EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CSIRT CAPABILITIES IN HEALTHCARE SECTOR

Status and Development

NOVEMBER 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use etl@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Adrian A. Baumann, ENISA
Apostolos Malatras, ENISA
Edgars Taurins, ENISA

LEGAL NOTICE

COPYRIGHT NOTICE

Catalogue number: TP-07-21-067-EN-N – ISBN: 978-92-9204-542-5 – DOI: 10.2824/201143

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

LIST OF ABBREVIATIONS 5

1. OVERVIEW AND SCOPE OF THE STUDY 6

1.1 CONTEXT OF THE STUDY 6
1.2 OBJECTIVES OF THE STUDY 7

2. METHODOLOGY AND DATA COLLECTION 8

2.1 OVERVIEW OF THE METHODOLOGY 8

3. KEY FINDINGS 10

3.1 IRC SET-UP AND LANDSCAPE 10
3.2 CREATION OF SECTORAL CSIRTS 15
3.3 CSIRTS SERVICES 19
3.4 IR TOOLS AND PROCEDURES 22
3.5 IR MATURITY DEVELOPMENT 26
3.6 CSIRTS CHALLENGES AND GAPS 28
3.7 CSIRTS LESSONS LEARNED 30

4. RECOMMENDATIONS 31

4.1 INTRODUCTION 31
4.2 RECOMMENDATION 1: ENHANCE AND FACILITATE THE CREATION OF HEALTH SECTORAL CSIRTS 31
4.3 RECOMMENDATION 2: CAPITALISE ON THE EXPERTISE OF THE HEALTH CSIRTS FOR HELPING OESS DEVELOP THEIR IR CAPABILITIES 31
4.4 RECOMMENDATION 3: EMPOWER HEALTH CSIRTS ROLE ON INFORMATION SHARING ACTIVITIES 32

5. BIBLIOGRAPHY 33

A ANNEX: SURVEY – QUESTIONNAIRE 37

EXECUTIVE SUMMARY

In recent years, digitalisation has turned everything into something connected and smarter. However, while creating numerous opportunities for the European economy and society, technologies bring forward several new challenges. According to a recent study[1], cyber threats increase year over year, as the popularity of emerging technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), big data, the large use of cloud computing, as well as connected devices, provide copious ways to invade an organisation.

An attack directed at a critical infrastructure, such as a hospital, can lead to physical damages and put the lives of patients at risk[2]. Therefore, there is a need for solid Incident Response Capabilities (IRC) in the health sector, in particular health care settings (including hospitals and private clinics). This sector indeed faces threats along its entire supply chain with potentially disastrous societal consequences for a multiplicity of stakeholders (citizens, public authorities, regulators, professional associations, large industries, SMEs), which become even more vulnerable in the context of the Covid-19 pandemic.

This report focuses on sectoral CSIRT capabilities status and development within the health sector since the implementation of the NIS Directive. The aim of the report is to offer insights on current incident response (IR) trends in order to draw practical recommendations about the development of IR capabilities in the health sector.

KEY FINDING

Based on a methodological approach, a series of findings is identified, as follows:

Key Finding #1 The main entity in charge of Incident Response in the health sector are National CSIRTs. Health Sectoral CSIRTs are still an exception across Member States. However, there is a strong trend in developing sector-wide CSIRTs collaborations, which include, but are not limited, to information sharing.

Key Finding #2 The creation of sector-specific IRC in the health sector appears to be the result of the lack of sector-specific knowledge of the National CSIRT, as well as lesson learned from past incidents, and the implementation of the NIS Directive.

Key Finding #3 National Health Sectoral CSIRTs tend to provide services more adapted to the sector's specificities and needs in addition to the generic services provided by National CSIRTs.

Key Finding #4 According to the respondents to the survey, the main resources and tools in place to support the development of constituents' IRC in the health sector are shared frameworks for incident classification and threat modelling, training and education activities and a network of IR actors.

[1] https://research.checkpoint.com/2020/the-2020-cyber-security-report/
[2] https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital

Key Finding #5 This study found out that the key forces driving CSIRTs' IR development are sector-specific clarifications on the security requirements and responsibilities of the organisations, and the exchange of IR related information.

Key Finding #6 When it comes down to IR, this study found out that the main challenges faced by the health CSIRTs are the lack of security culture among operators of essential services (OESs), the fact that management (and the security) of OESs IT infrastructure is often outsourced, and the lack of established cooperation tools and channels with OES incident response teams.

The study makes the following recommendations:

- Enhance and facilitate the creation of healthcare sectoral CSIRTs.
- Capitalise on the expertise of the healthcare CSIRTs for helping Operators of Essential Services (OESs) develop their IR capabilities.
- Empower healthcare CSIRTs role on information sharing activities.

