Swedish Civil Contingencies Agency

Co-financed by the European Union's Connecting Europe Facility

Digital Supply Chains Under Threat

50 Recommendations to Strengthen Societal Security

Digital Supply Chains Under Threat
– 50 Recommendations to Strengthen Societal Security

Cover photo: Shutterstock
Printing: DanagårdLiTHO
Layout: Advant

Publication number: MSB1955 - May 2022
ISBN: 978-91-7927-265-4

Preface

Over recent years, digital supply chains have become increasingly important to individuals, organisations and society at large. This development is in line with global digitalisation and neither can nor should be avoided. While the benefits are great, it is not without risks. In collaboration with others, it is our task to acquire and disseminate knowledge about our digital supply chains, how they work, what they may look like, the risks they entail, and what can be done to make them more secure. We also have a role to play in areas where the Swedish state can make a more tangible contribution. It goes without saying that the goal is for our digital supply chains to meet society's needs in terms of security and functionality.

A number of high-profile incidents occurring in or via digital supply chains in recent years have brought security issues to the fore. It is clear that we need to strengthen the entire ecosystem of organisations that produce, transport, and receive digital infrastructure, products and services, so that we are better equipped to meet identified threats. In recent years, developments in security policy have led us to reassess old perceptions, while the digital transformation hastened by the pandemic has also highlighted the need for innovative thinking in the digital field.

My hope is that the threat landscape and analytical framework presented in this report, as well as the account of the consequences, conclusions and recommendations, will help to increase the security of digital supply chains. At the end of the day, what we are dealing with here is a subset of the challenges that systematic and risk-based information security work should be able to tackle – and may well face. It is my firm belief that by approaching the issues more systematically and well-versed in the risks, we can reap the full benefits of digitalisation without compromising societal security. We will continue to do our part at the Swedish Civil Contingencies Agency, both through this report and forthcoming products and initiatives.

Stockholm, 10 November 2021

Åke Holmgren
Director of Cyber Security and
Secure Communications Department
The Swedish Civil Contingencies Agency (MSB)

Content

Glossary

This section defines some of the key terms used in this report.

Actor: For the purposes of this report, the term will be considered synonymous with "organisation".

Reverse engineering: A process by which a product is dismantled and its various components are analysed in order to infer how the product works.

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

Digital product: A data set (which can be established, stored and processed in information systems), a piece of software or hardware, or a service (maintained, developed and provided through information systems).

OES / DSP: Signifies Operator of Essential Services and Digital Service Provider in accordance with the NIS-directive (EU) 2016/1148.

Trust-based: A relationship between actors based on trust in which products and services are less likely to be checked and inspected than they might otherwise be.

Semiconductor: Semiconductors are materials intermediate in electrical conductivity between a conductor and an insulator (nonconductor). Because of this, they can be used as small switches in computer chips – and are therefore fundamental to modern electronics.

Digital supply chain incident:

1. An event in which something that:
    a. should be delivered in the digital supply chain (a success factor or protection) is not delivered, or
    b. should not be delivered in the digital supply chain (a threat or an obstacle) is nevertheless delivered, and
2. the results of which have either an unplanned negative impact[1] or fail to deliver a positive impact[2] on the confidentiality, integrity or availability of information systems, or the data contained therein.

Delivering organisation: An organisation that supplies (i.e., produces and transmits or transports) digital products along a digital supply chain.

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

Receiving organisation: An organisation that receives digital products in a digital supply chain.

Nodes: Organisations that are a starting point for many digital supply chains, or through which many digital supply chains pass.

Subcontractor: For the purposes of this report, synonymous with "delivering organisation".

---

1. For example, the installation of malware in an information system due to a software update sent out within the framework of a digital supply chain.

2. For example, a new component necessary to repair a broken information system is not delivered even though it is ordered.

Summary

Summary

Digital supply chains facilitate most of the essential societal services that we use and depend on in our everyday lives. Supply chain incidents can have far-reaching consequences and are likely to become increasingly common as digitalisation gathers pace.

The modern economy is characterised by the fact that many organisations focus on their core operations, specialising in what they are, and should be, good at. In order to do so, many organisations outsource operations and support functions that are not part of these core operations. This is particularly true of information flows, software and hardware, as well as digital services – so-called digital products. Similarly, many organisations choose to focus on their own, specific and limited niche in the value chain. As its own niche becomes narrower, an organisation's need to externally source components increases. When this development occurs in many organisations simultaneously, a situation arises in which organisations become dependent on increasing numbers of subcontractors, which in turn become dependent on more and more of their own subcontractors. The chains become more complex as more and more organisations become involved. When an organisation refines its niche, its products also become more distinctive – and when that happens, it can lead to a situation in which an organisation becomes the only, or almost the only, supplier/provider of a given type of product. Organisations that rely on such products can be said to have monodependencies.

The number of monodependencies in a given digital supply chain, and the number of organisations that have the same monodependency, seems to increase over time. This entails two growing risks: first, that disruption to the delivery of a particular digital product may halt operations at an increasing number of organisations; and second, that the pressing need to install, activate or use a delivered digital product as quickly as possible may lead the organisation to bypass testing and inspection to avoid lost time. This may result in the installation and activation of malware or other things that should not be included in the delivery by many parties at the same time. The scale of these two risks is now becoming apparent at a societal level.

Both of these risks can be realised and lead to incidents in a multitude of ways. In drafting this report, we have therefore applied an all-hazards approach. We have divided the threats that cause digital supply chain incidents into four overarching categories: system failures, natural phenomena, human errors och malicious actions. In our assessment, it is important to provide a broad picture of digital supply chain incidents. In part, this assessment is based on the fact that a number of digital supply chain incidents caused by malicious actions have attracted attention over the past year. At the same time, the incident reports received by MSB indicate that:

- incidents are very common in digital supply chains;
- the vast majority of such incidents are caused by human errors, system failures, and natural phenomena;
- and the consequences of digital supply chain incidents caused by non-antagonistic threats may be just as serious as those resulting from malicious actions.

We have also found that information sharing in our digital supply chains is often flawed, leaving many organisations unaware of their security status and unsure what to do when an incident occurs along one of the digital supply chains on which they depend. There is also a risk that incorrect or misleading information may lead to poor or ineffective decisions.

We have conducted our risk analysis at three levels: the organisational level, the national level, and the international level. The results have made it clear that the societal challenge posed by the risks associated with monodependencies in digital supply chains needs to be addressed in collaboration between the different levels. The report therefore contains recommendations to actors at all three levels: to delivering and receiving organisations at the organisational level; to organisations that support, regulate and supervise organisations in digital supply chains at the national level; and to states and governmental bodies at the international level.

In essence, we recommend that:

1. monodependencies be eliminated wherever possible;
2. ways are found to tackle new problems and challenges without establishing new or consolidating existing monodependencies;
3. greater security be built into our digital supply chains, thus reducing their inherent destructive potential; and
4. information sharing be improved so that incidents can be handled in a more coordinated manner by the organisations in a digital supply chain.

Conclusions and recommendations

Conclusions and recommendations

Gradual specialisation and digitalisation are leading to the establishment of an increasing number of digital supply chains, resulting in an ever-tighter web of interconnected, interdependent actors. This development makes digital supply chain incidents more likely, and such incidents will continue to have widespread effects unless, for example, monodependencies can be broken.

In this chapter, we present general conclusions and recommendations based on MSB's efforts to analyse the threats to and vulnerabilities of our digital supply chains. The threats may result in two types of incidents: those that result in the delivery of something undesirable[3], and incidents where things that should be delivered are not delivered[4]. We have divided the conclusions and recommendations into separate sections based on the report's primary target groups.

While digital supply chains face various types of threat, these can be broadly divided into the following categories:

1. System failures
2. Natural phenomena
3. Human errors
4. Malicious actions.

Having reviewed data from incident reports and events in the external environment, it is our assessment that, at least for receiving organisations in Sweden, the most common causes of digital supply chain incidents are human errors and system failures in conjunction with the delivery of digital products by actors. That said, malicious actors have a particular incentive to attack our digital supply chains, given that they can be used to provide access to sensitive systems operated by users along the chain. In addition to the impact of the COVID-19 pandemic on the production and transport of digital products, there are also many natural phenomena that pose a growing problem for digital supply chains, not least climate change.

3. Such as malware and other threats that are accidentally or intentionally built into the digital product being delivered, with or without the manufacturer's knowledge.

4. Such as human errors and sabotage in production or transport, barriers to trade, or natural phenomena.

Finally, we must stress that systematic and risk-based information security management is the single most important measure organisations can implement to achieve and maintain an appropriate level of information security and cybersecurity. Threats to supply chains should be identified and addressed as part of an organisation's systematic information security management, which should clarify the division of responsibilities and the working methods used to protect the organisation's data and information systems. Among other things, this implies evaluating the importance of data and information systems to the organisation and, where these are critical, assessing the inherent risks in terms of availability, integrity and confidentiality. Based on the outcome of the risk assessment, the organisation can prioritise which measures (technical and administrative) can be put in place to ensure the appropriate level of protection.

To delivering organisations in digital supply chains

MSB's review of incident reports and data from other sources demonstrates that it is common for organisations to suffer repercussions from incidents occurring at other organisations that deliver data, software, hardware, or services. According to MSB's incident report statistics[5], system failures and human errors have thus far been the most common known causes of incidents. Nonetheless, incidents such as this past summer's Kaseya ransomware attack (which in Sweden affected the supermarket chain Coop, among others) show that malicious actions committed via digital supply chains can also have serious consequences.

Organisations continue to specialise in most sectors of society and in order to do so, they outsource certain operations and support functions. More and more digital supply chains are being established as a result and certain organisations that provide these support functions do so to an increasing number of customers. This results in the formation of digital supply chain "nodes" and, in some cases, monodependencies. When incidents occur in nodes, they have consequences for many or all of the node's users. Two-thirds of the reports submitted to MSB pursuant to the NIS Directive[6] describe incidents that occurred at a service provider to an actor subject to the NIS Directive; i..e., an operator of essential services (OES) or digital service provider (DSP). The reports received by MSB show that OESs/DSPs often have limited insight into events at their subcontractor's place of business, including the causes of incidents. In those cases where an OES/DSP has been able to determine the cause of the incident, it has almost always been a system failure or mistake.

5. Cf, e.g., the Annual Report: *NIS-leverantörers it-incidentrapportering 2020 [OES/DSP IT Incident Reports 2020]*, MSB1695 - February 2021 (2021), link: https://rib.msb.se/filer/pdf/29491.pdf, and *Årsrapport statliga myndigheters it-incidentrapportering 2020: Utmaningar för en säker och robust informationshantering [Annual Report on State Authorities' IT Incident Reports for 2020: Challenges to secure and robust information management]*, MSB1692 - February 2021 (2021), link: https://rib.msb.se/filer/pdf/29488.pdf.

6. The EU Directive on the security of network and information systems (NIS Directive), transposed into Swedish law as the Act (2018:1174) on Information Security for Essential and Digital Services is aimed at providers of essential services and digital services. Among other things, it imposes requirements regarding systematic information security management, risk analyses, security measures and incident reporting.

As a result of the gradual outsourcing to organisations specialising in the provision of IT services, more and more organisations are becoming dependent on a relatively limited pool of subcontractors. When such providers reconfigure systems, add or remove components, or add new services without adequately verifying that the combined infrastructure or services are compatible and work as they should, incidents often occur. When such incidents consist of disruption to or changes in the functionality of services that their customers already use, the incident has consequences for many users at the same time.

Such scenarios are probably the most common cause of the human errors and system failures that occur in digital supply chains in Sweden. Although it appears to be less common, subcontractors do sometimes (inadvertently) deliver products with built-in errors that lead to negative consequences. For example, an information system may stop working, or the delivered products may lack embedded protection that the customer might reasonably expect them to have. As a result, the receiving organisation may suffer incidents against which it assumes it is protected.

Although there are no good and quality-assured statistics on this topic, high-profile events over the past two years indicate that malicious actions committed via digital supply chains are becoming increasingly common.[7] One reason is that malicious actors can direct malicious actions at many organisations simultaneously through a digital supply chain. Another is that those wishing to access a specific organisation's internal environment may have a greater chance of success if they use a "backdoor" provided by a digital supply chain. If the aim is to commit malicious actions against multiple, specific targets, all or many of which can be reached via a single digital supply chain, malicious actors may also deem a malicious action launched through a digital supply chain to be the most effective approach. All in all, organisations that make deliveries within the framework of a digital supply chain should expect to face increasingly frequent malicious actions in the future. This is especially true if they have many customers, if their customers are financially strong or strategically interesting, or if their customers, in turn, are part of a digital supply chain with many customers or customers that are financially strong or strategically interesting.

Recommendations

In light of developments in this area, delivering organisations should expect new, more stringent security requirements in the future, including the ones outlined below. The reason for this is that incidents at delivering organisations that have repercussions for (or through) digital supply chains are increasingly leading to serious consequences for both individual receiving organisations and for society at large.

7. At the international level, by disrupting or blocking deliveries of things that are supposed to be delivered, and more generally when malicious actors use our digital supply chains to deliver things that should not be delivered, such as malware in the form of ransomware or spyware.

