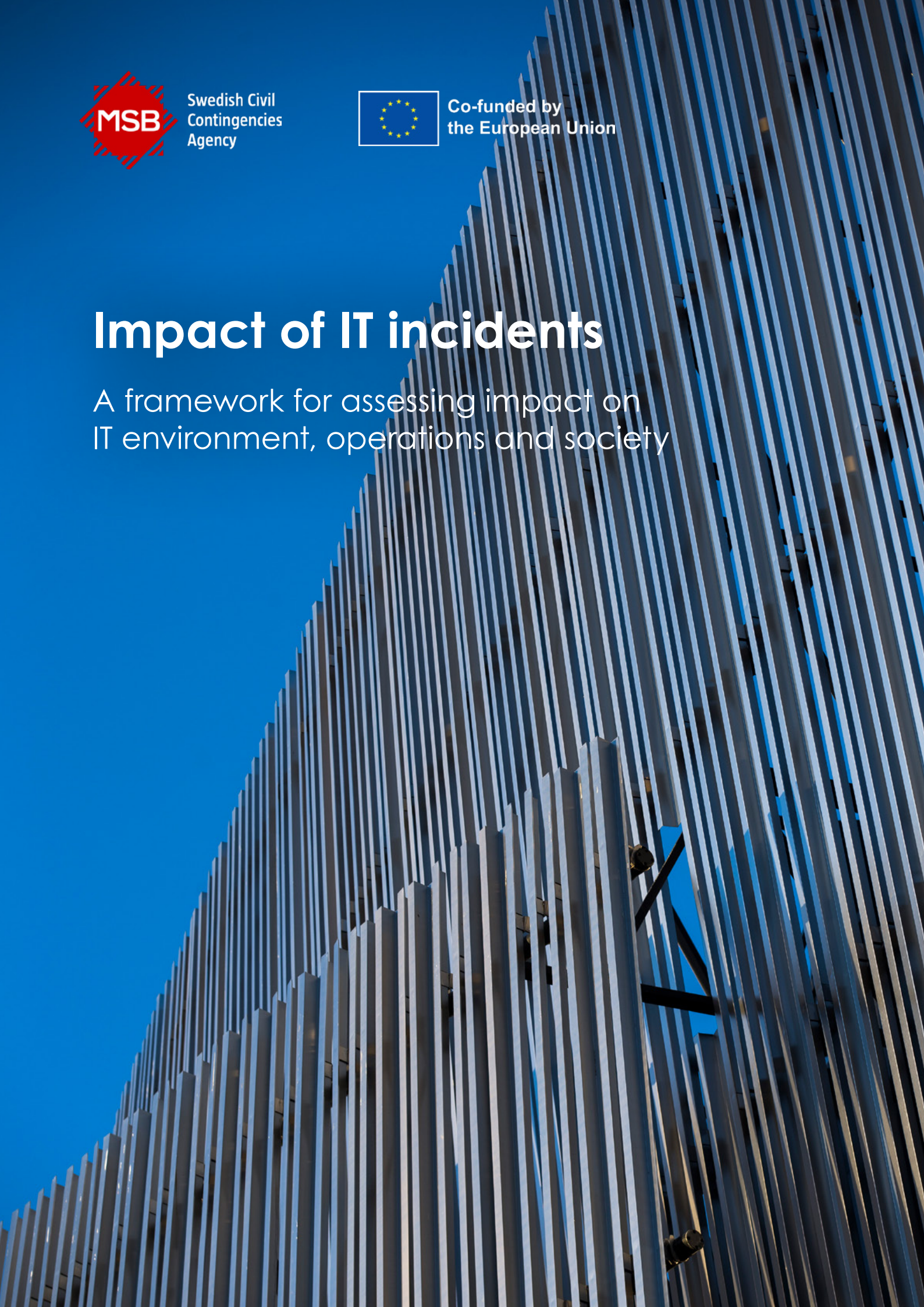
Swedish Civil Contingencies Agency

Co-funded by the European Union

Impact of IT incidents

A framework for assessing impact on IT environment, operations and society



Impact of IT incidents
– A framework for assessing impact on IT environment, operations and society

Photo cover: Johan Eklund
Photo: Alex & Martin Photographers, Johan Eklund, Melker Dahlstrand, Mikael Svensson
Printing: Åtta45
Layout: Advant
Publication number: MSB2596 – May 2025
ISBN: 978-91-7927-633-1

Preface

The Swedish Civil Contingencies Agency (MSB) has for many years received and analysed IT incident reports. This has enabled a data-driven development of our knowledge and methods, which we have subsequently presented in our thematic reports on digital supply chain security, change management, and cyber attacks. I would like to thank the organisations that have reported IT incidents to MSB.

IT incident reporting provides valuable insight into the types of incidents occurring in Sweden. This report emphasizes the variation in their characteristics and highlights the challenges involved in comparing diverse events. It also explores how these differences can be addressed to allow consistent assessment and classification within a unified framework.

The framework presented in this report is intended to support consistent and comparable analysis of IT incidents' impact on IT environments, operations, and society. The report also includes case studies to illustrate how the framework can be applied.

This work is important. The relevance of cybersecurity for societal resilience is growing, and so too is the need to analytically identify both the most frequent incidents and the most severe ones. For the same reason, it is also essential to strengthen our ability to communicate the severity of a situation – for example, in the event of a cyber crisis.

At the same time, this work remains ongoing. We are committed to further developing our methods for understanding, analysing, and assessing cybersecurity developments, and we welcome continued dialogue with all who wish to contribute to the advancement of society's resilience in the digital domain.

Stockholm, 2025-05-28

Johan Turell

Head of Strategic Cybersecurity Section,
Cybersecurity and Mission Critical
Communications Department,
The Swedish Civil Contingencies Agency (MSB)

Table of content

Glossary

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

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.

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

Confidentiality: an aspect of information security that, in brief, means that only authorised subjects, such as users and systems, can access information.

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

Essential services: services considered essential for maintaining critical societal or economic activities within the European Union.

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.).

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.

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.

Ransomware attack: a type of cyber attack where malicious software encrypts the victim's data and demands a ransom payment for the decryption key.

Redundancy: the duplication of critical components or functions of a system to maintain operational continuity.

Resilience: the ability of a system or organisation to withstand disruptions.

Risk: A possible undesirable event.

Robustness: the ability of a system to maintain its functionality and performance despite adverse conditions or disturbances.

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

Societal impact: the effect of an event, change, or disruption on society's institutions, fundamental values, and functions, including the rule of law, freedom of expression, individual rights, critical infrastructure, and national sovereignty.

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

Summary

Summary

The report aims to strengthen the capacity to understand and evaluate the consequences of IT incidents. By developing a framework for analysis and evaluation, the report presents a structured and consistent method for assessing the impact of incidents on the IT environment, operations, and society at large.

The framework presented in this report is based on a distinction between security events, defined as events where a threat or obstacle arises, and actual incidents, defined as events where benefit is prevented, or harm is caused. By analysing various events using a defined taxonomy, the framework enables nuanced reasoning and impact assessment related to reported incidents.

To validate the framework, the report includes an analysis of five case studies. The case studies are based on media sources and published analyses by the affected organisations, and include:

1. A date error in new payment systems at Ica stores and Apotek Hjärtat pharmacies.
2. A ransomware attack targeting the Swedish Church's administrative systems.
3. A ransomware attack targeting one of Tietoevry's data centres.
4. A faulty update automatically distributed by Crowdstrike.
5. A failed automatic refilling of liquid nitrogen to cryogenic freezers at Karolinska Institutet, caused by previous maintenance work.

These case studies demonstrate how the framework can be applied to actual events. The analyses are supplemented by insights regarding the framework and how it applies to the case. The cases demonstrate both the variation in impact and recurring patterns, especially in the lessons that can be drawn from the analysis. The framework shows for example that security events can happen long before they become an actual incident.

The framework has been developed based on the experience and knowledge accumulated by the Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB) through many years of receiving and analysing IT incident reports. The intention is that the framework will provide a shared terminology for assessing the impact of IT incidents. As both technology and society evolve over time, the framework will require ongoing development and refinement.

This report takes the first step towards a more nuanced assessment of IT incidents, their impact on IT environments, the affected operations, and society at large.

About the report

About the report

This report sets out criteria for assessing the consequences an IT incident may cause, including the extent to which such an incident implies societal impact. The absence of any established assessment criteria today contributes to speculation and arbitrary evaluations. The primary purpose of this report is to provide a framework for assessment, enabling the cyber security sector to adopt a shared approach towards IT incident assessment.

A deeper understanding of which IT incidents lead to societal impact is essential for strengthening resilience in a digitised society. By systematically analysing incidents, it becomes possible to identify patterns, vulnerabilities, and preventive measures.

The Swedish Civil Contingencies Agency (MSB) has, over many years, received and analysed IT incident reports. This work has yielded valuable insights into how IT incidents affect IT environments, operations, and society at large. These experiences have also led to the development of new methods, driven by the need to organise, analyse, and compare incidents in a consistent way. The methodology presented in this report is the outcome of this work and is intended to provide a structured framework for assessing the impact of IT incidents.

The report analyses the impact of IT incidents across the following dimensions: IT environment impact, operational impact, and, ultimately, societal impact.

The report has been produced with financial support from the EU under the ENIAC project (The Enhanced NIS2 Implementation And Cooperation Project). It is primarily intended for analysts, business developers and strategists within IT operations, as well as for security functions and support roles such as information security coordinators, CISOs[1], and equivalent key roles in information and cyber security.

1. Chief information security officer, CISO is responsible for the information security management in an organisation.

The chapter “Understanding impact at different levels” defines impact on the IT environment, the operations, and society in the context of IT incidents. The chapter “Case studies” analyses real-world incidents using the framework. The aim of the case studies is both to assess incident impact and to test the framework.

A central component of the report is the assessment framework presented in the chapter “Assessing IT incident impact.” The framework has been developed to provide a coherent and consistent assessment of the consequences of incidents. For MSB, it is critical that such a framework is well designed to serve its intended purpose. Classifications of incidents often become simplified interpretations of a more complex reality. It is therefore vital that such classifications are made with high precision, transparency and well-substantiated reasoning, ensuring they can withstand review and be appropriately addressed.

The final chapter, “Final Words,” summarizes key insights from the case studies and outlines proposed next steps.

Understanding impact at different levels

Understanding impact at different levels

IT incidents may have a negative impact that extends beyond individuals, businesses and organisations. They may also affect society, its institutions, core values, and essential functions. Understanding such impacts is crucial for improving and developing preventive measures that strengthen Sweden's resilience.

Core elements

The components of the framework are presented in full in Appendix 1. The framework is based on a logical distinction between security events and actual incidents. A security event is an undesirable event that affects the security of the IT environment, operations, or society. However, it does not necessarily result in actual harm, especially when security measures or redundancies are in place. An actual incident, by contrast, is a security event that has led to a tangible negative consequence – for instance, by causing a function to cease or by inflicting harm.