LIST OF ABBREVIATIONS

AEDs	Vital providers and providers of essential services
ANSSI	National Agency for the Security of Information Systems
CCB	Cyber Security Belgium
CERT	Computer Emergency Response Team
CII	National Critical Information Infrastructure
CSIRT	Computer Security Incident Response Teams
DSP	Digital Service Providers
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
ICT	Information and Communication Technology
IOC	Indicators of Compromise
IoT	Internet of Things
IR	Incident Response
IRC	Incident Response Capabilities
IT	Information Technology
MISP	Malware Information Sharing Platform and Threat Sharing
NCSC	National Cyber Security Center
OES	Operators of Essential Services
SOP	Standard Operating Procedure
TTP	Tactics, Techniques, and Procedures

1. OVERVIEW AND SCOPE OF THE STUDY

1.1 CONTEXT OF THE STUDY

The **volume and intensity of cyberattacks** on the health sector increased in 2020[3][4] (e.g., Ryuk ransomware[5]; shut down of the UVM Health Network[6]). Health care organisations in general and hospitals in particular have been a major target for cybercrime, primarily because of the value of data that can be obtained from an attack, as well as its disruptive impact[7].

The cyber threats are now **increasingly visible** to executive committees, boards, politicians and citizens. It is now mandatory for companies, governments, and citizens to think about and act upon cybersecurity[8]. To face such threats, Member States and public and private entities must strengthen their Incident Response (IR) capabilities and the coordination between Computer Security Incident Response Teams (CSIRT).

As critical infrastructure and services, health care organisations, including hospitals and private clinics must be prepared to face such cyber-attacks. **Disruption of their services would lead to fundamental impact on both governments and populations**.

Nevertheless, the number of highly technical-skilled cybersecurity experts is insufficient. To fill the gap between the demand and the human resources available, the public and the private sector have started to work together to create new training programmes and certifications for cybersecurity experts / IR experts. ENISA has also been working on the European Cybersecurity Skills Framework[9]. These new experts led to the multiplication of response teams (CSIRT) for both the public and the private sector.

Regarding this evolution of CSIRTs in the health sector, some new topics may emerge in which ENISA will be a key player. On one hand, **ENISA supports the NIS Directive enforcement as the Secretariat of the CSIRT Network**, tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request. ENISA also supports sectorial CSIRTs in the standardisation of exchanges and monitoring specific sectorial threats at national/European scale.

On the other hand, **ENISA works to strengthen public and private relationships within the health sector** by building a trust circle at European scale. For example, by setting up a collaboration platform dedicated to EU Member States and fostering relevant information sharing and analysis initiatives Several R&D initiatives at team levels need to be steered at European level to foster cross-CSIRTs developments, at least with guidelines about IR/Threat Intelligence priorities for EU.

[3] ENISA Threat Landscape 2021, https://www.enisa.europa.eu/topics/threat-risk-management
[4] https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-health care-sector-during-covid-19-pandemic
[5] https://edition.cnn.com/2020/10/28/politics/hospitals-targeted-ransomware-attacks/index.html
[6] https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html
[7] https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-health care-institutions-with-ransomware
[8] https://assets.kpmg/content/dam/kpmg/fr/pdf/2019/04/fr-complying-with-the-eu-nis-directive.pdf
[9] See https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

In this context of rapid growth of CSIRTs in Europe, this study supports ENISA and Member States towards a better understanding of sectorial CSIRTs and their current IR capabilities, on which they rely in case of major and systemic cyber-attack. The objectives of the study are explained in more detail in the following section.

1.2 OBJECTIVES OF THE STUDY

This study aims to support the understanding of the status and development of sectoral healthcare CSIRTs across EU[10]. The conclusions of the study should help ENISA and Member States to **identify and draw conclusions about the development of incident handling and response (IR) within the health sector** following the implementation of the NIS Directive.

The study looks into **potential gaps, overlaps and challenges** in the services offered as well as in the **procedures**, **processes** and **tools** in place. More specifically the study provides an overview of the key factors facilitating or hindering the development of sectoral CSIRTs in this particular sector, as well as the specific resources and tools in place to support the development of IRC in the health sector.

The main objectives of this study are the following:

- To **collect data** on the current IRC in the health care sector;
- To **analyse gathered information** to assess **current sectorial capabilities, services, processes, tools and cooperation mechanisms**; and
- To draw **conclusions and recommendations** based on the key aspects facilitating and or hindering IR procedures.

