ETSI TR 103 456 V1.1.1 (2017-10)

TECHNICAL REPORT

CYBER;
Implementation of the Network and Information Security (NIS) Directive

Reference

DTR/CYBER-0021

Keywords

cyber security, cyber-defence, information assurance, privacy

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document provides guidance on the available technical specifications and those in development by major cyber security communities worldwide designed to meet the legal measures and technical requirements relating to implementation of the NIS Directive, including the sharing of information and network based risks and incidents and necessary defence measures. The guidance includes: considerations for incident notification and best practices in cyber security risk management. The present document provides a broader cyber security context than the NIS Directive or the ENISA Standardization Gaps Report to facilitate evolution toward significant emerging open global platforms, and includes treatment of challenges associated with harmonizing the implementations across the diverse network and services sectors and Member State legal and operational environments.

Introduction

The Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 [i.1] concerning measures for a high common level of security of network and information systems across the Union (commonly called the NIS Directive or NISD contains legal measures which include:

- requiring Member States to be appropriately equipped, e.g. via Computer Security Incident Response Teams (CSIRTs) a competent national NIS authority for a number of sectors, and a national information security strategy;

- setting up a cooperation framework among Member States by means of a Cooperation Group, in order to support and facilitate strategic cooperation and the exchange of information among Member States, including and a CSIRT Network, for voluntary operational cooperation on specific cyber security incidents and sharing information about risks; and

- requiring Member States to provide the frameworks and necessary obligations on businesses in sectors identified by the Member States as operators of essential services, including those that operate in sectors identified in the Directive, as well as providers of certain digital services, are implementing appropriate security measures and notifying the relevant national authority of serious incidents having significant impact in their services.

These legal measures in turn invoke a set of common cyber security technical requirements that include:

- structured sharing of information on risks and incidents;

- notification of incidents;

- outcomes-focused cybersecurity risk management practices and controls to identify and protect assets, detect anomalous analyses and potential incidents, and respond to and recover from incidents that may impact network and information systems; and

- international cooperation to improve security standards and information exchange, and promote a common global approach to NIS issues through harmonised standards.

The present document provides implementation guidance for meeting these requirements based on ETSI's capabilities as a regional and global organization that brings together industry expertise and global cyber security knowledge, including its own cyber security technical specifications and report.

1 Scope

The present document provides guidance in accordance with the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 [i.1] concerning measures for a high common level of security of network and information systems across the Union (commonly called the NIS Directive or NISD) on the available technical specifications and those in development by major cyber security communities worldwide designed to meet the legal measures and technical requirements relating to the sharing of information on network based risks and incidents and also the necessary defence measures to enable the protection of its essential security interests.

The present document is intended be used by all that need to consider the effects, use or perform the legal transposition of the NIS Directive into national legislation. These include national regulators who need to update regulations or guidelines for specific industries identified in the NIS Directive as Operators of Essential Services (OES) or national policy makers wishing to provide guidance for Digital Service Providers (DSP). The present document might also be used by OES' and DSPs themselves for their own implementation. The present document is not intended to be prescriptive in the selection or use of technical specifications or requirements as organizational risk based approach yields the most effective industry wide implementations.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

NOTE: Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

[i.2] ENISA: "Gaps in NIS standardisation Recommendations for improving NIS in EU standardisation policy" V.1.0, November 2016.

[i.3] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence".

[i.4] ETSI TR 103 421: "CYBER; Network Gateway Cyber Defence".

[i.5] Transposition of the EU Network and Information Security (NIS) Directive, Digital Europe, Brussels, 5 July 2016.

[i.6] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.7] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.8] ETSI ETR 340: "Telecommunications Security; Guidelines for security management techniques".

[i.9] Recommendation ITU-T X.700 series (ISO/IEC 10160): "Information technology - Open Systems Interconnection - Systems Management".

[i.10] Recommendation ITU-T X.800 series (ISO/IEC 10181, ISO/IEC 11586): "Information technology - Open Systems Interconnection - Security frameworks for open systems, Generic upper layers security".

[i.11] Recommendation ITU-T X.1300 series: "Network security".

[i.12] Recommendation ITU-T X.1050 series: "Security Management".

[i.13] Recommendation ITU-T X.1200 series: "Cybersecurity".

[i.14] Recommendation ITU-T M.3000 series: "Security for the management plan".

[i.15] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.16] ISO/IEC 27000 series: "Information technology -- Security techniques -- Information security management systems".

[i.17] IEC 62443: "Industrial communication networks - Network and system security".

[i.18] ISACA: COBIT 5 series.

[i.19] ETSI GS ISI 001 (all parts): "Information Security Indicators (ISI)".

[i.20] ETSI TR 103 303: "CYBER; Protection measures for ICT in the context of Critical Infrastructure".

[i.21] ETSI Security Week 2017.

NOTE: Available at http://www.etsi.org/etsi-security-week-2017.

[i.22] ETSI Security Week, NFV Security Tutorial.

NOTE: Available at https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/04_NFVTUTORIAL/ETSI_ISGNFV_TUTORIALMATERIAL.pdf.

[i.23] ETSI Security Week, 5G Security: a government view.

NOTE: Available at https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/06_5GSECURITY/S02/NCSC_HAIGH.pdf.

[i.24] Sean Barnum: "The MITRE Corporation, Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)", 2012.

[i.25] ISO/IEC 15408: "Evaluation criteria for IT security".

[i.26] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[i.27] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[i.28] Recommendation ITU-T X.1500 series: "CYBEX Cyber security information Exchange".

[i.29] U.S. NIST Cybersecurity Framework.

NOTE: Available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[i.30] ETSI TR 103 305-4: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.31] CCRA: "Common Criteria for Information Technology Security Evaluation", Version 1.0.

NOTE: Available at https://www.commoncriteriaportal.org/cc/.

[i.32] Federal Ministry of the Interior: "National Plan for Information Infrastructure Protection".

NOTE: Available at http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf.

[i.33] Federal Ministry of the Interior: "Critical Infrastructure Protection (CIP) Implementation Plan".

NOTE: Available at http://www.qcert.org/sites/default/files/public/documents/GER-PL-CIP%20Implementation%20Plan-Eng-2007.pdf.

[i.34] IETF draft-ietf-inch-requirements-03: "Requirements for the Format for INcident information Exchange (FINE)".

[i.35] IETF draft-ietf-inch-iodef-02: "The Incident Data Exchange Format Data Model and XML Implementation".

[i.36] IETF draft-ietf-inch-rid-00: "Incident Handling: Real-Time Inter-Network Defense".

[i.37] IETF draft-ietf-inch-implement-00: "The Incident Object Description Exchange Format (IODEF) Implementation Guide".

[i.38] Recommendation ITU-T X.1500: "Overview of cybersecurity information exchange".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in the NIS Directive [i.1] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ANSSI	Agence Nationale de la Sécurité
BSI	German Federal Office for Information Security
CCDB	Common Criteria Development Board
CCRA	Common Criteria Recognition Agreement
CDXI	Cyber defence Data eXchange and Collaboration Infrastructure
CERT	Computer Emergency Response Teams
CIA	Confidentiality, Integrity, Availability
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
COBIT	Control Objectives for Information and related Technology
CPNI	Centre for the Protection of National Infrastructure
CSAF	Common Security Advisory Framework
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CTIP	Cyber Threat Intelligence Program
CVRF	Common Vulnerability Reporting Framework
CYBEX	cybersecurity information exchange
CybOX	Cyber Observable expression
DIB	Defense Industrial Base
DMARC	Domain-based Message Authentication Reporting and Conformance
DNS	Domain Name System
DSP	Digital Services Providers
ENISA	European union agency for Network and Information Security

FIRST	Forum of Incident Response and Security Teams
FYROM	Former Yugoslav Republic Of Macedonia
GDPR	General Data Protection Regulation
IAD	Information Assurance Directorate
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IODEF	Incident Object Description Exchange Format
ISAC	Information Sharing and Analysis Centre
ISACA	Information Systems Audit and Control Association
ISI	Information Security Indicators
IT	Information Technology
IXP	Internet eXchange Point
MACCSA	Multinational Alliance for Collaborative Cyber Situational Awareness
MAPP	Maturity Assessment, Profile and Plan
MEC	Mobile Edge Computing
MILE	Managed Incident Lightweight Exchange
MISP	Malware Information Sharing Platform
MS	Member State
MSRC	Microsoft Security Response Center
NATO	North Atlantic Treaty Organization
NCIRC	NATO Computer Incident Response Capability
NCSC	National Cyber Security Centre
NFV	Network Function Virtualization
NII	Network Information Infrastructure
NIS	Network and Information Security
NISD	NIS Directive
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OES	Operators of Essential Services
OSSI	Office of Security and Strategic Informatio
OTT	Over The Top
RID	Real-time Inter-network Defense
SDN	Software Defined Networking
SGDSN	Secretariat-General for National Defence and Security
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TC	Technical Committee
TLD	Top-Level Domain

4 Overview of the NIS Directive

4.1 The context for NIS

The NIS Directive (NISD) focuses on strengthening cyber authorities at the national level, increasing coordination among them and introduces security requirements for key industry sectors.