MSB therefore recommends that delivering organisations ensure that they:

1. are protected against external and internal threats, both antagonistic and non-antagonistic;
2. have insight into and control over their own digital supply chains;
3. have continuity management and redundancy in their own digital supply chains;
4. have taken security issues into account throughout the design phase of all deliverables;
5. have a high degree of transparency and can rapidly share detailed information with regard to quality assurance, security work, incidents, risks, threats and vulnerabilities;
6. conduct frequent audits of both quality management and security work, as well as the need for measures and improvements when vulnerabilities and deficiencies are discovered;
7. can guarantee delivery within agreed parameters (such as delivery time) if the deliverable constitutes a necessary component of the receiving organisation's product, or if the deliverable is deemed to be a strategic product;
8. can provide a guarantee to receiving organisations that the deliverable contains only what has actually been ordered and nothing else; and
9. can provide a guarantee to receiving organisations that the deliverable also includes appropriate protection.

Moreover, certain organisations that constitute providers within the framework of digital supply chains should expect that in future, some of the above recommendations may also become statutory requirements, for example when the revised Network and Information Security (NIS 2) Directive becomes Swedish law.

To receiving organisations in digital supply chains

As we noted in the previous section, the gradual specialisation of organisations in various sectors means that more and more digital supply chains are being established, and that some actors are increasingly taking on the role of nodes.

The effect of this development is that the ability of (receiving) organisations to conduct their own business or produce their own services and products is becoming increasingly dependent on everything in their providers'/suppliers' businesses working as it should. Unless they themselves take additional precautions, they will be increasingly vulnerable to the repercussions of inadequate quality assurance and security management on the part of their subcontractors. In order to prepare for disruptions to operations and to ensure the continuity of their business in other forms should disruptions nevertheless occur, they are also dependent on receiving advance information about impending changes and interventions in their subcontractors' systems.

This development also means that receiving organisations must be prepared for the threat that malicious actors may commit malicious actions against their suppliers/providers in order to access the receiving organisation's internal environment.[8]

This is particularly true in the case of financially strong or strategically interesting actors, especially if they otherwise maintain good information security and cybersecurity. Receiving organisations must take into account that the more financially strong or strategically interesting customers their supplier/provider has, the more interesting the supplier/provider will be for malicious actors. Ergo, the more likely the receiving organisation is to suffer either from a malicious action intentionally aimed at all of the supplier's/provider's customers, or collateral damage in a malicious action against someone else.

Recommendations

For receiving organisations, it is both important to get the deliveries they need, when they need them – and that the deliveries do not include anything that the receiving organisation does not want (such as embedded malware). To ensure that they get what they need, when they need it, MSB recommends that receiving organisations check whether the digital products they use or on which they depend[9]:

10. can only be delivered by a single actor and consider whether there are ways to adjust their own production so that they can use digital products from suppliers other than the current ones;
11. come from actors who can only deliver if they themselves first receive information, software or hardware which, in turn, can only be delivered by a single actor. Discuss with suppliers whether there are ways to adjust their production so that they can use digital products from suppliers other than the ones they currently use;
12. are supplied by actors who do not conduct systematic security management to prevent internal and external (antagonistic and non-antagonistic) threats. Review the requirements imposed on the relevant suppliers/providers, as well as whether there are other possible suppliers/providers that are more systematic in their security management. Consider whether it is best to continue the existing collaboration or start a new one with another supplier/provider.
13. are supplied by actors operating in jurisdictions where actions may be taken that adversely affect deliveries to you. Discuss with the suppliers/providers whether there are opportunities to establish production in other jurisdictions; or
14. are supplied by actors operating in places that are sensitive to natural phenomena or which may be adversely affected by climate change. Discuss the suppliers'/providers' preparedness to deal with natural phenomena and review requirement specifications regarding their preventive management.

8. Both by disrupting or blocking deliveries of things that are supposed to be delivered, and by using our digital supply chains to deliver things that should not be delivered, such as malware in the form of ransomware or spyware.

9. Dependency refers to three things: that the organisation uses something delivered by someone else in its production, that the delivery of such components is necessary for the receiving organisation's production, and that the receiving organisation cannot produce what is delivered itself.

To ensure that deliverables do not contain anything unwanted, MSB recommends that, within the framework of quality and security management, receiving organisations ensure that they:

15. regularly inventory the digital supply chains they use and on which they depend, as well as the extent to which they are trust-based;
16. as far as possible, inspect everything delivered through digital supply chains before it is installed, activated or used, in order to verify that the delivery includes everything ordered and nothing else;
17. have continuity management and redundancy regarding your suppliers of necessary components, where alternative suppliers are independent of one another both geographically and jurisdictionally, and are otherwise separated so that natural phenomena, trade barriers and other threats to one supplier do not also affect the other; and
18. have a plan for the orderly handling of any disruption to the delivery of certain necessary components, so that other supply chains do not suffer damage if their own production is reduced or delayed.

Moreover, MSB recommends that receiving organisations review requirement specifications for suppliers/providers and carriers in their digital supply chains so that they require:

19. protection against external and internal threats (whether antagonistic or non-antagonistic);
20. insight into and control over their own digital supply chains;
21. continuity management and redundancy in the supplier's/provider's own digital supply chains;
22. the supplier/provider give due consideration to security issues throughout the design phase of all deliverables;
23. transparency and information sharing on the part of the supplier/provider with regard to quality assurance, security management, incidents, risks, threats and vulnerabilities;
24. the supplier/provider conducts frequent audits of quality and security management and implements necessary measures and improvements when vulnerabilities and deficiencies are discovered;
25. the supplier/provider can guarantee delivery within agreed parameters (such as delivery time) when the deliverable constitutes a necessary or strategically important component for the receiving organisation;
26. the supplier/provider can guarantee that only what has been ordered will be delivered; and
27. the supplier/provider can guarantee that all deliverables include appropriate protections.

Moreover, certain organisations that constitute recipients within the framework of digital supply chains can expect the NIS 2 Directive to impose requirements for higher security in the supply chain, including with regard to the requirements of paragraphs 19 to 27.

To organisations that support, regulate or supervise actors that deliver or receive within digital supply chains

The role of regulation and supervision in strengthening security in digital supply chains is largely to minimise risk to society. This can be accomplished within four overall areas. It entails persuading delivering organisations to have a good capacity for continuity management, so that, to the greatest possible extent, they avoid interruptions in the production or transport of deliverables. It is also a matter of impelling delivering organisations to have good quality control and security when they make, send and transport the digital products they have been contracted to deliver, so that what is delivered does not pose a threat or lack functionality or protection.[10] It also means inducing receiving organisations to ensure that they have a good capacity for continuity management, including redundant sets of suppliers of necessary digital products, so that interruptions in production or transport from one supplier can be compensated for by obtaining what is needed from another supplier. Finally, it entails inducing receiving organisations to have good quality control and security, as well as reviewing what is received before it is installed, activated or used.

Recommendations

Support, regulate and supervise the work of delivering and receiving organisations in digital supply chains in a manner that incentivises them to:

28. order digital products that have the functionality and protection they need, and nothing more;
29. analyse, prevent and manage the risks presented both when things that should not be delivered are included in a delivery and when a delivery does not include everything it should;
30. impose requirements for appropriate quality assurance and security measures, including "security by design" and periodic audits[11], as well as transparency and information sharing on the part of the subcontractors that make up their digital supply chains;[12]
31. avoid monodependencies and lock-in effects;
32. establish redundant and diversified digital supply chains;
33. promote interoperability between their various suppliers/providers of data, software, hardware and services; and
34. maintain good information security and cybersecurity in general, and security regarding the management of information, software, hardware and services delivered within the framework of digital supply chains in particular.[13]

10. For the use of this term, please refer to the appendix *On the Analysis of Digital Supply Chain Incidents*.

11. As well as ongoing work with security measures that the audits show that the actor needs.

12. Some such work will be carried out within the framework of the EU Cybersecurity Act. Over the past year, countries including the US and the UK have started making lists of the content of products, known as a *"Software Bill of Materials"*, available to users.

13. One possible way to achieve this could be to draw inspiration from the *"principles of zero trust"*.

35. Avoid support and regulation that may: give rise to monodependencies through direct or indirect coercion or powerful incentives; or
36. consolidate pre-existing monodependencies.
37. Collaborate with delivering and receiving organisations to increase information sharing and disseminate experiences about both incidents and *best practices*.
38. strengthen knowledge and expertise about how to design requirements that promote a high level of security in digital supply chains;
39. strengthen knowledge about existing dependencies on digital supply chains, which subcontractors constitute nodes, and the available options for organisations that wish to select a supplier/provider that is less attractive to malicious actors;
40. develop models[14] that can be used by those who wish to implement systematic security management their digital supply chains;
41. share the costs of auditing the security of certain widely used digital supply chains and their associated products;[15] and
42. pool research and development resources, in order to create new solutions that enable receiving organisations to install, activate or use digital products more securely without significantly increasing costs or reducing efficiency.

To states and governmental bodies that work to strengthen societal security

States can do a great deal to secure digital supply chains. They can provide appropriate mandates, resources, and information to government agencies that support, regulate and supervise organisations within their own country that deliver or receive products or services within the framework of digital supply chains. They can also provide appropriate mandates, resources, and information to government agencies in order to establish a comprehensive knowledge base about which digital supply chains are critical to the country and how dependent it is on these digital supply chains, what systemic risks this entails, and what can be done about it. This is especially important in free societies such as Sweden, as it can be difficult for the state to obtain an in-depth picture of what the dependencies look like. States can also develop their relationships with one another, both in order to prevent incidents and build joint management capacity and to prosecute and deter malicious actors operating on behalf of or from other states.

14. For example, in the style of MSB's *Infosäkkollen* information security tool.
15. Such as code libraries.

Recommendations

MSB recommends that states and governmental bodies:

43. work preventively by establishing good relationships with other states through which critical digital supply chains pass, so that channels are already established in the event of an incident – and so that incidents can be prevented;
44. individually or in cooperation with other states, establish their own production of products of particular strategic importance, if there are well-founded expectations that such investments will pay off in future;
45. avoid statutory requirements that establish or consolidate mono-dependencies, create incentives to break up existing monodependencies and promote greater diversity;
46. introduce statutory requirements for different manufacturers of similar digital products to comply with the same standards and, as a general rule, ensure the interoperability of their products;
47. set appropriate requirement specifications for the security and quality of digital supply chains for public procurement, in order to create the conditions for actors and their products to always maintain a high minimum level of security with regard to digital supply chains;
48. advocate to ensure that the digital supply chains used by essential services are not subjected to malicious actions by state-sponsored actors, by creating incentives for actors to opt out of using digital supply chains that are particularly likely to be targeted by attackers;[16]
49. advocate to ensure that malicious actors who commit malicious actions against digital supply chains are prosecuted; and
50. advocate for the creation of international tools to deter and respond to malicious actions against digital supply chains.

16. This recommendation especially applies to supply chains in which particularly important products are delivered and where no alternative supply chains are available, and an interruption could thus have a major impact. The recommendation also applies in particular to supply chains based on in-depth access to the recipient's systems, where a malicious action via the supply chain could thus cause particularly great harm.

About the report

About the report

This report provides a picture of the threats facing digital supply chains and their vulnerability to malicious actions, human errors, system failures and natural phenomena. The report is based on the IT incident reports MSB receives from providers of essential and digital services.[17]

The report aims to give the reader a comprehensive picture of our digital supply chains and the challenges they pose from the perspective of individual organisations, as well as to make recommendations about how these challenges can be met.

Our points are the organisations that deliver hardware, software, data or services to other organisations ("delivering organisations"), and those that receive such hardware, software, data or services – either for their own use, or to process and refine the deliverables for use in their own product that then continues along the supply chain ("receiving organisations"). The report also aims to describe the challenges from the perspective of public authorities, in particular those government agencies that support, regulate or supervise delivering and receiving organisations in digital supply chains at the national level. Finally, the report aims to outline some of the challenges that may arise at the national policy level, as well as some of the digital supply chain challenges that arise between states at the international level.

17. Pursuant to the Swedish Act on Information Security for Essential and Digital Services (SFS 2018:1174), which applies to private and public sector actors who provide essential services in the banking, financial market infrastructure, transport, drinking water delivery and distribution, digital infrastructure, healthcare, and energy sectors, as well as certain digital service providers. For further information, see the annual report (in Swedish): *NIS-leverantörers it-incidentrapportering 2020 [OES/DSP IT Incident Reports 2020]*, MSB1695 - February 2021 (2021), link: https://rib.msb.se/filer/pdf/29491.pdf (retrieved 08.07.2021)

The report's target groups are:

1. employees of delivering and receiving organisations whose roles entail responsibility for security, business intelligence, analysis, or decision-making;
2. employees of organisations that assist with, support or manage security or digital supply chains at delivering or receiving organisations;
3. employees whose roles entail responsibility for security, business intelligence, analysis, or decision-making within authorities that support, regulate or supervise delivering and receiving organisations in digital supply chains at the national level;
4. employees of ministries and parliamentary bodies working with the Swedish state's international relations or with the development of new legislation; and
5. Policymakers working in areas such as national security and international relations.

MSB has assessed that a comprehensive summary and analysis of the challenges related to digital supply chains is a matter of some urgency. One reason for this is that the incident reports received by the agency indicate that the majority of reported incidents originated outside the reporting organisation. This means that they occurred at another organisation that provides data sets, software, hardware or services. Another reason is that a number of large-scale incidents in digital supply chains have recently come to light, actualising these issues and increasing the need for a knowledge overview.