The study aimed to collect relevant information in order to provide the following:

- Statistics of distribution of services offered to constituency by CSIRTs and other IR entities;
- Analysis of the tools used (e.g., open source / commercial / homemade) and their distribution within CSIRTs and other IR entities;
- Analysis of the IR setup (e.g., central, distributed, hybrid, etc.) and the resources needed to provide services (e.g., number of resources, skillset, etc.);
- Analysis of gaps and overlaps in services, processes, tools, resources, especially between CSIRTs and other IR entities within the health sector;
- Description of existing policies and guidelines applicable to IR;
- Good practices and lesson learned; and
- Conclusions and recommendations for the development of CSIRTs and other IR entities.

The study findings may also support ENISA with the delivery of the **Output 8.2 of "ENISA single programming document 2021-2023" Activity 8**: *'Provide targeted as well as general reports, recommendations, analysis and other actions on future cybersecurity scenarios and threat landscapes (incident response landscape mapping for NIS Directive sectors)'*.

To achieve the project objectives, a solid methodological approach was proposed based on **desktop research** and an **online questionnaire** distributed to EU National CSIRTs and Sectoral CSIRTs as well as OES Incident Response Teams. The methodological approach is further explained under section 2.

[10] Health care providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council.

2. METHODOLOGY AND DATA COLLECTION

2.1 OVERVIEW OF THE METHODOLOGY

This Chapter describes the methodological approach taken for identifying, collecting and analysing data on IR development and capabilities in the health care sector.

2.1.1.1 Definition of the research focus for the data collection

The scope of the research and the focus for data collection was mainly on the operational domain as outlined by ENISA based on current needs and previous work already conducted on IR. At this stage it was also decided that the data collection methods would be mainly desktop research and an online survey.

2.1.1.2 Desktop research on the health sector IRC

A literature review was conducted to investigate all aspects of IR responsibilities within the health sector for CSIRTs and other entities in each EU Member State. The desktop research was guided by the need to:

- **identify the relevant bodies and/or organisations** that play a role in the field of IR capabilities within the health sector in the European Union; and
- **analyse the IR responsibilities** of the different stakeholders, focusing on the **operational aspects of IR**.

While conducting desktop research we reviewed previous ENISA publications, policy documents, national strategies and other documents and reports made available by CSIRTs, National Cybersecurity Centres, and the European Commission. Additionally, studies carried out by technology research, strategic research companies, and academic researchers were consulted. The activities at this stage also included informal consultation with IR experts.

2.1.1.3 Designing and testing the online survey

Based on the categorisation of public available information, we were able to identify gaps and additional information needed to be collected to complement desk research. As such, a questionnaire was designed and made available online in order to collect relevant data on IR setup, and related services, procedures, processes and tools. The survey also covered the main enabling and hindering factors for establishing sectoral CSIRTs as well as the specific resources and tools in place to support the development of incident response capabilities (IRC) in the health sector.

Before being distributed to stakeholders the online questionnaire was extensively tested to ensure that the questions addressed the study objectives and that they are clear, coherent, and covered all relevant aspects of IR capabilities in the health sector. The final version of the questionnaire is available in **Annex A: Survey – questionnaire**.

2.1.1.4 Conducting the survey

Upon validation, the questionnaire was uploaded on EU Survey and the link was distributed by ENISA to the members of the CSIRTs Network (CNW), the CyCLONe Network, and the NIS Cooperation Group. The survey included an introduction to the objectives of the study, instructions on how to respond to the questionnaire, and a privacy statement.

The survey was available online for four weeks. ENISA followed-up weekly with the targeted audience and sent reminders to the respondents to complete their contributions. A total of 15 responses were provided representing 12 Member States.

2.1.1.5 Analysis and identification of recommendations

We performed an analysis of the raw data collected from the desktop research and the survey which were aggregated in a structured matrix. This preliminary analysis allowed the mapping of the key findings of the study.

2.1.1.6 Final report

Final remarks and/or feedback from the pool of experts that were used to validate the study (the study was distributed for validation to the same group of stakeholders to which the survey was distributed) were incorporated in the final report.

3. KEY FINDINGS

3.1 IRC SET-UP AND LANDSCAPE

The main entity in charge of incident response in the health sector are National CSIRTs. Health Sectoral CSIRTs are still an exception across Member States[11]. However, there is a trend in developing sector-wide CSIRTs collaborations, which include, but are not limited, to information sharing.[12]

The results of desk research and the survey targeting relevant bodies and organisations that play a role in the field of incident response capabilities within the EU health sector[13] shows that:

- 22 out of 27 Member States have no Health Sectoral CSIRTs, but 2[14] have plans to create one in the near future;
- 2 Member States[15] are currently setting up a Health CSIRT at national level; and
- 3 Member States[16] have a Health Sectoral CSIRT at national level. Among these Health Sectoral CSIRT, 2 (CERT Santé and HealthNet) were created respectively by the French and Luxembourgish government; meanwhile, Z-CERT, the Dutch Health Sectoral CSIRT, was created by operators of essential services.