The two main objectives of the NIS Directive are [i.5]:

1) ensuring a high level cyber security of the country's critical infrastructures;

2) establishing an effective cooperation mechanism among EU Member States to further advance this objective.

The Network Information Security domain is one of the many dimensions of the multi-dimensional cyber-security landscape that can be visualised as a set of linked questions:

a) What is cyber security?

b) Who or what is affected? i.e. What is the cyber environment?

c) What measures enable protection?

d) What measures enable threat detection?

e) What measures enable thwarting and other remedies?

f) What legal remedies exist?

The NIS scope and the scope of what is cyber-security have considerable overlap and whilst the focus of the NISD may be considered as questions c), d) and e) the reality is that the entire set of 6 questions needs to be considered in giving an assurance of NIS as required through the detail to be found in the articles of the NISD. A visual model of the relationship of NISD within cyber-security is shown in Figure 1.

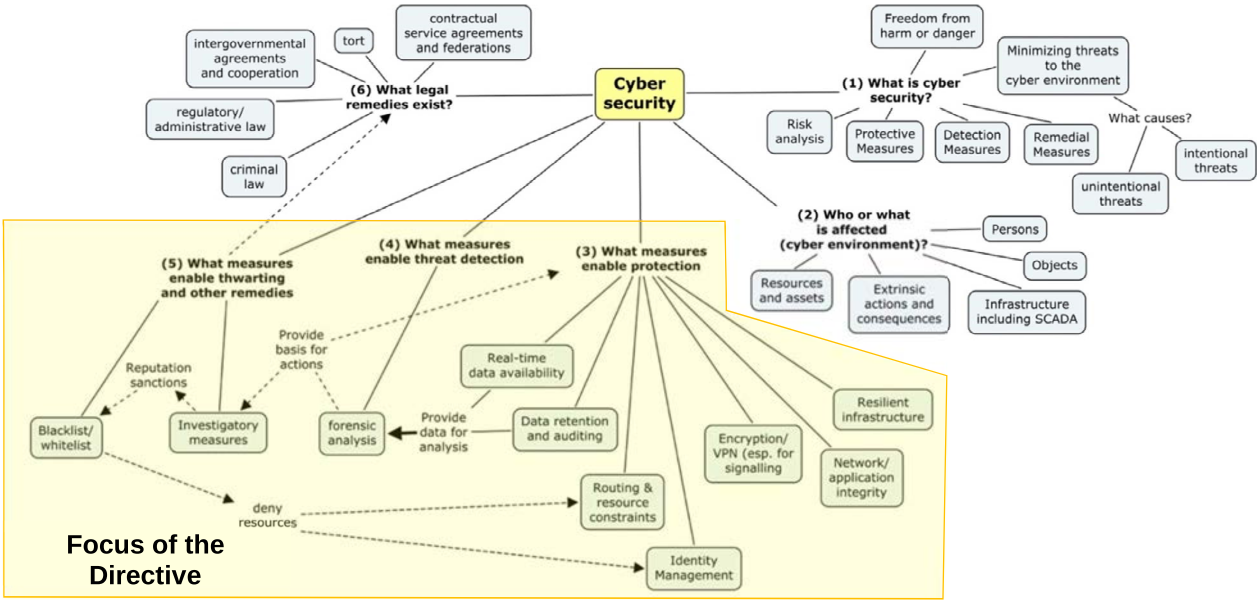

Cyber security
(6) What legal remedies exist?
intergovernmental agreements and cooperation
tort
contractual service agreements and federations
regulatory/ administrative law
criminal law
(1) What is cyber security?
Freedom from harm or danger
Minimizing threats to the cyber environment
Risk analysis
Protective Measures
Detection Measures
Remedial Measures
What causes?
intentional threats
unintentional threats
(2) Who or what is affected (cyber environment)?
Persons
Objects
Resources and assets
Extrinsic actions and consequences
Infrastructure including SCADA
(5) What measures enable thwarting and other remedies
(4) What measures enable threat detection
(3) What measures enable protection
Provide basis for actions
Reputation sanctions
Real-time data availability
Blacklist/ whitelist
Investigatory measures
forensic analysis
Provide data for analysis
Data retention and auditing
Resilient infrastructure
Encryption/ VPN (esp. for signalling
Network/ application integrity
Routing & resource constraints
deny resources
Identity Management
Focus of the Directive

Figure 1: Visualization of the relationship of NISD to cyber-security [i.2]

Defence against attack of Network and Information Systems share the same set of fundamental building blocks as any other system. The classical Confidentiality, Integrity, Availability (CIA) model of security risk assessment and management that leads to well-known and understood triples of (threat, security-dimension, countermeasures) such as interception, confidentiality and encryption. The role of the CIA paradigm is most often seen in 2 areas:

- risk analysis; and
- countermeasure deployment.

The CIA paradigm applies equally to NIS as to any other domain in cyber-security.

As can be seen in Figure 1, a considerable array of structured information exchange activity among the building blocks is necessitated. The NIS Directive has embedded within many provisions that relate to these structured information exchange requirements that are enumerated in Table 1.

Table 1: NIS Directive provisions relating to the structured exchange of cyber security information

Defensive measures information	Related to risks (static): • to resist, at a given level of confidence, any action that compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by or accessible via that network and information systems (Art. 3) • to manage the risks posed to the security of networks and information systems, etc. to ensure a level of security of networks and information systems appropriate to the risk presentedto prevent and analyses the impact of incidents affecting the security of the networks and information systems (Arts. 14 and 15) Related to incident handling (dynamic): • All procedures supporting the detection, analysis, containment and response to an incident (Art. 3)
Cyber security risk Information	Any reasonably identifiable circumstance or event having a potential adverse effect on the security of networks and information systems (Arts. 3 and 8)
Incident information	Any event having an actual adverse effect on the security of networks and information systems: • nature of the notified incidents, such as the types of security breaches (Art. 8a 3c - recital) • information that could support the effective handling of the incident (Art. 14 2a) • enable the competent authority or the CSIRT to determine the cross-border effect impact of the incident (Art. 14 2), including (a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident • other parameters for operators of essential service (Arts. 1, 2 and 14)
NOTE: Table 1 references are to [i.1].	

These provisions form the basis for much of the guidance contained in the present document. The NIS Directive mandates information sharing, although it is not expected that organizations that are covered by the NISD need implement an automated system of un-monitored reporting to their regulator or Member State (MS) Competent Authority. What is expected is some form of automated threat intelligence sharing. In implementing NISD, there is an important difference between mandatory reporting and voluntary sharing. Therefore, any guidelines should preserve space for voluntary cooperation and threat intelligence sharing.