Table 1. Overview of taxonomy for security events and actual incidents

Security event	Description	Example	Possible incident
Obstacle arises	Something blocks a function from operating as intended.	A faulty network configuration prevents a cloud service from communicating with others.	Benefit prevented/ Harm prevented
Success factor ceases	A critical factor required to maintain a function ceases to operate.	A critical backup system goes offline, making data loss unrecoverable.	Benefit prevented/ Harm prevented

Security event	Description	Example	Possible incident
Threat arises	A security event means an increased risk of negative impact.	Cyber espionage exposes sensitive business data to a competitor.	Harm caused/ Benefit provided
Protection ceases	A security measure previously preventing undesirable events ceases to work.	A firewall rule is removed, enabling external cyber attacks.	Harm caused/ Benefit provided

Impact on the IT environment, operations and society

This report presents a framework for analysing and assessing the severity of incidents based on their impact across three levels: the IT environment level, the operational level, and the societal level. These levels influence, and are influenced by, one another. The framework adopts a holistic perspective in which each level is understood as part of a larger context. The analysis therefore considers impact within a single level and also how impact is connected across levels.

- **IT environment level** refers to an organisation's information systems – both owned and leased, including cloud services provided by external suppliers. This constitutes the technical infrastructure where a great number of incidents first manifest.
- **Operational level** refers to the overall functionality and operations of the organisation. This level analyses how an IT incident affects the organisation's ability to deliver services, make decisions, and maintain operational continuity.
- **Societal level** refers to the aggregate of organisations' services that collectively support society's functionality (e.g. healthcare, energy, payments, transport) within a defined geographic area. At this level, the analysis concerns how an incident affects society's capacity to provide fundamental services to citizens, businesses, and other stakeholders.

The impact of an IT incident may manifest at one or more of these levels with varying degrees of severity. For example, an incident may affect a specific function within an organisation's IT environment while its impact on operations is manageable and its societal consequences negligible. To assess impact, the framework considers which functions were affected, the degree of disruption, and the existence of compensatory measures or redundancy to mitigate consequences. This enables a systematic and nuanced assessment of an incident, even in complex situations where various levels (IT environmental, operational, societal) are impacted differently and to varying extents.

What is IT environment impact?

IT environment impact refers to the consequence an incident has on an organisation's information systems, regardless of ownership. It includes servers, cloud services, networks, databases, and terminals. This category captures security events that compromise the organisation's IT environment. Examples include loss of confidentiality, integrity or availability (CIA) of systems, or of the information stored and processed within them. An actual incident at this level occurs when a component of the IT environment fails to operate as intended, and compensatory measures such as backups, redundancy or alternative systems are insufficient to maintain functionality.

What is operational impact?

Operational impact describes the extent to which an IT incident disrupts an organisation's ability to perform its core, administrative and supporting functions. The assessment focuses on the consequences for the organisation's functionality, decision-making, or delivery capacity, and extends to economic values or other critical interests of the organisation and its stakeholders.

This type of impact arises when a security event causes or contributes to an actual incident for the affected organisation. The incident may prevent benefit or cause harm to the organisation or its clients and stakeholders. It may also cause benefit or prevent harm to the organisation's competitors or others in a manner adverse to the organisation's interests.

Impact at this level is not necessarily dependent on prior IT environment impact, though such connections often exist. Operational impact occur when there are no alternative or fallback solutions to maintain operations as intended. This may involve missed deliveries, disruptions, delayed decisions, or loss of control and reputational damage. The analysis must identify which operational functions are affected, how severely, and to what extent the organisation can adapt, continue operations through alternative methods, or recover within a reasonable time.

What is societal impact?

Societal impact occurs when one or more events lead to changes in essential societal functions, services, or core values and conditions. Societal impact may be positive or negative, but the current framework is limited to negative impacts.

Societal impact can be direct or indirect. Direct impact arises immediately from an incident – for example, when a cyber attack disables an essential service, preventing people from withdrawing money, denying hospitals access to medical records, or disrupting transport. These consequences follow automatically, without further action by external actors.

Indirect impact results from reactions and consequences of the incident. This includes how society, authorities or businesses respond – such as through

crisis management, enhanced security measures, or regulatory changes. Indirect impact may also involve how other actors, such as competitors or adversaries, exploit the situation. For instance, a business may gain market share if a competitor suffers a major disruption, or public trust in digital services may be eroded, influencing behaviour and policymaking over time.

An actual incident at societal level arises when the impact is so extensive that societal benefit is lost, threatened or undermined – and there is insufficient capacity to compensate for or restore functionality within a reasonable timeframe.

Understanding both direct and indirect impacts is crucial for assessing the full societal effects of an incident. Strengthening societal resilience therefore requires a comprehensive perspective that considers both immediate and long term consequences.

IT incidents that cause or contribute to societal impact

IT incidents that lead to societal impact rarely occur in isolation; they are typically part of a chain of subsequent, contributing events. An incident may act as a trigger or exacerbate an already sensitive situation. For instance, a cyber attack on an energy provider during extreme weather could intensify the effects of a power outage.

Societal impact can be direct, such as when an attack on a hospital disables patient record systems and disrupts the provision of health care. It can also be indirect, as when an IT disruption delays crisis response – for instance, emergency services' communications during a natural disaster.

Example: societal impact

One example is the cyber attack on Synnovis in the United Kingdom in 2024. In the short term, 800 surgeries were cancelled due to the failure of blood test processing. In the longer term, the incident contributed to a national blood shortage, compounded by other societal factors. The IT incident had direct short term effects, and together with other factors also worsened long terms effects on national blood supply.[2]

According to MSB's framework, actual societal impact occurs either when *benefit is prevented* (a function ceases to operate) or when *harm is caused* (e.g. leaked personal data[3] or personal injury). The most common scenario involves benefit being prevented, especially where systems linked to essential societal functions are affected. Determining factors include the duration of the disruption, availability of alternatives, and the number of organisations or individuals affected.

2. BBC. *Blood stocks drop to 'unprecedentedly low levels*'. https://www.bbc.com/news/articles/cw4y2x2kn4ko (Downloaded 05/2024).
3. Leaked personal data not only constitutes a violation of the individual, but also affects the right to privacy. The right to privacy is a human right and a fundamental principle in a democratic society.

Robustness and resilience play a critical role. Robustness refers to the ability to withstand disruptions, for example through redundant systems or alternative procedures. Resilience refers to the ability to recover quickly, for example through effective incident management and recovery protocols. The relatively low frequency of IT incidents causing societal harm is likely due to the inherent robustness and resilience, which limits adverse effects. Nonetheless, it is essential to continuously develop and reinforce these capabilities, as the threat landscape evolves and the complexity of digital ecosystems increases.

MSB's previous analyses indicate that monodependencies – where many actors rely on a single provider – can result in significant consequences during incidents. However, alternative providers often exist, mitigating the impact. For example, in 2021, customers in Sweden were able to shop at other stores when Coop's point-of-sale systems went offline following the Kaseya cyber attack.[4]

The following table illustrates events that may result from one or more incidents:

Table 2. Events that may result from one or more incidents

Benefit prevented for society	Harm caused for society
The IT incident causes or contributes to: • A disruption resulting in prolonged power outages for homes and businesses. • A disruption resulting in the loss of a significant economic contribution.	The IT incident causes or contributes to: • A disruption resulting in death or injuries. • A disruption incurring substantial economic cost to society.
Harm prevented for others at society's expense	**Benefit caused for others at society's expense**
The IT incident causes or contributes to: • Disabling of military defence systems to enable an invasion. • Destruction of corruption evidence.	The IT incident causes or contributes to: • Disclosure of classified national defence plans to foreign parties. • Decisions benefiting adversaries at the expense of societal interests.

The examples above show that the framework differentiates between *direct causality* ("causes") and *indirect consequences* ("results in"). "Causes" is used when an IT incident directly leads to an event, without requiring additional triggers. "Results in" is used when an incident contributes to a consequence through an indirect effect or a chain of events. An example illustrating this distinction is a cyber attack that disables a hospital's IT systems, which causes patient records to become inaccessible, thereby resulting in reduced quality of care and, in some cases, life-threatening outcomes.

4. SVT. *It-attacken mot Coop – detta har hänt*. https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant (Downloaded 05/2025).

Assessing IT incident impact

Assessing IT incident impact

Introduction

The impact assessment framework is based on the premise that an IT incident has occurred. This means that a *security event* has occurred within an organisation's *IT environment*. The security event may, but does not necessarily, constitute an *actual incident* within the IT environment. Similarly, the IT incident may trigger or coincide with a security event at the level of operations, which in turn may, but does not necessarily, constitute an actual incident at that level. Correspondingly, the event may also represent a security event at the societal level, which under certain circumstances may constitute an actual incident affecting society.

Figure 1. Illustration of how IT incidents, security events and actual incidents are related

Security events span a continuum of severity: at one end are events that, in no respect, resemble an actual incident; at the other are events that clearly constitute actual incidents. The framework defines assessment classes by categorising the spectrum between these two extremes.

The framework comprises four assessment levels – critical, severe, significant, and moderate – each applied separately to evaluate impact on the IT environment, operations, and society. See the table below for a summarised description of the assessment framework.

The purpose of using assessment levels is to enable a structured method of assessing the severity of the situation, based on available information. Assessments begin within a delimited segment of a particular level – such as a specific part of an organisation's IT environment or a section of the electricity grid in a municipality. If information is available concerning additional areas at the same level – such as another part of the IT environment or another part of the electricity supply – these too can be assessed using the same classification scheme.

Below is a simplified illustration of how assessments may be carried out in each area.

Table 3. The effects of an IT incident may vary across different levels

Severity	IT environment	Operations	Society
Critical	Critical		
Severe		Severe	
Significant			Significant
Moderate			

The table indicates that the current IT incident has been assessed as critical in the IT environment, with severe impact on operations, and significant impact on society. Such an assessment could, for example, be based on a scenario where a municipality experiences a cyber attack resulting in unavailability of all or most of its IT environment. Due to insufficient continuity planning, this leads to serious consequences for the municipality's ability to maintain operations, which in turn causes significant societal impact.

It is important to note that each assessment level encompasses a broader range of components. If only one part of a level has been assessed – such as the e-mail servers within an organisation's IT environment – the classification for that component may still serve as an indicator of the broader situation. The assessment of e-mail servers may suggest potential impact across the IT environment, just as an analysis of a municipality's electricity supply can imply wider implications.[5]

To enable the use of a specific assessment – and to ensure that others can replicate the analysis – what is being assessed must be clearly defined and delimited. This delimitation consists of five elements:

1. Define the scope within the IT environment, operations or society.
2. Define the internal conditions.
3. Distinguish between separate incidents.
4. Distinguish between incidents and reactions to incidents.
5. Define time frame and duration.