In addition to Z-CERT, the data collected highlight that an increasing number of sectoral CSIRTs is being created by operators of essential services[17]. Evidence of this trend is HelseCERT, Norway health and care sector's national centre for cyber security[18]. Although Norway is not a member of the European Union, HelseCERT is an interesting Health Sectoral CSIRT to mention among the CSIRTs operating in the European Free Trade Association (EFTA) countries.

Table 1 provides a summary of the sectoral IR layout and set-up at European level in the health sector[19].

[11] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
[12] https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1
[13] Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q5. Do you know if the health sector has, or is going to have a dedicated CSIRT in your country of operation? N=15.
[14] Austria and Croatia.
[15] Bulgaria and Denmark.
[16] Luxembourg, France, and the Netherlands.
[17] https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1
[18] https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert
[19] The information related to the following 12 Member States were collected through the survey: France; Bulgaria; Czech Republic; Latvia; Austria; Croatia; Finland; Estonia; Cyprus; Hungary; Spain; Denmark. The remaining findings come from desk research.

Table 1: Overview of all MS' basic IR set-up in the health sector (with available data collected)

Countries	Summary of national approach towards IR in the health sector	Presence of Health Sectoral CSIRT	Development status
Austria	CERT.at[20] is the Austrian national CERT. CERT.at is the primary contact point for IT-security in a national context. In the case of significant online attacks against Austrian health care infrastructure, CERT.at will coordinate the response by the targeted operators and local security teams.	No	Planned to be developed
Belgium	The federal Computer Emergency Response Team, in short CERT.be[21], is the operational service of the Centre for Cyber Security Belgium (CCB) and acts as National CSIRT in the CSIRTs Network. CERT.be acts as coordinator for all Sectoral CSIRT at national level. Belgium currently does not have a dedicated entity for the health sector.	No	N/A
Bulgaria	CERT Bulgaria[22] (English) is the National Computer Security Incident Response Team. Bulgaria is currently creating Sectoral CSIRTs to facilitate the implementation of the NIS Directive. However, it does not have yet a Health Sectoral CSIRT.	No	In progress
Croatia	National CERT (CERT.hr[23]) is responsible for prevention from cyber threats and protection of the security of public information systems in the Republic of Croatia. Croatia does not have a dedicated Health Sectoral CSIRT.	No	Planned to be developed
Cyprus	CSIRT-CY[24] is the National Computer Security Incident Response Team for Cyprus. In Cyprus, there is no dedicated entity for the health sector.	No	N/A
Czech Republic	CSIRT.CZ[25] is the National CSIRT of the Czech Republic. The Czech Republic does not currently have a dedicated Health Sectoral CSIRT.	No	N/A
Denmark	The Centre for Cyber Security (CFCS)[26] is the national IT security authority. In Denmark, there is a Health Sectoral CSIRT, the Danish Health Data Authority, which is currently under development[27].	No	In progress
Estonia	CERT-EE[28], established in 2006, is an organisation responsible for the management of security incidents that occur in Estonian networks. There is no dedicated entity for the health sector.	No	N/A

[20] https://cert.at/de/
[21] https://cert.be/en
[22] https://www.govcert.bg/BG
[23] https://www.cert.hr
[24] https://csirt.cy
[25] https://csirt.cz/cs/
[26] https://www.cybersecurityintelligence.com/centre-for-cyber-security-cfcs-denmark-3071.html
[27] Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q5. Do you know if the health sector has, or is going to have a dedicated CSIRT in your country of operation? N=15.
[28] https://www.ria.ee/en/cyber-security/cert-ee.html

Countries	Summary of national approach towards IR in the health sector	Presence of Health Sectoral CSIRT	Development status
Finland	The National Cyber Security Centre Finland (NCSC-FI[29]) is responsible for the supervision of all Finnish CSIRTs. The Social Insurance Institution of Finland that operates the national health information database is considered to make an efficient supervisory authority for the health sector. However, there is no concrete plans to implement a sector specific CSIRT.[30]	No	N/A
France	Within the *Agence nationale de la sécurité des systèmes d'information* (ANSSI), the CERT-FR[31] is responsible to put in place the necessary means of protection and to respond to incidents or computer attacks within France. According to the survey[32] findings, France has a dedicated Sectoral CSIRT for the health sector, CERT Santé (previously called *Accompagnement Cyber sécurité des Structures de Santé)*, which has been in place since 2017[33].	Yes	In place
Germany	CERT-Bund[34] (Computer Emergency Response Team for Federal Agencies) is the central point of contact for preventive and reactive measures regarding security-related computer incidents. There is no dedicated entity for the health sector in Germany.	No	N/A
Greece	The Hellenic Computer Security Incident Response Team (GR-CSIRT[35]) is the Nation's flagship cyber defense, incident response, and operational integration centre. Greece does not currently have a Health Sectoral CSIRT.	No	N/A
Hungary	The National Cyber Security Centre (NCSC) for Hungary helps with the entire information security lifecycle of the electronic information systems, from its evolution, the planning phase, the regulation, to control and the incident handling. There are three organisational units in the National Cyber Security Centre according to their tasks. The GovCERT-Hungary[36] unit is responsible for incident handling issues. There is no dedicated entity for the health sector.	No	N/A
Ireland	CSIRT-IE[37] is the body within the National Cyber Security Centre (NCSC) that provides assistance to constituents in responding to cyber security incidents at a national level for Ireland. CSIRT-IE also acts as a national point of contact for cyber-attacks involving health care entities within Ireland. There is no dedicated entity for the health sector.	No	N/A