4.2 ENISA recommendations on standardization

ENISA's report on gaps in NIS standardization makes the following broad recommendations in order to extend the technical basis for information sharing [i.2]:

- Adoption of threat exchange open standards based on the globally accepted STIX/TAXII/CyBOX platform to be prepared as an EN defining the syntax and semantics of the data and the necessary transfer protocol, and an accompanying guide to the implementation of the standard.

- Extension of the risk analysis and defensive measures capabilities defined in current standards to allow Member States to address the provisions necessary to mitigate risk both at national and regional level. This should be prepared as an EN extending the capabilities already described in ETSI TS 102 165-1 [i.7], ETSI TR 103 305 [i.3], ISO/IEC 15408 [i.25] and in relevant ISO/IEC JTC1 27000 series standards [i.16].

It is noted that it is not possible to separate provisions for NIS from general provisions for cyber security which have been developed by a broad array of ICT standards bodies. It is also noted that NII, NIS and cyber security cannot be geographically isolated in its provisioning, in the origin of attack, or in defense measures, and that this distributed complexity should be considered in implementation of the necessary information sharing required for effective NIS. Thus many of the capabilities of the NII will of commercial necessity be implemented using software and hardware from a global market.

4.3 Processing of personal data

The NIS Directive requires in Art. 2 that the processing of personal data be carried out in accordance Directive 95/46/EC [i.26] and with Regulation (EC) No 45/2001 [i.27], and Art. 15 requires cooperation with data protection authorities, but does not otherwise treat the subject. As the NIS explanatory preamble notes "*personal data are in many cases compromised as a result of incidents and in this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents*" [i.1]. The requirements for cooperation are referenced in preamble clause (72) [i.1]. Because the purposes of the NIS Directive are also aimed to meet these same requirements and simply ancillary to the NIS Directive provisions, the protection of personal data is not explicitly treated in the present document.

5 Cyber threat intelligence sharing: incidents and risks

5.1 Introduction

5.1.1 Context

This clause addresses implementation of the NIS Directive's incident notification requirements that arise from many different provisions enumerated in Table 1. In addition, Art. 7 of the NIS Directive required this capability as part of a national strategy "*defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems*" [i.1].

Some sector specific implementations are also required. For example, within Art. 14(3), the NIS Directive requires that operators of essential services "*notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of essential services they provide*." Moreover, within Art. 14(4), the NIS Directive posits that the number of users affected by the disruption of the essential service, the duration of the incident, and the geographical spread of the area affected by the incident may all be relevant criteria for determining the "*significance*" of an incident's impact. Although not subject to obligations, the Directive emphasizes that "information about incidents is increasingly valuable to the general public and businesses, particularly small and medium-sized enterprises" [i.1].

Following good practices will be critical to implementing incident notification requirements that empower competent authorities or CSIRTs to take action to mitigate the impact of significant incidents without overburdening such authorities/CSIRTs or creating additional ecosystem risk:

- the scope of incidents for which operators of essential services and digital services providers may be mandated (subject to national law) to provide notification should be sufficiently narrow so that it does not overlap with other EU laws and regulations or result in duplication of notification requirements;
- if notification is required, the thresholds should be structured in a way that accounts for the divergent risks and criticalities as well as the variations embedded in different technology architectures that support those services; and
- with regard to Operators of Essential Services, the national approaches for scoping and structuring thresholds for incident notification requirements should be sufficiently aligned such that these operators security response teams can focus on responding to and recovering from incidents rather than complying with fragmented requirements.

5.1.2 Scope of incidents

The scope of incidents for which operators of essential services are required to provide notification under the NIS Directive should be sufficiently narrow so that it does not overlap with other EU laws and regulations or result in duplication of notification requirements. In particular, the scope should not overlap with notification requirements included within the EU's GDPR, resulting in multiple disclosures to multiple regulatory agencies in the event of one security incident as well as inefficiencies and diverted resources. For instance, an incident involving a breach of confidentiality is already covered by data breach notification requirements under the GDPR.

According to Art. 14(3), the NIS Directive's incident notification requirements cover "*incidents having a significant impact on the* ***continuity*** *of essential services*" (emphasis added) for operators of essential services (emphasis added). Article 16(3) of NIS Directive requires digital service providers to notify an "*incident having a substantial impact on the provision of a service*" [i.1]. Continuity of services refers to their availability over time, supporting users' ability to access them and/or rely on their availability. In contrast, a breach may impact a user's ability to have assurance of confidentiality, but it may not necessarily impact a user's ability to access data or services.

In addition, the NIS Directive's incident notification requirements should be narrowly scoped around incidents that have an "actual adverse effect," consistent with the Art. 4 definition of an incident. Incidents that have a potential effect, such as attempted breaches, should not be scoped into notification requirements, helping to ensure that competent authorities/CSIRTs are not inundated with non-critical information and instead receive more prioritized and actionable information. In addition, such prioritization protects information about operators of essential services and digital service providers' tactics for isolating malicious attackers and mitigating the impact of network intrusions; if exposed to attackers, such information would likely help them to more quickly and effectively evolve offensive techniques.

5.1.3 Incident notification thresholds

What incidents will meet Art. 14(3)'s articulation of "*a significant impact*" may vary by service and technology architecture. As such, incident notification thresholds under the NIS Directive should be structured in a way that accounts for the divergent risks and criticalities of different essential services as well as the variations embedded in different technology architectures that support those services. Specifically:

- In different contexts, the relative importance of the number of users affected by the disruption of an essential service, the geographical spread of the area affected by the incident, and the duration of an incident may vary. For instance, the impact of the continuity/availability of a credit institution's web page will be different than the continuity/availability of an oil production, refinement, storage, or transmission operator's web page.

- Considering the NIS Directive criteria for measuring the significance of an incident's impact, "users" and "geographical impact" may mean different things to or be measured in different ways by different service providers and at different infrastructure layers. In some contexts, it may be more relevant for operators of essential services to consider "instances of use" than "users" as individuals. In other contexts, in compliance with EU privacy laws, operators of essential services may be limited to tracking "users" as customers, which may include multiple individual end users, rather than each individual end user. Likewise, depending on how a service is provisioned, an operator of essential services may have different ways of measuring the geographical impact of an incident and that way may not correspond with, for instance, national borders (e.g. particular number countries impacted as an incident notification threshold). Moreover, for flexible services with elastic demand, weighing the importance of the number of "users" impacted or the extent of geographical impact may vary over time.

Ensuring that requirements are appropriately calibrated for different services and architectures is consistent with the NIS Directive's risk-based articulation of requirements, stipulating that different types of services should be treated according to the risk that they pose.

In addition, the criteria that trigger a "disruption" to continuity/availability should also meet a high threshold to prioritize and ensure focus on significant incidents. In other words, the threshold for significant impact should only be when an entire service or a core functionality of a service is affected. Even if a non-core functionality or ancillary feature (i.e., not central to the service function) is disrupted broadly or over a significant period of time, it should not be considered to meet the threshold of reportability. Similarly, impact to essential services should be measured and incident notification requirements triggered only if an incident transpires and no failover processes are in place to absorb the incident. Unless there's an actual and noticeable impact, incident notification should not be required.

Considering the diverse contexts that impact how governments can measure the significance of an incident impacting operators of essential services, they could develop requirements through public-private partnerships that build from industry perspective. In particular, they should leverage the insights of both operators of essential services and the technology providers that often support services that may be scoped in to notification requirements (for example to the newly established NIS Cooperation Group), ensuring that the scope and thresholds of those requirements sufficiently ensure that notification will be useful to Competent Authorities/CSIRTs in fulfilling their missions without putting the ecosystem at increased risk.

5.1.4 Alignment of approaches

Approaches to scoping and structuring thresholds for incident notification requirements should be sufficiently aligned such that operators of essential services' security response teams can focus on responding to and recovering from incidents rather than complying with fragmented requirements. To the extent that requirements for incident notification are sufficiently narrowly scoped and apply appropriate thresholds for various services, they will progress toward requirements that are likely somewhat aligned. Continued focus on alignment will then result in additional efficiencies and cross-border coordination.

