International Cybersecurity Law Review (2023) 4:371–386
https://doi.org/10.1365/s43439-023-00097-8

The outcome efficacy of the entity risk management requirements of the NIS 2 Directive

Donald David Stewart Ferguson

Received: 11 May 2023 / Accepted: 2 July 2023 / Published online: 17 August 2023

Abstract The NIS 2 Directive (2022/2555) of the European Union (EU) identifies the cybersecurity risk management requirements for essential and important entities in EU member states. The principal question we address is, how effective are the cybersecurity risk management measures of the NIS 2 Directive against cyberattacks on essential and important entities in EU member states? It was observed, through statutory interpretation and cyber kill chain model analysis, that the cybersecurity risk management measures of the NIS 2 Directive may be significantly limited in their effectiveness against cyberattacks on essential and important entities in EU member states. The limited effectiveness is primarily due to the narrow scope of the cybersecurity risk management measures, including the lack of specific measures focused on the reconnaissance phase of a cyberattack.

Keywords Cybersecurity · Incident · Cyberattack · Cyber kill chain · Advanced persistent threat actor

1 Introduction

The European Union (EU) Directive 2022/2555 (NIS 2 Directive) seeks to lay down the minimum measures required to achieve a high level of cybersecurity across the EU [1, Arts. 1(1), 5]. The measures include the cybersecurity risk management measures required of essential and important entities (EIEs) across the EU, including entities in the energy, transportation, banking, finance, and health sectors [1, Arts. 1(2)(b), 2, 3, 21].

Donald David Stewart Ferguson
Masaryk University, Brno, Czech Republic

University of Göttingen, Göttingen, Germany
E-Mail: donald.ferguson@stud.uni-goettingen.de

The cybersecurity risk management measures are required to address cybersecurity incidents caused by system failures, human error, malicious acts, and natural phenomena [1, Art. 21(2), rec. 79]. Malicious acts, also known as cyberattacks, are particularly interesting among the causes of cybersecurity incidents, as they represent an intentional attempt to challenge the cybersecurity risk management measures of EIEs.

1.1 Principal question

The principal question to be addressed is, how effective are the cybersecurity risk management measures of the NIS 2 Directive against cyberattacks on EIEs?

1.2 Methodology

The principal question will be addressed through statutory interpretation, followed by model analysis using the modified Lockheed Martin cyber kill chain model of cyberattacks (mLM-CKC) [2, p. 6, 3].

The mLM-CKC has been selected for model analysis as it provides a framework for analysis of the outcome efficacy of cybersecurity legislation across the common tactical phases of a cyberattack [3, pp. 70–73]. The mLM-CKC is particularly relevant for an analysis of the NIS 2 Directive as the Lockheed Martin cyber kill chain, upon which the mLM-CKC is based, models cyberattacks by advanced persistent threat (APT) actors [4, pp. 1–2]; APT actors are particularly capable threat actors that may target and impact the EIEs addressed by the NIS 2 Directive [5–7, p. 4, 8, pp. 22–30, 9–15].

The model analysis will focus on the first four phases of the mLM-CKC: reconnaissance, weaponisation, delivery, and exploitation [3, pp. 70–73, 4, p. 4]. The first four phases have been selected as they are the threshold to a successful cyberattack. Once a threat actor has successfully completed these phases, the threat actor may establish an entrenched, agile position in the subsequent installation and command and control phases of a cyberattack, from which the threat actor may have a significant and persistent impact on EIEs [4, pp. 4–6].

2 Cybersecurity risk management requirements of EIEs

The NIS 2 Directive requires EU member states to ensure that EIEs take appropriate and proportionate technical, operational, and organisational measures to do the following:

1. manage the risks posed to the security of network and information systems that those entities use for their operations or for the provision of their services (the risk management requirement), and

2. prevent or minimise the impact of incidents on recipients of their services and on other services (the incident impact requirement) [1, Art. 21(1)][1]

2.1 The risk management requirement

European Union member state EIEs are required to manage the risks posed to the security of network and information systems which those entities use for their operations or provision of their services [1, Art. 21(1)]. The definitions of the terms "risk," "incident," and "security of network and information systems" in the NIS 2 Directive provide further clarity [1, Arts. 6(2), 6(6), 6(9)].

The term "risk" is defined in the NIS 2 Directive as "the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident" [1, Art. 6(9)]. An "incident" in turn is defined as "an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems" [1, Arts. 6(1), 6(6)]. The term "security of network and information systems" refers to "the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems" [1, Arts. 6(1), 6(2)]. In other words, the security of network and information systems is the ability of network and information systems to resist, at a given level of confidence, any incident [1, Arts. 6(2), 6(6)].

Considering these definitions together, the risk management requirement may be understood as follows: EU member state EIEs are required to manage the potential for an incident to cause loss or disruption in the ability of the network and information systems EIEs use for their operations or service provision to resist, at a given level of confidence, any incident [1, Arts. 6(2), 6(6), 6(9), 21(1)]. There are three observations about this interpretation that are particularly relevant to the principal question.