[29] https://www.kyberturvallisuuskeskus.fi/en/
[30] Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Comment to Q6. What are the key reasons to create such sector-specific incident response capacities? N=15.
[31] https://www.cert.ssi.gouv.fr/
[32] Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q5. Do you know if the health sector has, or is going to have a dedicated CSIRT in your country of operation? N=15.
[33] https://esante.gouv.fr/securite/cert-sante
[34] https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html
[35] https://csirt.cd.mil.gr/
[36] http://www.cert-hungary.hu/
[37] https://www.ncsc.gov.ie/CSIRT/

Countries	Summary of national approach towards IR in the health sector	Presence of Health Sectoral CSIRT	Development status
Italy	Computer Security Incident Response Team - Italia sits within the Italian Department of Security Information[38]. Computer Security Incident Response Team - Italia promotes the use of common practices and standards in risk management and incident-response, as well as classification of incidents, risks and information. There is no dedicated entity for the health sector in Italy.	No	N/A
Latvia	CERT.LV[39] is the Information Technology Security Incident Response Institution of the Republic of Latvia. Its mission is to promote information technology (IT) security in Latvia. Latvia does not have a Health Sectoral CSIRT.	No	N/A
Lithuania	CERT-LT[40] is the national electronic communications network and information security incidents investigation service operating as the national Computer Emergency Response Team. There is no dedicated entity for the health sector in Lithuania.	No	N/A
Luxembourg	There are two National CSIRT in Luxembourg. The Computer Incident Response Centre Luxembourg (CIRCL) and GOVCERT, which provide a systematic response facility to computer security threats and incidents. HealthNet-CSIRT[41] (HealthNet Computer Security Incident Response Team) is the point of contact for processing computer incidents encountered by the various stakeholders active in the health domain.	Yes	In place
Malta	CSIRT Malta supports critical infrastructures organisations in Malta on how to protect their information infrastructure assets and systems from cyber threats and incidents. There is no dedicated entity for the health sector in Malta.	No	N/A
Netherlands	The National Cyber Security Centre (NCSC.NL)[42] is responsible for the coordination of incident response measures for Dutch government institutions, as well as entities engaged with critical infrastructure. The Netherlands has a dedicate Heath Sectoral CSIRT: Z-CERT. Z-CERT[43] is a Computer Emergency Response Team (CERT), developed specifically for institutions in the health care sector.	Yes	In place

[38] https://csirt.gov.it/
[39] https://cert.lv/lv
[40] https://www.cyberwiser.eu/lithuania-lt
[41] https://www.esante.lu/portal/lu/service_project/doc_manager/download.php?&vars=_pK_T42MKWdx7OkFVlRBZcp9cqjjQ26EcabnfG3otSw
[42] https://www.ncsc.nl/
[43] https://www.z-cert.nl/

Countries	Summary of national approach towards IR in the health sector	Presence of Health Sectoral CSIRT	Development status
Poland	The three National CSIRTs are the Computer Security Incident Response Team (CSIRT GOV)[44], the Polish MOD Computer Security Incident Response Team (CSIRT MON)[45] and the Computer Emergency Response Team CERT POLSKA[46], which all contribute to ensuring cyber security at the national level. There is no dedicate health care entity.	No	N/A
Portugal	The CERT.PT[47] is a service integrated in the Portuguese National Cybersecurity Centre that coordinates the response to incidents involving the national cyberspace. Portugal does not have a Health Sectoral CSIRT.	No	N/A
Romania	CERT.RO[48] is the national Computer Emergency Response Team of Romania, established as an independent structure for research, development and expertise in the field of cyber-security. There is no dedicated entity for the health sector in Romania.	No	N/A
Slovakia	The National Cyber Security Centre SK-CERT[49] provides national and strategic activities in the field of cyber security management, threat analysis as well as coordination of national security incident resolution. There is no dedicated entity for the health sector.	No	N/A
Slovenia	SI-CERT[50] (Slovenian Computer Emergency Response Team) is a designated national computer security incident response team (CSIRT) that operates within the framework of the Academic and Research Network of Slovenia public institute. Slovenia does not have a dedicated entity for the health sector.	No	N/A
Spain	INCIBE-CERT[51] is the reference security incident response centre for citizens and private law entities in Spain, operated by The Spanish National Cybersecurity Institute (INCIBE), under the Ministry of Economic Affairs and Digital Transformation through the Secretary of State for Digitalisation and Artificial Intelligence. There is no dedicated entity for the health sector.	No	N/A
Sweden	CERT-SE[52] is Sweden's National CSIRT (Computer Security Incident Response Team) with the task of supporting society in the work of managing and preventing IT incidents. Sweden does not currently have a dedicated health sectoral CSIRT.	No	N/A