5.1.5 Incident classification indicators and metrics

A simple and high-level incident classification and related indicators and associated metrics are more and more important for organizations/companies and countries to measure the effectiveness of their security controls and get a common understanding of their overall security posture and to (possibly) benchmark themselves against statistical state-of-the-art figures. This quick move towards a real quantitative cyber security is nowadays approved almost unanimously. These indicators should be positioned at the relevant level between general controls of general reference frameworks (such as described in clause 6) and detailed and more technical incident classifications, that are found in Structured Threat Intelligence eXchange (STIX) are at a too low level to make statistical figures production really possible [i.6]. The ETSI Information Security Indicator (ISI) provide an ability to generate standardized metrics [i.19].

5.2 Concepts, models, and technical methods

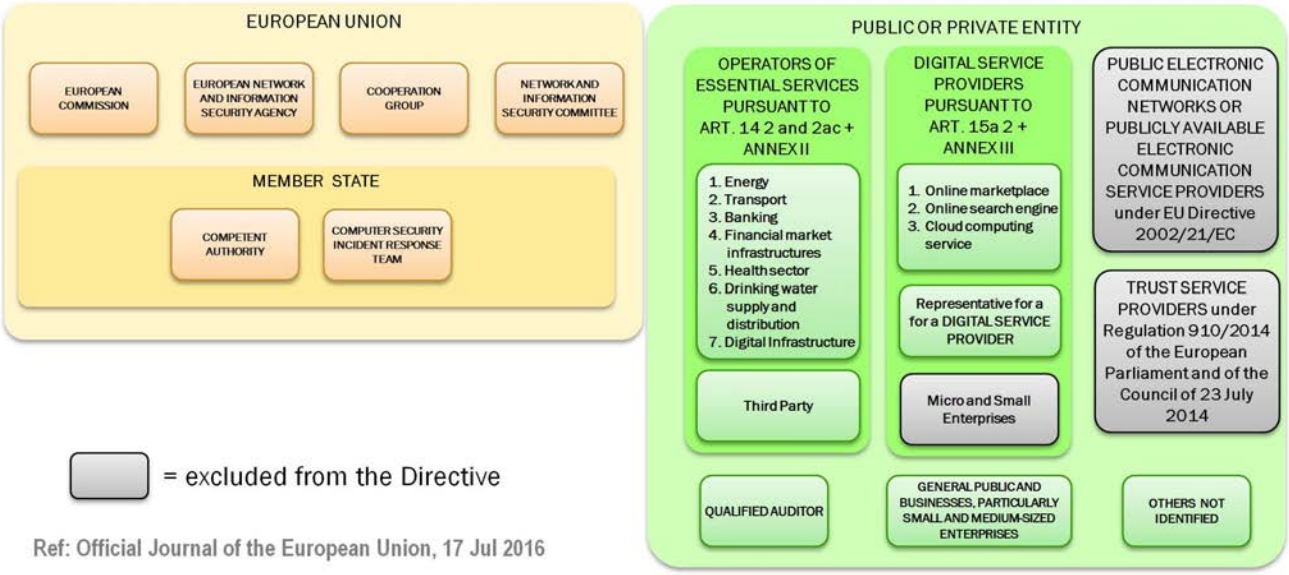
Historically, cyber threat intelligence in the form of information concerning incidents, vulnerabilities, risks, and remediations, have been unstructured and generally kept within organizations or industry sectors. The needs for widespread, rapid exchange of this information in operating legacy telecommunication networks could be accomplished through telephone calls and emails of audit information. It was not until the widespread emergence of distributed Internet Protocol based networks that requirements emerged to capture and exchange threat intelligence because of mounting attacks and other incidents being experienced. A brief history is provided in annex A.

Over the past five years the Structured Threat Intelligence eXchange (STIX) platform and its subtending specifications for TAXII (Trusted Automated Exchange of Indicator Information), and CybOX (Cyber Observable Expression) have become the principal means among diverse industry and government communities for exchanging cyber threat intelligence, and its continuing evolution is occurring within OASIS [i.6]. STIX is generally envisioned as the principal common means for meeting cyber threat intelligence requirements such as those identified in the NIS Directive and the ENISA Experts Technical Report [i.2].

5.3 Cyber threat intelligence entity practices

5.3.1 Introduction

Individual sectors identified in the NIS Directive generally have their own specifications and practices for the exchange of cyberthreat intelligence information - although generally there is an evolution toward the common models and expressions described in clause 5.2. The number and diversity of these entities is depicted in Figure 2. The present document attempts to provide guidance on how available industry specifications can provide for interoperability in the exchange of threat intelligence and defence information pursuant to the NIS Directive among these entities.


EUROPEAN UNION
EUROPEAN COMMISSION
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY
COOPERATION GROUP
NETWORK AND INFORMATION SECURITY COMMITEE
MEMBER STATE
COMPETENT AUTHORITY
COMPUTER SECURITY INCIDENT RESPONSE TEAM
= excluded from the Directive
PUBLIC OR PRIVATE ENTITY
OPERATORS OF ESSENTIAL SERVICES PURSUANT TO ART. 14 2 and 2ac + ANNEX II
1. Energy
2. Transport
3. Banking
4. Financial market infrastructures
5. Health sector
6. Drinking water supply and distribution
7. Digital Infrastructure
Third Party
DIGITAL SERVICE PROVIDERS PURSUANT TO ART. 15a 2 + ANNEX III
1. Online marketplace
2. Online search engine
3. Cloud computing service
Representative for a for a DIGITAL SERVICE PROVIDER
Micro and Small Enterprises
PUBLIC ELECTRONIC COMMUNICATION NETWORKS OR PUBLICLY AVAILABLE ELECTRONIC COMMUNICATION SERVICE PROVIDERS under EU Directive 2002/21/EC
TRUST SERVICE PROVIDERS under Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014
QUALIFIED AUDITOR
GENERAL PUBLIC AND BUSINESSES, PARTICULARLY SMALL AND MEDIUM-SIZED ENTERPRISES
OTHERS NOT IDENTIFIED

Ref: Official Journal of the European Union, 17 Jul 2016

Figure 2: Identified NIS Directive entities involved in the exchange of cyber threat intelligence

5.3.2 Operators of Essential Services

The operators of Essential services have certain additional treatment under the NIS Directive pursuant to Articles 14-15, and Annex II [i.1]. Such operators include energy, transport, banking, financial market infrastructure, health sector, drinking water supply and distribution, and "digital infrastructure" defined to include IXPs, DNS service providers and TLD name registries.

The sharing of threat intelligence within these sectors has typically relied on specialized and generally closed platforms and ISACs. Some are described in clause 5.3.4. Increasingly, however, these services are moving to common interoperable platforms such as STIX [i.6].

5.3.3 Digital Service Providers

Similarly, Digital Service Providers have certain additional treatment under the NIS Directive pursuant to Articles 16-17 and Annex III [i.1]. Such providers are defined to include services in the "online marketplace, online search engine[s], and cloud computing services. The sharing of threat intelligence within these sectors has also typically relied on specialized and generally closed platforms and ISACs. Some are described in clause 5.3.4. Increasingly, however, these services are moving to common interoperable platforms such as STIX [i.6].

5.3.4 Specialized, limited use, structured threat intelligence sharing platforms

Some of the specialized and limited use threat intelligence sharing platforms and activities identified include the following. To the extent that the platforms have identified published informative references, they can be found in ETSI TR 103 331 [i.6].

- **IODEF and RID:** Incident Object Description Exchange Format (IODEF) and Real-time Inter-network Defence are among the oldest and most widespread of structured threat intelligence exchange platforms - going back to the earliest formation of network CERTs and still persisting among many of them today. The specifications have been developed and evolved as RFCs in the IETF MILE committee and replicated in the Recommendation ITU-T X.1500 CYBEX series [i.28].

- **CSAF and CVRF:** The Common Vulnerability Reporting Framework (CVRF) has been used for some years among some vendor and provider communities and is now being standardized as Common Security Advisory Framework (CSAF) by OASIS.