The first observation is that the risk management requirement has a narrow scope. The risk management requirement applies only to the impact of incidents on the ability of specific network and information systems to resist incidents [1, Art. 21(1)]. The specific network and information systems are those which EIEs use for their operations, or for the provision of their services, and may be a subset of the network and information systems that EIEs use [1, Art. 21(1)].[2] The risk management requirement applies to the impact of incidents on only one ability of those spe-

[1] The measures are required to address the physical and environmental security of network and information systems to protect such systems from incidents caused by system failures, human error, malicious acts, and natural phenomena [1, Art. 21(2), rec. 79]. The consistency of the measures with the requirements of the EU Resilience of Critical Entities Directive should be taken into account [16].

[2] The network and information systems outside of this subset may vary by the entity and may include, for example, the network and information systems EIEs use for entity finance purposes, which have access to financial resources of possible interest to threat actors, and the network and information systems EIEs use for research and development purposes, which contain trade secrets of possible interest to threat actors.

cific network and information systems, specifically the ability of those network and information systems to resist incidents [1, Arts. 6(2), 6(6), 6(9), 21(1)].[3] The risk management requirement does not explicitly apply to the impact of incidents on EIE operations or service provision or to the impact of incidents on the recipients of EIE services [1, Art. 21(1)]. This is important for outcome efficacy as, for example, a given incident may have a major impact on each of: the operations of an EIE, the services provided by an EIE, and the recipients of services provided by an EIE; but not impact the ability of specific network and information systems to resist incidents, and hence not fall within the scope of the risk management requirement [1, Art. 21(1)]. This is particularly relevant when we consider that the scope of the risk management requirement may be interpreted to refer to the current ability of EIEs to resist incidents. For example, an EIE with a very poor ability to resist incidents may not need to implement significant measures under the risk management requirement, as there may be a low potential for an incident to cause significant loss or disruption in that very poor ability to resist incidents.

The second observation is that EIEs are not required to manage the events that could lead to an incident, but instead are required to manage the loss or disruption caused by an incident that has occurred. This represents a significant departure from the approach to risk management under the NIS Directive, where risk management is focused on events that could lead to an incident [17, Arts. 4(7), 4(9), 14(1), 16(1)].[4] The observation is important for outcome efficacy under the NIS 2 Directive, since the risk management requirement under the NIS 2 Directive may be met by EIEs engaging in measures that do not prevent incidents but instead manage specific losses or disruptions caused by incidents that have already occurred.[5] Indeed, the risk management requirement does not explicitly require EIEs to prevent incidents [1, Art. 21(1)], although that was available to be explicitly required [1, rec. 78]. The word "prevent" is included in the same sentence as the risk management requirement, but only with respect to the incident impact requirement, and specifically with respect

[3] For example, an incident may compromise the security controls of network and information systems that EIEs use for their operations or for the provision of their services, in a way that impacts the ability of those network and information systems to resist the current incident and future incidents.

[4] The term "risk" is defined in the NIS Directive as "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems" [17, Art. 4(9)]. This would reasonably include events that lead to an incident. The definition of the term "risk" changed in the NIS 2 Directive to no longer refer to the events leading to an incident but instead to refer to the potential consequences, specifically losses or disruption, caused by an incident that has materialised: "'[R]isk' means the potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident" [1, Art. 6(9)].

[5] This reflects the practical reality that not all incidents can be prevented, and not all impacts of incidents can be prevented, but the impacts of incidents can be minimised. For example, the measures available to prevent a denial-of-service attack may take time to identify the attack compared to a legitimate high level of service use, and it may take time for the network and information systems impacted by the denial-of-service attack to adapt to prevent the attack from continuing, while concurrently allowing legitimate service use. During the identification and adaptation periods, the denial-of-service attack may impact EIE network and information systems, EIE services, and recipients of EIE services.

to the impact of incidents on recipients of EIE services and on other services [1, Art. 21(1)].[6]

The third observation is that the risk management requirement is stated using nonspecific terms, such as "manage," "resist," and "at a given level of confidence," which are not defined in the NIS 2 Directive and do not clearly contribute to outcome efficacy on literal interpretation [1, Art. 21(1)].[7] This may be illustrated by substituting these terms with other terms used in the NIS 2 Directive that are more specific and more clearly contribute to outcome efficacy, such as "minimise," "detect," "prevent," and "recover" [1, Arts. 6(5), 6(8), 11(3), 21(1), 23(7), 29(1), 32(4)(b), recs. 78, 86, 95, 110, 119–121]. For example, EIEs are required to minimise the potential for an incident to cause loss or disruption in the ability of the network and information systems they use for their operations and service provision to detect, prevent, and recover from any incident. While this is only an illustrative example, it identifies that the nonspecific terms "manage," "resist," and "at a given level of confidence" could have been replaced with more specific terms already present in the NIS 2 Directive that could more clearly contribute to the outcome efficacy of the risk management requirement. The same nonspecific terms are present in the NIS Directive risk management requirements, and the drafting of the NIS 2 Directive may have been an opportunity to provide more specific terms [17, Arts. 14(1), 16(1)].

2.2 The incident impact requirement

European Union member state EIEs are required to prevent or minimise the impact of incidents on recipients of their services and on other services [1, Art. 21(1)]. There are three observations about the incident impact requirement under the NIS 2 Directive that are particularly relevant to the principal question.