MSB has therefore compiled data from the incident reports received by the agency and conducted a review of the international outlook. The aim of this work is to provide both an analysis of the situation in Sweden and an account of events abroad that are significant to anyone seeking an overall picture of the field. The descriptions of digital supply chains and the associated threats, vulnerabilities and risks as presented here are not, however, unique to providers of essential and digital services. Indeed, they may be valuable for many different types of organisations and in many different situations.[18]

An all-hazards approach has permeated our work in compiling this report. Among other things, this is reflected in the descriptions of the threats to digital supply chains presented in the forthcoming chapters. We have also included parts of MSB's analytical methodology, thereby enabling others to conduct their own analyses of digital supply chains and related challenges, please see Appendix A for further information.

The report also contains impact assessments, conclusions and a number of recommendations on what can and should be done at both the organisational and societal level to improve the resilience and security of the digital supply chains on which we all depend.

The report was produced with the support of the Connecting Europe Facility, an EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at the European level.

18. For example, as Sweden develops its total defence capabilities, we must be mindful of our dependence on deliveries of software and hardware components and digital services within the context of security of supply. It is thus important to take the threats and vulnerabilities presented in the report into account in both regular operational planning and crisis preparedness as well as in total defence planning.

About digital supply chains

About digital supply chains

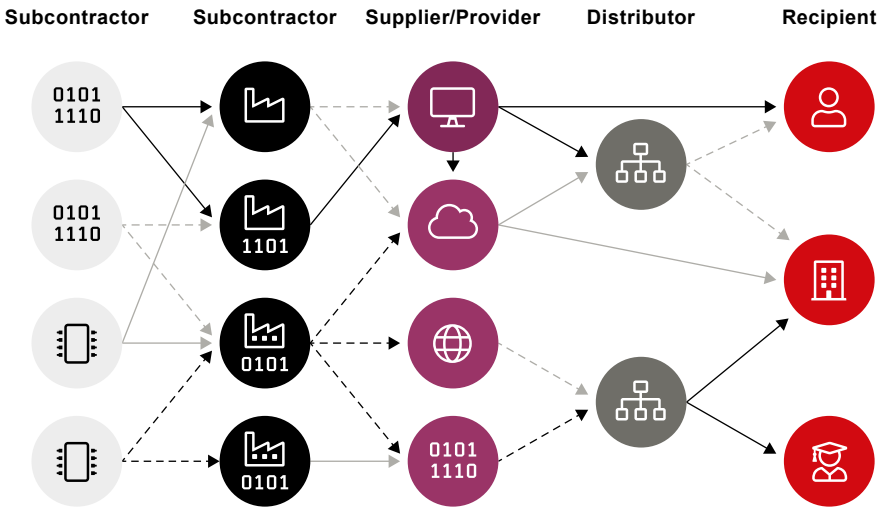
Digital supply chains are the lifeblood of our society. Today, there are digital supply chains behind virtually all goods and services and these chains are therefore essential to our most basic and vital societal functions and operations. Without the secure and continuous delivery of data sets, a steady supply of hardware components, software updates or access to services and storage over the internet, much of our modern communication and information management would come to a standstill.

When MSB refers to a *digital supply chain*, we mean the following:

The services and infrastructures that deliver or enable the delivery of a digital product used to establish, maintain, develop or restore an organisation's information management and information systems.[19]

The digital supply chain often consists of many links, each of which is supplied by many different actors, such as manufacturers, suppliers/providers and subcontractors, carriers, distributors and retailers.

Figure 1. Shows a simplified representation of different levels of actors in a digital supply chain and how even with only a few levels, there can already be many complex dependencies.



19. This can be done either individually or jointly, and sometimes also in series in which parts from several different sources are combined.

A digital supply chain is a type of supply chain characterised by the fact that it is largely based on, includes or contributes to digital products. While there are many similarities, there are also some distinctive features that distinguish digital supply chains from many other types of supply chains, such as the fact that they largely include the production of digital products that:

- once created, can normally be copied and transported without substantial additional costs (e.g., a software update that is downloaded directly over the internet);
- are delivered in real time and can then be interacted with in real time by the receiver (such as sensor data used to monitor and control a drinking water plant);
- are used in almost all operations, including essential services and digital services on which many people depend; and
- due to their complex and connected nature, are both fragile and easy to infiltrate in ways that cause harm.

In addition to having certain specific features, digital supply chains are also worthy of particular study because of the crucial role they play in ensuring the continuous functioning, development and post-incident recovery of information systems, systems that in turn maintain the majority of the vital societal functions and economic activities of digitalised societies. This makes digital supply chains a highly valuable strategic asset to a country like Sweden.

The following are examples of digital products delivered within the framework of digital supply chains:

1. **Software and software updates:** Modern software, such as administrative support, security software, games, etc. are delivered in a standard format and supplied with updates over the internet.
2. **Externally provided software libraries:** In modern software development, it is common to try to avoid developing all the necessary features of the program under development. Instead, these features are obtained from externally provided services.[20]
3. **Security software:** Modern security software is usually based on the further, continuous supply of updates even after the date of purchase. This continuous supply is essential in order for the end customer to have access to the latest virus definitions, among other things.
4. **Semiconductors:** The availability of semiconductors is a prerequisite for the vast majority of the hardware components that in turn are required to establish, maintain, repair or develop digital infrastructure.
5. **Cloud services:** Cloud services are currently used for everything from specific software to entire information systems. Providers of such services or underlying infrastructures are essential to many IT environments.

20. The service that provides the code will not necessarily be the same as the one that wrote the code. One example of this is the online service GitHub, which serves as a platform for a global community of developers. Individual developers upload their own code to solve specific tasks in GitHub, which is then available to other users.

The journey of a component or a byte of data through a digital supply chain can either be initiated when an actor orders or obtains something through the chain (such as when a company orders semiconductors they need as a component in something they manufacture), or when an actor sends something (such as when a software company sends out a security update for one of its products). Digital supply chains are capable of both continuous supply (such as updating statistics in real time) and limited deliveries (such as a certain number of semiconductors or software licenses).

Digital supply chains are crucial to digitalisation and digitalised societies. Incidents in these supply chains can have serious consequences for both individual actors and multiple actors, either simultaneously or one after the other. Ultimately, these incidents and the underlying threats present a risk to societal security.

When MSB refers to a digital supply chain incident, we mean:

1. an event in which something that:
    a. should be delivered in the digital supply chain (a success factor or protection) is not delivered, or
    b. should not be delivered in the digital supply chain (a threat or an obstacle) is nevertheless delivered, and
2. the results of which have either an unplanned negative impact[21] or fail to deliver a positive impact[22] on the confidentiality, integrity or availability of information systems or the data contained therein.

21. Such as when malware is installed in an information system due to a software update sent out within the framework of a digital supply chain.

22. Such as when a new component necessary to repair a broken information system is not delivered even though it is ordered.

Example: A digital supply chain for an OES/DSP

In both elderly care and certain other forms of care, personal alarms are issued to users so that they can alert carers if they have a problem or accident. These alarms are often worn around the neck or wrist.

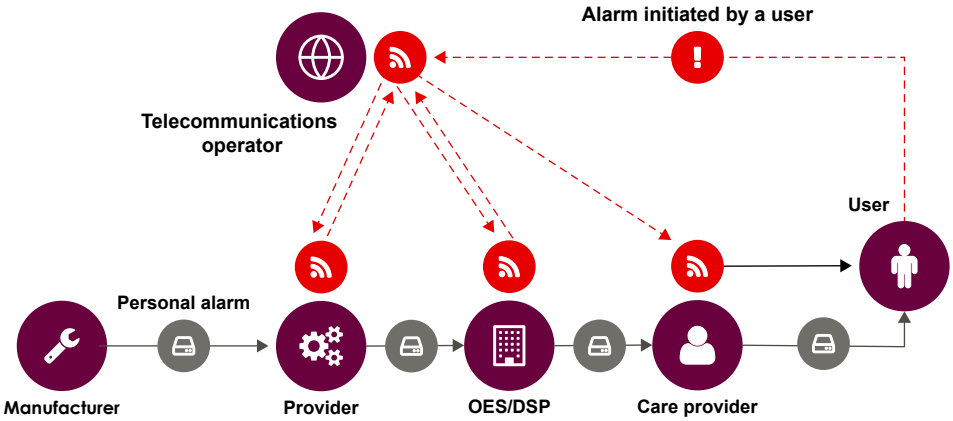
Such alarms are not usually manufactured by the provider of the vital societal service (i.e., the care provider). Rather, they are purchased or rented from another actor (the "alarm supplier"). In their turn, the alarm supplier buys the alarms from a manufacturer and integrates them into its own IT infrastructure. The business idea is to rent alarms via a subscription that includes both maintenance and the successive supply of new alarms and the replacement of old ones.

In purely technical terms, individual alarms connect to the alarm supplier's IT environment by transmitting signals over the telecommunications network, from there they are either transmitted to the care provider's own IT environment or directly to the mobile phones or other devices used by the care provider's staff.

So, in order to quickly detect that someone requires urgent assistance, care providers use a digital supply chain in the form of the alarm supplier's alarm service. The alarm supplier, in turn, uses two digital supply chains: a signal transmission service provided by a network operator and a hardware and software supply service (provided by an alarm manufacturer). Furthermore, all these actors often rely on additional digital supply chains in order to operate their businesses.

This vital societal service can therefore be disrupted by an incident in the alarm supplier's IT infrastructure (preventing incoming alarms from being sent to the care staff's mobile phones), problems in the network (preventing alarm signals from reaching the alarm supplier's IT infrastructure), or hardware defects or software errors in alarms (preventing them from working correctly when a caretaker presses the alarm button).

Figure 2. Shows the supply chain a personal alarm such as the ones used in elderly care follow from one actor to another (and in the meantime is possibly configured and adjusted), until it reaches the user, and subsequent operations. The graphic above shows how an alarm from the user, which is transmitted from the personal alarm, first goes to a telecommunications operator, who passes it on to the supplier of the personal alarm (if the OES/DSP outsources such a service) or to the OES/DSP (if the OES/DSP has its own such service), and how a signal is then transmitted back to the telecommunications operator, who, in turn, sends it on to the care provider.



A web of niche actors

Organisations that endeavour to streamline their operations in various ways have an ongoing need for higher and more specialised performance. As the development of the components that this level of performance demands is expensive, challenging and requires a large concentration of niche expertise, industries working in the field of digitalisation increasingly operate in a global marketplace. Despite this, the number of actors with the ability and financial means to remain at the cutting edge of technology and research has gradually diminished in certain areas (such as advanced semiconductor design and manufacturing). Clusters of companies providing different components of the total supply have coalesced in different parts of the world. As a result, products and services consisting of many different components have gradually become reliant on an increasing number of organisations in chains along which the various components are created, refined, combined and passed on in a constant flow between different parts of the world.

Our digital infrastructure consists of hardware and software, the components of which are generally manufactured, combined, integrated and forwarded between different organisations located in different parts of the world. For example, a computer consists of a range of components, such as a motherboard, hard drive, graphics card, RAM memory and network adapters. These are often manufactured by multiple suppliers in various parts of the world. The components themselves consist of a variety of subcomponents, some of the smallest of which are computer chips with microprocessors and memory. These in turn may have been manufactured at additional stages by subcontractors. Semiconductors are among the smallest electronic components. Most hardware components also have associated software, while the final product, the computer itself, has many application programs (many of which are vital for the computer to work) that are also often sourced from different manufacturers and different locations.

While the construction and supply of computer software has a similarly complex structure, the "manufacturing process" can be even more widely distributed. Different providers, each with their own their programmers, have different operating systems, network protocols, and a variety of applications that must be able to communicate with each other correctly. Applications and protocols, in turn, are based on different pieces of source code or software text. The source code can often be a mixture of different pieces of code that different programmers have written, sometimes over a long period of time and in several organisations or by private individuals. Not infrequently, different software programs consist of ready-made code, where the developer has used existing code libraries in the development process. Documentation is often lacking about which code libraries or versions are included in the finished product. It must, in turn, be possible to compile[23] and run the ready-made code and software in such a way that various programs can do what they are meant to do. Together these factors create a complex chain of actors and sources behind virtually all software currently on the market.[24]

---

23. Translation of code from programming language to machine code.

24. For an overview of the structure and complexity of information systems, see the Swedish Defence Research Agency report [in Swedish] *Säkra leveranskedjor för Informationssystem [Secure Supply Chains for Information Systems],* FOI-R--4851--SE (2019), link: https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4851--SE (retrieved 2021-04-16).

Continuous trust is a prerequisite

Digital supply chains generally do not merely involve the production of a product and its shipment to a recipient. Once the product has been delivered, the supply chain also often includes support for installation, activation or use, as well as both updates and various forms of maintenance in the event that the product does not work properly. Most organisations need a continuous influx of technical components such as computers, mobile phones, servers, routers, etc. Each technical component usually requires a separate software program. New features are often regularly added via updates, and vulnerabilities are discovered and must be addressed through security updates. Software often relies on other software, which, in turn, can change in an equally dynamic way. Although uncommon, the actual updating of a software program itself can cause the software to become vulnerable or result in the emergence of a new threat. A more frequent problem for many organisations is that the provider of a digital product eventually chooses to shut down its digital supply chain for that particular product, whereupon the product ceases to be developed with new features or receive new protections as new ways to improperly use or commit malicious actions against the product are discovered. Often, the provider decides to shut down the digital supply chain for a particular product when it has launched a new product in the same category.[25]

The continuous need for maintenance and supplementations means that the digital supply chain requires a high degree of trust in a whole range of involved parties. One example of this is the management of security updates from software service providers. The content of the constant influx of updates and security updates is almost impossible to review, and for security reasons it is often recommended to implement them as soon as possible. Similarly, the use of managed services, antivirus protection or other security solutions requires a high level of trust, as these also often require privileged access to their customers' systems and networks. This means that the importance of a foundation of trust in software products or providers extends long after the date of purchase. When purchasing and using software, organisations commit to a long-term, trust-based dependency on their provider, and by extension on their subcontractors, all the software involved, and the dependencies they have. Hopefully, this is founded on the provider and subcontractors conducting stipulated and continuously verified systematic security work during the contract period, with the possibility of follow-up, control and action on the part of the customer.