[44] https://csirt.gov.pl/cee
[45] https://csirt-mon.wp.mil.pl/en/
[46] https://cert.pl/
[47] https://www.cncs.gov.pt/pt/certpt//
[48] https://cert.ro
[49] https://www.sk-cert.sk/sk/aktuality/index.html
[50] http://sicert.net/
[51] https://www.incibe-cert.es/
[52] https://www.cert.se/

As illustrated in Table 1, at national level, incident response set-up is structured around:

- IR services are provided by the national/governmental CSIRT in each EU Member State for all sectors, including the health sector. This applies in particular to countries with a centralised incident response model, which do not plan to develop specific sectoral CSIRT capabilities since IR tend to be managed by the OES and supervised by the National CSIRT or governmental CSIRT[53].
- For three[54] Member States, dedicated sectoral CSIRTs coordinate incident response at national level, supervised by the National CSIRT.

To conclude, it is worth mentioning the existence of the Health Information Sharing and Analysis Centre (H-ISAC). H-ISAC is a global, non-profit, member-driven organisation offering health care stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other[55]. Launched in 2010 in the US, H-ISAC dropped its national focus in favour of an international one in 2018[56]. Nowadays H-ISAC facilitates knowledge transfer across the world through educational summits, webinars, workshops and white papers, supporting in this way the exchange of information and the building of relationships that may contribute to make the health sector more resilient and proactive in the face of future cyberattacks.

H-ISAC is not an isolated initiative. There is a multiplication of ISACs and networks to foster information exchange and increase awareness among stakeholders within a sector, even for sectors than are not defined in the NIS Directive [57].

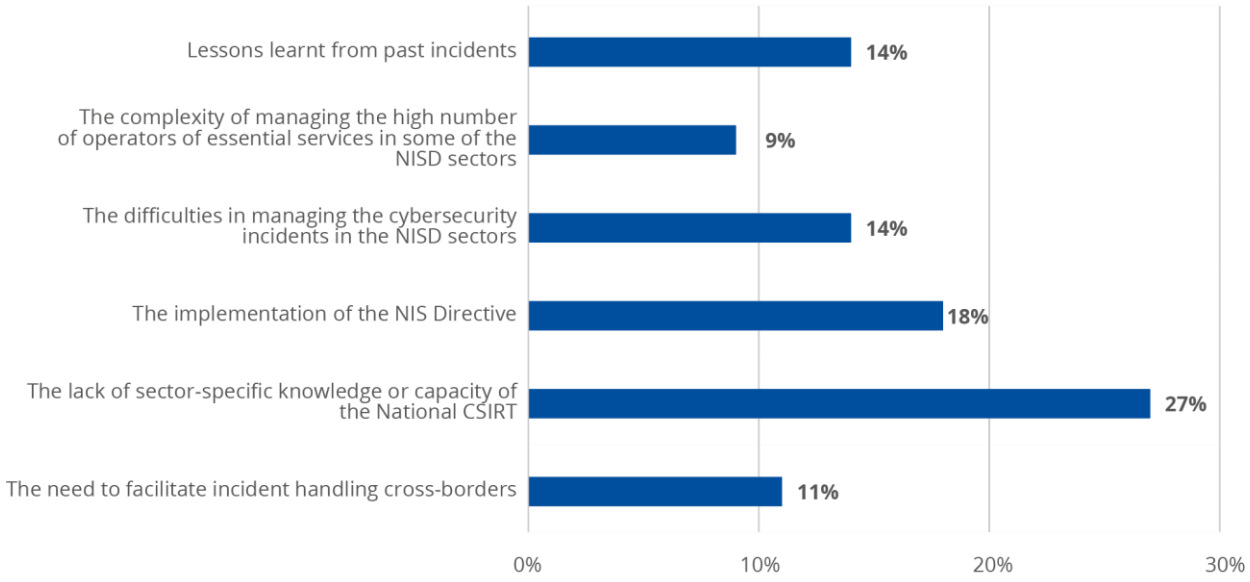
3.2 CREATION OF SECTORAL CSIRTS

The creation of sector-specific IR capacities in the health sector appears to be the result of the lack of sector-specific knowledge of the National CSIRT, as well as lessons learned from past incidents, and the implementation of the NIS Directive.