The first observation is that EIEs are not required to prevent incidents. EIEs are only required to prevent or minimise the impact of incidents [1, Art. 21(1)]. In other words, an EIE meets the incident impact requirement if, regardless of the number and severity of incidents they experience, they prevent or minimise the impact of those incidents on recipients of their services and on other services. Incidents that would not, on their own, impact the recipients of EIE services and other services, such as an extensive breach of confidential EIE data, are outside the scope the incident impact requirement.

The second observation is that EIEs are not required to prevent or minimise the impact of incidents on themselves, or with respect to their services [1, Art. 21(1)]. This represents a significant departure from the NIS Directive, where prevention and minimisation apply to the impact of incidents on the security of network and

[6] The word "protect" in Article 21(2) may appear to be equivalent to the word "prevent," but because Article 21(2) refers specifically to Article 21(1), the word "protect" in Article 21(2) should be interpreted in a manner consistent with Article 21(1), in which the risk management requirement does not require EIEs to prevent incidents [1, Arts. 21(1), 21(2), rec. 79].

[7] For example, with the term "resist," resistance may be present but can vary between a very low level of resistance and a very high level of resistance. Also, because resistance may refer to the effort to resist rather than to the result of that effort, a very high level of effort to resist may be present while resulting in very little effective resistance.

information systems used for their services, with a view to the continuity of those services [17, Arts. 14(2), 16(2)]. Under the NIS 2 Directive, EIEs are only required to prevent or minimise the impact of incidents on the recipients of their services and on other services. For example, an EIE may be completely prevented from offering their services due to an incident, but if they can substitute an alternative entity to provide similar services to recipients and other services, they may meet the NIS 2 Directive incident impact requirement.

The third observation is that EIEs are not required to both prevent and minimise the impact of incidents, but instead are required to either prevent or minimise the impact of incidents [1, Art. 21(1)]. This also represents a departure from the approach under the NIS Directive, where both the prevention and the minimisation of the impact of incidents are required [17, Arts. 14(2), 16(2)]. The consequence for outcome efficacy is significant. An EIE may fulfill the incident impact requirement under the NIS 2 Directive with measures that would never prevent the impact of incidents on the recipients of their services or on other services, but that could minimise impacts that have already happened to the recipients of their services and to other services. This is particularly significant because minimisation is relative to what can realistically be achieved in the context of the specific incident that has occurred. Once an incident has occurred, the measures available to meaningfully minimise the impact of the incident on the recipients of EIE services and on other services may be significantly limited. For example, there may be little that an EIE can do themselves to minimise the impact to recipients of their services from a breach of confidential service recipient data that may already be in the hands of threat actors.

2.3 Appropriate and proportionate measures

European Union member state EIEs are required to take appropriate and proportionate measures to meet the risk management requirement and the incident impact requirement [1, Art. 21(1)].[8]

The minimum set of appropriate measures are listed in the NIS 2 Directive, with provision for further clarification on their technical and methodological requirements in subsequent implementing acts [1, Arts. 21(2)–(3), 21(5)]. It is not explicitly stated which measures among this minimum set of appropriate measures apply to the risk management requirement and which measures apply to the incident impact requirement [1, Arts. 21(2)–(3)]. Some measures may appear to apply to the risk management requirement, such as policies on risk analysis, while some measures may appear to apply to the incident impact requirement, such as business continuity [1, Art. 21(2)]. It is important that EIEs do not have to guess which measures apply to each requirement, as there may be significant consequences to EIEs for lack of compliance with the minimum set of appropriate measures [1, Arts. 32(4), 32(5), 32(7)(b), 32(7)(c), 32(7)(e), 33(4), 34(1)–(5), 36].

The proportionality of the measures is to be based on an assessment of the size of the EIE, the exposure of the EIE to risks, the likelihood and severity of incidents

[8] This represents an improvement compared with the NIS Directive, in which proportionality is not included in the incident impact requirements [17, Arts. 14(2), 16(2)].

(including their societal and economic impact), the state of the art, relevant European and international standards, and the cost of implementation [1, Arts. 21(1), 25(1), 25(2), recs. 81, 82].[9] In the case of European standards, EIEs may be required by member states, or through delegated acts of the Commission, to use specific information and communication technology products, services, or processes certified under European cybersecurity certification schemes [1, Arts. 24(1), 24(2)]. The subsequent implementing acts identifying the technical and methodological requirements of the minimum set of appropriate measures are not explicitly required to address proportionality [1, Art. 21(5)].

There are two observations about appropriateness and proportionality that are particularly relevant to the principal question.

The first observation is that each of the minimum set of appropriate measures are stated broadly, and as such appear to contribute significantly to outcome efficacy; but, when interpreted within the narrow scopes of the risk management requirement and the incident impact requirement, the minimum set of appropriate measures may contribute significantly less to outcome efficacy. This may be illustrated by looking at the stated appropriate measure of incident handling.

