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/ (downloaded 07/2023).

108. CERT-SE stands for Computer Emergency Response Team – Sweden. It is Sweden's national Computer Security Incident Response Team (CSIRT) tasked with supporting Swedish society in the work of managing and preventing cyber security incidents, https://www.cert.se/.

109. MSB. *Threats and opportunities in change management: 20 recommendations for improving information security during changes.* 2022. https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/ (downloaded 06/2023).

Digital supply chains

Security in digital supply chains is important because IT incidents resulting from cyber attacks can have an impact not only on the organisation that is affected, but also other organisations that are part of the same supply chain.

Challenges

- Information on IT incidents
- Complex supply chains
- Monodependencies

20 percent of the total number of reported attempted cyber attacks are supply chain incidents. Organisations whose activities depend on services from a provider that suffers from a cyber attack are at risk of having far-reaching consequences. The IT incident reports show that a disruption resulting from a cyber attack on a provider lasts for 18 hours on average. The median case lasts for about eight hours and here too, there are a few incidents that are driving up the average. However, the above time information is based on a limited selection. The fact that these incidents result in disruptions that have an organisation impact and can last for a long time indicates that organisations have challenges in the work with digital supply chains.[110]

What can be a challenge that prevents organisations from succeeding in controlling the security of their digital supply chains includes the lack of information about occurred IT incidents from suppliers, complex supply chains and monodependencies.

The fact that organisations do not receive information about IT incidents that are ongoing or have occurred at a supplier makes it difficult for them to know how to act or what security measures need to be taken. It also makes it difficult or impossible for them to further convey information about the incident to their customers. Incomplete information can in turn lead to speculation and the spread of rumours with impact and other consequences that could have been stopped.[111] In order to avoid this, clear clauses on the suppliers' obligation to provide information about IT incidents that in any way affected or is affecting their organisation should be included in agreements. The organisations must be able to require that they are informed during the time the supplier is under attack in order to make informed decisions.[112] In addition to the time when the service is expected to work again, it is important to know if it is suspected that the organisation's information is accessible to unauthorised personnel or otherwise compromised.

110. For more information, see the section *Cyber attacks in digital supply chains* in the chapter *Cyber threat landscape*.

111. The fact that organisations do not receive information from their suppliers also means that the incident reports to MSB lack important information. This information is central to being able to inform other organisations that could take preventive measures, for future analyses and for planning the cyber security work of organisations and the whole of Sweden.

112. The obligation to provide information must apply even if it is not the supplier itself has the incident, i.e., if the supplier itself has suffered a supply chain incident.

A particularly difficult challenge arises when many organisations have a strong need to use a service provided through a digital supply chain, and there is only one, or a few, providers of such a service, i.e., when there is a *monodependency*. A monodependency risk means that an organisation depends on one provider's service and if there are no alternative services, the organisation will be vulnerable if the service ceases or becomes unavailable. In preventive work, plans for alternative solutions are important, as are plans and working methods for how the organisation should act and coordinate with the supplier if an IT incident occurs.

Cloud Hopper – a sophisticated supply chain attack

- **Type:** Phishing and malware
- **Actual incident:** Benefit caused

On Wednesday, 5 April 2017, the companies PwC and BAE, as well as the British National Cyber Security Centre (NCSC-UK) revealed a worldwide cyber attack believed to have been ongoing for months, perhaps even years.[113] The attack was alleged to be part of extensive government-funded cyber espionage where Sweden was one of the 15 affected countries.[114] The high-profile attack was aimed at companies that manage IT services, in this case cloud services in the form of data storage space and server capacity, for other companies, organisations and authorities. The attack therefore came to be called Cloud Hopper.

By attacking the weakest link in the supply chain, the attackers were able to effectively access sensitive information stored by actors in the public sector, IT, communication, energy and research.[115] Several Swedish companies and organisations were affected by the attack. Exactly how many actors had their sensitive information stolen is unclear.