The delimiting elements are described in the following sections.

5. See below "Overall assessments across levels".

Define the scope within the IT environment, operations or society

Regardless of the level assessed, the IT environment, the organisation's operations, or society, the evaluation must be conducted within a clearly defined scope. Some organisations operate multiple separate IT environments or clearly segmented systems. Others consist of distinct operational parts, such as municipalities with various departments or corporate groups with multiple subsidiaries. At the societal level, essential services may be delivered by different providers across various geographic tiers – for example, grocery services in a municipality, transport infrastructure at the regional level, national online banking services, or internationally operated cloud services. Resilience, redundancy, and geographic distribution are key factors when assessing whether, and to what extent, an IT incident affects the IT environment, operations, or society.

If an essential service – such as the provision of drinking water – is disrupted in a municipality due to failure in the supporting IT system, the impact may be severe. If the ability to restore the service (resilience) is limited, leading to prolonged downtime, and no alternative solutions (redundancy) exist within the municipality, the service may be unavailable to society for an extended period.

In such a scenario, the impact on the community's capacity to deliver this function may be assessed as severe or critical, particularly if the disruption is for an extended time period. If the affected service is also the only one available in the geographic region, functionality will be impacted more extensively. However, if other water treatment facilities in the region can provide support using separate IT systems, the societal impact at the regional level may be assessed as partially critical, while for the individual municipality it may remain severe or critical.

When applying the framework, it is essential to clearly define the subject of assessment. For instance, the assessment may specify that it concerns the entirety of company X's IT environment, the web production system of company Y, or the drinking water supply in municipality Z.

Define the internal conditions

Assessments are limited to conditions internal to the entity. For IT environment impact, this means evaluating disruptions such as the extent to which email server functionality is affected. For operational impact, the focus is on the organisation's capacity to carry out activities affected by the incident, such as the ability to process and dispatch customer orders. For societal impact, the analysis centres on society's ability to maintain or provide the disrupted function, such as delivering healthcare in the absence of digital patient records.

Therefore, when applying the framework, it is essential to specify that the assessment concerns the internal conditions of the selected level within its defined scope.

Distinguish between separate incidents

A single incident may cause or lead to additional incidents. The framework requires assessment for one incident at a time and for one level at a time – that is, for the IT environment, operations, or society.

If, for example, an incident in the IT environment causes disruption to the organisation's operations, which in turn has consequences for society, these must be treated as three separate incidents – one per level. This ensures clarity in identifying causality and understanding the extent of consequences.

Example: An incident that causes additional incidents

An incident occurs in the control system of a water treatment plant. As a result, filtration of drinking water stops while the facility continues pumping water into the municipal supply network.

- IT environment impact: The original incident is a fault in the control system – this constitutes an actual incident in the water facility's IT environment.
- Operational impact: Since the IT failure results in untreated water being distributed, the facility's operations no longer function as intended. This represents a separate actual incident at the operational level.
- Societal impact: Drinking water provision has failed. This constitutes yet another actual incident – this time at the societal level. A further consequence is that people in the area consume contaminated water and fall ill.

Even though these three events are causally linked, they must be analysed separately. This is because they represent different phenomena, each with distinct types of impact, often requiring different expertise or response measures. The IT incident may require technical remediation, the service disruption must be addressed by facility operators, and the health effects require action from healthcare and public health authorities.

Effective incident management requires both coordination and clearly defined responsibilities. Societal crisis management relies on information on operational effects – and operational stakeholders need to understand the root cause.

When applying the framework, it must be clearly indicated which incident is being analysed, at what level, and how it is distinguished from its subsequent consequences.

Distinguish between incidents and reactions to incidents

In analysing the impact of IT incidents on the IT environment, operations, and society, it is essential to distinguish between immediate consequences of an incident and the effects resulting from responses to that incident. A response is not an automatic outcome of the event itself, it is a trigger of a new causal chain.

For instance, when an organisation reacts to an incident – by investing in new equipment or recovering systems – those measures are reactions. They also add additional consequences such as financial costs, organisational changes, or altered risk perception.

Separating direct consequences from reactive secondary effects is not a way to downplay the importance or cost of responses. On the contrary, it is a key analytical distinction for understanding both how incidents affect systems at various levels and how response strategies shape long term cybersecurity outcomes. This separation also allows for more precise analysis of decisions and strategies, and their influence on the longer term consequences of the incident.

When applying the framework, it must therefore be stated whether the assessment concerns the incident itself or a response to the incident.

Define time frame and duration

As demonstrated by previous example, the duration is often critical in assessing and managing incidents. If an incident disrupts value delivery in the IT environment, operations, or society, its duration becomes a key consideration in the evaluation.

However, the time factor may not always be significant. If the incident involves unauthorised access and data exfiltration, the duration of the breach may matter less than the fact that protected information is no longer secure.

When applying the framework, the duration of the incident should therefore be specified if necessary for the assessment.

Different assessments at different levels

The same incident may be assessed differently across levels. An incident in which ransomware shuts down an IT environment may be assessed as critical at the IT environment level. However, if the organisation's operations can continue by other means without IT support, the impact at the operational level may not be considered critical.

The reverse may also apply. If data leakage occurs from an IT environment, the IT impact may only be moderate, but the incident could cause major operational impact.

Overall assessments across levels

The framework supports classification and assessment of incidents at the IT environment, operational, and societal levels within a defined scope at each level. Impact may arise across multiple areas at a single level. For example, the same incident may affect both an organisation's ability to provide web services and its ability to process customer orders. If the incident completely disrupts web services while order processing remains partially functional, the impacts differ across areas of the organisation. The overall assessment of operational impact should therefore be based on the area that is most severely affected.

For instance, if an IT incident affects all e-mail servers – a defined part of the organisation's IT environment – and persists or is expected to persist for an extended period, assessing the impact on this component becomes critical. If the impact on other IT components is unknown, the framework states that, based on the available information, the overall impact on the organisation's IT environment is at worst critical. As more information becomes available on the impact to other IT components, the aggregated assessment is updated, using the most severe assessment level as its basis. If all affected components are also assessed as critical, the overall impact remains critical. If other areas are less severely affected, the aggregate assessment may be downgraded – for example, to partially critical.

As a result, a single incident may affect multiple domains at the societal level.

Example: Impact across levels

The cyber attack against Kalix Municipality in December 2021 illustrates how a single incident can generate multiple types of impact. As the municipality is responsible for a broad range of essential services and functions, the attack caused disruptions at several levels: from the IT environment to the organisation's operational capacity, and ultimately to societal impact.

IT environment impact. The attack on Kalix Municipality affected the entire digital infrastructure.[6] Affected systems were offline for three weeks, causing extensive disruption across the entire technical environment. As the attack resulted in a complete shutdown of systems and required all computers to be updated with security patches, the impact on the IT environment is *critical* under the assessment framework. However, recovering activities were initiated quickly, limiting further spread and long term consequences.

Operational impact. The cyber attack had serious consequences for the organisation's operations, particularly within the Department of Social Services. The department was forced to revert to manual procedures, including paper-based documentation, telephone coordination, and planning boards. Despite these measures, the department's operations experienced disruptions, such as difficulties in disbursing financial assistance and managing social services cases. Thanks to crisis management training and continuity plans, essential functions were maintained. The impact on the department's operations is assessed as *significant.* The overall assessment for the municipality's operations is *significant impact at worst.*

Societal impact. The social services are responsible for several essential societal functions, including elderly care, healthcare and financial assistance. The attack affected multiple areas within this scope. However, critical services such as digital locks and emergency alarms still operated, mitigating the effects on the most vulnerable groups. Rapid response efforts and alternative ways of working resulted in a societal impact on elder care, health and social care, and financial assistance is assessed as *significant.* The overall assessment of societal impact is therefore *significant impact at worst* within the geographic area under the municipality's responsibility.

6. Since the IT environment analysis includes the entire digital infrastructure, the assessment is also an overall assessment.

Applying the framework in practice

The framework is designed to be applicable both for long term strategic analysis and for the assessment of ongoing incidents during operational management – for example, in the context of cyber crisis response.

Information regarding an ongoing incident is often updated continuously, which may revise previous assessments. At an earlier stage, the impact within a specific segment of an organisation's operations may have been assessed as *critical*, and that assessment may have defined the overall maximum impact of the IT incident on the organisation's operations. As new information emerges, it may become evident that the impact within that segment was not as severe as initially assessed. At the same time, new information may indicate that another defined segment of the organisation's operations warrants a classification of *severe impact*. In that case, the assessment for that segment becomes the defining factor. The overall assessment of the incident's impact on the operations is revised from *critical at worst* to *partially severe at worst*.

A fictional example illustrates application in practice:

A large public-sector organisation identifies an IT incident in which its document management service has experienced a service disruption. The incident prevents employees from accessing documents and systems required for daily operations, resulting in delays. At this stage, it remains unclear whether other systems are affected. The impact is assessed as *significant* for the document management service within the organisation's IT environment, and *significant at worst* for the entire organisation.

Subsequent analysis reveals that multiple databases have become corrupted and that critical files are at risk of being lost. Recovery will require more time than initially estimated, and several departments are unable to operate effectively in the meantime. It also becomes clear that the document management service plays a more important role than previously assumed, with its disruption affecting other administrative processes. The incident is re-evaluated and now classified as *severe* for the affected service, and *severe at worst* for the organisation overall.

Further investigations confirm that several other critical systems – such as e-mail, finance, and HR platforms – are not affected. Alternative procedures, including the use of older copies and printed documents, have been implemented, enabling the organisation to manage the situation more effectively. The assessment is therefore revised to reflect that the impact on the entire organisation *partially severe at worst*, as certain areas continue to operate normally while others remain disrupted.

The scenario illustrates how an IT incident may be re-evaluated with new information and highlights the importance of a stepwise assessment to support informed decision-making on response and damage mitigation.

Assessning impact on the IT environment, operations and society

Below are examples of IT incidents impact, as evaluated against the framework's defined criteria. These examples provide guidance for the assessment of an IT incident at each level. The following criteria apply to each level of impact:

An IT incident has critical impact on (all or part of) the IT environment, operations or society if at least one security event has occurred (i.e. a threat has emerged, a protection has ceased, a success factor has ceased, or an obstacle has arisen), and at least one actual incident has occurred (i.e. harm has been caused, harm has been prevented, benefit has been prevented, or benefit has been caused).

An IT incident has severe impact on (all or part of) the IT environment, operations or society if it does not meet the criteria for critical impact but at least one security event has occurred, and it is more accurate to assess that at least one actual incident has occurred than to conclude that no actual incident has occurred.

An IT incident has significant impact on (all or part of) the IT environment, operations or society if it does not meet the criteria for severe impact, and at least one security event has occurred, and it is not more accurate to assess that only one or more security events have occurred.

An IT incident has moderate impact on (all or part of) the IT environment, operations or society if it does not meet the criteria for significant impact.