Incident handling is defined in the NIS 2 Directive to include "any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from an incident" [1, Art. 6(8), rec. 78]. On literal interpretation, incident handling has two components, and incident handling may be seen to be present if only one of the two components is present. The use of the disjunctive "or" in the definition of incident handling separates the first component, which consists of actions and procedures aiming "to prevent, detect, analyse, and contain" an incident, from the second component, which consists of actions and procedures aiming "to respond to and recover from" an incident [1, Art. 6(8)]. The separation of the components is also apparent from the observation that the terms "detect, analyse, and contain" in the first component could be encompassed by the term "respond to" in the second component. One further observation of relevance of literal interpretation is that the use of the conjunctive "and" in the first component may be interpreted such that all of the terms "prevent, detect, analyse, and contain" are required to be included in the aims of the actions and procedures in the first component. This is relevant because neither the risk management requirement nor the incident impact requirement requires EIEs to prevent incidents, and as such may not require EIEs to apply the first component of incident handling [1, Arts. 6(2), 6(6), 6(8), 6(9), 21(1)]. The consequence is that only the second component of incident handling: actions and procedures aiming to respond to and recover from an incident, may be required of EIEs by the risk management requirement and the incident impact requirement. It is relevant to note that incident handling under the NIS 2 Directive also applies to other aspects of the NIS 2 Directive, such as the responsibilities of computer security incident response teams (CSIRTs), where the first component of the definition of incident handling may apply more clearly [1, Arts. 10(1), 21(2), recs. 42, 92, 102].

[9] The NIS 2 Directive provides significantly more clarity on proportionality than the NIS Directive [17, Arts. 14(1), 16(1), recs. 53, 57].

The second observation is that a significant portion of the minimum set of appropriate measures is necessary for the outcome efficacy of the risk management requirement and the incident impact requirement, but these measures are not sufficient on their own to contribute to the outcome efficacy of the risk management requirement or the incident impact requirement. For example, policies on risk analysis and information system security, policies and procedures to assess the effectiveness of cybersecurity risk management measures, and policies and procedures regarding the use of cryptography and encryption are each necessary for the outcome efficacy of the risk management requirement and the incident impact requirement, but they are not sufficient on their own [1, Arts. 21(2)(a), 21(2)(f), 21(2)(h), 21(2)(i)]. The mere presence of the policies and procedures, without implementation and testing, does not contribute significantly to the outcome efficacy of the risk management requirement or the incident impact requirement.

The next step is to augment the analysis of the principal question with model analysis of the common phases of a cyberattack.

3 Modified Lockheed Martin cyber kill chain model early-phase analysis

The mLM-CKC models the phases of a cyberattack [3, pp. 70–73, 4, pp. 4–5]. In the early phases of a cyberattack, the attack is planned by a threat actor (reconnaissance phase), the resources for the attack are prepared (weaponisation phase), and then delivered to target network and information systems (delivery phase), where they may be used to exploit vulnerabilities in targeted network and information systems (exploitation phase) [3, pp. 70–73, 4, pp. 4–5]. The threat actor may then install themselves in network and information systems (installation phase) in order to achieve an entrenched and agile position in targeted network and information systems (command and control phase), from which they can seek to achieve the objectives of the attack (action on objectives phase) [3, pp. 70–73, 4, pp. 4–5]. In the remaining phases of an attack, the damage from the attack is assessed (damage assessment phase), recovery from the attack is attempted (recovery phase), communication of the attack occurs to stakeholders (communication phase), evidence is gathered with respect to the attack (evidence-gathering phase), and legal action may be pursued in relation to the attack (legal-proceedings phase) [1, Art. 23, 3, pp. 70–73].

We will focus on the early phases of a cyberattack as they are often determinative of the outcome of the cyberattack: reconnaissance, weaponisation, delivery, and exploitation. The measures available to EIEs in each phase may reflect a variety of tactics, including detection, denial, deception, disruption, degradation, and destruction [4, p. 5]. The tactic of destruction of threat actor network and information systems will not be considered in the model analysis as it may be considered an illegal activity in the EU [1, rec. 57, 18, Arts. 3–8].

3.1 Reconnaissance

During the reconnaissance phase, threat actors identify and research EIEs [4, p. 4]. EIEs may seek to detect threat actor research, and where possible deny, disrupt, and degrade threat actor research [4, p. 5]. EIEs may also employ deception to limit the useful information that threat actors obtain during research of the EIE [4, p. 5, 19, p. 36].

Threat actor research of EIEs may assess a variety of sources, including publicly available information on EIE operations; publicly available information on EIE employees, vendors, partners, and customers; publicly available information on EIE vulnerabilities, which may include EIE vendor vulnerabilities; and information available in threat actor communities about an EIE [1, Arts. 6(15), 12(2), recs. 58–63, 20–22]. Threat actor research of EIEs may also be more direct, including the scanning of EIE network and information systems; the scanning of network and information systems connected to EIE network and information systems; contact with EIE employees, partners, and customers to gather information; and the use of EIE services [20–22]. Threat actor research may also focus on third parties that legitimately have security information about EIEs, such as security auditors used by EIEs, and regulatory authorities with extensive EIE inspection powers, including competent authorities and CSIRTs under the NIS 2 Directive [1, Arts. 10(3)–(4), 10(7), 11(1)(b), 11(1)(d), 11(3)(a), 11(3)(c)–(e), 12(1), 13(2), 13(3), 13(5), 14(4)(i), 14(5), 15(3)(a), 15(3)(c), 15(3)(e), 15(3)(f), 19(1), 19(5)–(6), 19(9), 21(1), 23(1), 23(4), 23(6), 23(8), 23(10), 27(2)(f), 30(1), 30(2), 31(3), 32(2), 32(10), 33(2), 33(6), 35(1), 37(1), recs. 18–19, 24–26, 30, 40, 42–44, 61–63, 67, 73–74, 87, 101, 105, 122, 123, 20].