The attackers behind Cloud Hopper entered the targets' subcontractors through phishing. By carefully tracking IT service providers and their staff, such as through social media, the attackers were able to tailor e-mails targeting employees. When an employee opened the e-mail, malware was installed that enabled an attacker to access the servers where data related to the IT service provider's customers were stored. Once the attacker had penetrated the information system, the attacker could move discreetly, which is why the intrusion was able to continue secretly for so long. It is unclear how much information the attackers managed to collect, altough if it is probably a very large amount.[116]

113. Sallinen, Jani. *Så angrep Kina "naiva" Sverige i det fördolda [How China surreptitiously attacked "naïve" Sweden]*. Svenska Dagbladet. 2018-04-21. https://www.svd.se/a/xRbQdQ/sa-angrep-kina-naiva-sverige-i-det-fordolda (downloaded 9/2023).

114. SVT. *Stor internationell cyberattack avslöjad – Sverige drabbat [Major international cyberattack revealed – Sweden hit]*. 2017-04-05. https://www.svt.se/nyheter/inrikes/stor-internationell-cyberattack-avslojad-sverige-drabbat (downloaded 9/2023).

115. Sentor. *Cloud Hopper – en supply chain-attack som gav eko [Cloud Hopper – a supply chain attack that resounded]*. 2021-03-29. https://www.sentor.se/artikel/cloud-hopper-en-supply-chain-attack-som-gav-eko/#Vilka%20utsattes%20f%C3%83%C2%B6r%20Cloud%20Hopper (downloaded 9/2023).

116. SVT. *Stor internationell cyberattack avslöjad – Sverige drabbat [Major international cyberattack revealed – Sweden hit]*. 2017-04-05. https://www.svt.se/nyheter/inrikes/stor-internationell-cyberattack-avslojad-sverige-drabbat (downloaded 9/2023).

Future outlook

Future outlook

The deteriorated security situation combined with an increasingly rapid technological development may change the cyber threat landscape against Swedish organisations. The future outlook addresses some of the factors that may affect the occurrence, as well as the effect, of future attempted cyber attacks. The chapter concludes with a brief account of how future EU regulations and initiatives in the cyber area will affect organisations' work on malicious cyber threats in the future.

Several government agencies assess that the security situation has deteriorated in recent years.[117] This of course does not automatically mean that more cyber attacks attempts will be conducted in the short term, but it may affect the malicious actor's incentive to carry out different forms of attacks in an unfavourable direction. Uncertainty, distrust and conflict, both internal and external, can contribute to an increased interest among malicious actors in using cyber attacks. When cyber attacks are deemed to be an effective tool for achieving strategic goals, the activity can increase and the methods become increasingly sophisticated.

One factor that could contribute to the long-term worsening of the cyber threat landscape is the increasing spread of disinformation and a negative image of Sweden on increasingly fragmented social media platforms. The Swedish Psychological Defence Agency shows how the amount of disinformation directed at Sweden and Swedish organisations has increased in the past year.[118] With increased disinformation or a changed image of Sweden, the incentives to carry out attacks on Swedish organisations and essential services could increase. The denial-of-service attacks that were carried out in the aftermath of the "Quran burnings" in the first half of 2023 exemplify consequences due to the impact on the perception of Sweden abroad.[119] It is therefore justified for organisations to conduct horizon scanning and pay particular attention to increased disinformation or a changed image of Sweden.

---

117. Swedish Security Service. *Cyberangrepp ständigt pågående hot mot Sverige [Cyber attacks a constantly ongoing threat against Sweden]*. 2022-03-11. https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2022-03-11-cyberangrepp-standigt-pagaende-hot-mot-sverige.html (downloaded 06/2023).

118. Swedish Psychological Defence Agency (MPF). Ökad *spridning av desinformation riktas mot Sverige [Increased disinformation is being directed at Sweden]* https://www.mpf.se/2023/08/18/okad-spridning-av-desinformation-riktas-mot-sverige/ (downloaded 12/2023).

119. Svenska Institutet (SI). *Koranbränningen 2023 [Burning of the Koran in 2023]*, https://si.se/koranbranningen-2023/ (downloaded 12/2023).

In a troubled world, the likelihood of disruptions in digital supply chains occurring and becoming long-lasting increases. Accordingly, even cyber attacks on actors outside Sweden can have serious consequences for Swedish organisations. Organisations should assess the risk that the digital supply chains they depend on suffer from long-term disruptions or other problems.