An IT incident has no impact on (all or part of) the IT environment, operations or society if it has not resulted in a security event affecting the IT environment, operations or society.

Assessing impact on the IT environment

Table 4. Overview showing example events and their impact on the IT environment

Security event	Actual incident	Critical	Severe	Significant	Moderate
Threat arises	**Harm caused; benefit prevented**	Malicious code is installed and encrypts all storage media.	Malicious code encrypts more than half of storage media.	Malicious code encrypts less than half of storage media.	Malicious code is installed and encrypts a small number of storage media.
Protection ceases	**Benefit prevented; harm caused**	All firewalls cease functioning.	More than half of firewalls cease functioning.	Less than half of firewalls cease functioning.	Fewer than half but more than a few firewalls cease functioning.
Success factor ceases	**Benefit prevented**	All servers are unavailable.	More than half of the servers are unavailable.	Less than half of the servers are unavailable.	Fewer than half but more than a few servers are unavailable.
Obstacle arises	**Benefit prevented**	Complete blocking of communication solutions.	Extensive but not complete blocking of communication solutions.	Partial blocking of communication solutions.	Partial blocking of communication solutions preventing normal traffic flow.

Assessing impact on the organisation's operations

Table 5. Overview showing example events and their impact on operations

Security event	Actual incident	Critical	Severe	Significant	Moderate
Threat arises	**Harm caused; benefit prevented**	Malicious code is installed that encrypts the information systems used by the organisation to operate a customer-facing cloud service. The service is entirely unavailable to all users.	Malicious code is installed that encrypts the information systems used by the organisation to operate a customer-facing cloud service. The service is entirely unavailable to more than half of users.	Malicious code is installed that encrypts the information systems used by the organisation to operate a customer-facing cloud service. The service is entirely unavailable to fewer than half, but more than a few users.	Malicious code is installed that encrypts the information systems used by the organisation to operate a customer-facing cloud service. The service is entirely unavailable to a few users.
Protection ceases	**Benefit prevented; harm caused**	An attack targets a central access management system and disables multi-factor authentication. The organisation's intrusion defences are entirely disabled.	An attack targets a central access management system and disables multi-factor authentication. More than half of the organisation's services are left unprotected.	An attack targets a central access management system and disables multi-factor authentication. Fewer than half of the organisation's services are unprotected.	An attack targets a central access management system and disables multi-factor authentication. Only a few services are left unprotected.
Success factor ceases	**Benefit prevented**	All data is erased from systems used for daily work and cannot be recovered from any source. Tasks cannot be completed on time.	All data is erased from systems used for daily work. Less than half of the data can be recovered. Several tasks cannot be completed on time.	All data is erased from systems used for daily work. More than half of the data can be recovered. Some tasks cannot be completed on time.	All data is erased from systems used for daily work. Most of the data can be recovered. A few tasks cannot be completed on time.
Obstacle arises	**Benefit prevented**	A coordination service fails, and the real-time information required to conduct operations is entirely missing.	A coordination service fails, and more than half of the real-time information required for operations is missing.	A coordination service fails, and less than half of the required real-time information is missing.	A coordination service fails, and only minor parts of the required real-time information are missing.

Assessing impact on society

Table 6. Overview showing example events and their impact on society

Security event	Actual incident	Critical	Severe	Significant	Moderate
Threat arises	**Harm caused; benefit prevented**	Malicious code is installed in the information systems that support a cloud service where the region stores all radiographic images. No backups exist elsewhere.	Malicious code is installed in the information systems that support a cloud service where the region stores all radiographic images. A few images are stored elsewhere.	Malicious code is installed in the information systems that support a cloud service where the region stores all radiographic images. Fewer than half, but more than a few, are stored elsewhere.	Malicious code is installed in the information systems that support a cloud service where the region stores all radiographic images. More than half, but not all, are stored elsewhere.
Protection ceases	**Benefit prevented; harm caused**	All water purification systems at a local drinking water facility stop functioning.	More than half of the purification systems at a local drinking water facility stop functioning.	Fewer than half of the purification systems at a local drinking water facility stop functioning.	A few purification systems at a local drinking water facility stop functioning.
Success factor ceases	**Benefit prevented**	All available telecommunications networks in a specific area are destroyed.	More than half of the available telecommunications networks in a specific area are destroyed.	Fewer than half of the available telecommunications networks in a specific area are destroyed.	A few available telecommunications networks in a specific area are destroyed.
Obstacle arises	**Benefit prevented**	All available telecommunications networks in a specific area are blocked.	More than half of the available telecommunications networks in a specific area are blocked.	Fewer than half of the available telecommunications networks in a specific area are blocked.	A few available telecommunications networks in a specific area are blocked.

Sample scenario for consolidated impact assessment

Malicious code is installed and encrypts all storage media within the organisation's IT environment. The code causes the information systems used to operate a cloud service – offered by the organisation to its customers – to be encrypted. The cloud service becomes fully unavailable to all users. The region stores all radiographic images in this cloud service. Fewer than half, but more than a few, of the radiographic images are also stored elsewhere.

Assessment classifications at each level:

- *Critical* impact on the IT environment's storage media; *at worst, critical* impact on the overall IT environment.
- *Critical* impact on the cloud service provided by the organisation to its customers; *at worst, critical* impact on the organisation's overall operations.
- *Significant* impact on the region's ability to deliver healthcare supported by radiographic images; *at worst, significant* impact on all healthcare operations within the region's geographic area.

If additional information later becomes available, the assessment classifications may be revised as follows:

- *Critical* impact on the IT environment's storage media; *at worst, partially critical* impact on the overall IT environment.
- *Critical* impact on the cloud service provided by the organisation; *at worst, partially critical* impact on overall operations.
- *Severe* impact on the region's ability to deliver healthcare supported by radiographic images; *at worst, partially severe* impact on all healthcare operations within the region's geographic area.

Information that could lead to such a reassessment might include, for example, the discovery of a recoverable backup, or confirmation that certain systems within the IT environment are still operational or can quickly be isolated and secured. In such cases, the overall impact may be mitigated.

Case studies

Case studies

In this chapter, the framework for assessing IT incidents is applied to real world events. Through a series of brief case studies, insights are provided on how the framework can be applied to evaluate impact and contribute to a more resilient society.

This chapter presents concise case studies in which current IT incidents are analysed using MSB's framework for assessing the impact of IT incidents on the IT environment, operations, and society. The case studies have been simplified to make the assessments and reasoning easier to follow. These summaries are drawn from open-source media coverage and public reports.

Each case study is structured as follows:

- **Summary:** Provides an overall assessment of the incident and its impact.
- **Incident description:** Contains an overall description, based on open sources, with balanced details to assess the impact of the incident on the IT environment, operations and society.
- **Analysis of IT environment impact:** Contains an analysis of the incident's impact on the IT environment, based on MSB's IT incident assessment framework.
- **Analysis of operational impact:** Contains an analysis of the incident's impact on the organisation's operations, based on MSB's assessment framework.
- **Analysis of societal impact:** Contains an analysis of the IT incident's impact on society, according to MSB's assessment framework.
- **Lessons learned:** Summarises key lessons derived from the case study and the analysis of impact at different levels.

Ica and Apotek Hjärtat

- **Incident:** A date related error in newly implemented payment systems caused card terminals to malfunction on the leap day.
- **Actual incidents:** Actual incidents occurred at the IT environment level (card terminal system), the operational level (sales and customer flow), and the societal level (access to groceries and pharmaceuticals).
- **IT environment impact:** *Moderate* until the day before 29 February, and *critical* during parts of 29 February.
- **Operational impact:** *Moderate* until the day before 29 February, and *significant* during parts of 29 February.
- **Societal impact:** *Moderate* until the day before 29 February, and *moderate* during parts of 29 February. *Significant* in areas where ICA and Apotek Hjärtat were the only available sources for groceries and pharmaceuticals.

Incident description

On the morning 29 February 2024, card payment functionality failed across all ICA stores and Apotek Hjärtat pharmacies nationwide. The problem affected all bank cards, regardless of issuer. Alternative payment methods such as cash, Swish, or in-app payments continued to work.[7]

The incident was caused by from the absence 29 February (leap day) in the payment system, preventing terminals from processing card payments.[8] This fault had not occurred during previous leap years and was linked to the introduction of new terminals. Around noon, the same day, ICA Group announced that card payments had been restored in most stores and pharmacies.[9]

Analysis of IT environment impact

The analysis of impact on the IT environment is limited to systems managing card payments. Due to a system fault 29 February was missing from the payment system, which prevented terminals from processing transactions. The absence of this date constituted a security event categorised as *success factor ceases*. This security event had existed since the new terminals were introduced. Prior to 29 February, it did not constitute an actual incident, but it became one on that date, of the type *benefit prevented*, when the system failed to process payments due to the unrecognised date. No alternative functionality was in place to compensate. There are no indications that other IT systems at ICA

7. SVT, Betalproblemet hos Ica löst: *"Skottdagsproblem"*. https://www.svt.se/nyheter/inrikes/betalproblem-pa-ica-kort-funkar-inte (Downloaded 04/2025).
8. Dagligvarunytt!. Betalhaveriet hos Ica löst. https://www.dagligvarunytt.se/i-butik/sakerhet/betalhaveriet-hos-ica-lost/ (Downloaded 04/2025).
9. SVT, Betalproblemet hos Ica löst: *"Skottdagsproblem"*. https://www.svt.se/nyheter/inrikes/betalproblem-pa-ica-kort-funkar-inte (Downloaded 04/2025).

or Apotek Hjärtat were affected. The incident was isolated to the part of the IT environment related to card payments. The impact is therefore assessed solely on that component. The incident is assessed as having *moderate impact* until 28 February and *critical impact* during parts 29 February.

Analysis of operational impact

The analysis of operational impact focuses on the ability to process payments for groceries, medicines, and other pharmacy goods. Accepting card payments on February 29 was not possible since new terminals were installed. This constituted a security event, in which a *success factor ceases*. The security event had been ongoing for some time. On 29 February, the inability to process card payments constituted not just a security event but an actual incident, because payment through card terminals were unavailable. However, it was still possible to pay using other methods such as Swish, apps, or cash at most locations. Some sales were lost on 29 February, with likely *moderate impact* over the longer term. No data is available on how many card payments failed or how many were completed using alternative methods. Operational impact is therefore assessed as *moderate* until 28 February, and *significant* during parts of 29 February.

Analysis of societal impact

The analysis of societal impact is assessed in terms of access to groceries, medicines, and other pharmacy goods. In locations where ICA and Apotek Hjärtat were the only available providers, a security event at the societal level – *success factor ceases* – had existed since the installation of the new terminals.