- **NATO CDXI and NCIRC:** Within the Cyber Defence and Assured Information Sharing NATO Communications and Information Agency, at the Hague, Netherlands, the definition of a Cyber Defence Data Exchange and Collaboration Infrastructure (CDXI) capability emerged as part of a larger NATO Computer Incident Response Capability (NCIRC). Within NATO member communities, CDXI is used for the exchange cyber security intelligence.

- **CTIP:** The Cyber Threat Intelligence Program (CTIP) was established within the U.S. Department of Health and Human Services, Office of Security and Strategic Information (OSSI), in 2014. The OSSI CTIP monitors and analyses all-source intelligence on cyber threats to the Healthcare and Public Health sector; provides timely, actionable cyber threat information; and solicits feedback and information requirements from the sector.

- **MISP:** Malware Information Sharing Platform (MISP) is an initiative among a set of developers who have created a set of open threat information sharing tools. As the MISP project expanded, MISP not only covered malware indicators but also fraud or vulnerability information. The platform also includes the core MISP software and a myriad of tools (PyMISP) and format (core format, MISP taxonomies, warning-lists) to support. It is used among some CSIRTS.

- **MAPP:** Maturity Assessment, Profile, Plan (MAPP) is a proprietary analytics engine that combines other threat sharing metrics to produce status reports.

- **MSRC and OpenIOC:** Microsoft Security Response Center (MSRC) and OpenIOC are respectively the proprietary threat intelligence exchange platforms of Microsoft's Security Tech Center and of Mandiant - a FireEye security company. They are two among many used among Operators of Essential Services and Digital Service Providers.

- **MACCSA:** Multinational Alliance for Collaborative Cyber Situational Awareness (MACCSA) was an experimental project to encourage exchange of threat information using structured expressions.

6 Role of risk analysis in protecting NIS

6.1 Introduction

This clause addresses implementation of the NIS Directive's cyber risk management requirements that arise from many different provisions enumerated in Table 1. The Directive requires operators of essential services (OES) and digital service providers (DSP) to implement cyber risk management measures. With regard to OES, Art. 14(1), the NIS Directive requires that "*Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations…having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed*" [i.1].

With regard to DSP, Art. 16(1) of the directive has a similar requirements (albeit subject to the light-touch approach for DSPs as explained in recitals (49), (60) and (66): "*Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union...having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; In compliance with international standards*."

Cyber security risk management is an approach that involves assessing a range of risks in the context of an organization's environment, understanding assets, resources, and processes that are fundamental to the organization, and taking steps to ensure that the organization continuously improves how it protects, detects threats, and responds to incidents involving those assets, resources, and processes. In the context of the NISD and Arts. 14(1) and 16(1), cyber security risk management practices are relevant to security measures, which should highlight the importance of these steps rather than just require implementation of prescriptive security controls, which are not sufficiently agile for the rapidly evolving technology ecosystem.

Industry experience has derived a common set of best practices and principles that reflect cyber security risk management lessons learned that are relevant for security measures [i.9] to [i.18]:

- **Risk Based:** Risk-based and prioritized security measures ensure that organizations are able to make security investment decisions that best correlate with their varying risk landscapes, recognizing that no organization has unlimited security resources. Risk-based and prioritized security measures are able to reflect an organization's particular business drivers and security considerations.

- **Communications-enabling:** Security measures that articulate a prioritized set of cyber risk management best practices should also be framed in a way that is communications-enabling, facilitating communication across boundaries, both within and between organizations, by establishing a common language and reference point that can be used by security practitioners, managers, and executives as well as among suppliers and buyers. Establishing a common language in particular helps to facilitate horizontal and vertical communication within an organization, enabling executives to have greater visibility into cyber risk management efforts and to make more informed security resourcing decisions.

- **Outcomes-focused:** Outcomes-focused approaches provide organizations with sufficient flexibility to manage security in a way that is consistent with changing threats and technology developments.

- **Flexible:** Flexible security measures focus on cyber risk management processes, allowing organizations to iterate and incorporate new learnings into those processes over time. There are certain crucial elements of a meaningful process, including having a formal owner that is accountable for planning, developing, implementing, testing, reviewing, and improving cyber security risk management processes.

Clause 6, Method Process of ETSI TS 102 165-1 [i.7] provides a useful cost benefit analysis part of the risk calculation.

The starting point should be cross-sector baseline security measures, i.e. there will be many security measures relevant across sectors. Then, there may be additional sector specific security measures that should be layered on top of the cross-sector baseline. Having a cross-sector baseline supports efficiencies for government security assessors and for interdependent sectors. In addition, it supports greater information and best practices sharing among government and industry stakeholders. Meanwhile, the flexibility to add relevant sector-specific security measures on top of a cross-sector baseline ensures that sector-specific risks are also addressed.

6.2 Concepts, models, and technical methods

6.2.1 Introduction

Much of the history of cyber risk management concept, models, and technical methods follows a history similar to that for cyber threat intelligence sharing described in clause 5.2. Both ETSI and the ITU-T published sets of generic methods for cyber risk management, such as the Critical Security Controls. In addition, other specialized bodies such as NATO and the CCDB/ published global specifications such as the Common Criteria, and national authorities have issued frameworks - as described in the clause 6.2.3. These methods vary in level of detail and implementation guidance.

These cyber security methods are useful because they address a range of risks and defence measures that are applicable across many environments. As many organizations leverage technologies and resources from other sectors and organizations, a common baseline enables those organizations to meet suppliers' regulatory or contractual requirements and drives cyber security best practices across the ecosystem. Cross-sector methods are particularly valuable because, increasingly, there is horizontal integration across vertical sectors. Baselines can set minimum requirements common across sectors and be complemented by sector-specific requirements as appropriate.

The development of a national strategy requires a consistent and iterative approach to identifying, assessing, and managing risk and evaluating implementation of the methods. A consistent approach is important to support coordination across an organization and to be able to measure progress internally. An iterative approach is important because both the technology ecosystem and threat landscape are constantly evolving. New technologies create additional ways to manage existing and new risks. New threats require different risk mitigation techniques.

Whether embedded in a cyber security framework or articulated as baseline security measures, a set of policies, outcomes, activities, practices, and controls are relevant to help manage cyber security risk. Systems-security, outcomes-focused approaches encourage organizational processes and controls that call for actionable steps. They are complementary and valuable components.

6.2.2 Critical Security Controls

ETSI TR 103 305 [i.3] together with associated implementation guides, provide an effective, implementable controls-based approach that are widely adopted.

These ETSI Controls and associated implementation guides capture and describe the top twenty enterprise industry level cyber security best practices that provide enhanced cyber security, developed and maintained by the Center for Internet Security (CIS) as an independent, expert, global non-profit organization and published by ETSI. The CIS provides ongoing development, support, adoption, and use of the Critical Security Controls. The Controls reflect the combined knowledge of actual attacks and effective defences of experts from every part of the cyber security ecosystem. This ensures that the Controls are an effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from those attacks.

The Controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions. The defences identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defence and response capability that can be maintained and improved. The five critical tenets of an effective cyber defence system as reflected in the Critical Security Controls are:

- Offense informs defence: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defences. Include only those controls that can be shown to stop known real-world attacks.
- Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in a computing environment.
- Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.
- Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures, and to help drive the priority of next steps.
- Automation: Automate defences so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

The Controls have the additional benefit of being already used in some EU countries for the purposes meeting the NIS Directive [i.1].

6.2.3 National and intergovernmental programmes

Although the Critical Security Controls represent the most extensive, actionable cyber defence mechanism appropriate for the NIS Directive, they exist among an array of national and intergovernmental strategies, frameworks, and programmes that have emerged over the past several decades. Some of the more prominent - especially for EU Members - are described here.