The ability of EIEs to detect, deny, disrupt, and degrade threat actor reconnaissance and to engage in deception against threat actor reconnaissance is significantly limited. Threat actor reconnaissance activities may occur on sources of information that are not controlled by EIEs, and where threat actor reconnaissance occurs on sources of information controlled by EIEs, it may be difficult to distinguish a threat actor request for information from a legitimate request for information. EIEs may use denial to limit the information available to threat actors across a variety of sources, but auditing and disclosure requirements of EIEs, including those under the NIS 2 Directive, may limit denial as an effective tactic against threat actor reconnaissance [1, Arts. 11(3)(a), 13(2), 23(1), 23(4), 23(6), 23(8), 27(2)(f), 32(2), 33(2), recs. 18, 101, 122, 124]. Threat actor reconnaissance appears to be challenging for EIEs, but it is important to place reconnaissance in context.

Threat actor reconnaissance assists threat actor decisions on tactics, techniques, and procedures (TTPs) for the subsequent phases of an attack. EIEs have access to many of the same sources of information available to threat actors about the EIE (the EIE reconnaissance footprint), and have access to further information that is not readily available to threat actors, for example through vulnerability scanning of internal resources and penetration testing in depth [23, 24].[10] In addition, EIEs may

[10] Threat actors may perform deep reconnaissance into EIE network and information systems to identify these vulnerabilities, but that may increase their risk of detection.

anticipate the TTPs a threat actor may select by reviewing historical information on the TTPs that threat actors have used against the EIE (internal threat intelligence) and the TTPs used by threat actors against other entities (external threat intelligence) [1, Arts. 11(3)(a), 14(4)(c), 29(1), 29(2), recs. 57, 90, 119, 120, 8, 25, 26]. In symmetry with threat actors using the EIE reconnaissance footprint to make decisions on their TTPs for the subsequent phases of an attack on an EIE, the EIE may use their reconnaissance footprint, together with internal vulnerability scanning, penetration testing in depth, and internal and external threat intelligence, to anticipate, through the use of threat modelling, the TTPs likely to be selected by threat actors.

The risk management requirement of EIEs does not require EIEs to use the tactic of denial to limit the information available to threat actors about the security of network and information systems that EIEs use for their operations and service provision [1, Arts. 21(1)–(3)].[11] The risk management requirement also does not require EIEs to assess their reconnaissance footprint, perform vulnerability scans of internal resources, perform penetration testing in depth, review internal or external threat intelligence, or perform threat modelling with respect to the security of the network and information systems that EIEs use for their operations and service provision [1, Arts. 21(1)–(3)]. It is possible that these measures may be considered in future implementing acts.[12]

The incident impact requirement similarly does not require EIEs to use the tactic of denial in order to limit the information available to threat actors that could influence the impact of incidents on recipients of EIE services and on other services [1, Arts. 21(1)–(3)]. The incident impact requirement also does not require EIEs to assess their reconnaissance footprint, perform vulnerability scans of internal resources, perform penetration testing in depth, review internal or external threat intelligence, or perform threat modelling to limit the impact of incidents on recipients of EIE services and other services [1, Arts. 21(1)–(3)]. It is possible that these measures may be considered in future implementing acts [1, Art. 21(5)].

The observation that the risk management requirement and the incident impact requirement do not require EIEs to engage in reconnaissance measures is important for the outcome efficacy of the NIS 2 Directive. The reconnaissance phase is about relative information superiority to prepare for the next phases of an attack. EIEs have the intrinsic ability to be in a superior position with respect to the information available to prepare for the next phases of a cyberattack. If EIEs do not act on that ability by minimising the information available to threat actors about the EIE, while concurrently performing threat modelling on the basis of the EIE reconnaissance footprint, internal EIE vulnerabilities, and internal and external threat intelligence, then EIEs may be in an inferior position, relative to threat actors, with respect to the information necessary to prepare for the next phases of an attack. This is

[11] Policies on risk management and information systems security may provide for these measures but do not on their own provide these measures [1, Art. 21(2)(a)].

[12] The measures may extend from the requirement that appropriateness should consider the risks posed, the requirement that proportionality should consider the degree of EIE exposure to risks, and the inclusion of supply chain vulnerabilities in the minimum set of appropriate measures that EIEs are to implement [1, Arts. 21(1)–(3)].

particularly relevant to the weaponisation phase, where EIEs identify and prepare the appropriate and proportionate technical, operational, and organisational measures to address threat actor TTPs in subsequent phases of an attack.

3.2 Weaponisation

During the weaponisation phase, threat actors identify and prepare the resources to support their TTPs for the next phases of the attack [4, p. 4, 27]. The majority of threat actor weaponisation may occur beyond the visibility of EIEs, limiting direct EIE detection, denial, disruption, degradation, and use of deception to limit threat actor weaponisation [28]. If threat actors interact with EIE network and information systems during weaponisation, for example by testing resources on EIE network and information systems, the interaction may simulate the delivery and exploitation phases of an attack, which we will address subsequently.