Figure 1 presents the findings of the survey (all respondents provided an answer) in relation to the key reasons that motivated Member States to create sector-specific incident response capacities in the health sector.

[53] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
[54] Luxembourg, France, and the Netherlands.
[55] https://h-isac.org/
[56] https://www.prnewswire.com/news-releases/nh-isac-changes-name-to-health-isac-h-isac-300706786.html
[57] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report

Figure 1: Reasons to create sector-specific IR capacities[58]



Source: Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q6. What are the key reasons to create such sector-specific incident response capacities? (N=15).

The need to overcome the lack of sector-specific knowledge or capacity of the National CSIRT appears to be the most relevant reason behind the creation of sector specific IR capacities (27% of responses). Similarly, 'The difficulties in managing the cybersecurity incidents in the NIS Directive sectors' (14% of responses), together with the 'Lessons learned from past incidents' (14% of responses), highlighted the need for sector-specific IR capacities in the health sector, according to the survey respondents.

However, the second most important reason with 18% of responses is the implementation of the NIS Directive. This confirms the ENISA finding related to the sector-specific capabilities of the Energy and Air transport sectors[59]: European legislation has an important and positive impact in pushing actors to develop sectoral capacities.

In particular, the survey respondents indicated that the NIS Directive had the following impacts on their activity related to the creation of sectoral IR capacities[60]:

- Provided additional financial support for security measures;
- Changed the structures and architectures of the existing cybersecurity measures; and
- Expanded the scope of CSIRTs' responsibilities.

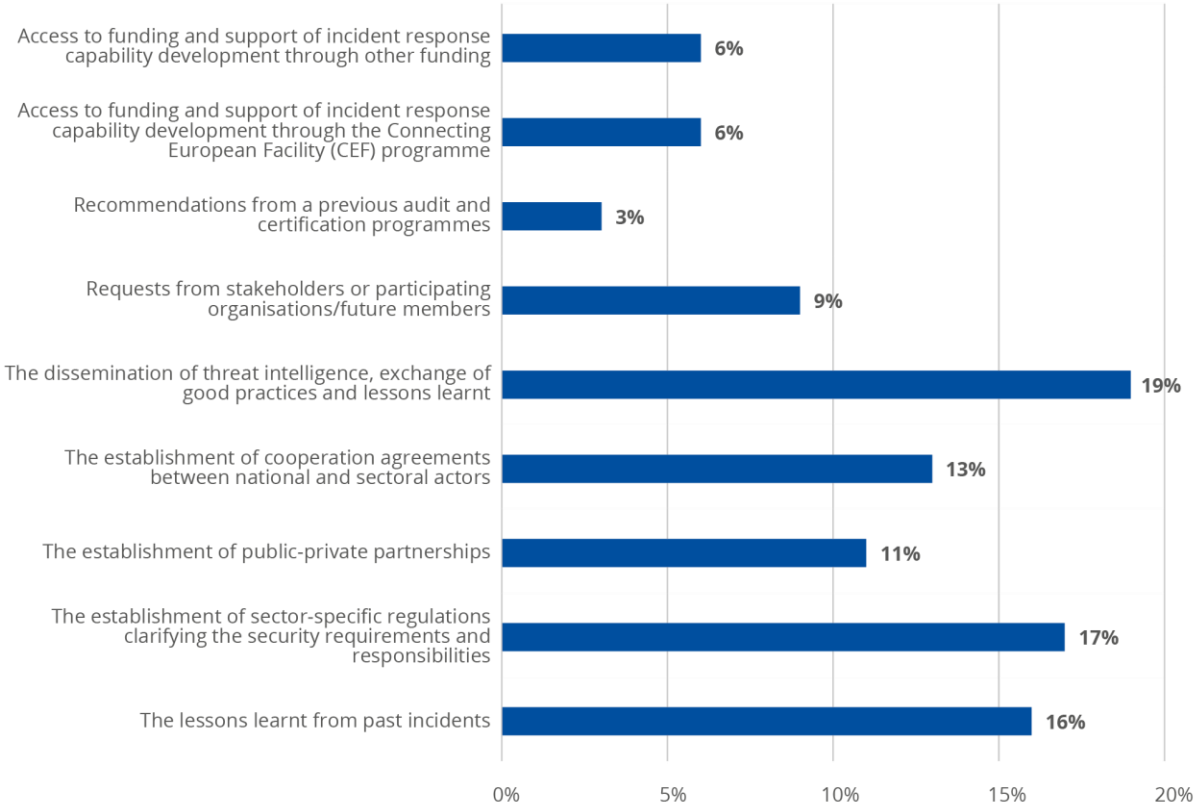
The expansion of the scope of the CSIRTs' responsibilities, combined with the provision of additional financial support for new security measures, appear to have encouraged the creation of sector-specific IR capabilities.