25. For example, this can happen when operating system manufacturers release a new version of their operating system and want to create incentives to buy into the new operating system, instead of keeping the old one. Or perhaps a mobile phone manufacturer releases a new mobile phone and wants you to invest in it.

Example: Antivirus software updates

One example of a trust-based dependency is the one between information systems in which antivirus software has been installed and the information systems of the manufacturer of that antivirus software. The antivirus software works in such a way that newly discovered threats such as malware are described in a so-called “signature”. In order for antivirus software to detect and address new malware, it needs a continuous supply of new signatures that allow it to handle the constant stream of new malware.

Antivirus software programs often requires a high level of access permissions in the systems and clients they are supposed to protect, often right down to the core functions of the operating system. This is necessary in order to ensure that the protection against malware covers all levels of the software. This makes trust in the antivirus software provider critical to the organisation that uses it.

In order for the antivirus software to handle new threats effectively, it must be able to instal new signatures as quickly as possible after they are released by the antivirus software manufacturer. For this to be possible, the transmission between the manufacturer’s and users’ information systems must proceed as quickly as possible. For this reason, such products usually come with a ready-made solution that uses a trust-based network connection to the manufacturer’s information system. This enables automated transfer and installation, eliminating the need for the customer to review each incoming signature and code. This is yet another factor that makes the foundation of trust in the supply chain and the supplier/provider so critical.

The combination of in-depth access and change permissions (which can be used to both control and sabotage) and the low level of scrutiny and control that many people who use such software have over these programs makes their use attractive to malicious actors.

Situational overview of the security of digital supply chains

Situational overview of the security of digital supply chains

In recent years, there have been a variety of disruptions in digital supply chains due as a result of malicious actions, human errors and natural phenomena. In this chapter, we describe what the incident reports have revealed, as well as the overall threat picture and examples of incidents resulting from these threats.

Situational overview based on NIS reporting

From the beginning of 2020 until the end of June 2021, two-thirds of all reported incidents at operators of essential services (OESs) or digital service providers (DSPs) originated in a supply chain. This speaks to the relatively high proportion of threats, vulnerabilities and risks tied to the resources and components of external parties, but which nevertheless affect the security and continuity of these providers' own operations. It also says something about how common it has become for OESs to be highly dependent on various types of digital supply chains and their associated suppliers/providers. The reporting indicates that most incidents have been related to communication systems or networks, but that they are also common in systems for process control or supervision, as well as administrative systems.

The reported incidents usually last a few hours, although the time span ranges from minutes to months. The timeframe includes the period from when the incident occurred to when it was discovered, dealt with, and finally ended. Often the incidents are detected directly, usually by the organisation's own staff when someone discovers that a service they use is unavailable or is not working as usual. In some cases, however, the incident is only brought to the organisation's attention when the subcontractor notifies them. In other cases, especially those related to banking and drinking water supply, the incident has been detected by internal detection systems. In a few cases, it has been reported that the incident was detected by external detection systems. So, even if the incident occurs in the supply chain, the first signal that an incident has occurred is usually the impact internally within an organisation.

Examples from reports

A drinking water supplier experienced problems with its process control system when their system provider's VPN server suffered an incident. Several functions were affected; for example, the flow of information from remote facilities (e.g., water towers) was interrupted for about five hours. According to the supplier, there was no risk to human health during the disruption to services.

Underlying threats and vulnerabilities

Based on the information in the reports received, a very small percentage of incidents originate from antagonistic acts such as intrusion, ransomware[26] or DDoS[27] attacks. This can be compared to the extensive international media reporting of malicious actions targeting digital supply chains during the same period. This disparity may be due to both the fact that, compared to some other countries, Sweden has emerged relatively unscathed from the major international malicious actions[28] committed during this period, and because the news media tends to focus on intentional threats such as malicious actions rather than on threats such as human errors and system failures.[29] In fact, system failures and human errors have been the most common known causes of incidents, and these have often occurred in conjunction with change management or upgrades. As systems become more complex and difficult to understand, it becomes even more important to secure both processes and skills that can deal with these tasks at the minimum possible risk of incidents.

The causes of over 60 per cent of reported incidents originating in a digital supply chain are unknown to the OES/DSP.[30] In comparison to this strikingly high percentage, the corresponding figure for incidents of unknown origin occurring within the reporting organisation is just over 20 per cent, i.e., only a third as many. This highlights the problem of the lack of insight and information about incidents that take place in the digital supply chain. It also shows that, in the vast majority of cases, the threats to and vulnerabilities of our digital supply chains are unknown to operators of essential services and digital service providers.

26. Ransomware comes from the English words "ransom" and "software". A ransomware attack may encrypt all or part of an organisation's information system and the information it contains, preventing access by authorised personnel. By encrypting the information, the attackers hope to force the organisation to pay a ransom to gain access to the decryption key to retrieve the lost information.

27. Distributed Denial of Service attacks. A DDoS attack may make all or part of an organisation's online systems unavailable by flooding the targeted systems with incoming requests or messages. However, the malicious action against Kaseya had an impact on several large Swedish organisations. For more information about this malicious action, see the chapter "Intentional threats to digital supply chains (malicious actions)".

28. However, the malicious action against Kaseya had an impact on several large Swedish organisations. For more information about this malicious action, see the chapter "Intentional threats to digital supply chains (malicious actions)".

29. For a more detailed review of the public discourse on information security, see the MSB report [in Swedish] *Is IT safe? En studie av den publika diskursen av informationssäkerhet i Sverige. [Is IT safe? A study of the public discourse of information security in Sweden].* MSB1802, July 2021 (2021), link: https://rib.msb.se/filer/pdf/29705.pdf (retrieved 21.09.2021). For a further discussion on how the discourse and focus on certain problem areas, rather than others, are gradually being shaped in the field of information and cybersecurity, see the report by MSB and the Stockholm International Peace Research Institute (SIPRI) *Cyber-incident Management: Identifying and Dealing with the Risk of Escalation. SIPRI* Policy Paper 55, September 2020 (2020), link: https://www.sipri.org/publications/2020/sipri-policy-papers/cyber-incident-management-identifying-and-dealing-risk-escalation (retrieved 2021-09-28).

30. Based on other information in the reports, there is nothing to suggest that the causes of these incidents would not be normally distributed between other causal categories.

The fact that this is the case is worrying in several ways, not least because of the difficulty in building safeguards to respond to an unknown threat or to remedy an unknown vulnerability. It is therefore important to prepare agreements with providers to both ensure that adequate security work is conducted and that the receiving organisations has sufficient insight into this work, as well as to review how redundancy is ensured for the most critical resources when an incident nevertheless occurs.

Disruptions caused by incidents

Even where incidents were caused by events in the supply chain to an operator of essential services or digital service provider, most reports state that the incident did not cause disruption to other actors further along the chain, beyond the OES or the DSP. Nor have any of those incidents been deemed to have caused disruption that has had consequences for another EU Member State. While this may indicate that there are few incidents with cross-border consequences, it could simply demonstrate the difficulty of obtaining an overview of the dependence of actors in other countries on a particular service.[31] Furthermore, the reporting organisations assess that the negative impact of disruptions primarily relates to the health of individual citizens, if only to a small or limited extent. This can partly be explained by the fact that the health sector accounts for a large percentage of reports, and that this sector is relatively well-prepared for and accustomed to switching to other working methods when the situation demands it. The general assessment is that, above all, it is the confidence of users in the essential service that is most affected by the disruption.

Over 40 per cent of OES/DSPs assess that incidents originating in their digital supply chain caused major disruption to the service which meant that all or multiple functions of the service could not be provided. One third reported that only certain functions were affected while others remained available. The remainder stated that the disruption only affected the service to a limited extent, and that the essential service could still be fully provided in the meantime, in several cases because alternative manual procedures were in place. That said, the use of such alternative procedures usually imposes an increased workload on the organisation, and thus a drop in efficiency.

31. Since it is the operator of essential service that files the report, but the incident to which the report relates has occurred at a subcontractor, it is probably difficult for the OES to get an overview of who is affected by the incident, regardless of whether the organisations in question are in Sweden or abroad.

Handling incidents and preventive measures

In nearly half of reports dealing with incidents that have occurred at a subcontractor to an operator of essential services or digital service provider, the reporting organisation states that they have suffered similar incidents and disruptions on previous occasions. However, there is a difference in how OES/DSPs handle incidents that originate with a subcontractor. When it comes to describing the causes of an incident, a difference emerges between incidents that occurred within one's own organisation and those originating with a subcontractor. In the majority of cases in which the incident occurred in a digital supply chain, at the time its report was submitted, the reporting organisation had no idea what caused the incident and was awaiting an incident report from the subcontractor. In some cases, reports state that the subcontractor is unstaffed at weekends, leading to long response times regarding what the problem is and how long it may take to rectify. In other cases, incident handling has been delayed and complicated by the need to accommodate service windows in other countries.

When it comes to planning how they can prevent similar incidents, the primary recourse of many OES/DSPs is to review their own procedures or purchase new hardware. Another common planned measure is to review communication with the subcontractor. In some cases, the provider states that they will review their service level agreement (SLA) with the subcontractor, and in a few cases they go so far as to say that they plan to replace the subcontractor. In general, it is clear that many OES/DSPs not only outsource their services, but also expertise about those services, and without information from subcontractors they are sometimes at a loss when asked to describe what has happened.

Threats to digital supply chains

In this section, we address threats to digital supply chains across four overarching categories: malicious actions, human errors, system failures and natural phenomena. For our purposes, the term *threat*[32] refers to anything that causes, or may cause, a digital supply chain incident.

32. See the Appendix *On the Analysis of Threats, Vulnerabilities and Risks in Digital Supply Chains.*

Deliberate threats to digital supply chains (malicious actions)

In this section, we divide antagonistic threats into four motive-based categories and address them in separate subsections.[33] We present likely choices of strategies and the intended outcomes and effects of each overall motive. In each subsection, we also provide an account and classification of a contemporary malicious action involving digital supply chains.[34]

It is important to remember that an antagonist may simultaneously have several different motives, and that it is possible to have one motive in the short term another long-term motive. Of course, how an antagonist behaves will also be determined by other factors aside from their motive; perhaps the type of actor involved, the resources and capabilities of the antagonist or how risk-averse they are, etc.

When the antagonist's intention is to cause harm

This motive may be a matter of causing harm to the target of the malicious action, or to others via that target. Antagonists seeking to inflict harm may choose to commit a malicious action against the actor by taking advantage of trust-based channels between the actor and the service providers along their digital supply chains. These channels may grant the attacker access to the actor's secure IT environment from where they can cause significant damage. An attacker may choose to take such a "detour" in order to gain access to secure environments and systems either because they have other intended targets that they can also access via the service provider's system or because they consider it easier to breach the real target's security via the channel than through a direct attack.

The antagonist may also commit a malicious action against any of the real target's suppliers to gain access to their systems and introduce threats or remove protections in the digital products they supply to the real target. The introduced threat can then cause harm when the hardware or software is installed, or when the attacker takes advantage of a protection being removed to access the real target's system. There are however risks involved for an attacker in a strategy based on introducing threats into the provider's services. Firstly, the threat may cause an incident at another organisation that installs the service or product earlier than the actual target, whereupon the real target may become aware of the threat and avoid installing the product or service themselves. Secondly, the harm caused by the threat will also affect many others who install the product or service, provoking a greater backlash against the malicious action. If the introduced threat has the capability to replicate itself and spread, there is also the additional risk that the attacker itself, or others to related to the attacker, may ultimately suffer incidents.

33. The motives are a way of gathering together all the overall driving forces that an antagonist may have. They are to: (1) cause harm to the target of the malicious action, or to others via that target; (2) benefit the attacker or others on behalf of whom the antagonist carries out the malicious action; (3) prevent harm to the attacker or others on behalf of whom the antagonist carries out the malicious action (a preemptive malicious action); or (4) prevent benefits to the target of the malicious action, or to others via that target.

34. See the analysis framework in the appendix *On the Analysis of Threats, Vulnerabilities and Risks* for more information on how incidents in and malicious actions against digital supply chains can be analysed.

The malicious action against Intellect-Service's digital supply chain (NotPetya)

Type of digital supply chain incident: Delivery of something (a threat and an obstacle) that should not be delivered.

Sometime before 22 June 2017, attackers succeeded in using stolen user data to gain access to the development environment of Intellect-Service (now called Linkos Group). The company was the developer of the accounting software M.E. Doc, which was used by most people who needed to deal with tax matters or do business in Ukraine. The program was therefore used by a large proportion of the country's OESs, as well as by international companies operating in the country.

Once the attackers had secured access to the development environment and satisfied themselves that they had not been detected, they introduced malware to an update to M.E.Doc, which was subsequently sent out to Intellect-Service customers. This malware came to be known as NotPetya[35], and has been called the world's most destructive cyberweapon. NotPetya was equipped with a number of software features, including the EternalBlue penetration tool, allegedly stolen from the US National Security Agency, and Mimikatz, a previously known method of exploiting Windows vulnerabilities. This allowed NotPetya to spread rapidly once it gained a foothold in an organisation's system. NotPetya was also equipped with features that encrypted both the master boot record[36] on computers, making it impossible to start them, as well as their files. Moreover, the encryption was irreversible, so all data that NotPetya came across was lost.