Technical development

Artificial intelligence (AI), the Internet of Things (IoT) and quantum computing[120] are some areas of technology where there have been major advances in recent years and where development is likely to accelerate further. How innovations in these areas will affect the cyber threat landscape against Swedish organisations depends in part on how and to what extent they will be integrated into organisations' activities. If organisations hastily make themselves dependent on, for example, new IoT or AI solutions that at a later stage prove to have critical vulnerabilities, it can be exploited by malicious actors. In addition, the cyber threat landscape could be influenced by the extent to which the malicious actor will be able to use these technologies to carry out attacks, especially against older information systems. In connection with major technology shifts, problems may arise if older solutions that are still used by many organisations no longer meet the desired level of security.

In the past year, there has been a great deal of speculation about AI's positive future role in society as well as the security risks AI may entail. AI can be used to streamline and further develop cyber attack methods, for example, "generative AI" can be used to construct more sophisticated phishing messages. Malicious actors can also use AI to figure out user passwords, perform automated vulnerability scanning and customisable development of malware.[121] Conversely, organisations can use AI to increase their protection against attacks or harm mitigation. With the help of AI, it is easier to identify patterns of cyber attacks against critical infrastructure and network activity, and to discover malware in real time. This information will make it easier to identify and understand risks.

EU regulations

In November 2022, the European Commission adopted the proposal for a revision of the NIS Directive, known as the NIS 2 Directive. In short, the directive aims to increase the level of harmonisation between Member States in order to increase cyber security throughout the Union, but also to reduce the burden on organisations operating in several countries.[122] The directive provides for minimum requirements for security measures, increased and more specified reporting obligations and the establishment of a European vulnerability register.

120. Quantum computing is a computer science area based on the principle of quantum physics (the study of how atomic particles exist and interact with each other). It explains the behaviour of matter and energy on atomic and subatomic levels.

121. Islam, Rabiul. *AI And Cybercrime Unleash A New Era Of Menacing Threats*. Forbes. 2023-06-23. https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/ (downloaded 06/2023).

122. European Commission. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (downloaded 06/2023).

In parallel with the NIS 2 Directive, the CER Directive (Critical Entities Resilience)[123] will also be introduced, which imposes requirements on measures to strengthen the resilience of certain essential services. This directive interacts and complements the NIS 2 Directive (which focuses on networks and information systems) to address the ability of entities to prevent, protect against, react to, manage and recover from hybrid attacks, natural disasters, terrorist threats and public health situations.[124] Both Directives aim to raise the demands on organisations and thereby make society more resilient to IT incidents.

One legislative proposal that may have a major impact within the EU is the AI Regulation. The EU's AI Regulation aims to ensure that AI systems used in the EU are secure, transparent, traceable, non-discriminatory and environmentally friendly. In order to prevent malicious effects, AI systems should also be supervised by people to help ensure that the systems are used in an ethically responsible manner. The drafting of the law itself is currently being negotiated between the EU countries with the goal of reaching an agreement by the end of 2023.[125] It remains to be seen how the final law will be worded.

The EU Cyber Solidarity Initiative is a further proposal for new regulatory frameworks aimed at strengthening cyber security in the EU. The initiative consists of three parts: The establishment of a Cybersecurity Skills Academy, changes to the EU Cyber Security Act and a proposal for a Cyber Solidarity Act. The Cyber Solidarity Act, in turn, consists of three parts: the European cyber shield (a network of SOC or CERT-like organisations working to monitor the cyber environment and detect malicious cyber threats), the European cyber emergency mechanism (a structure with "cyber response teams" that can be deployed to manage large-scale cyber incidents) and an evaluation mechanism (a kind of IT accident investigation commission that will evaluate large-scale cyber incidents after they have occurred, in order to secure lessons learned and enhanced preventive work).

As previously mentioned, the deteriorating security situation and rapid technological developments may affect the cyber threat landscape against Swedish organisations. However, by constructively implementing the upcoming regulations and continuing to work systematically and risk-based with information and cyber security, from an all-hazards approach, we are better equipped.

123. The Official Journal of the European Union. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC*. 2022-12-27 https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32022L2557&from=SV (downloaded 06/2023).

124. The Council of the European Union. *EU resilience: Council adopts a directive to strengthen the resilience of critical entities*. 2022-12-08. https://www.consilium.europa.eu/en/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/ (downloaded 06/2023).

125. The European Parliament. *EU AI Act: first regulation on artificial intelligence*. 2023-06-14. https://www.europarl.europa.eu/news/sv/headlines/society/20230601STO93804/eu-s-ai-akt-forsta-forordningen-om-artificiell-intelligens (downloaded 06/2023).