There were no known incidents affecting competitors of ICA or Apotek Hjärtat on 29 February. Groceries and pharmaceutical goods could still be purchased from affected stores and pharmacies using other payment methods on that day. In areas where there were competitors to ICA or Apotek Hjärtat, societal impact was therefore *moderate*, if any, during parts of the day. In areas where ICA or Apotek Hjärtat were the sole available provider for groceries and pharmaceuticals, the societal impact was *significant*.

Thus, societal impact (with respect to access to groceries and pharmaceuticals) is assessed as *moderate* until 28 February, and *moderate* during parts of 29 February. In areas where ICA or Apotek Hjärtat were the only alternatives, the impact was *significant* during parts of the day.

Lessons learned

This case study shows that a security event can remain latent and only manifest actual impact under specific conditions. A concealed system error, such as the absence of leap day in the new terminals, can exist unnoticed for a long time. This exemplifies how a *success factor ceases* event may persist before escalating into an actual incident. It highlights the importance of testing and analysing undesirable scenarios when implementing upgrades.

The analysis also demonstrates how impact is assessed within defined boundaries: IT environment impact was limited to card payment systems, and operational impact to the ability to accept payments. The framework supports such functional delineation and gradual escalation, from *moderate* to *significant* impact during the period when terminals ceased to function.

Both ICA and Apotek Hjärtat had access to alternative payment methods, allowing continued sales despite the disruption. The framework helps illustrate how access to alternative solutions can reduce the overall impact. Finally, the case shows that the framework enables assessment based on the most affected segment at each level. It becomes evident that although many locations were minimally affected, the societal impact is assessed based on the circumstances in areas where ICA and Apotek Hjärtat were the only available providers within a defined geographic area.

Svenska kyrkan

- **Incident:** A ransomware attack forced the shutdown of the Svenska kyrkan's administrative systems.
- **Actual incidents:** Actual incidents occurred at the IT environment level (administrative systems), operational level (administrative functions and funeral services), and societal level (funeral operations).
- **IT environment impact:** *Severe* impact.
- **Operational impact:** *Significant* impact.
- **Societal impact:** *Moderate* impact on funeral services during the incident; *significant* impact in the longer term due to loss of control over personal data.

Incident description

In November 2023, Svenska kyrkan (the Church of Sweden) was targeted by a ransomware attack. Upon detecting the incident, the Church took immediate measures to protect its IT systems and data. This included shutting down access to affected systems and resetting all passwords. Intense efforts to restart the systems followed, prioritising functions critical to parish operations.

Eight days before the attack, MSB/CERT-SE had sent a warning email about potential threats of this kind. However, the alert was delivered to a shared inbox typically used for user inquiries and was not treated as a high-priority security notice at the time.[10] According to Svenska kyrkan, security alerts from vendors like Microsoft and government agencies like MSB are frequent, which complicates the process of identifying which ones require urgent action.

Responsibility for computers and IT security has relied on local entities. Following the attack, several issues were identified: some computers were incorrectly registered and could not be located for reinstallation; certain servers had not received security updates in years; and users had been granted excessive administrative privileges.[11]

The attack affected systems handling finance, billing, payroll, and funeral services.[12] As a result, administrative functions across parishes nationwide were impacted. For example, it became impossible to schedule weddings or baptisms. Tasks had to be managed using pen and paper.[13]

10. TT. *Det fortsatta arbetet efter cyberangreppet.* https://via.tt.se/pressmeddelande/3393640/det-fortsatta-arbetet-efter-cyberangreppet?publisherId=1344892&lang=sv (Downloaded 04/2025).
11. Kyrkans Tidning, *Darknet, lösensummor och telefonkedjor – läs om cyberattacken mot Svenska kyrkan*. https://www.kyrkanstidning.se/nyhet/darknet-losensummor-och-telefonkedjor-sa-gick-cyberattacken-mot-svenska-kyrkan-till (Downloaded 04/2025).
12. TT. *Det fortsatta arbetet efter cyberangreppet.* https://via.tt.se/pressmeddelande/3393640/det-fortsatta-arbetet-efter-cyberangreppet (Downloaded 04/2025).
13. SVT. *Stora problem efter cyberattack mot Svenska kyrkan.* https://www.svt.se/nyheter/lokalt/helsingborg/stora-problem-efter-cyberattack-mot-svenska-kyrkan--wv-2vhq (Downloaded 04/2025).

Svenska kyrkan reported that funeral operations proceeded with minimal disruption in most areas. The main issue, as reported in media, was access to the "grave registry" – a record of previous interments in family plots. Without it, grave digging risked disturbing previously buried remains.[14]

Svenska kyrkan's website remained offline until January 2024, and it took additional time to restore all content. In May 2024, it was confirmed that a large volume of stolen data had been published on the dark web. Most of the files originated from 3,100 devices, representing around 10% of the computer users, and from servers.

Analysis of IT environment impact

The analysis is limited to central administrative systems at Svenska kyrkan. Under MSB's framework, the security event represents a case of *threat arises*, as it involves new attack methods targeting weaknesses in unpatched or outdated systems.[15]

This was followed by another security event: a successful attack leading to a *success factor ceases*, as systems were taken offline and a large volume of data was encrypted and exfiltrated. The actual incident involved systems for finance, payroll, billing, and bookings, thus – *benefit prevented*. The impact is assessed as *severe* for the core administrative systems, and at *worst severe* for the IT environment overall, since large parts, but not all, were affected.

Analysis of operational impact

The operational impact covers administrative functions nationwide. The security event involved the inability to use digital systems for essential tasks, a *success factor ceases*. Utility was prevented when services like wedding and baptism scheduling could no longer be conducted digitally. The incident also led to delays and extra workload due to the shift to manual processes.

Given that several critical areas were impacted for an extended period, the impact is considered *significant* for administrative operations, and at *worst significant* across the Svenska kyrkan operations. Some redundancy existed in the form of manual alternatives.

14. TT. *Det fortsatta arbetet efter cyberangreppet.* https://via.tt.se/pressmeddelande/3393640/det-fortsatta-arbetet-efter-cyberangreppet?publisherId=1344892&lang=sv (Downloaded 04/2025).
15. Since absence of a security update is not a change in itself, the security event is the altered threat.

Analysis of societal impact

Societal impact is assessed in relation to the church's role in funeral services and the consequences of data breaches. A security event of the type *success factor ceases* led to an actual incident when the cyber attack disrupted core systems for finance, billing, HR, bookings, and funerals.

Benefit was prevented across the country's parishes and dioceses, but many processes continued manually. In most areas, funerals proceeded without major issues. The disruption primarily affected family grave services, which make up a smaller proportion of all funerals. Additionally, physical copies of grave registries helped mitigate local impact.

Overall, despite the prolonged incident, the impact on funeral services was *moderate*, and at *worst moderate* at the societal level. However, the leak of personal data represents another actual incident, this time of the *harm caused* type, with potentially *significant* long term consequences for public trust and privacy rights.

Lessons learned

The analysis also highlights how different areas of an organisation may be affected to varying degrees. In this case, missing updates and misconfigurations constituted a long-standing issue that became visible only once the attack occurred. It underscores the importance of detection capability and proactive vulnerability management to address issues before they escalate.

The analysis also shows how different parts of an organisation may be impacted unevenly. The most affected area determines the overall classification for each level. For example, the central systems were hit hardest, whereas other IT components remained largely unaffected.

The case further demonstrates that societal impact may be limited, even in long-lasting incidents, if there is redundancy and fallback procedures in place. The framework helps identify that the effect was localised and confined to specific funeral types.

Finally, the case illustrates how the framework allows for separate classification of emerging secondary impacts, such as the consequences of leaked personal data.

Tietoevry

- **Incident:** A ransomware attack on one of Tietoevry's data centers.
- **Actual incidents:** Actual incidents occurred in the IT environment (data center), at the operational level (cloud service delivery), and at the societal level (access to support systems).
- **IT environment impact:** *Critical* impact.
- **Operational impact:** *Critical* impact.
- **Societal impact:** *Severe* impact.

Incident description

During the night between 19 and 20 January, 2024, a ransomware attack targeted one of Tietoevry's data centers in Sweden. When Tietoevry's monitoring detected suspicious and unusual activity, measures were taken to limit the impact of the attack. Among other actions, a decision was made to temporarily isolate the affected platform.[16]

The incident affected many government agencies when the HR system Primula, administered by the Swedish Government Service Center (Statens Servicecenter), became inaccessible. Primula is used by 120 government agencies with a combined total of approximately 60,000 employees. During the disruption, organisations using the service were unable to administer payroll or employee self-reporting, such as sick leave or vacation.

Statens Servicecenter stated that fallback procedures were implemented when the incident occurred, and that the event did not affect the January payrolls, which had already been processed.[17]

The incident also affected several organisations within the healthcare sector, including many regions and municipalities. This was primarily because the Prator platform, used for communication between healthcare institutions, was unavailable. The disruption meant that several healthcare entities had to use alternative working methods for tasks such as patient discharge. This created additional work for healthcare staff and, in some cases, delays. Several regions, including Region Blekinge, Sörmland, and Uppsala, activated crisis management to handle the disruption. By February 2, Prator was operational in Region Västerbotten and Region Blekinge, while Regions Sörmland and Uppsala took longer. According to

16. Tietoevry. *Tietoevry: Slutsatser gällande ransomware-attacken*. https://www.tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/pressmeddelande/2024/04/tietoevry-slutsatser-gallande-ransomwarattacken/ (Downloaded 04/2025).
17. Statens servicecenter. *Cyberattack påverkar Tietoevrys tjänster till ett antal kunder i Sverige*. https://www.statenssc.se/nyheter/nyhetsarkiv/2024-01-21-cyberattack-paverkar-tietoevrys-tjanster-till-ett-antal-kunder-i-sverige (Downloaded 04/2025).

Region Västerbotten, healthcare adapted well despite the disruptions, although it did cause extra strain. Their experience is that pen and paper still play an important role during a crisis.[18]

In at least two cases, information belonging to customer organisations that had been encrypted could not be restored. In Vellinge municipality, much of the affected information – including patient records from nursing homes and the social services – was considered lost.[19] Many of the information systems operated by Tietoevry also had to be restored from scratch, causing extensive extra work for the municipality. The consequences of the incident amounted to a major administrative puzzle, but there was never any risk to life or health. According to the municipality, all patients received care as planned and there are no indications that personal data was leaked.[20]

The Swedish Dental and Pharmaceutical Benefits Agency (TLV) was also significantly affected. Among other things, the price and decision database, the e-application for pricing and subsidies, and the reporting function for unavailable drugs at pharmacies were impacted.

Analysis of IT environment impact

The impact analysis on the IT environment is limited to the affected data center at Tietoevry. The security event consisted of a *threat arising* when the data center was exposed to a ransomware attack. All information stored in the center's cloud solutions was encrypted, and the attackers demanded a ransom to decrypt the data. The actual incident means that *benefit was prevented* and is assessed as *critical* for the affected part of Tietoevry's IT environment, as the event had a *significant* impact on the functionality of the data center. The impact on the overall IT environment is at *worst critical*. Additional security events and consequences in the form of actual incidents are not covered in this assessment.