In lieu of EIE visibility into threat actor weaponisation, EIEs may anticipate threat actor weaponisation through penetration testing, reviews of internal and external threat intelligence, and threat modelling. The absence of these measures from the risk management requirement and the incident impact requirement significantly limits the ability of EIEs to anticipate threat actor weaponisation [1, Arts. 21(1)–(3)]. EIE anticipation of threat actor weaponisation is important for outcome efficacy because during the weaponisation phase, EIEs identify and prepare the resources to address threat actor weaponisation and TTPs in the next phases of the attack. In particular, during the weaponisation phase, EIEs identify and prepare the appropriate and proportional measures to address the risk management requirement and the incident impact requirement [1, Arts. 21(1)–(3)]. The assessment of the appropriateness and proportionality of these measures by an EIE would require a strong understanding of the risks faced by an EIE, for example through penetration testing, reviews of internal and external threat intelligence, and threat modelling [1, Arts. 21(1)–(3), recs. 81, 82].

3.3 Delivery

During the delivery phase, threat actors attempt to obtain initial access to EIE network and information systems, and may deliver resources, such as malware, to EIE network and information systems [4, p. 4, 29–31]. EIEs may attempt to detect, deny, disrupt, degrade or use deception to limit threat actor initial access and resource delivery to EIE network and information systems [4, p. 5, 32–35].

Threat actor initial access to EIE network and information systems may occur through the use of valid credentials that threat actors obtain, for example in threat actor communities or through access to permissions that threat actors may leverage, such as through phishing, supply chain attacks, or direct network and information systems vulnerability exploitation [32–34].[13]

[13] Threat actors may also target EIE network and information systems indirectly in the delivery phase by first targeting network and information systems that may interact with EIE network and information systems [1, Arts. 21(2)(d), 21(3), recs. 85, 86, 36].

Threat actor initial access to EIE network and information systems and resource delivery to those systems do not, on their own, represent incidents under the NIS 2 Directive. They do not, on their own, compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or of the services offered, or accessible, by network and information systems [1, Art. 6(6)]. For example, a person entering an office and placing a bag on the floor of the office does not, on its own, lead to the person compromising the availability, authenticity, integrity, or confidentiality of information in the office or the services offered through the office. It is the acts subsequent to that which may, or may not, represent a compromise. The consequence of threat actor actions during the delivery phase not being considered an incident under the NIS 2 Directive is that the delivery phase may not be required to be addressed by the risk management requirement or the incident impact requirement.

A notable exception is the case of a denial-of-service attack, where the scale of initial access or resource delivery may exploit a vulnerability in network and information system scalability, leading to a compromise in the availability of EIE network and information systems [37]. Under the risk management requirement, EIEs would be required to manage the potential for compromise in the availability of EIE network and information systems to cause loss or disruption in the security of EIE network and information systems they use for their operations or provision of their services [1, Art. 21(1)]. For example, an EIE may implement incident handling measures, such as request throttling, to respond to and assist with recovery from a potential impact of compromise on the security of EIE network and information systems they use for their operations or provision of their services [1, Arts. 6(8), 21(2)(b)]. Under the incident impact requirement, EIEs would be required to prevent or minimise the impact of a compromise in the availability of EIE network and information systems on recipients of their services and on other services [1, Art. 21(1)]. For example, an EIE may implement business continuity measures to provide services to EIE service recipients and other services through alternative network and information systems [1, Art. 21(2)(c)].

3.4 Exploitation

During the exploitation phase, threat actors use initial access to EIE network and information systems, and potentially resources transferred to EIE network and information systems, to exploit EIE vulnerabilities [1, Art. 6(15), 4, p. 4].[14] EIEs may attempt to use detection, denial, disruption, degradation, or deception in order to limit threat actor exploitation of EIE vulnerabilities [4, p. 5, 32–34].

[14] Threat actors may have already engaged in exploitation of vulnerabilities in network and information systems of another entity, including outside the EU, to obtain access to EIE network and information systems, where they may seek to exploit further vulnerabilities. The exploitation of vulnerabilities at an entity outside the visibility and control of an EIE, but which facilitates threat actor access to EIE network and information systems, may be addressable by sharing threat intelligence and incident reporting on a timely basis within and outside of the EU [1, Arts. 4(2)(b), 10(7)–(8), 11(3)(a)–(b), 13(2), 13(5), 14(4)(c), 15(3)(c), 15(3)(f)–(h), 15(3)(n), 23(1)–(2), 23(4), 23(6)–(8), 23(10), 29(1), 29(2), 30(1)–(2), recs. 23, 24, 28, 30, 40, 57, 71, 72, 74, 90, 93, 94, 97, 101–103, 119, 120–121].

The exploitation of an EIE vulnerability will typically represent an incident under the NIS 2 Directive, as it will often compromise the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the services offered by, or accessible via, network and information systems [1, Art. 6(6), 38]. That is not sufficient, however, for the risk management requirement or the incident impact requirement to apply to the exploitation of an EIE vulnerability. The exploitation would, in addition, need to clearly have the potential to impact the security of specific EIE network and information systems in order to fall within the scope of the risk management requirement, or need to clearly have an impact on the recipients of EIE services and on other services in order to fall within the scope of the incident impact requirement [1, Art. 21(1)]. The exploitation of a vulnerability will typically focus on a discrete aspect of a network and information system, and as such will often have a limited initial impact within that network and information system [38]. The consequence is that the exploitation may not, at that point, clearly have the potential to impact the security of specific EIE network and information systems or the recipients of EIE services and other services. Further steps by a threat actor following the exploitation of a vulnerability may be necessary before the risk management requirement or the incident impact requirement would apply.