The Common Criteria Development Board (CCDB) was the earliest of the intergovernmental cyber defence efforts and remains important because of its focus on critical infrastructure. The Common Criteria for Information Technology Security Evaluation (Common Criteria) was developed by the governments of Canada, France, Germany, Netherlands, UK, and U.S. in the mid-90's. Common Criteria (CC) was produced by the willing to unify the security evaluation standards to avoid re-evaluation of products addressing international markets, and Common Criteria version 1.0 was issued in 1994 [i.31]. Today there are 26 nations part of the arrangement, including most EU Members. The CC is today undergoing significant changes - likely in ways that are compatible with the Critical Security Controls.

Cyber defence is part of NATO's core task of collective defence. In cyber space, NATO's priority is the protection of its communication and information systems. Allies are responsible for their own cyber defences, but NATO helps them in many ways that include:

- sharing real-time information about threats through a dedicated malware information sharing platform, as well as best practices on handling cyber threats;

- maintaining rapid reaction cyber defence teams that can be sent to help allies in handling cyber challenges;
- developing targets for allies to facilitate a common approach to their cyber defence capabilities;
- investing in education, training and exercises.

Several bodies associated to NATO are also helping the Alliance to improve cyber defences. The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia is a NATO-accredited research and training facility dealing with cyber defence education, research and development. It maintains an extensive collection of national cyber defence strategies and frameworks for reference.

Table 2: European nations and regional organization programmes and frameworks

European region countries	ETSI EU member	EU member	Schengen area	EFTA State	Council of Europe	NATO member	CCRA member
Albania	X	T			X	X	
Andorra		O			X		
Armenia		O			X		
Austria	X	X	X		X		C
Azerbaijan		O			X		
Belgium	X	X	X		X	X	
Belarus		O					
Bosnia & Herzegovina	X	P			X		
Bulgaria	X	X			X	X	
Croatia	X	X			X	X	
Cyprus	X	X			X		
Czech Republic	X	X	X		X	X	C
Denmark	X	X	X		X	X	C
Estonia	X	X	X		X	X	
Finland	X	X	X		X		C
France	X	X	X		X	X	A
Georgia	X	O			X		
Germany	X	X	X		X	X	A
Greece	X	X	X		X	X	C
Hungary	X	X	X		X	X	C
Iceland	X	O	X	X	X	X	
Ireland	X	X			X		
Italy	X	X	X		X	X	A
Kazakhstan							
Kosovo		P					
Latvia	X	X	X		X	X	
Liechtenstein		O	X	X	X		
Lithuania	X	X	X		X	X	
Luxembourg	X	X	X		X	X	
Macedonia (FYROM)	X	C			X	A	
Malta	X	X	X		X		
Moldava	X	O			X		
Monaco		O			X		
Montenegro	X	T			X		
Netherlands	X	X	X		X	X	A
Norway	X	O	X	X	X	X	A
Poland	X	X	X		X	X	
Portugal	X	X	X		X	X	
Romania	X	X			X	X	
Russia	X	O			X		
San Marino		O			X		
Serbia	X	T			X		
Slovakia	X	X	X		X	X	
Slovenia	X	X	X		X	X	
Spain	X	X	X		X	X	A
Sweden	X	X	X		X		A
Switzerland	X	O	X	X	X		
Turkey	X	T			X		A

European region countries	ETSI EU member	EU member	Schengen area	EFTA State	Council of Europe	NATO member	CCRA member
Ukraine	X	O			X		
United Kingdom	X	X			X	X	A
Vatican City		O					
NOTE: Key: X = member T = transposition underway O = potential member A = authorizing member C = consuming member Ap = applied							

The ITU-T over the past decade developed a collaborative relationship with multiple cyber defence agencies and initiatives, and working with NATO, FIRST, the Trusted Computing Group, IETF, and other organizations published many of the best-of-breed of Information Assurance Directorate (IAD), and MITRE platforms as ITU-T standards. See the Recommendation ITU-T X.1500 series specifications [i.28] - especially those dealing with the exchange of vulnerability and state information [i.6]. At the national level, most EU Members have cyber defence programs and frameworks. Among these, several are worth noting.

The UK National Cyber Security Centre (NCSC) recently added to its long standing CPNI initiative by creating four Active Cyber Defence programmes that include: protected DNS, DMARC anti-spoofing, web check, and phishing and malware mitigation. The CPNI promulgated its version of the Critical Security Controls shortly after they were originally developed by IAD in the U.S. as high-priority information security measures and controls that can be applied across an organization in order to improve its cyber defence. They are especially significant a core part of the UK framework under the NIS Directive.

In France, the 2013 White Paper on Defence and National Security established its critical infrastructure protection policy as a means of strengthening the Nation's resilience. As the linchpins of this system, critical operators are required to analyse the risks to which they are exposed and apply the protection measures within their remit - particularly the VIGIPIRATE plan. The strategy consists of a permanent security stance (cybersecurity), as well as incorporating reinforced-protection measures tailored to changes in the threat. OES apply information-technology security measures that are specific to their sector. The policy establishes the National Network and Information Security Agency (ANSSI) under the Prime Minister and the Secretary General for Defence and National Security (SGDSN) with a six-part framework:

1) Strengthening the security of information systems;

2) Augmenting cyber security research;

3) Education and training, thereby reinforcing the manpower;

4) Developing the cyber defence centre;

5) Furthering international cooperation; and

6) Furthering the emergence of a national cyber defence community.

In Germany, newly created National Cyber defence Centre is the government agency established to respond to attacks on government computers in Germany. Both the 2005 "National Plan for Information Infrastructure Protection" [i.32] directed at both government and industry, and the 2007 "Critical Infrastructure Protection (CIP) Implementation Plan" [i.33] address IT crisis response and provide recommendations for business continuity management of critical business processes in the event of a major cyber incident. On a continuing basis, the German Federal Office for Information Security (BSI) is the national cyber security authority for Germany and the central cyber incident reporting office and has published several cyber defence related BSI standards.

To the extent they are applicable to the NIS Directive implementation, other prominent cyber defence programmes and frameworks include:

- The Australian Signals Directorate Strategies to Mitigate Cyber Security Incidences and the "Top 4" and the "Essential Eight" mitigation strategies to protect an ICT system plus additional guidance on mitigation strategies to prevent malware delivery and execution, to limit the extent of cyber security incidents, and to detect cyber security incidents and respond.

- The U.S. Defense Industrial Base (DIB) Computer Security program allows eligible DIB participants to receive Government furnished information and cyber threat information from other DIB participants, thereby providing greater insights into adversarial activity. The platforms were developed by an array of U.S. government security agencies that provide Information Assurance advisories and an array of other cyber defence information.

- The U.S. NIST Cybersecurity Framework [i.29] provides an operational risk management framework that's intended to help organizations assess and improve their ability to identify and protect assets and networks, detect anomalies and incidents, and respond to and recover from incidents. It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes", allowing organizations to integrate cybersecurity risk management into broader enterprise risk management functions and engage leadership on security priorities and needed investments. As it is risk-based and outcomes-focused, it also enables organizations to have flexibility in implementing steps to continuously improve their management of cyber risks. Version 1.0, published in 2014, was originally aimed at operators of critical infrastructure, but it is also being used by a wide range of businesses and even government organizations to be proactive about risk manage. ETSI TR 103 305-4 [i.30] provides a mapping of the Controls to the NIST Framework's Informative References to implement actual cyber defence capabilities [i.3].

6.3 Cyber defence and cyber security risk management practices

6.3.1 Introduction

Cyber defence and cyber security risk management practices relevant to baseline security measures should focus on establishing a security-management, outcomes-focused framework or baseline that incorporate controls. This approach ensures that risk management processes are embedding into organizational practices from the outset.

Beginning in the late 1980s, the entire array of telecommunications/ICT communities embarked on multiple security management, outcomes-focussed specifications for risk management that included the formation of new groups and culminated in extensive specifications published in the 1990s and have continued to this day [i.9] to [i.18]. For example, ETSI's 1996 ETR on Security Management Techniques provided an introduction and guide on how to identify security management functions that are necessary to monitor and control security functions in a system and provided pointers to other security management, outcomes-focussed standards at three different levels of a telecommunications system, corresponding to systems security, security services and security mechanisms [i.8].