Analysis of operational impact

The analysis of operational impact concerns the delivery of Tietoevry's cloud service. Security events at the operational level involved the *loss of a success factor* when customer data stored in the data center was encrypted. The actual incident concerns the type *benefit prevented* when the cloud services could not be delivered as intended. Note that the incident at Tietoevry resulted in separate incidents affecting customers who use Tietoevry as an IT service provider. These security events and resulting actual incidents are not included in this assessment. The operational impact on Tietoevry's cloud service delivery is assessed as *critical*.

18. Dagens Medicin. *Regionchefer drar lärdomar efter hackerattacken.* https://www.dagensmedicin.se/vardens-styrning/digitalisering/regionchefer-drar-lardomar-efter-hackarattacken/ (Downloaded 04/2025).
19. Vellinge kommun. I*T-attacken som drabbat Vellinge kommun får stora följder.* https://vellinge.se/nyhetsarkiv/2024/01/it-attacken-som-drabbat-vellinge-kommun-far-mycket-stora-foljder/ (Downloaded 04/2025).
20. SVT. *Efter hackerattacken i Vellinge: Journaler spårlöst borta.* https://www.svt.se/nyheter/lokalt/skane/efter-hackerattacken-journaler-sparlost-borta-i-vellinge (Downloaded 04/2025).

Operational impact also occurs in the organisations affected by the cloud service outages. According to the method, these are separate incidents assessed independently from the main incident and from operational impact in Tietoevry's own operations. An example of operational impact is the disruption at agencies that use the Primula HR system for administration. When the system is unavailable, it constitutes a security event of the type *success factor ceases* in the part of the operation that handles personnel matters. *Benefit was prevented* in the absence of alternative working methods. The operational impact is assessed as *at worst, significant* for the personnel administration functions at the affected agencies until alternative procedures were implemented and the impact reduced.

Analysis of societal impact

Societal impact related to the Tietoevry incident consists of outages in access to information and information systems used in the daily operations of many of Tietoevry's customers. The security event at the societal level was classified as a *success factor ceases*. The actual incident concerns *benefit prevented* for many government agencies as well as municipalities, companies, and actors in the healthcare sector. Tietoevry was able to restore most affected systems during the first few days following the attack, but in a small number of cases the services and data remained inaccessible through mid-March. In a limited number of cases, the encrypted information could not be restored.[21] Overall, the societal impact meant that *benefit was prevented* to a *severe* degree for the societal functions affected.

The event also led to cascading incidents at the societal level. As with the earlier example of operational impact at the agencies using Primula, such secondary incidents that result in societal impact are analysed separately. An example of a incident with societal impact is the effect on the healthcare sector when the Prator communication platform was unavailable. The security event was of the type *success factor ceases*. Where alternative working methods were lacking, it impacted the ability to carry out healthcare services, resulting in *benefit being prevented*. The impact on healthcare operations is assessed as *significant* and involved both additional workloads and delays.

21. Tietoevry. *Tietoevry: Slutsatser gällande ransomware-attacken*. https://www.tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/pressmeddelande/2024/04/tietoevry-slutsatser-gallande-ransomwarattacken/ (Downloaded 04/2025).

Lessons learned

The case study demonstrates that the framework distinguishes between main incidents and separate incidents resulting from the main incident, which is essential for a structured analysis. The disruption in Tietoevry's data center spread to multiple other organisations. The framework provides analytical support by clarifying that operational and societal impacts in customer organisations are secondary incidents and should be analysed separately from the supplier's incident. This allows for more nuanced assessments for each stakeholder. The attack on the data center triggered both technical and operational security events. The framework enables the classification and understanding of these events, even when they occur simultaneously. The case study also provides examples of how assessments of limited components form the basis for the overall evaluation.

Crowdstrike

- **The Incident:** A faulty update was automatically distributed.
- **Actual incidents:** Actual incidents occurred at the operational level (software distribution), and at the societal level (access to several critical societal services).
- **IT environment impact:** *No impact.*
- **Operational impact:** *Severe* impact due to the faulty distribution, and at worst significant due to reputational damage.
- **Societal impact:** *At worst, severe.*

Incident description

On the morning of 19 July 2024, widespread global disruptions were reported in the security platform Crowdstrike. The company confirmed that the disruptions were caused by a faulty update that had been automatically distributed to customers. This was followed by secondary effects in customer's servers and clients running Microsoft Windows and the Falcon Sensor software, which ceased to function entirely after receiving the update. Later that same morning, Crowdstrike withdrew the update and issued a new version to correct the error.[22] According to Microsoft, approximately 8.5 million devices were affected globally.[23] Many customers were unable to install the fix because their systems were already down.

The incident led to extensive disruptions across sectors worldwide. In Australia, the federal government convened a crisis meeting.[24] The media sector was impacted; for example, the British news channel Sky News had to temporarily shut down operations.[25] Air traffic was disrupted across both the U.S. and Europe, affecting ticketing and check-in systems, causing delays and temporary airport closures – including seven U.S. airports and Berlin's airport.[26] [27]

22. Crowdstrike. *Remediation and guidance hub: Channel file 291 incident.* https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/ (Downloaded 04/2025).
23. SVT. *Experten: Det kan vi lära oss av it-haveriet.* https://www.svt.se/nyheter/inrikes/experten-det-kan-vi-lara-oss-av-it-haveriet (Downloaded 04/2025).
24. Dagens PS. *Global krasch: "Värre än en cyberattack".* https://www.dagensps.se/varlden/global-krasch-varre-an-en-cyberangrepp/ (Downloaded 04/2025)
25. Ibid.
26. Dagens Nyheter. *Problemen kan dröja kvar i dagar efter globala it-haveriet.* https://www.dn.se/varlden/flyg-stoppas-over-hela-varlden-efter-globalt-it-haveri/ (Downloaded 04/2025).
27. Svenska Dagbladet. *Globalt it-kaos – flera flygplatser har stängt.* https://www.svd.se/a/OooP1l/it-problem-varlden-over-flyg-stalls-in (Downloaded 04/2025).

The healthcare sector in the U.K., U.S., and Germany also faced disruptions, with issues in electronic medical record systems, cancelled surgeries, and even interference with emergency services like 911 in the U.S. The banking and financial sectors were also affected globally, with problems accessing trading platforms and payment systems.[28]

In Sweden, disruptions were primarily noted in the transportation sector. Several regions reported problems with websites and ticketing systems in public transportation during the morning of 19 July, but these issues were quickly resolved, and there were no significant traffic impacts. Airports experienced delays due to international disruptions, and both SAS and Ryanair reported being affected.[29] LKAB's mine in Malmberget was evacuated as a precautionary measure, but production resumed the same day.[30] Karlstad municipality reported disturbances in three systems, but without any major consequences.[31]

Analysis of IT environment impact

An analysis of the impact on Crowdstrike's own IT environment concludes that the event did not affect its security platform. While the incident did not constitute a security event at Crowdstrike, the faulty update caused secondary effects in customers' servers and clients running Microsoft Windows and Falcon Sensor, which became inoperable after receiving the update. In environments lacking redundancy, this likely constituted a security event of the type *obstacle arises*, resulting in actual incidents where *benefit was prevented*. The conclusion that Crowdstrike's IT environment was unaffected does not account for the secondary effects experienced by customers and their respective IT environments.

Analysis of operational impact

The operational impact analysis focuses on the software delivery process. The security event occurred when a *success factor ceased* as a result of the erroneous update being automatically distributed. A secondary issue – reputational damage – arose from customers and stakeholders losing trust in the service, potentially leading them to switch vendors.

28. Dagens Nyheter. *Problemen kan dröja kvar i dagar efter globala it-haveriet.* https://www.dn.se/varlden/flyg-stoppas-over-hela-varlden-efter-globalt-it-haveri/ (Downloaded 04/2025).
29. RTE. *Ryanair cancels flights, NCTs disrupted over IT outage.* https://www.rte.ie/news/ireland/2024/0719/1460766-ryanair-cyber-outage/ (Downloaded 04/2025).
30. SVT. *Efter utrymningen – gruvan I Malmberget öppen igen.* https://www.svt.se/nyheter/lokalt/norrbotten/gruvan-i-malmberget-utrymt-pa-grund-av-it-problem (Downloaded 04/2025).
31. Arvika Nyheter. *Regionen höjer beredskapen efter IT-haveriet – så påverkas kommun och räddningstjänst.* https://www.arvikanyheter.se/2024/07/19/regionen-hojer-beredskapen-efter-it-haveriet-sa-paverkas-kommun-och-raddningstjanst-fbe50/ (Downloaded 04/2025).

The classification of the actual incidents as *benefit prevented* reflects the failure to deliver critical services as intended. The impact is assessed as *severe* for the faulty delivery, and at *worst significant* due to reputational harm. This reputational fall-out may constitute a secondary incident resulting from the original error.

Analysis of societal impact

The societal impact analysis concerns multiple sectors such as aviation, health-care, media, banking and finance, and transportation. The security event on the societal level is characterized by the failure of a key success factor (*successfactor ceases*) due to the erroneous update. This resulted in disrupted access to numerous critical services, effectively preventing their proper operation, an actual incident of the type *benefit prevented*.

The severity of the societal impact is based on the widespread disturbance to essential functions – including surgery cancellations, disrupted flights, and interference with emergency services. The impact is therefore assessed as *at worst, severe*.

Lessons learned

The Crowdstrike case caused disruptions across millions of customer systems. The case study shows that downstream incidents in customer environments are analysed separately. This provides clarity and structure in wide-scale events, ensuring that assessments are made at the correct level and scope.

The case illustrates how security events can rapidly escalate into actual incidents. The framework's classification system helps trace the development from a hin-drance to a full utility disruption, emphasizing the need for rigorous quality control before distributing updates.

The case also shows how societal impact can arise indirectly through technology vendors. While Crowdstrike itself does not deliver essential services, the framework helps identify how a technical failure in its environment can lead to societal-level effects.

Finally, the framework supports aggregation of impact across sectors without exaggeration. Societal impact is assessed as "*at worst severe*" in accordance with the principle of basing the assessment on the most affected area. This ensures clarity in cases of uneven or dispersed impact.

Karolinska Institutet

- **The Incident:** Failed automatic refilling of liquid nitrogen to cryogenic freezers.
- **Actual incident:** Actual incident occurred at the operational level (destroyed research material) and societal level (access to research results).
- **IT environment impact:** *Severe* impact.
- **Operational impact:** *Critical* impact until the material can be replaced.
- **Societal impact:** *At worst severe* impact until the material can be replaced.