The observation that the risk management requirement and the incident impact requirement may only apply to threat actor steps following threat actor exploitation of an EIE vulnerability may reflect an appreciation of the realities that EIEs face. In particular, not all vulnerabilities known to threat actors may be known to EIEs, not all vulnerabilities are readily susceptible to remediation or mitigation by an EIE, and not all events during an act of exploitation of EIE vulnerabilities may be readily detectible as threats by an EIE.[15] The consequence, however, is that following exploitation of an EIE vulnerability, a threat actor may be in a strong position to have a significant impact on the security of EIE network and information systems, and a significant impact on recipients of EIE services and on other services.

Where the exploitation of an EIE vulnerability, on its own, clearly has the potential to cause a loss or disruption in the ability of EIE network and information systems used for operations and service provision to resist an incident, that is within the scope of the risk management requirement [1, Art. 21(1)].[16] EIEs may, for example, assert multifactor authentication to limit threat actor access within their network and information systems [1, Art. 21(2)(j)]. More advanced cyber hygiene practices focused on zero-trust architecture may also assist, including micro network segmentation, dynamic device configuration, dynamic identity and access management, and use of multifactor authentication on each access to a resource; but, these may not be considered among the basic cyber hygiene practices that EIEs are required to take [1, Arts. 21(2)(g), 21(2)(j), recs. 49, 89, 39, pp. 6–7].

[15] For example, "zero day" vulnerabilities are not known to EIEs, and vulnerabilities in third-party components used by EIEs—in particular, industrial control system legacy components—may not have fixes or workarounds readily available.

[16] Threat actors may target vulnerabilities in the security of network and information systems to compromise the ability of EIEs to detect, deny, disrupt, or degrade the subsequent phases of the attack.

When the exploitation of an EIE vulnerability, on its own, has a clear impact on recipients of EIE services and on other services, that is within the scope of the incident impact requirement [1, Art. 21(1)]. In particular, where the exploitation directly impacts the availability of EIE services, EIEs may engage in business continuity measures to minimise the impact on recipients of EIE services and on other services, for example through the use of redundant network and information systems [1, Art. 21(2)(c)].

4 Conclusion

The application of statutory interpretation and cyberattack model analysis indicate that the cybersecurity risk management measures required of essential and important entities under the NIS 2 Directive may be significantly limited in their effectiveness against cyberattacks.

The principle observation through statutory interpretation was that the cybersecurity risk management measures, comprised of the risk management requirement and an incident impact requirement, are not focused on the prevention of cyberattacks, but instead are focused on limiting the impact of cyberattacks on the ability of specific network and information systems to resist incidents and limiting the impact of incidents on recipients of their services and on other services. The consequence is that cyberattacks with serious, persistent impacts on essential and important entity network and information systems are permitted by the risk management requirement and the incident impact requirement, as long as they do not impact the ability of specific network and information systems to resist incidents or impact recipients of their services and other services.

The principal observation on cyberattack model analysis was that a threat actor may progress through the early phases of a cyberattack largely unhindered by the risk management requirement or the incident impact requirement. At that point, the threat actor may proceed to establish an entrenched, agile position in essential and important entity network and information systems, from which to have a significant, persistent impact on EU member state essential and important entities.

In particular, it was identified during cyberattack model analysis that the perspective of information superiority is important during the reconnaissance phase of a cyberattack. Essential and important entities may be significantly assisted in selecting effective, appropriate, and proportional measures under the risk management requirement and the incident impact requirement by engaging in the following measures during reconnaissance: assessment of their reconnaissance footprint, vulnerability scanning of internal resources, penetration testing in depth, reviews of internal threat intelligence and external threat intelligence, and threat modelling. These measures are not explicitly required by the risk management requirement or the incident impact requirement, and it is recommended that these measures be considered in subsequent implementing acts of the NIS 2 Directive.

Acknowledgements I am grateful to Katharina Margot Drescher, for research and review of drafts, and to Louis C. Ferguson, for review of drafts.

Funding This research was supported by the ERDF project "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (no. CZ.02.1.01/0.0/0.0/16_019/0000822).

Funding Open Access funding enabled and organized by Projekt DEAL.

Conflict of interest D.D.S. Ferguson declares that he has no competing interests.