Organizational best practices for cyber security risk management are coalescing around a few critical concepts. As outlined in ETSI TR 103 303 [i.20], a holistic protection lifecycle includes the following events: plan; detect; react; and recover. All measures, including those of NCSC, AGDSN/ANSSI and NIST highlight the importance of the following functions: identify; protect; detect; respond; and recover. ETSI TR 103 303 [i.20] highlights a number of areas under each event; for instance, under planning measures, ETSI recommends an assessment of business objectives, asset management, threat assessment, risk management, and incident response plans. Similarly, within the identify function, the measures include the following categories: asset management; business environment; governance; risk assessment; and risk management strategy. The measures also include more detailed subcategories with accompanying informative references.

This construct of "events" or "functions" with more detailed, accompanying guidance is helpful for organizations implementing cybersecurity risk management practices because the guidance can be understood at an altitude that's appropriate for different internal stakeholders. Executives that make decisions about security investments can understand and track an organization's progress at the event or function level, whereas information security practitioners can reference more details guidance or informative references. In this way, a cybersecurity risk management approach is communications-enabling, facilitating communication across boundaries by establishing a common language and reference points.

6.3.2 Operators of essential services

Cyber defence and cyber security risk management practices for operators of essential services have typically relied on specialized and generally closed platforms and ISACs. Some are included in the platforms discussed above. Increasingly, however, these services are moving to common interoperable platforms such as the Critical Security Controls. Cyber defence and cyber security risk management practices for operators of essential services should be consistent with a communications-enabling framework that is risk-based, outcomes-focused, and flexible. Such a framework should be framed in way that highlights desired security outcomes and references potential implementation mechanisms, including relevant controls (e.g. the Critical Security Controls).

6.3.3 Digital service providers

Cyber defence and cyber security risk management practices for digital service providers should be consistent with a communications-enabling framework that is risk-based, outcomes-focused, and flexible. Such a framework should be framed in way that highlights desired security outcomes and references potential implementation mechanisms, including relevant controls (e.g. the Critical Security Controls).

7 Challenges and solutions

7.1 Introduction

The challenges and obstacles of implementing the NIS Directive are diverse and constantly evolving. It is not possible to fully treat this subject here. However, ETSI's annual Security Week archive of materials [i.21] represent a best-of-breed, constantly updated enumeration of challenges and ongoing activities to meet those challenges provided by industry, organizational, and government representatives, including a special focus on the NIS Directive [i.1]. Some of the perspective of the most recent Security Week is provided in the subsequent sub-clauses. Key points relative to the NIS Directive included:

- There is basically no cyber security standards gap:
  - There are too many standards, and many are not actionable or particularly useful.
  - The real need is to converge toward useful, interoperable sets of standards.
  - Standards that are not freely available on-line, constantly evolving, and well-versioned have diminished value and represent cyber security impediments.
  - TC CYBER sought to discover the ecosystem and focus on identifying the most effective platforms and specifications and that have the broadest industry support.
- There are no simple or easy cyber security solutions:
  - Cybersecurity as such is not achievable given the enormity of constantly evolving vulnerabilities.
  - What you can do is implement sets of defence measures (Critical Security Controls), and threat exchange measures (STIX ensemble) that can reduce the risks.
  - Whilst encryption has positive benefits, there are adverse effects of end-to-end encryption which need urgent attention.
  - Rapidly evolving new industry platforms such as NFV-SDN/5G and quantum computing need urgent attention to control the cyber security risks.

7.2 New technologies and services

Network Functions Virtualization + Software Defined Networks. Service Providers want to make their networks agile and efficient to meet the challenges of exponential bandwidth demands and be able to create revenue streams with innovative services and new business models. Network Function Virtualization (NFV) and Software Defined Networking (SDN) has emerged as the paradigm that has the potential to transform the industry by delivering cloud style agility and innovation and enhancing economic viability. By 2020 SNS Research estimates that SDN and NFV can enable service providers (both wireline and wireless) to save up to $32 Billion in annual CapEx investments ACG Research estimates that NFV will reduce capital expenditure by 68 % and reduce operating expenditure by 67 %. NFV+SDN implementations require an array of new and altered approaches to cyber threat information sharing and cyber defence [i.22].

5G Mobile Networks, Mobile Edge Computing and IoT. In 5G, there are substantial changes in network architecture where NFV+SDN support highly dynamic networking, and network slicing supports multi-tenancy. These capabilities in turn support an array of new mobile and wireless fixed implementations that include transport systems, smart infrastructure autonomous vehicles, manufacturing and robotics. Mobile Edge Computing (MEC) moves powerful processing and storage capabilities out to the Radio Access Network edge of mobile networks. The new security models will necessarily permeate all parts of the supporting infrastructures and be interoperable [i.23].

Over the Top (OTT) services, and "encrypt everything" initiatives. A significant cyber security challenge emerging today is the combination of Over the Top services combined with "encrypt everything" initiatives that generated potentially huge amounts of traffic between some arbitrary service portal somewhere in the world, and an end user's terminal - even an application on a device. Some Internet of Things implementations also fall into this category. While these steps meet significant needs today, these practices may have adverse effects such as impeding detection of malware and other cyber security threats, as well as managing network traffic and meeting a broad array of business, organizational, and regulatory requirements. A balanced approach is needed that provides support to all the requirements that exist today [i.4].

7.3 New techniques

7.3.1 Use of middlebox security protocols for cyber defence

The rapidly increasing use of server to end user client transport path encryption is causing significant network management and compliance obligation difficulties, including the provision of cyber defence. The encryption of traffic occurring between end points where network application servers are interacting directly with software clients on end user devices [i.4]. The use cases consist of an array of business and compliance obligations within the scope of the NIS Directive. Network gateway cyber defence related activities including new standards-based specifications have increased significantly. Cyber defence capabilities are increasingly implemented using what are usually referred to as "middleboxes" that may be integrated into traffic routers that typically exist at boundaries between networks. Network gateways are critically important points for implementing cyber defence in conjunction with other essential functions.

The related cyber defence technical requirements to meet the NIS Directive include:

1) secure and controlled exposure of traffic observables;

2) sufficient observable information for acquisition and analysis for defence measures; and

3) the ability to institute defence measures as part of gateway management.

Middlebox Security Protocol capabilities meet these cyber defence requirements [i.4].

7.4 Harmonizing implementations across the diverse network and service sectors and Member State legal and operational environments

One of the most challenging aspects of implementing the Network and Information Security (NIS) Directive [i.1] is harmonizing those implementations across the diverse network and service sectors and EU Member State legal and operational environments. While this is recognized here, it is a matter out of scope of the present document.

8 Recommendations

8.1 Operators of essential services

The operators of Essential Services should be encouraged to adopt common interoperable platforms such as STIX for cyberthreat intelligence sharing and the Critical Security Controls for Effective Cyber Defence, as well as critical capabilities such as the Middlebox Security Protocol to deal with the mounting challenges of encrypted traffic [i.3], [i.4] and [i.6].

8.2 Digital service providers

Digital Service Provider should be encouraged to adopt common interoperable platforms such as STIX for cyberthreat intelligence sharing and the Critical Security Controls for Effective Cyber Defence, as well as critical capabilities such as the Middlebox Security Protocol to deal with the mounting challenges of encrypted traffic [i.3], [i.4] and [i.6].

8.3 Facilitative mechanisms for network and information security

In general, the use of the facilitative mechanisms described in Part 4 of ETSI TR 103 305 [i.3] including privacy impact assessments, mappings to national cyber security frameworks, cyber hygiene programmes, and governance strategies, can significantly enhance network and information security.

Annex A:
Historical development of cyber threat intelligence sharing

The mounting cyber threats in the 1990s resulted in the formation of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTS). These bodies formed an international organization known as FIRST (Forum of Incident Response and Security Teams) in 1990. The need for the structured exchange of threat intelligence to facilitate automation emerged from efforts of the Amsterdam-based Trans-European Research and Education Networking Association (TERENA) Task Force on Collaboration of Security Incident Response Teams (TF-CSIRT) creation of the INCident Handling Working Group (INCH) in the IETF in 2001. INCH in turn produced four deliverables [i.34], [i.35], [i.36] and [i.37] that remain conceptually the foundation in the sector.