NotPetya became one of the most expensive cyberattacks in history. These costs arose due to the major disruptions caused by the malicious action, all the data that was lost, and all the hardware that was destroyed and needed to be replaced. Large swathes of Ukraine's IT-supported infrastructure were affected and made inaccessible – including banks, power stations, hospitals and airports. It is estimated that 10 per cent of Ukraine's computers were destroyed as a consequence of the malicious action. The effects also extended beyond Ukraine's borders. Danish logistics company Maersk was one of the hardest-hit stakeholders globally. Among other things, the company's transport flows were affected in several ports, leaving large cargoes of containers stranded. NotPetya is believed to have entered Maersk's network via a single computer in an office in Ukraine on which the M.E. Doc software had been installed. From there, the malware spread via the company's network to other systems all over the world.

35. The malware was known as NotPetya to connote its similarity (but at the same time major differences) to the ransomware Petya, which was discovered in 2016.

36. Commonly abbreviated to MBR.

When the motive of the attack is to benefit the antagonist

The motive of these types of attack is to benefit the antagonist or others on whose behalf the malicious action is carried out. As with the previously discussed motive, antagonists seeking to obtain undue benefits for themselves – by stealing sensitive information, for example – may use malicious actions targeted against or through digital supply chains. By gaining unauthorised access to a supplier's system, the attacker can either use trust-based channels to gain direct access to the real target's system, or manipulate the supplier's products or services to introduce threats or remove protection. When the product or service is subsequently installed or activated, the threat can remove, deactivate or block the real target's security measures, take control of affected systems, or send data directly to the attacker. Alternatively, the service or product may create a backdoor that can be used to access the system at a later date.

A malicious action against a supplier may mean that everyone who receives, installs or uses the manipulated product or service, not just the target, will also install the concealed threat, or at best will have a product or service with compromised security. This does, however, increase the likelihood that someone will swiftly detect and take measures to address the threat or security issue, which in turn jeopardises the attacker's ability to evade detection and access the resources it is seeking.

This motive and the last one, or sometimes a combination of the two, appear to be the most common motives for attackers.[37]

37. Based on what we can see in the incident reports that MSB receives regarding this field. It also seems to be consistent with other results from compilations and databases such as the Council on Foreign Relations' *Cyber Operations Tracker*; cf. https://www.cfr.org/cyber-operations/.

The malicious action against SolarWinds' digital supply chain

Type of digital supply chain incident: Delivery of something (a threat and an obstacle) that should not be delivered.

On 11 December 2020, the cybersecurity firm FireEye discovered that attackers had accessed and manipulated updates to SolarWinds' Orion software. Orion is a network monitoring and administration tool with a high level of privileges and access to its customers' IT environments. The software is widely used in large organisations and, at the time of the incident, it was used by hundreds of thousands of companies and government agencies around the world. FireEye's disclosure presaged the discovery of one of the most widespread malicious actions against digital supply chains to date, attracting unprecedented media coverage.

The first step in the malicious action was to gain access to SolarWinds' development environment (the information systems and software that SolarWinds employees use to input, modify and remove code in programs such as Orion). After some experimentation, and without being detected, the attacker managed to introduce malware the sole purpose of which was to add, at precisely the right moment, a custom-built package of malware (which later came to be called Sunburst). Completely unaware of the resulting changes to the code, SolarWinds developers followed their usual procedure for sending out an update – whereupon their customers started installing it.

As a result, some 18,000 customers received the update and thus also the malware. The malicious action was not, however, aimed at all of these customers, it was specifically targeted at US government agencies, and the fact that so many customers had received the malware increased the risk of detection for the attacker. Sunburst was designed to manage that risk; it initially lay dormant for two weeks from the time the code was installed on a system (probably to avoid drawing attention to how the malware got into the system in the first place), after which it cautiously checked to see whether certain security software was installed. If this software was found, Sunburst attempted to deactivate or incapacitate it. If the attempt proved unsuccessful, Sunburst deactivated itself. If Sunburst managed to circumvent the installed protection, the code then made a concealed attempt to contact an external server. Once contact was established, Sunburst sent data to the server about the system on which it was installed, thus allowing the attacker to determine whose system it was, or at least make a qualified guess as to who it might belong to. If the system did not belong to any of the intended targets, a command could be sent to Sunburst to uninstall itself – and this appears to have been the case on many occasions. However, if the system was of interest, Sunburst could be employed to introduce additional malware designed to carry out the espionage that had always been the objective of the malicious action.

Unlike NotPetya, the SolarWinds incident did not in itself cause harm or prevent benefit to those whose systems the malware was installed on. However, the data stolen by the attacker may have provided security-policy benefits. In addition, the need for incident management, investigations, replacement of compromised equipment and other aspects resulted in considerable expense to affected organisations.

When the antagonist's intention is to prevent harm

The motive of these types of attacks is to prevent harm to thus actions that cause both types of incidents in supply chains; i.e., incidents in which something that should not be delivered is delivered and incidents in which something that should be delivered is not.

As demonstrated in the previous two sections, malicious actions against digital supply chains that result in the delivery of something that should not be delivered can be used by attackers to gain access to or directly harm the attacker's real target(s). This type of malicious action may be preferred by an attacker if the real target is deemed to be well-protected, if the supplier against whom the initial attack is launched has trust-based channels into sensitive systems belonging to multiple targets, or if the attacker wishes to undermine an existing function or capability of the real target.

Antagonists may also launch malicious actions that cause the second type of digital supply chain incident – i.e., that something that should be delivered is not delivered – in order to ensure that the real target cannot maintain production, develop new capabilities or services, or restore systems after an incident has occurred. Barriers to trade that affect strategic products such as specialised microchips are examples of incidents that bring production and innovation at affected receiving organisations to a standstill.

Preemptive US cyber operations aimed at protecting the 2020 presidential election

Type of digital supply chain incident: Delivery of something (a threat and an obstacle) that should not be delivered.

In the run-up to the United States presidential election of November 2020, US Cyber Command conducted a number of operations against Iranian, Russian and Chinese actors suspected of planning various types of operation to influence results.

One malicious action attributed to the US Cyber Command initiative was the elimination of large portions of the infrastructure that underpinned the botnet TrickBot[38], which could have been used to cripple online election equipment or the IT systems that maintain essential services. The botnet was controlled from Eastern Europe and had been programmed by Russian-speakers. A particularly strong indicator that TrickBot was intended to interfere with the election was that the botnet had been equipped with surveillance features that could be used to spy on infected devices, thereby determining whether the device belonged to or was being used by, for example, an election official.

The malicious action against TrickBot was carried out by taking control of servers containing the botnet's control and monitoring systems, whereupon an update was sent out to the connected devices that made up the botnet. The update reprogrammed the malware installed on the devices to take commands from the device on which the malware was installed, instead of the servers that contained the botnet control and monitoring systems.

When the antagonist's intention is to hinder operations

The motive of these types of attacks may be to prevent benefits accruing to the target, or to others via the target. Like attackers driven by the previous motive, antagonists seeking to prevent their targets from accruing benefits[39], for example by halting an organisation's production of certain hardware, may use malicious actions that cause both types of digital supply chain incident.

38. A network of (at the time of the election) up to two million connected devices hijacked via intrusion and the installation of malware. The malware could have been, and had been, used to introduce ransomware directly into the hijacked devices. It is a relatively common practice among cybercriminals to specialise in various fields and share the profits of their criminal activity. The actor or group that created TrickBot specialised in conducting intrusions and establishing control from the inside. For the right price, this control could then be used by other parties who, for example, wanted to spy on users by copying and transmitting data from infected systems. It was also possible to use that control and the path it cleared to infect systems with additional malware, such as ransomware.

39. Although the motives for seeking to prevent benefits from accruing to a target and seeking to cause harm to a target are similar, they differ in as much as the former may, for example, cause the victim to lose income (i.e., a benefit they would otherwise have received), while the latter (in addition to potential lost income) causes the victim to incur higher costs as a direct consequence of the malicious action (rather than through the reactions it elicits, such as refund demands or claims for damages due to non-delivery). This distinction is important in some contexts, such as in analysing why certain organisations choose to pay a ransom in order to rid themselves of ransomware. In many cases, it is not the costs of restoring affected systems that make payment the better financial decision – but rather the revenue lost during the period in which the systems are down. Another important difference is that it is possible to commit a malicious action that prevents an organisation from accruing benefits by harming its suppliers and halting a necessary supply chain. In this situation, although the harm is initially inflicted on someone else, the end result is that the real target is prevented from accruing benefits, such as the profit from manufacturing products.

Antagonists may attempt to cause incidents in which something that should not be delivered is delivered, for example by implanting malware in a supplier's product in order to cause the real target to unwittingly instal the malware itself. Once the malware is installed on the real target's system, it can be activated to shut down infected systems.

Antagonists may also seek to cause incidents in which things that should be delivered are not delivered, with the result that the real target must reduce or shut down production or is unable to develop new features or recover from earlier incidents.

The malicious action against Kaseya's digital supply chain

Type of digital supply chain incident: Delivery of something (a threat and an obstacle) that should not be delivered.

On the evening of Friday 2 July 2021, Swedish supermarket chain Coop suffered major disruption to its cash register system (it was also reported that similar disruption had been suffered by others, including in the transport, fuel supply and pharmacy sectors). As a result of the disruption, supermarkets were unable to charge their customers. Approximately 800 Coop supermarkets in large parts of the country were forced to close for the day. It would later become apparent that other Swedish companies had also suffered disruptions in their payment systems.

The following day, it was confirmed that the disruption was caused by a ransomware attack. The malicious action was not directly targeted at the affected Swedish companies, nor was payment services provider Visma EssCom the actual target. In fact, the target of the malicious action was the Kaseya Virtual System Administrator (VSA), software used for the remote control, administration and operation of various online systems. The attackers breached Kaseya's internal network and inserted the ransomware into an update, which Kaseya subsequently distributed. When the update was installed by customers, including Visma EssCom, the ransomware was activated, after which it infected all devices in contact with the VSA; in Coop's case, their point-of-sale (POS) system.

Coop's stores remained closed for several days. Some 150 technicians had to be deployed to manually reinstall the POS system on-site in each of the company's supermarkets. The media reported that the supermarket chain lost millions of Swedish kronor as a result of the shutdown. As in the case of NotPetya and Intellect-Service, it later emerged that Kaseya and VSA were poorly protected having neglected their security.

Unintended threats to digital supply chains (human errors and system failures)

This section provides examples of human errors[40] and system failures have resulted in large-scale supply chain incidents. Thus far, the incident reports submitted by OES/DSPs and government agencies to MSB each year have shown that human errors and system failures cause more incidents (including serious incidents) than malicious actions.

While motive is a useful basis for analysing antagonistic threats, it is less suited to the analysis of threats associated with accidents and human error. When incidents are caused unintentionally, they often occur because people are trying to do the right thing but are misinformed or focused on the wrong things. For example, human errors can occur when there is an excessive focus on either not making errors (perhaps preventing the achievement of the effect that one intends to achieve) or achieving the effect one intends to achieve (thus failing to take into account all the side-effects that certain interventions may have). Unintended incidents can also occur when time and resources are insufficient or when an intervention is interrupted before it has been fully implemented.

A Google crash during the COVID-19 pandemic interrupted remote teaching

Type of digital supply chain incident: Failure to deliver something (a success factor or protection) that should be delivered.

On 14 December 2020, Google experienced an internal problem with the storage capacity of its authentication systems. As a result, several of the company's services that require users to log in became unavailable. The issue was caused by a compatibility error that occurred when parts of a system that handles requests during authentication were updated. The affected services – such as email accounts, calendars, maps and sharing, as well as data storage – are widely used by Swedish citizens and organisations. Although the disruption lasted for less than an hour, the impact on society was noticeable; for example, teaching was interrupted at several upper-secondary schools, as it was being conducted remotely due to the COVID-19 pandemic and was dependent on Google's affected services.

There is also a grey zone between malicious actions and human errors; actors may choose to focus on doing things that benefit themselves, even if this entails negative consequences for others (although the negative consequences are not in and of themselves the purpose).

In addition to incidents caused by deliberate actions that either have unfortunate consequences or benefit oneself while negatively affecting others, recklessness is also a common cause of incidents. System failures may also occur if, for example, one neglects the necessary maintenance of information systems and support systems to prevent wear and tear.

40. Failed interventions, see the analysis framework in the appendix *Analysis of Threats, Vulnerabilities and Risks in Digital Supply Chains*.

A fire in OVHcloud's data centre prevented access to millions of web pages

Type of digital supply chain incident: Failure to deliver something (a success factor or protection) that should be delivered.

Sometime after midnight on Wednesday 10 March 2021, about two per cent of all .fr domains, as well as pages from other domains – including government and public authority websites in several countries – suddenly became unavailable. In total, approximately 3.6 million websites went dark. The company acted quickly to re-establish affected web pages by providing service from other data centres. Still, it was not until Tuesday 6 April that 80 per cent of the capacity of the primary service provided by the affected data centre had been restored. While the company announced that the definitive cause of the fire would not be announced until sometime in 2022, several sources have suggested that the cause was careless maintenance work performed on the data centre's backup power system.

There are also unintended threats to digital supply chains that arise as a side-effect of conflicts. For example, complications in the supply of certain hardware or software components in the EU may arise as a side-effect of the trade restrictions the US and China impose on one another.