References

1. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80.
2. Lenaerts K, Gutiérrez-Fons JA 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (European University Institute 2013). https://heinonline.org/HOL/LandingPage?handle=hein.journals/coljeul20&div=11&id=&page=. Accessed 24 Sept 2019
3. Ferguson DDS (2022) 'European Cybersecurity Certification Schemes and cybersecurity in the EU internal market.' Int Cybersecur Law Rev 3:51–114. https://doi.org/10.1365/s43439-021-00044-5
4. Hutchins EM, Cloppert MJ, Amin RM 'Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains' (Lockheed Martin 2010). https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. Accessed 19 July 2019
5. 'advanced persistent threat' (NIST CSRC). https://csrc.nist.gov/glossary/term/advanced_persistent_threat. Accessed 5 Mar 2023
6. 'Groups' (MITRE ATT&CK). https://attack.mitre.org/groups/. Accessed 5 Mar 2023
7. 'Threat Landscape Report Volume 1' (CERT-EU, 11 June 2021). https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf#page4. Accessed 5 Mar 2023
8. 'ENISA Threat Landscape 2022' (ENISA, October 2022). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/. Accessed 5 Mar 2023
9. 'JP-23-01—Sustained activity by specific threat actors' (CERT-EU, ENISA, 15 February 2023). https://cert.europa.eu/files/data/TLP-CLEAR-JointPublication-23-01.pdf. Accessed 5 Mar 2023
10. 'Russia Cyber Threat Overview and Advisories' (CISA). https://www.cisa.gov/russia. Accessed 5 Mar 2023
11. 'China Cyber Threat Overview and Advisories' (CISA). https://www.cisa.gov/china. Accessed 5 Mar 2023
12. 'Iran Cyber Threat Overview and Advisories' (CISA). https://www.cisa.gov/iran. Accessed 5 Mar 2023
13. 'North Korea Cyber Threat Overview and Advisories' (CISA). https://www.cisa.gov/northkorea. Accessed 5 Mar 2023
14. 'Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure' (CISA, 01 March 2022). https://www.cisa.gov/news-events/alerts/2022/01/11/understanding-and-mitigating-russian-state-sponsored-cyber-threats-us. Accessed 5 Mar 2023
15. 'Control System Defense: Know the Opponent' (CISA, 22 September 2022). https://www.cisa.gov/news-events/alerts/2022/09/22/control-system-defense-know-opponent. Accessed 5 Mar 2023
16. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJ L333/164.

17. Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.
18. Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8.
19. Heckman KE et al 'Denial and Deception in Cyber Defense' (2015) 48/4 Computer. https://ieeexplore.ieee.org/abstract/document/7085646. Accessed 7 Nov 2019
20. 'Reconnaissance' (MITRE). https://attack.mitre.org/tactics/TA0043/. Accessed 3 Jan 2023
21. 'CVE' (MITRE). https://cve.mitre.org. Accessed 3 Jan 2023
22. 'National Vulnerability Database' (NIST). https://nvd.nist.gov. Accessed 3 Jan 2023
23. 'CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks' (CISA, 28 February 2023). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a. Accessed 9 Mar 2023
24. 'Vulnerability Scanning' (MITRE). https://attack.mitre.org/mitigations/M1016/. Accessed 7 Mar 2023
25. 'CISA Analysis: FY2021 Risk and Vulnerability Assessments' (CISA, May 2022). https://www.cisa.gov/sites/default/files/2023-02/fy21-rva-analysis_508c_0.pdf. Accessed 9 Mar 2023
26. 'Threat Intelligence Program' (MITRE). https://attack.mitre.org/mitigations/M1019/. Accessed 7 Mar 2023
27. 'Resource Development' (MITRE). https://attack.mitre.org/tactics/TA0042/. Accessed 8 Jan 2023
28. 'Pre-compromise' (MITRE). https://attack.mitre.org/mitigations/M1056/. Accessed 8 Jan 2023
29. 'Initial Access' (MITRE). https://attack.mitre.org/tactics/TA0001/. Accessed 8 Jan 2023
30. 'Initial Access' (MITRE). https://attack.mitre.org/tactics/TA0108/. Accessed 8 Mar 2023
31. 'Initial Access' (MITRE). https://attack.mitre.org/tactics/TA0027/. Accessed 8 Mar 2023
32. 'Enterprise Mitigations' (MITRE). https://attack.mitre.org/mitigations/enterprise/. Accessed 9 Mar 2023
33. 'ICS Mitigations' (MITRE). https://attack.mitre.org/mitigations/ics/. Accessed 9 Mar 2023
34. 'Mobile Mitigations' (MITRE). https://attack.mitre.org/mitigations/mobile/. Accessed 9 Mar 2023
35. 'Weak Security Controls and Practices Routinely Exploited for Initial Access' (CISA, 08 December 2022). https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a. Accessed 9 Mar 2023
36. 'Protecting Against Cyber Threats to Managed Service Providers and their Customers' (CISA, 11 May 2022). https://www.cisa.gov/news-events/alerts/2022/05/11/protecting-against-cyber-threats-managed-service-providers-and-their. Accessed 9 Mar 2023
37. 'Joint CISA FBI MS-ISAC Guide on Responding to DDoS Attacks and DDoS Guidance for Federal Agencies' (CISA, MS-ISAC). https://www.cisa.gov/news-events/alerts/2022/10/28/joint-cisa-fbi-ms-isac-guide-responding-ddos-attacks-and-ddos-guidance-federal-agencies. Accessed 9 Mar 2023
38. '2022 CWE Top 25 Most Dangerous Software Weaknesses' (MITRE). https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html. Accessed 25 Mar 2023
39. Rose S et al 'NIST Special Publication 800-207: Zero Trust Architecture' (NIST, August 2023). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. Accessed 9 Mar 2023