The data model concept is shown in Figure A.1.

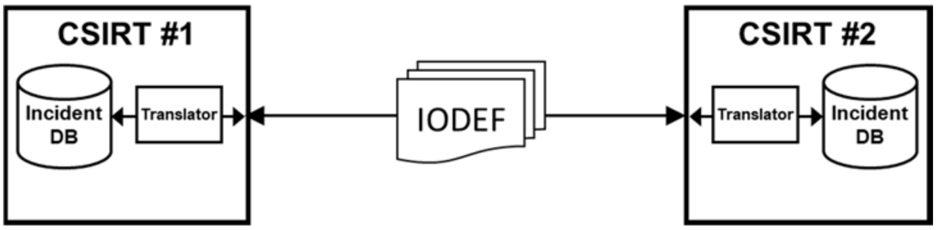


Figure A.1: IODEF based threat intelligence exchange model concept

The original activity continues within the IETF under the aegis of the Managed Incident Lightweight Exchange (MILE) Working Group which has introduced some extensions to the original specifications.

The requirements and work scaled significantly during the 2000s with work at the MITRE Corporation in developing an array of new means for exchanging structured cyber security information that were introduced in the ITU-T Study Group 17 Rapporteur Group on Cyber security (Q4/17) beginning in 2008 as an expansive framework known as CYBEX (Cyber security information Exchange). See Recommendation ITU-T X.1500 series [i.28]. Many of the MITRE and other specifications were published or identified as Recommendations ITU-T X.1500 series in four "exchange clusters":

- Weakness, vulnerability and state.
- Event, incident and heuristics.
- Information exchange policy.
- Identification, discovery and query.
- Identity assurance.
- Exchange protocol.

Somewhat similar to and fully compatible with the IETF model, the CYBEX concept is essentially identical - only allowing for a more diverse and expansible array of exchange mechanisms, including an ontology model, that are kept current in the Recommendation ITU-T X.1500 appendix [i.38] which is updated twice a year. See Figure A.2.

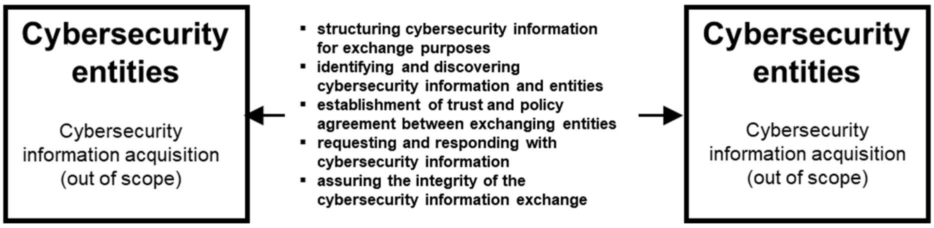

Cybersecurity entities
Cybersecurity information acquisition (out of scope)
▪ structuring cybersecurity information for exchange purposes
▪ identifying and discovering cybersecurity information and entities
▪ establishment of trust and policy agreement between exchanging entities
▪ requesting and responding with cybersecurity information
▪ assuring the integrity of the cybersecurity information exchange
Cybersecurity entities
Cybersecurity information acquisition (out of scope)

Figure A.2: Recommendation ITU-T X.1500-based intelligence exchange model concept [i.28]

In 2012 during the course of diverse discussions on how to expand cyber threat intelligence exchange capabilities, the concept of uniform yet flexible model was advanced in White Paper by a researcher at MITRE in the form of STIX (Structured Threat Information eXpression). See Barnum [i.24]. The paper stated the basic value proposition.

"It is becoming increasingly necessary for organizations to have a cyber threat intelligence capability and a key component of success for any such capability is information sharing with partners, peers and others they select to trust. While cyber threat intelligence and information sharing can help focus and prioritize the use of the immense volumes of complex cyber security information organizations face today, they have a foundational need for standardized, structured representations of this information to make it tractable."

STIX quickly became the cyber security equivalent of the Unified Field Theory in physics and over the subsequent four years became the principal means and work effort among diverse communities for exchanging cyber threat intelligence. In 2015, the intellectual property was transferred to the OASIS standards organization and has continued under the stewardship of its Cyber Threat Intelligence Technical committee which grew rapidly in numbers, diversity, and activity to include organizations worldwide. Its activities include the maintenance of several Githubs with available running code for implementations. See https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti. Within the STIX specification ensemble, CybOX (Cyber Observable Expression) is the means for capturing threat observations and TAXII (Trusted Automated Exchange of Indicator Information) is the protocol for communication those threats.

TAXII continues to rapidly evolve a global community in the OASIS CTI Technical Committee with a Version 2.0 adopted in May 2017 and future versions under continuing development. ETSI TR 103 331 [i.6] provides a comprehensive overview on all the various means for describing and exchanging cyber threat information in a standardized and structured manner, including extensive information on the STIX use cases, components, and architecture. See Figure A.3.

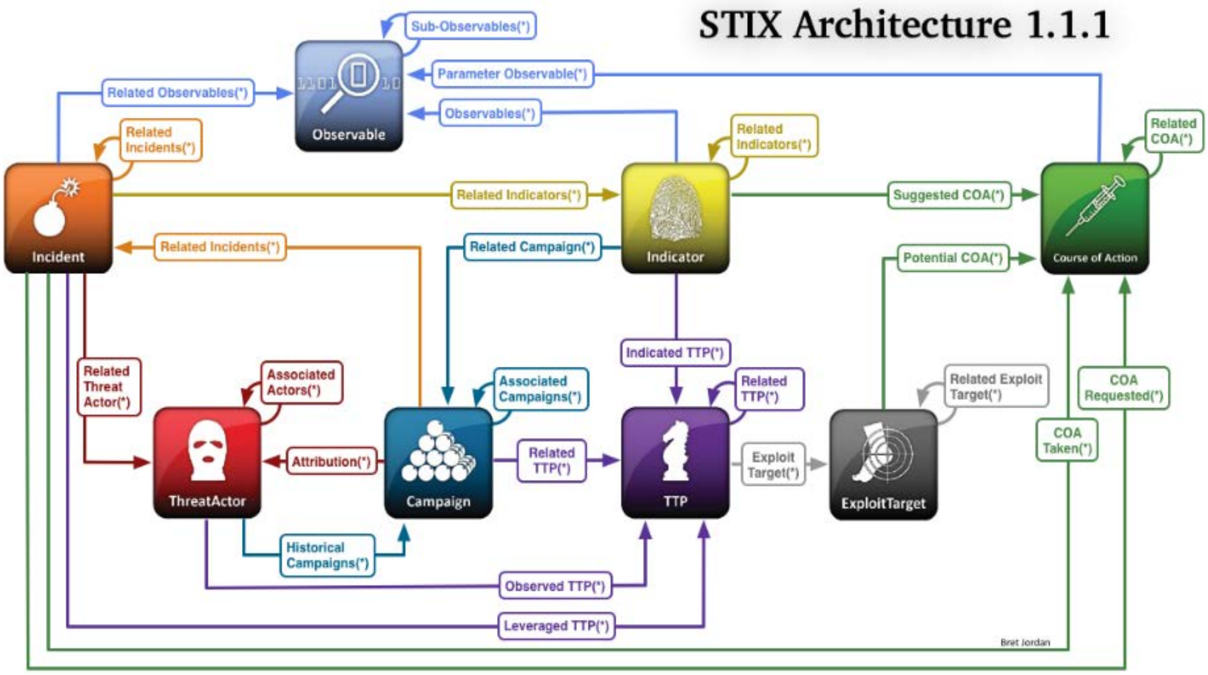


Figure A.3: STIX individual component data models [i.6]

History

Document history		
V1.1.1	October 2017	Publication