It is also important to remember that, while digital supply chains have a certain degree of dynamic capacity to meet changes in demand, there are still limits to how much capacity can be scaled up at short notice. This became clear during 2020/21, when demand for certain hardware products first fell and then increased sharply, due in part to the global pandemic. The transitional difficulties affected both manufacturers and (global) logistics operators. In the case of the latter, a kind of global queue formed when ports did not have the capacity to receive containers and deliveries from all calling vessels. As a result, manufacturers have had to wait to have their products picked up, which in turn forced them to keep their production rates low or eventually pay to warehouse units they had already manufactured pending shipment. This led to increased costs and long waiting times for certain hardware products, in addition to the delays caused by incidents of various kinds.

Threats or vulnerabilities in basic design or new functionality

Even small human errors that occur in the production of the products and services delivered within the framework of a digital supply chain can have far-reaching consequences. When an incorrect configuration (a threat) is implemented in software or hardware that is then mass-produced, the effects will be seen simultaneously in many devices that have that configuration. If the incorrect configuration has tangible consequences for the software or hardware in which it is located, and if organisations that acquire the software or hardware do not also have access to or a supply of other software or hardware that can be used for the same purpose, this can be highly problematic.

Approximately 1,000 of Region Västra Götaland's computers crashed in 2019

Type of digital supply chain incident: Delivery of something (a threat and an obstacle) that should not be delivered.

In the autumn of 2019, the hard drives of about one thousand of Region Västra Götaland's computers crashed over the course of a few weeks. The computers were of the same brand and it later emerged that they had probably been wrongly configured from the beginning, so that after a certain number of hours of use they would stop working. As Region Västra Götaland is the regional health authority, this placed many healthcare professionals in a difficult situation, including being unable to access digital health records and other data on the network. Some facilities were forced to increase staffing to ensure that adequate care could be provided until the problem could be solved.

The same or similar problems can arise when new functionality needs to be established in pre-existing software and hardware, for example in connection with updates that include malware or when new, insufficiently protected (and therefore vulnerable) features are added.

Vulnerabilities in Microsoft Exchange email servers in 2021

Type of digital supply chain incident: Failure to deliver something (a success factor or protection) that should be delivered.

In early 2021, a number of previously unknown vulnerabilities were discovered in locally installed (i.e., not remotely installed by external actors) Microsoft email servers. These vulnerabilities meant that unauthorised actors could take control of the email server and obtain high-level permissions. Organisations that had set up their own local email servers by installing Microsoft software had thus received email servers that were insufficiently protected against certain forms of requests.

It was not long after the vulnerabilities were discovered that malicious actions exploiting these vulnerabilities were detected. However, it should be noted that while the "introduction" of vulnerabilities by organisations that set up local email servers with the support of Microsoft Exchange was a supply chain incident, the malicious actions were not, as they were directly targeted at the actors who had the vulnerability, rather than going through Microsoft and on to the intended victim via a trusted channel.

Unsuccessful change management and system failures in services or information flows

In addition to digital supply chain incidents that occur in connection with the supply of new software, hardware, or updates, unintended human errors and system failures cause incidents in services that are continuously provided within the framework of digital supply chains. This is very common among OES/DSPs, for example when a subcontractor is hired that delivers medical record, alarm or sensor systems to many actors at the same time. When things go wrong in connection with maintenance or development work, or when the systems are inadequately maintained (so that they wear out, are not made compatible with new systems, or become overloaded) and incidents occur, they affect many actors at the same time.

The reason why digital supply chain incidents caused by human errors are reported so frequently can generally be explained by three factors: the large number of organisations that subcontract operations and support functions, the relatively limited number of subcontractors, and the relative frequency with which subcontractors experience incidents. These three factors interact in such a way that most subcontractors (possibly with the exception of a few smaller actors in the market) each have many customers, which is why many organisations are simultaneously affected every time the subcontractor experiences an incident that has repercussions on the service they provide. This, in turn, means that many organisations are simultaneously affected by an incident that they have a duty to report. So, if the subcontractor has a number of incidents each year, those incidents will quickly dominate the statistics.

Software updates to CDN services provided by Fastly and Akamai prevented access to media services and government and global corporate web pages

Type of digital supply chain incident: Failure to deliver something (a success factor or protection) that should be delivered.

On Wednesday 12 May 2021, content delivery network (CDN)[41] provider Fastly implemented a software update in its service that contained a bug that, in the event of a specific type of interaction with a customer system, could trigger an outage in the entire company's service. On the morning of 8 June, precisely such an interaction occurred. On the evening of 21 June and the afternoon of 22 July, the CDN provider Akamai carried out similar work. The resulting disruption to each service had global repercussions, making websites and services using Fastly's and Akamai's CDN services unavailable. The effects of this lack of availability were that companies and government agencies that lacked backup solutions could not provide their services and that, for example, media became difficult to access. While Fastly's incident and Akamai's first incident lasted about half a day, Akamai's later service interruptions were significantly shorter.

41. A content delivery network (CDN) is a geographically dispersed network of servers and other information infrastructure used to simultaneously provide web services requested from different parts of the world in the vicinity of the regions from which the requests originate, thereby shortening response times and reducing the load on a particular domain. The CDN service is generally provided by an actor that collectively controls, maintains and provides the service to a large number of customers worldwide. The governance and maintenance of the entire CDN service's aggregated information infrastructure is centrally managed, which is why an error associated with reconfigurations or updates can knock out the entire CDN service at the same time, thereby also affecting all the organisations that use the CDN service.

Natural phenomena threats to digital supply chains

Some digital supply chains are based on ongoing deliveries of, for example, microchips or semiconductors from a limited number of producers, who in turn manufacture their products in a small number of production centres. Such centres must themselves fulfil extensive requirements, but the environment must also meet specific needs. For example, the manufacture of many hardware components demands that humidity, temperature and other factors be highly stable. Production also requires large amounts of electricity and water, which in turn are drawn from resources in the surrounding area. Furthermore, the water used must be very clean, as the presence of even minute quantities of radioactive particles can affect the sensitive silicon structure of a semiconductor. Since the success of the production process demands such great precision, production becomes sensitive to factors such as earthquakes. This means that many natural phenomena also threaten the digital supply chain.

An earthquake in Ibaraki, Japan halted the production of Renesas' chips

T***ype of digital supply chain incident: Failure to deliver something (a success factor or protection) that should be delivered.***

On Saturday 13 February 2021, an earthquake struck Ibaraki, Japan. The prefecture is home to a factory owned by the Renesas Semiconductor Manufacturing Co., Ltd. The earthquake led to power outages, which in turn interrupted chip production. The plant may also have suffered damage. The same factory was also affected by the catastrophic 2011 earthquake that caused the Fukushima Daiichi Nuclear Power Plant to suffer a meltdown. On that occasion, the factory's main building was destroyed and it took three months to get production back up and running.

As climate change progresses, extreme weather events are expected to become more frequent. Heatwaves, which are expected to become more common in some places, create greater demand for cooling, putting pressure on the electricity supply and district cooling to levels that cannot always be met at short notice. Cold weather and snowstorms, which are also expected to become more common in certain regions, create sudden demand for more energy that the electricity grid is not always able to meet. This means that priorities must be set, channelling the limited electricity to essential societal operations (and sometimes to residential heating), thus disrupting industrial production. Once production has been interrupted, it takes a long time to restart the process, which includes hundreds of steps that must be precisely followed in a strict order.

A Texas snowstorm brings Samsung, NXP and Infineon microchip production to a standstill

Type of digital supply chain incident: Failure to deliver something (a success factor or protection) that should be delivered.

In February 2021, freak whether conditions in North America saw unusually low temperatures, snow and ice reaching far further south than usual. The weather system covered much of the continent and covered Texas in snow for at least a week, with temperatures well below normal. The storm caused major damage in a state where such phenomena are very rare and preparedness to deal with such events was not fully developed.

As a consequence of the storm, the power grid was rapidly overloaded, with the result that many industrial operations had to be shut down or suspended, including production at chip manufacturers NXP, Samsung (where the outage lasted more than a month) and Infineon (where production capacity was expected to be restored by June 2021). In March 2021, about one month into the production stoppage, NXP announced that there were several reasons for the shutdown: the electricity shortage had lasted for some time after the storm had passed; it was necessary to analyse whether the storm had caused any damage to the plant; the start-up of production had to be conducted in a controlled manner; and the handling of the situation had to take the pandemic and applicable restrictions into account. The company estimated its losses due to the storm and the ensuing production shutdown at $100 million.

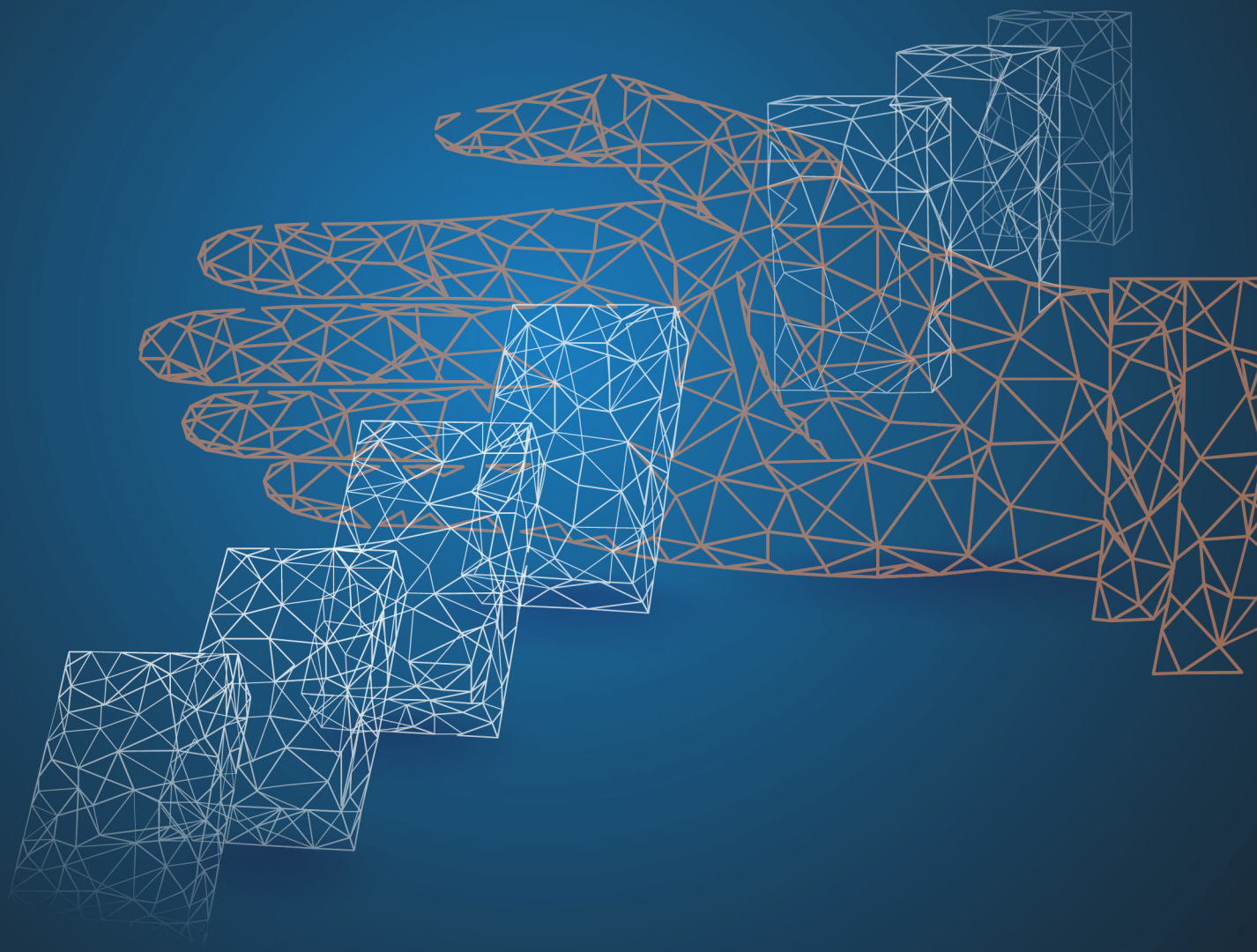
At the same time, the production of hardware components requires large amounts of water that is collected from the surrounding area. The need for water makes production sensitive to any reduction in precipitation reaching the watercourses from which the water is drawn, but it also means that production needs may be in competition with other needs for water.

In Taiwan, the failure of monsoon rains led to water shortages and drought, as well as production problems for the Taiwan Semiconductor Manufacturing Company (TSMC)

Taiwan has had no monsoon rains since 2020, despite historically being one of the world's wettest places. The drought has forced the government to implement strict rationing measures, with the result that many businesses, including in the agricultural sector, have had to cut back or suspend their operations.

Thanks to TSMC, the country accounts for approximately 90 per cent of the world's total production of certain forms of advanced microchips. The company needs copious amounts of water for its production. In 2019, its facilities in Taiwan consumed 156,000 tonnes of water per day. Although much of the water can be reused, this massive demand means that significant proportions of the island's water resources must be allocated to TSMC if production is to continue there.

Taiwan has been classified as a high-risk area in terms of the undesirable effects of climate change, and shortfalls in expected precipitation may thus become increasingly common.



Consequences for societal security

Consequences for societal security

Incidents in organisations' information systems can lead to serious consequences and necessitate extensive management efforts by both individual organisations and within and between states. In this chapter, we analyse the consequences at the three levels specific to digital supply chain incidents.