Annex 1

Annex 1: Framework for analysis of IT incidents

In order for the reader to be able to follow how MSB's work on this report has generally analysed threats, vulnerabilities, risks and IT incidents that enabled or arose in connection with malicious activity, this chapter presents the framework used by the authority. The framework can also be used by organisations that wish to systematise their own analysis of incidents.

The appendix is divided into four parts:

- **Basic concepts:** The twelve concepts below provide a starting point for the majority of the analyses carried out in the strategic analysis in the area of information and cyber security at MSB.
- **Security events and actual incidents:** Based on the basic concepts and some additional concepts, a taxonomy for incidents is defined divided into two types: security events and actual incidents. This taxonomy, together with that presented in the following section, has formed the basis for classifying the course of events described in the IT incident reports analysed in the work on this in-depth report.
- **Causal chains of events in complex information systems:** Taken together, several events may have created the conditions for an incident to arise. Similarly, contextual factors will influence the incident's consequences. The concepts of *mechanisms, components* and *triggers* constitute a taxonomy for classifying the elements of the incident and thereby facilitate the understanding of the causal course of the incident. This taxonomy, together with the taxonomy in the previous section, constitutes the basis for the classification of the reported incidents that have occurred in the context of the work on this report.
- **Application of the concepts to IT incidents caused by cyber attacks:** This shows how the basic concepts, the taxonomy for classification of incidents in security events and actual incidents, as well as the taxonomy for classifying events based on causal processes, can be used for analysis of incidents caused by cyber attacks.

Basic concepts

The analysis is based on a rigorous application of the following concepts:

Table 2. Basic concepts

Concepts	Explanation
Incident	An undesirable event that has occurred.
Success	A desired event that has occurred.
Threat	Something that causes, or contributes to, an incident.
Obstacle	Something that prevents, or helps prevent, a success.
Success factor	Something that leads to, or contributes to, a success.
Protection	Something that prevents, or helps prevent, an incident.
Risk	A possible undesirable event.[126]
Chance	A possible desired event.
Vulnerability	The lack of something that prevents, or helps prevent, an incident.
Deficiency	The absence of something that causes, or contributes to causing, a success.
Opportunity	Absence of something that prevents, or contributes to preventing, a success.
Freedom	Absence of something that causes, or contributes to causing, an incident.

Security events and actual incidents

In order to better account for the impact of IT incidents, this report makes a distinction between incidents that can be described as *security events* and incidents that can be described as *actual incidents*. A security event can be understood as an event where something ceases or arises that potentially affects the organisation's IT environment negatively. A security event does not have to result in any harm actually occurring, or any benefit actually being prevented. Organisations that have redundant systems and functioning protection can suffer from security events without actual incidents occurring.

An actual incident can in turn be understood as an incident where a security event has occurred without compensating redundancy or appropriate protection being in place, so harm arises or benefit is prevented for the organisation. While the concept of a security event thus refers to events that affect the security of an information system, an actual incident describes an event that directly or indirectly disadvantaged the own organisation. In this report, the concept of *organisation impact* has also been used to describe this phenomenon. Both security events and actual incidents are examples of incidents, but an actual incident cannot occur if a security event has not occurred.

126. It is common for risk to be defined, or expressed, in terms of consequence and probability. In this nomenclature, a risk (i.e., a possible undesirable event) can be *assessed* in terms of the consequences it would entail if it occurred, as well as the probability of it occurring.

There are four types of security events (defined using the basic concepts presented in the previous section) and four types of actual incidents. They are:

- **Threats arise:** something is introduced to the IT environment that causes, or contributes to cause, an incident to occur. Examples of this could be that ransomware is installed in the information system, or that a file area containing sensitive information is established and made freely accessible from the internet.
- **Protection ceases/vulnerability arises:** something is removed from the IT environment that previously prevented or contributed to preventing an incident from occurring (especially if no other protection is introduced that can block the threats that are otherwise no longer blocked). Examples of this could be that a firewall is deactivated or that one fails to add requirements for login when making a file area with sensitive information accessible to the internet.
- **Success factors cease/deficiencies arise:** something in the IT environment ceases that previously caused or contributed to causing a success (especially if no other success factor is introduced that causes the successes that are otherwise no longer caused). For example, a router loses the ability to channel traffic, or a hard drive breaks down and data that is on it can no longer be accessed.
- **Obstacles arise:** Something is introduced to the IT environment that prevents, or helps prevent, a success from arising. Examples may include the addition of a fire-wall rule that causes legitimate traffic to be blocked, or that an antivirus software incorrectly stops attempts to open non-malicious files.