Incident description

On the evening, 22 December 2023, an alarm was triggered at the freezer facility in the Neo building at Karolinska Institutet. The alarm indicated that the routine automatic refill of liquid nitrogen to the cryogenic freezers, necessary for maintaining the required temperature, had failed. The freezers contained large quantities of unique research material and patient samples collected over 30 years from multiple institutions.[32] When the temperature rose due to the nitrogen supply interruption, much of the material was destroyed. Karolinska Institutet estimates the cost of the incident at approximately half a billion SEK.[33]

Earlier that same day, scheduled maintenance work was carried out near the freezer facility. The maintenance triggered an alarm, which caused a valve at the external storage tank – where the liquid nitrogen is stored and from which it is automatically refilled – to close. After the maintenance, the alarm should have been acknowledged and reset, but this did not happen, and the valve remained closed.[34] As a result, the freezers were not refilled with nitrogen, and their internal temperatures began to rise.

During the Christmas holidays, staff at Karolinska Institutet noticed several times that the freezers were sounding alarms and reported this to supervisors. However, no checks were carried out until the afternoon 27 December – almost five days after the refill failed.[35] A thorough inspection on 28 December revealed that 16 out of 19 cryogenic freezers had elevated temperatures and that a substantial portion of their contents had been destroyed.

32. DN. *KI kände till brister i larmsystemet – världsunikt material förstört.* https://www.dn.se/sverige/ki-kande-till-brister-i-larmsystemet-varldsunikt-material-forstort/ (Downloaded 04/2025).
33. Aftonbladet. *Kostnaden för fryshaveriet: En halv miljard.* https://www.aftonbladet.se/nyheter/a/0Q5pg0/karolinska-institutet-polisanmaler-fryshaveriet-kostnad-pa-en-halv-miljard (Downloaded 04/2025).
34. Karolinska Institutet. *Utredning fryshaveri Neo.* https://nyheter.ki.se/media/144225/download (Downloaded 04/2025).
35. Karolinska Institutet. *Utredning fryshaveri Neo.* https://nyheter.ki.se/media/144225/download (Downloaded 04/2025).

Karolinska Institutet's incident investigation points to organisational deficiencies as the root cause. The event was not due to a single failure, but rather a combination of unclear roles, mandates, communication, and information sharing. There were also gaps in knowledge and expertise necessary to secure critical systems.[36]

Analysis of IT environment impact

The IT environment impact is limited to the technical systems monitoring the freezers. The system failed due to an oversight – critical actions during maintenance were not taken. This caused a security event of the type *obstacle arises* when the valve failed to open as expected. According to MSB's framework, this constitutes an actual incident of the type *benefit prevented*, with *severe* impact on the valve's function and, at worst, partial serious impact on the overall IT environment.

Analysis of operational impact

The operational impact includes access to the research material stored in the freezers. The security event classified as *protection ceases* when the automatic refilling stopped functioning, which led to the destruction of the material. There were no alternative data sources available, and the institution's ability to conduct research is expected to be negatively affected for a long time. The organisation faces significant costs in trying to remedy the loss. The actual incident is assessed as *utility prevented* for the affected freezers and the research relying on their contents, at the *critical* level. The assessment applies to the period until the material can be replaced.

Analysis of societal impact

The societal impact concerns access to research outcomes. The security event is defined as a *success factor ceases* when the world-unique research material and patient samples collected over three decades were lost. The material cannot be replaced, and the actual incident is classified as *utility prevented*. Society will no longer benefit from the potential discoveries that might have stemmed from that research material. The societal impact is assessed as *at worst severe*, based on the loss of capacity to sustain scientific research and experimental development until the material can be replaced.

36. Karolinska Institutet. *Utredning fryshaveri Neo.* https://nyheter.ki.se/media/144225/download (Downloaded 04/2025).

Lessons learned

This case study illustrates how the framework helps identify when a security event, such as the loss of protection, evolves into an actual incident, and that such analysis must include technical, human, and organisational factors. The case provides an example of long term operational impact. The framework also supports classification in situations where effects are delayed, unclear, or non-economic in nature.

Final words

Final words

IT incidents can impact key societal values. This report has presented a framework for assessing impact of IT incidents, with the aim of providing a common approach. However, society is a dynamic system that continuously adapts, requiring assessment criteria to evolve accordingly.

Measuring the societal impact of an IT incident is a complex task. The effects may range from significant economic consequences for critical institutions to social and health-related effects that influence, for example, public wellbeing or productivity. This can involve both short-term, disruptive changes and consequences that only become observable in the longer term.

The case studies demonstrate that MSB's framework for assessing the impact of IT incidents is a useful tool for understanding technical, organisational, and societal consequences. The incident involving Svenska kyrkan (the Church of Sweden) how newly developed attack methods exploited outdated systems. The case involving ICA and Apotek Hjärtat shows how a latent weakness in the IT environment can manifest later, and how alternative procedures help reduce operational and societal impact. The incidents at Tietoevry and Crowdstrike show how disruptions at a supplier can result in separate secondary incidents at customer organisations, and how the framework supports analyzing them independently. The case at Karolinska Institutet shows that organisations may experience long term impacts and that societal consequences can be severe even when not immediate.

By using a shared assessment framework and a unified terminology – a common taxonomy – for different types of impact, we improve our ability to interpret, describe, and compare the consequences of IT incidents. This strengthens our collective capacity to communicate risks, plan measures, and allocate resources – both within individual organisations and across society.

To strengthen the ability to assess the consequences of IT incidents, MSB will apply the presented framework in its own analytical work. The framework will be used for both operational analyses of individual incidents and for monitoring long term threat trends. The aim is to ensure that consequences are assessed systematically, in a structured way, and with consideration for technical,

operational, and societal dimensions. The agency also encourages other actors – both public and private – to actively use the framework in their own work. The framework serves as a tool to enable consistent, transparent, and nuanced analyses of IT incidents.

The framework is not static. Just as society evolves, our understanding of incident impacts must be continuously refined. Lessons from actual incidents, new research findings, and societal developments will all be crucial to how the framework is further developed. This report therefore marks not an end, but a first step toward a living framework for assessment.

Appendix 1

Appendix 1: Framework for classification and assessment of incident impact

Assessing the consequences of an IT incident is crucial for understanding its impact on society. By increasing the understanding of how IT incidents affect individual operations as well as society at large, it is possible to establish a foundation for evidence-based decision-making. This enables better prioritisation and preventive measures.

By increasing the understanding of how IT incidents affect individual operations as well as society at large, a foundation can be established for evidence based decision making. This enables better prioritisation and preventive measures.

This report presents case studies of real IT incidents and their classified and assessed impact on IT environments, operations, and society. The purpose of the method is that, based on a larger number of assessments, it will deepen the knowledge base about how many and which IT incidents affect the IT environment, the operations, or society – even though, in individual cases, it may involve difficult trade-offs when the information on which the assessment is based is incomplete or missing.

Fundamental concepts

The following basic concepts form a starting point for the analyses conducted within the strategic analysis of information and cybersecurity at MSB.

Table 7. Fundamental concepts

Concept	Explanation
Incident	An occurred undesirable event.[37]
Success	An occurred desirable event.[38]
Threat	Something that causes, or contributes to causing, an incident.
Obstacle	Something that prevents, or contributes to preventing, a success.
Success factor	Something that causes, or contributes to, success.
Protection	Something that prevents, or contributes to preventing, an incident.
Risk	A possible undesirable event.
Opportunity	A possible desirable event.
Vulnerability	Absence of something that prevents, or contributes to preventing, an incident.
Deficiency	Absence of something that causes, or contributes to, success.
Freedom	Absence of something that causes, or contributes to causing, an incident.

37. It is important to note that the event here should be understood as undesirable based on what it leads to, i.e., that an undesirable effect occurs, rather than as an event that happens instead of a desired event. For example, if an email filtering service mistakenly flags a legitimate business email as spam, this constitutes an undesirable event because the expected event was that the email would be correctly delivered to the recipient. However, such an event is not classified as an incident within this framework.
38. In accordance with the preceding footnote, it is important to note that the event here should be understood as desired based on what it leads to, i.e., that a desired effect occurs, rather than as an event that happens instead of an undesirable event. For example, when an email is sent and received by the intended recipient after the sender clicks “Send,” this is a desired event in the relevant sense. The fact that malware was not installed when a user clicked on an unknown link – that is, that an undesirable event did not occur – does not constitute a success within this framework.

Types of incidents

In this analytical framework, a distinction is made between two types of events: security events and actual incidents.

Security events

A **security event** is defined as an event that negatively affects the security of the IT environment, the organisation's operations, or society. It is important to note that a security event does not necessarily mean that actual damage has occurred. Organisations with redundant systems and effective protective mechanisms can manage security events without them leading to any problems.

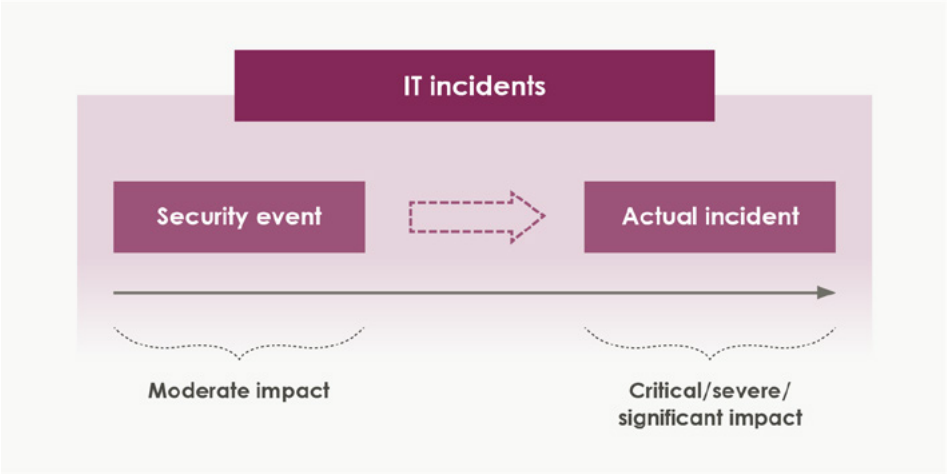
Actual incidents

An **actual incident** occurs when a security event causes direct or indirect negative impact on the IT environment, the organisation's operations, or society. This happens when compensatory mechanisms, such as redundancy or protection, are not sufficient. An actual incident means that damage has occurred, or that the organisation has lost the utility of a certain function.

An actual incident is always caused by (at least) one security event, but not all security events necessarily cause or lead to actual incidents.

The terms **IT impact, operational impact,** and **societal impact** in the framework refer to such security events or actual incidents that result in undesirable events within the IT environment, operations, or society, respectively.

Figure 2. Illustration of how it-incidents, security events and actual incidents relate to each other



Security events

There are four types of security events:

Threat arises

Definition: Something that can cause or contribute to causing an incident occurs (a threat arises).

Example: IT environment

Ransomware is installed that can encrypt data and make it inaccessible. Another example is a file share containing sensitive information being made freely accessible on the internet.

Example: Operations

Ransomware encrypts information systems used to maintain a cloud service provided by the organisation to its customers.