Consequences for OES/DSPs and other organisations

When something that should not be delivered is nevertheless delivered

Nowadays, most organisations use digital supply chains. Common to all such supply chains is that receiving organisations generally strive to achieve maximum efficiency in delivery management by limiting the extent to which they inspect and test what is sent to them within the framework of the digital supply chain. Organisations will usually start using deliverables as quickly and as widely as possible once they have been delivered. To minimise the time between receipt and application, there is often a prepared channel into the organisation. This is especially true of software updates. Receiving organisations establish such a channel both when they trust the delivering and shipping organisation(s), and when delays in application or narrow application may result in the loss of the benefits that the procured product or service is intended to generate. If, for example, a deliverable contains malicious code that causes harm or prevents benefit, the effects of that code can materialise in several parts of the organisation at the same time.

In the case of certain software delivered via digital supply chains, such as security updates to software that has already been installed, organisations are generally advised to carry out installation as quickly and as widely as possible. The reason for this is that the organisation that produced the update has discovered, or has been made aware of, a vulnerability that needs to be patched or a threat that needs to be blocked. While it is generally appropriate to instal security updates without delay, this means that if malware is present in the update, the update may undermine security in certain cases while enhancing it in others. The pressing need to quickly fix a known vulnerability or threat,

combined with the relationship of trust between the provider and the recipient of the update, makes trusted software update providers an attractive target for attackers. This is especially true if the provider delivers updates to several or many of the attacker's intended targets.

There is also an inverse problem with security updates. If such an update is made generally available, it can be downloaded by anyone, including malicious actors. In some cases, if such actors have good knowledge of reverse engineering, they may analyse the code in the security update in order to infer what vulnerability the update is designed to protect against.[42] Having done so, they can create a malicious attack method that exploits the vulnerability, possibly in the form of a software application. As a result, organisations that wish to avoid becoming victims of malicious actions are under a great deal of pressure to install security updates immediately, because the risk of a malicious action that exploits the vulnerability that the security update is designed to address increases when the security update is released.

Security software presents a similar challenge. In order for an organisation to be able to develop protection against new forms of malware, it must be granted access to monitor and collect data in many of the most sensitive parts of an information system. The data it collects must then be transmitted back to the organisation for analysis and, if malware is detected, the development of a method for blocking, deactivating or removing the malware. Such organisations may therefore have access to sensitive systems and data that are worthy of protection. If, however, the organisation providing the service leaks data that come into its possession – whether by its own volition, by mistake or through a malicious action, or is forced to do so by someone else (such as the state where it is based) – a service intended to enhance security can be used to undermine it.

The consequences for the confidentiality, integrity and availability of data of undesirable content in hardware or software depends on the nature of that undesirable content. Malicious content can lead to direct consequences for:

3. **Confidentiality.** Unauthorised persons gain control of an information system or data are copied and passed on to unauthorised persons.
4. **Integrity.** Information systems are reconfigured to behave differently than expected, data sets are altered so that they convey other information or cannot be trusted.
5. **Availability.** Authorised persons lose control of an information system[43] or data becomes inaccessible to those authorised to access it.

42. A vulnerability is defined as the lack of something that prevents, or helps prevent, an incident. A protection is defined as something that prevents, or helps prevent, an incident. A protection therefore replaces a vulnerability. See the appendix *On the Analysis Digital Supply Chain Incidents* for more information about the report's terminology and analytical methodology.

43.As happened during the incident that affected Region Västra Götaland described earlier in the report.

The malicious content can also lead to indirect consequences when it blocks, deactivates or removes protections that have previously prevented undesirable events, whereupon malicious actions or human errors may result in the occurrence of such events.[44]

It is important to note that the ways in which organisations process deliveries within the framework of their digital supply chains may undermine some of the protections they have implemented. Organisations may, for example, have segmented their internal networks and chosen never to locate all their sensitive data in a single segment of the network. However, if instances of a software update containing malware are installed simultaneously in several or all of those segments, each instance can separately copy and pass on sensitive data contained in each segment.

Many of the most high-profile malicious actions in recent years have relied on leveraging the relationships of trust on which digital supply chains are based. When demands for efficiency lead organisations to expose themselves to their suppliers, it presents an enticing path into sensitive systems – especially for attackers who have an interest in penetrating many organisations and are grappling with the gradual overall development of cybersecurity. In the worst cases, the consequences can be extremely costly. In the wake of NotPetya, for example, Maersk incurred costs running to hundreds of millions of dollars as a result of destroyed equipment and major disruption to its operations. Similarly, other ransomware attacks have cost organisations a great deal of money, whether through the payment of high ransoms, temporary production stoppages, or damage to their brand.

The Kaseya incident originated with a supplier to Coop's payment system provider. Visma EssCom's payment service was based on software supplied by Kaseya. This shows how difficult it can be to gain a well-founded understanding of just how exposed one's organisation is. When the service provided by the first organisation is a component of a second organisation's service, and thousands of organisations depend on the second organisation's service, a malware infection in the first organisation's service (a service organisations further down the chain from the second organisation may not even know exists) will strike all or nearly all of the organisations dependent on the second organisation, immediately and unhindered.

When something that should be delivered is not delivered

Digital supply chains can be divided into four types: hardware, software, services, and data.

The first type of supply chain is subject to all the challenges of modern logistics chains. Organisations generally do not stock hardware for their information systems, relying instead on just-in-time deliveries. In many cases, it makes little sense to stock hardware components either, given the risk that they will be obsolete and incapable of meeting the organisation's needs when the time comes to take them out of storage and instal them. When it comes to the second type of supply chain, organisations with efficient operations management often have a form of warehousing, in the sense that they have backups and other

44. As in the case of the malicious action against SolarWinds described earlier in the report.

solutions that enable the recovery to previous, and stable, versions of software. However, such recovery capabilities do not solve problems arising from digital supply chain incidents of this type, because it is not new copies of the exact same software that need to be delivered, but rather new versions of the software, or completely new software with added functionality or security features that previous versions lacked.

The effect of disruptions in digital hardware or software supply chains may be that the organisation that should have received the hardware components or software must reduce or shut down its production, processes or provision of services, that new functions that were supposed to be introduced cannot be introduced, or that incidents that require the installation of new components continue instead of being remedied. The problems can be especially great if the disrupted delivery relates to something on which the organisation has a monodependency. Organisations that rely on continuous supply (in the form of a service or information flows) in real time via digital supply chains are particularly vulnerable to this – and at the same time disruptions to essential services caused by digital supply chain incidents that continuously deliver a service or data in real time are among the most common incidents in the reports received by MSB.

Hardware and software can also be delivered in an incomplete form. This may mean that hardware or software are delivered but do not contain all the components or functions that they should have, or are incorrectly configured. The consequence of implementing such hardware or software may be that an organisation mistakenly believes that is protected from human errors and malicious actions that may lead to the kind of consequences for the confidentiality, integrity and availability of data described in the previous section.

In many ways, the results of shortcomings in the delivery of services or data are similar to those that occur in the event of disruptions to the delivery of software or hardware. When a disruption occurs in the delivery of a service, the functionality or protection that the service is supposed to provide ceases. When an information flow is interrupted, systems and functions that need information delivered through that flow will either not work at all, or (for example) will not work in accordance with the latest instructions. For example, if an antivirus program is not supplied with the threat signatures it should be looking for, the software will continue to look for threats whose signatures it has already received, but not for new threats whose signatures would have been delivered if the flow worked as it ought to.[45]

The telephone game problem and uncertainty

Since many organisations may constitute the links in a digital supply chain, the *telephone game* problem may also arise. This means that information that is established and passed on by an organisation far "upstream" in the chain is gradually reinterpreted, augmented, edited and forwarded to organisations downstream. This often occurs in such a way that the information that was originally passed on is not the same information that reaches organisations a few links further down the chain.

45. Or at least threats that function in a dissimilar way to threats with which the software is already familiar.

Such problems are repeatedly seen in NIS reporting. A typical example is that an operator of an essential service (OES) rents a sensor service from another organisation. The organisation that provides the sensor service (the sensor provider) in turn hires a service from a third organisation (the data transfer provider) to transmit data from its deployed sensors to the OES. The data transfer provider in turn has an agreement with a fourth organisation (the infrastructure provider) to use its infrastructure. If the infrastructure provider is affected by an incident, that organisation may report it to the data transfer provider. The data transfer provider interprets the data it receives, after which it writes its own incident report, which it forwards to the sensor provider. The incident report consists of an interpretation of the infrastructure provider's information, as well as certain additions about what the incident means for the data transfer provider. In addition, some information in the infrastructure provider's report to the data transfer provider has not been included in the report prepared by the data transfer provider. When the sensor provider receives its report from the data transfer provider, the same thing happens again, after which the OES eventually receives a report from the sensor provider. When this happens, the information received by the OES may be radically different, and at worst contradictory, to that which has been conveyed earlier in the chain.

The telephone game effect can make it difficult for organisations to make informed decisions about how to react when incidents occur, or give them an incorrect picture of what needs to be done. For the same reason, it can also lead organisations to make bad decisions.

Aside from the problem that the telephone game may gradually distort information as it passed along the chain, it is also by no means certain that the first actor in the chain will necessarily share the information that subsequent actors need, especially in the case of actors a few links down the chain. If information sharing is not subject to statutory requirements or some other formal system-wide regulation, it is generally only regulated in contracts between an actor and its immediate neighbours upstream and downstream. In some cases, an actor will have included clauses in contracts with neighbours in the chain requiring them to impose certain information sharing requirements on their own suppliers. Still, it is difficult to require that another actor imposes its own requirements in a way that ensures that additional requirements continue to be imposed further along the chain. If the actor needs information from an actor beyond its immediate neighbours and its neighbours have not agreed to share such information, the prospect of obtaining it is entirely dependent on goodwill between those involved.

As digital supply chains grow longer and have more and more branches, it becomes increasingly difficult (and, ultimately, practically impossible) for organisations far "downstream", acting on their own initiative to gain insight into and understand the threats they face, what their vulnerabilities are and what dependencies they have, and just how strong those dependencies are. This is partly because such investigations become increasingly resource-intensive the more complex and long supply chains become, and partly because actors covered by such investigations are not necessarily prepared to share information.

Consequences for states

Digital supply chain incidents have huge potential for negative societal impact. The overall impact on society depends on what the incident consists of; the installation of malware that causes a data leak has certain consequences, while a production delay due to a lack of components has others. The overall impact also depends on contextual factors, of which the following are particularly important:

1. How many organisations use the same digital supply chain.
2. How many of those organisations are vital to the national economy or the economies of individual regions.
3. How many of the organisations are operators of essential services.
4. How many organisations or individuals are in turn affected by the impact to essential services.
5. Whether the organisations and people that normally use these services have alternatives.

When something that should not be delivered is nevertheless delivered

Digital supply chains often operate on a "one-to-many" principle; many instances of a single product, such as a software update, are sent to or downloaded by many organisations at the same time. The effects of, for example, malware being conveyed through digital supply chains and then installed at the receiving organisations[46] can thus be very widespread. In addition to the factors listed in the previous section, the number of organisations that[47] install harmful software or components within a short period of time is particularly crucial.

In such a situation, many organisations will potentially require support to deal with the incident and restore their systems. This involves the additional risk that a heavy burden will be placed on societal support functions such as the Computer Emergency Response Team (CERT) and Computer Security Incident Response Teams (CSIRT), the emergency services and personnel performing vital societal functions and technical functions that maintain essential services (such as water and sanitary engineers, electricians, etc.).

When something that should be delivered is not delivered

There are two variants of this type of digital supply chain incident: when hardware, software or data is not delivered at all; and when hardware, software or data is delivered in an *incomplete format*.

The first variant, if it proves prolonged, may force actors vital to the national or regional economy to reduce or suspend production or processes, potentially resulting in job losses if a solution to the problem does not materialise. If a large

46. Such as shutting down or losing control of information systems and the services they maintain, data leaks, etc.

47. That is, in many systems or network segments.

and centrally located actor suffers disruption to, for example, the supply of semiconductors, whereupon production is first reduced and then halted, that actor will not need components from other suppliers until production resumes. A disruption in the supply chain may therefore force a receiving organisation to suspend deliveries from other chains. Major actors are often at the centre of a regional cluster of subcontractors that supply them with components and services. The actor's need to reduce deliveries can therefore generate a negative cascade effect, the impact of which will be felt widely within a region. The consequences may be reduced tax revenues and increased welfare spending to deal with growing unemployment.

The second variant may mean that a piece of hardware or software lacks the functionality or protection that it should have. When such hardware or software is installed and used, problems may emerge when expected features or effects are found to be lacking or fail to arise. Another problem may be that many organisations install something that lacks protection, leaving them all vulnerable to malicious actions or human errors that they have no reason to expect will be harmful to them. For example, if many organisations install the same software updates at roughly the same time, many of them will share the same vulnerabilities. It is important to note that vulnerabilities or threats arising in systems – in conjunction with updates, for example – will not necessarily have consequences such as human errors or malicious actions that lead to extensive undesirable effects. In certain cases, the missing protection can be added or the identified threat can be removed or blocked before anything else happens. However, if a mistake or malicious action occurs and the protection that was lacking has not been added or the threat that was introduced has not been removed or blocked, the effects and consequences may be the same as those described in previous sections, including high costs and enormous strain on the various support functions called on to manage the incident.