Actual incidents in turn include events when:

- **Harm caused:** Harm is caused to the organisation, or to others, in a way that is not in the organisation's interest. Examples of such harm may be that components in an IT environment are harmed, or that costs arise.
- **Harm prevented:** Harm is prevented for other organisations or actors at the expense of the organisation. Examples of such harm may include that defence systems (in military contexts) cannot be fired, or that information that may be harmful to someone cannot be published (e.g. that a media report on wrongdoing cannot be published).
- **Benefit prevented:** Benefit is prevented for the organisation, or for others, in a way that is not in the organisation's interest. Examples of such benefit may be that services provided by the organisation become unavailable, whereupon the organisation cannot be paid and the organisation's customers cannot use the service, or that a flow (such as data, electricity or cooling) that the organisation is to deliver to other organisations is interrupted.
- **Benefit caused:** Benefit is caused to other organisations or actors at the expense of the organisation. Examples of such benefit may be that business secrets are sent out or provided to competitors, or that the organisation's electricity and the processing power and memory capacity of the information systems are used for crypto-hijacking and thereby to illicitly generate profits for someone else.

Of central importance in the model is that all incidents are security events, but not all incidents are actual incidents. On the other hand, all actual incidents are also security incidents. Here are some examples that illustrate this:

- **Benefit need not be prevented simply because an obstacle arises or because a success factor ceases:** If an organisation has redundancy for the components of its information systems, a blocked or broken component of an information system does not have to mean that there are no longer any components that fulfil that function in the information system at all. For example, if a hard drive breaks down or is blocked, information can continue to be stored if there are other hard drives with unused space available. If, however, information can no longer be stored (benefit prevented) it will be because the organisation's storage media is full or broken (success factor ceases) or blocked (obstacles arise).
- **Harm does not need to be caused just because a threat arises or because a protection ceases:** If an organisation has protection in its information systems, the introduction of a threat into the information system does not have to mean that the threat causes an incident – the protection may block the threat. If an organisation has a protection in an information system (a firewall, for example) and that protection ceases, it does not necessarily mean that there is a threat in the information system that causes an incident. If, however, a component is destroyed and must be replaced (harm is caused) then at the same time it will be that that component fulfilled some kind of desirable function (which is why a success factor ceases) or constituted a protection (which is why a protection ceases).

Causal chains of events in complex information systems

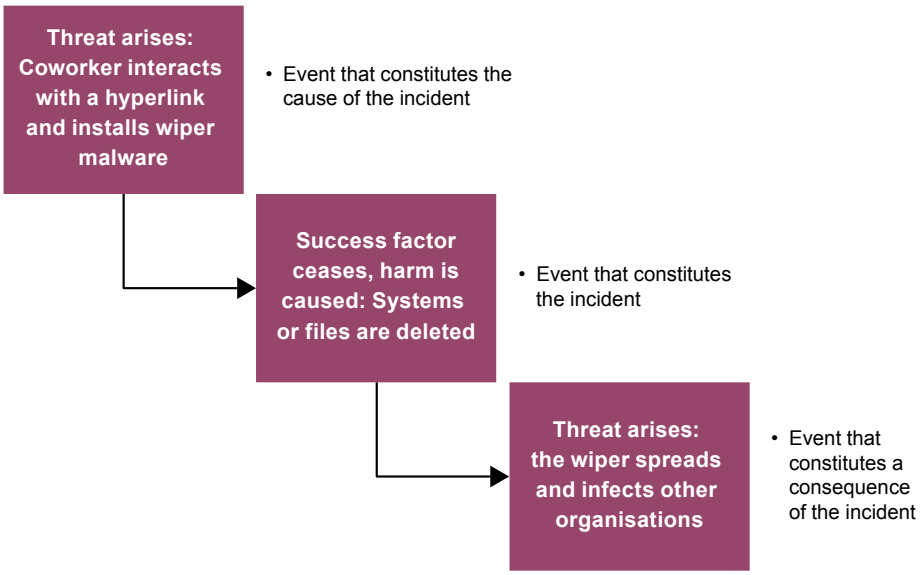
In complex information systems, events that occur are the result of several factors working together and interacting in different, sometimes unpredictable, ways. An output from an information system does not arise simply by adding an input to the system. Before the input can be made, the information system needs to be arranged in a certain way, and have some built-in elements. For example, the information system needs to have a memory, a processor, an operating system and an algorithm that can take the input and, based on it, perform a number of instructions that result in something new, which then becomes the output. The information system's respective parts, the electricity it is powered by and the algorithm it contains all constitute *components* of a *mechanism*. The application of a specific input to the mechanism is the *trigger* that, together with the components of the mechanism, causes a specific output to be produced. If a purpose of the information system is to be able to generate a certain type of output and there is no memory in the information system, or if the algorithm needed to generate the requested output is missing in the information system, then the mechanism is *incomplete* in relation to that purpose.