Example: Society

Ransomware is installed in information systems maintaining the cloud service where a region stores all its radiology images.

Protection ceases

Definition: Something that can prevent or help prevent an incident from occurring ceases (a protection fails).

Example: IT environment

A firewall that protects against unauthorized access is deactivated during a configuration change.

Example: Operations

An attack targets a central access management system and disables multi-factor authentication. The organisation's protection against intrusion has thus ceased.

Example: Society

All purification systems at a drinking water facility in a particular location have ceased functioning.

Success factor ceases

Definition: Something that causes or contributes to causing a success ceases.

Example: IT environment

A router loses the ability to route traffic correctly. Another example is a hard drive failing, making the data it contained inaccessible.

Example: Operations

All data is deleted from systems normally used for operations.

Example: Society

All available telecom networks in a specific area are destroyed.

Obstacle arises

Definition: Something occurs that prevents or contributes to preventing a success from taking place.

Example: IT environment

A new firewall rule is added, which blocks legitimate network traffic. Another example is antivirus software mistakenly blocking access to files.

Example: Operations

A real-time coordination service stops functioning.

Example: Society

All available telecom networks in a specific area are blocked.

Actual incidents

When a security event occurs, it may either be managed without impact or lead to an actual incident. This depends on whether the organisation has sufficient redundancy or alternative solutions. There are four types of actual incidents: *harm caused, harm prevented, benefit prevented,* and *benefit caused.*

Table 8. Illustration of which security events constitute actual incidents

Type of security event	Description	Example	Possible incident type
Obstacle arises	Something blocks a function from working as intended.	A faulty network configuration prevents a cloud service from communicating with other systems.	Benefit prevented/ harm prevented
Success factor ceases	A key factor needed to maintain a function stops working.	A critical backup system goes offline, making data loss unrecoverable.	Benefit prevented/ harm Prevented
Threat arises	A security event results in increased risk of negative impact.	Cyber espionage reveals sensitive company data to a competitor.	Harm caused/ benefit caused
Protection ceases	A protection system that previously prevented undesired events stops working.	A firewall rule is removed, enabling an external cyber attack.	Harm caused/ benefit caused

Harm is caused

Definition: Harm is caused to the entity, or to others, in a way that is not in the entity's interest. In the framework, the entity is either the organisation or society.

Example: IT environment

Malicious code causes the hard drives it is installed on to be encrypted (the security event). The malicious code infects all the organisation's hard drives.

Example: Operations

Malicious code infects the organisation's information systems and encrypts the systems used to maintain a cloud service provided to customers. This constitutes the security event itself as it affects the availability of operations. Since all information systems necessary for the cloud service to function become unusable, the organisation's ability to deliver the service to customers ceases. This impact on operations means the security event becomes an actual incident, as it directly prevents the organisation from conducting its core business.

Example: Society

By encrypting the cloud service, the malicious code also encrypts X-ray images, and the tools used to analyse and process them, which regional healthcare organisations had stored there. This constitutes a security event because it affects access to critical medical information and tools. Since all images and tools are stored only in the compromised cloud service, there are no alternative means to analyse new images. This makes the security event an actual incident at the societal level, as it directly affects regional healthcare services and may negatively affect diagnostic accuracy and patient outcomes.

It is important to note that adverse effects may arise at one level without necessarily leading to harm to others. For example, harm may occur in the IT environment by encrypting storage media with malware, but if the organisation has backups or alternate systems, operations can continue relatively unaffected. Similarly, harm may occur in the organisation's operations without necessarily resulting in harm to society. If certain X-ray images are stored in regional or municipal systems, or another cloud service can be used to analyse the images, the societal consequences can be mitigated.

What makes the incident an actual incident of the type "harm is caused" (it may also be of other types) at different levels is that:

1. A component in the organisation's IT environment is destroyed, and there are no redundant components that allow the IT environment to function as intended.
2. A component in the organisation's operations is destroyed, and there are no redundant components that allow operations to function as intended.
3. A component in critical societal operations is destroyed, and there are no redundant components that allow public services to function as intended.

Harm is prevented

Definition: Harm is prevented to the entity's competitors, or to others, in a way that is not in the entity's interest.[39]

Example: IT environment

A cyber attack disables information systems used to control a defence system. The attackers have installed malicious code in the network managing communication between the command centre and the operational air defence systems. As a result, the system cannot send or receive orders. Because the control function depends on digital communication and no alternatives exist, this security event constitutes an incident affecting the defence organisation's IT environment.

Example: Operations

At the operational level, the security event involving the control system means the defence organisation cannot perform its mission of protecting national airspace and repelling enemy attacks. Defence personnel depend on digital systems to operate air defences, and without them, threats cannot be countered in time. This constitutes an incident affecting operations, as the organisation's defensive capability is temporarily neutralized.

Example: Society

The attack affects national security as the enemy can launch attacks without resistance from air defences. Since missile defences cannot be used and no immediate countermeasures exist, this is an actual incident at the societal level.

It is also important to note in this example that harm can be prevented at one level without necessarily being prevented at others. For example, IT systems may be blocked by a cyber attack, but if a parallel system or alternative communications exists, the defence organisation may still launch weapons by other means. Similarly, operations might be disrupted by missile defence outages, but if other countermeasures – such as manned flights or other weapons systems – can be activated, the impact at the societal level may not be critical.

If the nation has other defence systems in place, other air defences or allied support, the societal impact may be mitigated, even if harm has been prevented at the IT and operational levels.

39. This framework has been developed solely for analytical purposes to enable a systematic assessment of the impact of IT incidents at various levels. Its purpose is to provide comprehensive and structured support for analysis – not to promote, encourage, or legitimize actions aimed at causing harm or negatively affecting systems, organisations, or societal functions. The framework is neutral and intended for incident analysis and risk assessment with the goal of strengthening resilience and security, not to support or inspire harmful activities.

What makes the incident an actual incident of the type ”harm is prevented” (even if it may be of other types) at different levels is that:

1. A component in the organisation’s IT environment is disabled, and no technical alternatives exist to allow continued IT operations as planned.
2. A component in the organisation’s operations is disabled, and no internal alternatives exist to replace the function.
3. A component of society’s defence capability is disabled, and no redundant defence systems exist to fulfill the same function.

Benefit is prevented

Definition: Benefit is prevented for the entity, or for others, in a way that is not in the entity’s interest.

Example: IT environment

An attack encrypts a pharmaceutical wholesaler’s database used for order processing and automated logistics. This is the security event. The system cannot process orders, and its functionality is completely blocked. This constitutes an incident of the type ”benefit is prevented” because distribution functionality is entirely unavailable.

Example: Operations

The wholesaler cannot accept new orders from hospitals and pharmacies. Some manual warehouse handling still works, but the distribution chain is affected, and no new drugs can be dispatched. This makes the security event an actual incident preventing benefit at the operational level.

Example: Society

Disruption to the distribution service means hospitals and clinics don’t receive new deliveries of medicines. Some treatments are delayed or restricted. This makes the security event an actual incident at the societal level, as it directly impacts healthcare delivery and may affect patient treatment.

Just as in previous examples, benefit may be prevented at one level without necessarily being prevented at others. For example, IT systems might be affected, but if the wholesaler has backups or manual alternatives, operations can continue (though they are less efficient). If alternative suppliers exist or healthcare providers have local stock or can redistribute drugs, the impact on society may be reduced.

What makes the incident an actual incident of the type ”benefit is prevented” (even if it may be of other types) at different levels is that:

1. A component in the organisation’s IT environment is disabled, and no technical alternatives allow it to function as intended.
2. A component in the organisation’s operations is disabled, such as the wholesaler’s inability to fulfill orders. No redundant solutions exist within the organisation, so drug distribution halts.
3. A component in critical societal operations is disabled, such as hospitals and clinics not receiving medicines in time. Since no adequate alternative distribution exists, society cannot maintain full access to medication.

Benefit is caused

Definition: Benefit is caused to the entity’s competitors, or to others, in a way that is not in the entity’s interest.

Example: IT environment

The security event involves attackers exploiting a vulnerability in the hospital’s storage infrastructure, leading to an actual incident when they use storage and computing resources to mine cryptocurrency. Storage is filled with mining data, preventing hospital systems from functioning optimally.

Example: Operations

Since the hospital’s IT systems are burdened by crypto-mining, digital patient records are no longer real-time. This is the security event. Healthcare staff struggle to retrieve test results, X-rays, and other vital data, delaying medical decisions and constituting an actual incident at the operational level.

Example: Society

The security event involving disrupted access to patient records due to capacity being used by others constitutes an actual incident at the societal level, as it impacts healthcare delivery and could affect patient treatment.

As in previous examples, benefit may be caused at one level without necessarily being caused at others. For example, attackers may exploit IT resources for crypto-mining without directly affecting hospital operations – if the hospital has adequate IT resilience and alternatives, operations may continue. Similarly, if internal processes are affected but emergency care continues via manual or alternate systems, the societal impact may be limited. If critical data is available via external portals, medical staff can still retrieve essential information.

What makes the incident an actual incident of the type ”benefit is caused” (even if it may also be of other types) at different levels is that:

1. A component in the organisation’s IT environment is exploited for someone else’s benefit, and there are no safeguards to prevent continued exploitation.
2. A component in the organisation’s operations is misused to the organisation’s detriment, with no alternatives allowing operations to continue smoothly.
3. A component of critical societal operations is exploited in a way that causes negative consequences for society, and there are no redundant systems to ensure uninterrupted healthcare.

All incidents are security events, but not all incidents are actual incidents

This section presents some examples illustrating that all incidents are security events, but not all incidents are actual incidents. However, all actual incidents are also security events.

Benefit does not necessarily have to be prevented just because an obstacle arises or a success factor ceases. An organisation can avoid benefit being prevented by having redundancy in its information systems. If a component, such as a hard drive, fails or is blocked, it does not necessarily mean that the function the hard drive contributes to completely ceases – as long as there are other hard drives with available space. Redundant systems can ensure that information is still saved and services continue to operate. However, if information can no longer be saved, benefit is prevented either because all storage media are full or broken (success factor ceases) or because they are blocked (obstacle arises).

Harm does not necessarily have to be caused just because a threat arises or a protection ceases. A threat introduced into an organisation’s information systems does not necessarily cause harm, especially if there are effective safeguards such as security software that detects and neutralizes malware, or a firewall that blocks the threat from spreading. Similarly, a protection ceasing to function does not necessarily mean that harm is caused, if there is no threat simultaneously present that can exploit the vulnerability the protection previously prevented. However, if harm does occur – such as a component being destroyed and needing replacement – it is because the component contributed to functionality (success factor ceases), or was part of the organisation’s protection (protection ceases).

651 81 Karlstad Phone +46 771-240 240 **www.msb.se/en**
Publication number MSB2596 – May 2025 ISBN: 978-91-7927-633-1