Monodependencies

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

Sometimes, as in the NotPetya incident, a state's own policies and laws can cause incidents to be worse than they might otherwise have been. Forcing organisations to use a certain type of software (in the case of NotPetya, for tax accounting and business purposes), rather than allowing organisations to choose from a range of different programs that fulfil the same function, increases the likelihood that many of them will be simultaneously harmed when an incident occurs in the digital supply chain of the software they all use. This situation also increases the incentives for antagonists to use the digital supply chain to carry out malicious actions.

When something that should not be delivered is nevertheless delivered within the framework of a monodependency in which many organisations are entangled (as in the NotPetya incident) it means that extensive harm can occur within many organisations at the same time. Using NotPetya as an example once again, if a monodependency is concentrated in organisations within or tied to a particular state, that state may suffer many simultaneous and serious consequences.

When things that should be delivered are not delivered at all within the framework of a monodependency, it is impossible to avoid disruption to production or processes, remedy an incident, or develop a function by using an alternative solution. While monodependencies that are not statutorily enforced leave organisations free to investigate whether there are ways to deal with delivery disruptions through more extensive transitions, forced monodependencies may leave organisations with no choice but to wait for the disruption to deliveries to pass. If the disruption is prolonged, they may need to make cuts in their own organisation, which may lead to unemployment and other challenges.

International consequences

Digital supply chains are often global and involve deliveries across many national borders. For organisations, dependence on cross-border deliveries is a vulnerability, especially when it has a monodependency.

Particularly significant dependencies can have geopolitical ramifications. If a state sees that organisations within its borders that maintain essential services, or are crucial to the national economy, are dependent on digital supply chains emanating from one or more organisations in another state, this may affect that state's relationship with the other state. If the state receives indications that such deliveries are insecure or that, through human errors or malicious actions, deliveries along the digital supply chain may pose threats, lead to vulnerabilities or do harm, this may affect how that state views its relationship with the other state. Moreover, if the second state is disinclined to cooperate in strengthening security, or if the first state suspects that the second state may use the dependency for its own ends, this may also affect how the state views its relationship with the other state.

One example of such geopolitical ramifications is the US Federal Communications Commission's ban on the use of Kaspersky cybersecurity products by government agencies and defence industry organisations after the company was singled out as an enabler of Russian state-sponsored hacking. Another example can be found in the 5G field, where companies such as Chinese-owned Huawei and ZTE have been excluded from contracts to construct 5G networks in certain countries due to concerns that the companies are assisting Chinese intelligence activities[48] or that they could threaten to halt the necessary supply of new components for the maintenance or development of such networks[49] if the state where the network is located or organisations operating there act in a manner that China finds objectionable.

48. For example, components provided by the companies could contain code or subcomponents that read and pass on communications that pass through the 5G networks (a case of something that should not be delivered nevertheless being delivered), or such components could intentionally lack protection against certain types of malicious actions that could then be used to access the networks once they are established (an example of when something that should be delivered is not delivered).

49. An example of when something that should be delivered is not delivered.

Many countries regard the key components of digital supply chains, such as semiconductors and microchips, as strategic resources. When distrust arises about the security of the delivery of such resources from other states, states and associations of states may take steps to eliminate the dependence on deliveries from states whose intentions are suspect. A shortage of semiconductors and microchips in 2020 and 2021 led to broad discussions in the EU and US about the need to secure domestic production. President Biden sought $50 billion in US government investment, stating that "China and the rest of the world is not waiting"[50], while the European Commissioner for Industry and Entrepreneurship called the Union's stance "far too naïve and transparent" and asserted the need to double EU chip production. One important ambition of EU policy in this area is to foster innovation and research in order to strengthen the EU's long-term capacity to provide the services and products that are in demand and needed. Research funding will be used to develop the technologies and services necessary for secure digitalisation, but also to defend against identified risks and threats. In March 2021, the European Commission also presented a number of digitalisation targets for 2030, one of which was that European production of semiconductors should account for one fifth of global production.

Enormous investment is required to remain on the cutting edge and break the dependency on deliveries from mistrusted states. At the same time, market developments in the manufacture of products such as semiconductors have left fewer and fewer manufacturers able to compete. The repercussions of strategic choices in such industries can last for many years, and even a single misstep may make it impossible to regain a leading position once other actors that have made other choices gain the upper hand. Major investments in building up industries that can reduce dependence on global digital supply chains are therefore fraught with risk, and will not necessarily result in industries that can handle the competition unaided.

Moreover, particular focus can be placed on the political consequences when a state, or an actor in that state, is suspected or confirmed to have targeted a malicious action against a digital supply chain that adversely affects another state.[51] Furthermore, if the state suspected of having carried out a malicious action or of harbouring the perpetrators neither admits the malicious action nor contributes to resolving the incident or its causes, there may be major consequences for international relations. In the worst-case scenario, the affected state or states could view the event as an act of war.

50. The White House, 12 April 2021, *Remarks by President Biden at a Virtual* CEO *Summit on Semiconductor and Supply Chain Resilience*, link: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/12/remarks-by-president-biden-at-a-virtual-ceo-summit-on-semiconductor-and-supply-chain-resilience/ (retrieved 16.07.2021) and The White House, 31 March 2021, *fact sheet: The American Jobs Plan*, link: https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/ (retrieved 16.07.2021).

51. For example, as in the case of the malicious action against the SolarWinds supply chain.

On the Analysis Digital Supply Chain Incidents

Appendix 1: On the Analysis Digital Supply Chain Incidents

In order for the reader to be able to follow how we have comprehensively analysed threats, vulnerabilities, risks and incidents related to digital supply chains in the preparation of this report, and to enable the reader to conduct their own analyses, here we present the framework that we have used.

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

The concepts of the framework	
Incident: An undesirable event that has occured	**Risk:** An undesirable event that could occur
Success: A desirable event that has occured	**Chance:** A desirable event that could occur
Threat: Something that causes, or contributes to cause, an incident	**Vulnerability:** Lack of something that prevents, or contributes to prevent, an incident
Obstacle: Something that prevents, or contributes to prevent, a success	**Deficiency:** Lack of something that causes, or contributes to cause, a success
Success factor: Something that causes, or contributes to cause, a success	**Opportunity:** Lack of something that prevents, or contributes to prevent, an success
Protection: Something that prevents, or contributes to prevent, an incident	**Freedom:** Lack of something that causes, or contributes to cause, an incident

These concepts can be combined to deepen an analysis. For example, an event may become an incident when a threat or obstacle arises, or when a success factor or protection ceases (i.e., a deficiency or vulnerability "arises")[52]. Similarly, an event may be counted as a success if it eliminates a threat or obstacle (i.e., an opportunity is taken or freedom "arises"), or it creates a success factor or provides protection.

52. To the extent that a lack of something can be said to arise.

When we refer to a digital supply chain incident, we mean:

1. an event in which something that:
    a. should be delivered in the digital supply chain (a success factor or protection) is not delivered, or
    b. should not be delivered in the digital supply chain (a threat or an obstacle) is nevertheless delivered, and
2. the results of which have either an unplanned negative impact[53] or fail to deliver a positive impact[54] on the confidentiality, integrity or availability of information systems or the data contained therein.

The first kind of digital supply chain incident may involve a success factor or protection (such as a new software feature or antivirus signature in an update) not being delivered or, if it is delivered, not working correctly. The second type of digital supply chain incident, on the other hand, may involve the delivery of a threat or obstacle (such as a virus concealed in a software update or a limiting configuration in a component) that should not have been delivered.

For the purposes of this report, the term *software and hardware* threats refer to code, configurations, components or other things found in software or hardware that may cause, or contribute to, incidents. The term *software and hardware vulnerabilities* refers to code, configurations, components, or other things missing from software or hardware that could have prevented, or helped prevent, an incident from occurring.

MSB divides the causes of incidents into three main categories: human action, technical or system failure, and natural phenomena. Human action may have an antagonistic purpose, i.e., it is a malicious action or more colloquially an attack. Human action can also have various non-antagonistic ends. A human error is a human action, or inaction,[55] but there are also deliberate acts carried out with a motive other than causing an incident. Acts that are not human errors, but that have no antagonistic intent, include acting deliberately out of self-interest, even though one's actions may have undesirable consequences (for others).

Based on the definitions and the different ways in which human actions can result in digital supply chain incidents, the following framework can be used to analyse supply chain risks.

53. Such as when malware is installed in an information system due to a software update sent out within the framework of a digital supply chain.

54. Such as when a new component necessary to repair a broken information system is not delivered even though it is ordered.

55. A software supplier may make a programming error in the design, configuration or updating of a service or information system, or a hardware supplier may make an error when installing a component. It is reasonable to assume that this type of mistake is the most common reason why threats and vulnerabilities exist in today's software and hardware.

Malicious actions and interventions in digital supply	
Let us suppose that a transmitting organisation **T** that delivers a digital product **P** (**P** could be various types of hardware components, software updates, code libraries, data, etc.) to a receiving organisation **R**. Let us also suppose that there is an actor **A** (**A** can be the transmitting organisation **T**, any employee of **T**, some other organisation, etc.).	
A commits a successful malicious action against a digital supply chain if...	**A commits a failed intervention on a digital supply chain (a mistake) if...**
(1) **A** does something with **P** or with the infrastructure used to transmit **P** from **T** to **R**;	(1) **A** does something with **P** or with the infrastructure used to transmit **P** from **T** to **R**;
(2) **A** is not entitled to do what **A** does to **P**;	(2) **A** is entitled/is not entitled to do what **A** does to **P**;
(3) **A** does what **A** does to **P** for an antagonistic purpose;	(3) **A** does what **A** does to **P** for a non-antagonistic purpose;
(4) There is an incident in **P**'s digital supply chain in the form of something that should not be delivered (a threat or an obstacle) nevertheless being delivered; *or* something that should be delivered (a success factor or protection) is not delivered, and thus the confidentiality, integrity or availability of **R**'s information system, or of data in **R**'s information system, is adversely affected; *or* a positive impact on the confidentiality, integrity or availability of **R**'s information system, or data in **R**'s information system, which would otherwise have occurred, fails to materialise[56]; *or* an information system or data in an information system that would otherwise have been created is not created.	(4) There is an incident in **P**'s digital supply chain in the form of something that should not be delivered (a threat or an obstacle) nevertheless being delivered; *or* something that should be delivered (a success factor or protection) is not delivered, and thus the confidentiality, integrity or availability of **R**'s information system or of data in **R**'s information system, is/are adversely affected *or* a positive impact on the confidentiality, integrity or availability of **R**'s information system, or of data in **R**'s information system, which would otherwise have occurred, fails to materialise; *or* an information system or data in an information system that would otherwise have been created is not created.
(5) **A** achieves such effects, and only such effects, as were the purpose of what A did with **P** or with the infrastructure used to transmit **P** from **T** to **R**. (It is this condition that makes the malicious action "successful")	(5) A does not achieve the desired effect, or achieves effects other than those that were the purpose of what **A** did with **P** or with the infrastructure used to transmit **P** from **T** to **R**. (It is this condition that makes the malicious action "unsuccessful")

Of course, in addition to the two possibilities discussed in the table, unsuccessful malicious actions and successful interventions may also occur, both of which may result in an incident.

Please refer to the chapter "Threats to Digital Supply Chains" above for some examples of how some contemporary and high-profile incidents can be understood with the support of the model.

56. This condition means that an intervention or malicious action instead results in an incident in which one or more of the permissions described in the forthcoming tables "Impact on information systems" and "Impact on data in information systems" cannot be corrected, or in which new functionality in terms of confidentiality, integrity or availability cannot be created.

If an intervention or malicious action results in an incident of the type (4.1), what makes the event an incident may be the impact on the existing confidentiality, integrity or availability of information systems, or data in information systems. Examples of such impact (i.e., circumstances arising from the incident) can be found in the following two tables:

Impact on information systems		
Confidentiality	Integrity	Availability
Authorised users have been given too high a level of access permissions to an information system	Configurations have been added to an information system	Authorised users have been given too low a level of access permissions to an information system
Unauthorised persons are able to access an information system	Configurations have been altered in an information system	Authorised persons are unable to access an information system
Unauthorised persons have access to an information system	Configurations have been removed from an information system	An interruption has occurred in the existing access of authorised users to an information system
Information can be received from unauthorised users in an information system	Configurations in an information system have been made unreliable	Information cannot be received from authorised users in an information system
Information from unauthorised users can be processed in an information system	The information system does not execute the tasks it is supposed to execute	Information from authorised users cannot be processed in an information system
Information from unauthorised users can be sent in an information system	The information system executes tasks it is not supposed to execute	Information from authorised users cannot be sent in an information system
Tasks are executed at the request of unauthorised persons in an information system	The information system does not execute tasks it is configured to execute	Tasks are not executed at the request of authorised users in an information system
The information system can be configured by unauthorised users	The information system executes tasks it is not configured to execute	The information system cannot be configured by authorised users

Impact on data in information systems		
Confidentiality	Integrity	Availability
Authorised users have been given too high a level of access permissions to information assets	Data has been added to information assets	Authorised users have been given too low a level of access permissions to information assets
Unauthorised persons are able to access information assets	Changes have been made to the data in information assets	Authorised users are unable to access information assets
Unauthorised persons have access information assets	Data have been deleted from information assets	An interruption has occurred in the existing access of authorised users to information assets
Confidentiality has been compromised in other ways	Data in information assets have been made unreliable	Availability has been negatively affected in other ways
	Integrity has been negatively affected in other ways	

A collaboration between:

Swedish Civil Contingencies Agency

Co-financed by the European Union's Connecting Europe Facility

651 81 Karlstad Tel: +46 (0)771 240 240 **www.msb.se**
Publ.no. MSB1955, May 2022 ISBN 978-91-7927-265-4