Threats, obstacles, success factors and protection can all constitute mechanisms or be components of mechanisms. The occurrence or termination of an IT incident can contribute to changes in the IT environment that in turn can contribute to

instability and increased risk during different stages of a causal chain. The event that a mechanism or component arises may constitute (1) a cause, a trigger, for an incident within an information system to arise, but it may also constitute (2) the incident itself as a result of a triggered trigger or (3) a consequence of the incident. Upon closer examination of the course of events linked to an IT incident, it is important to be able to distinguish security events from each other in order to identify how components and mechanisms interacted and thus why it resulted in an overall negative outcome.

Applications of the concepts to IT incidents caused by cyber attacks

In this report, the IT incident that arose as a result of a cyber attack is in focus and hence the security event/s and actual incidents that the attacks resulted in. However, in order to understand how the incident arose and what consequences it will have, it is important to also investigate the entire course of events. For example, when a malicious actor sends large amounts of data traffic towards an organisation's IT environment, this can in itself be described as a threat arising. This, in turn, is one reason why, in the next phase, an obstacle blocks access to affected IT components. The obstacle that arose constitutes the security event that affects the IT environment and can be described as the main incident.



Which security events constitute the incident itself can be simply described as the event or events that compromised the availability, confidentiality and/or integrity of the organisation's IT environment. In cases where the reporting organisation describes a security event that did not result in an incident, described security events are presented only as potential *causes* of an incident being able to arise. In cases where an incident can also be classified as an actual incident, this has been categorised separately.

Below are a number of example scenarios to demonstrate how the classification of IT incident reports was implemented.

Example incident 1: Installation of malware

Events that constitutes the cause of the incident:

1. Own staff deactivates the firewall (protection ceases/vulnerability arises).
2. Employees receive phishing e-mails that would have been blocked if the firewall was not disabled (threats arise).
3. Employees click on the link in the e-mail (trigger: threats arise).
4. Wiperware is installed automatically (threats arise).

The event that constitutes the incident:

5. Information systems and files are destroyed and deleted (success factor ceases, Actual incident: damage caused, benefit prevented).

Events that constitutes a consequence of the incident:

6. The wiperware spreads to other organisations through the affected organisation (threats arise).

Example incident 2: Denial-of-service attack

Events that constitutes the cause of the incident:

1. A technician accidentally changes a configuration in existing overload protection in a way that reduces the capability of the protection (protection ceases/vulnerability arises).
2. An attacker sends large amounts of data traffic, such as initiating TCP session requests, to an organisation's web server (trigger: threats arise).

The event that constitutes the incident:

3. The web server becomes overloaded and users during the time of the attack cannot access content on the organisation's website or related e-services (obstacles arise, Actual incident: benefit prevented).

Events that constitutes a consequence of the incident:

4. The amount of data traffic is reduced and the server's responsiveness is re-established (obstacles end, no consequence).

Example incident 3: Failed attempted cyber attack

Events that constitutes the cause of the incident:

1. An e-mail containing malware is sent to employees at an organisation (trigger: threats arise).

The event that constitutes the incident:

2. Antivirus software flags for malicious content. The harmful code is isolated and removed (threat ends, no incident).

A collaboration between:

Swedish Civil Contingencies Agency

Co-financed by the Connecting Europe Facility of the European Union

651 81 Karlstad Tel: +46 (0)771 240 240 **www.msb.se**
Publ.no. MSB2395 – September 2024 ISBN 978-91-7927-524-2