Factors facilitating the development of sectoral CSIRTs

As Figure 2 shows, apart from the main reasons that lead to the creation of sectoral CSIRTs and/or incident response capacities, there are also key factors facilitating their development.

[58] 7% of responses were 'Other'. This option was chosen when the question was not applicable to the survey respondent or to provide additional information related to the options mentioned in the graph.
[59] https://www.enisa.europa.eu/publications/sectoral-csirt-capabilities-energy-and-air-transport
[60] Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q7. What impact(s) do you think the NIS Directive had on your activity? (N=15).

Figure 2: Factors facilitating the development of sectoral CSIRTs



Source: Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q11.Based on your experience, what are the key factors facilitating the development of sectoral CSIRTs and/or incident response capacities? (N=15).

According to the survey respondents, the main enabling factors are the following[61]:

- **The dissemination of threat intelligence, exchange of good practice and lessons learned** (19% of responses): There is an emerging trend in which actors, and CSIRTs in the same sector go beyond information sharing to organise IRC[62]. Sectoral actors make use of existing reporting schemes such as the NIS Directive reporting and build trusted sectoral communities of users, which can securely exchange both ex-ante and ex-post incident information leveraging existing tools and automated solutions[63].

- **The establishment of sector-specific regulations clarifying the security requirements and responsibilities** (17% of responses): Sector specific regulations, including guidelines and requirements for reporting and management of incidents, tend to act as a key driver to enhance capabilities at the sectoral level[64]. An example of sectoral regulation is Regulation (EU) 2017/745 on medical devices (MDR)[65], which bound manufacturers of medical devices to consider cybersecurity risks when placing product in the market.

[61] The lessons learned from past incidents was already considered among the main reasons that lead to the creation of sectoral CSIRTs, therefore, it has not been taken into consideration as a key facilitating factor.
[62] https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025
[63] https://www.enisa.europa.eu/publications/sectoral-csirt-capabilities-energy-and-air-transport/at_download/fullReport
[64] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
[65] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0745-20200424

- **The establishment of cooperation agreement between national and sectoral actors** (13% of responses)[66]: The support of National CSIRTs and other Sectoral CSIRTs to the development of Health Sectoral CSIRTs and capabilities tends to be of great added value because it capitalises on existing expertise. Sectoral actors can benefit from the experience and knowledge of National and other Sectoral CSIRTs, for instance, through the appointment of a liaison officer, sharing of know-how, expert advice or tailored training.[67] A noteworthy initiative, pre-dating the NIS Directive, is that of the Dutch NCSC, which provided incentives and guidelines to support the creation of CERTs [68].

- **The establishment of public-private partnership** (11% of responses): Public-private partnerships are also a tendency in some Member States, as they play a key role in certain IR related activities. For instance, they can encourage the sharing of lessons learned on the use of open-access or commercial tools, especially those automated within a specific sector to better benefit from each other's experience and accelerate the maturation of newly created IR entities. However, desk research indicated that among all the tasks under the scope of the CSIRTs, establishing cooperation relationships with the private sector was one of the tasks with the least allocated time[69].

Overall, from Figure 2, it appears that a blend of bottom up and top down incentives could lead the way to the creation of sectoral CSIRTS and IR capabilities. Funding and the guidance of National CSIRTs are as important as the cooperation and information sharing across sectoral actors for the development of Sectoral CSIRTs[70].

Table 2 presents the reasons and enabling factors that lead to the creation of a Health Sectoral CSIRT in the Netherlands.

[66] This finding was confirmed by the answer provided by the survey respondents to the following question: Q13. Does your organisation need / have you asked for any specific support or guidance from external stakeholders to design and implement sectoral incident response capacities.The majority of the respondents (53%, 8 out of 15) reported that their organisation asked for specific support or guidance from external stakeholders to design and implement sectoral incident response capacities, in particular the support of National Authorities and CSIRT communities and peers.
[67] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
[68] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
[69] https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1/language-en
[70] https://www.enisa.europa.eu/publications/sectoral-csirt-capabilities-energy-and-air-transport/at_download/fullReport

Table 2: Case Study – Creation of the Z-CERT (The Netherlands)

Case study - The Netherlands
The Z-CERT was founded in 2017 by a group of Dutch hospitals, to help health care institutions with cyber security protection and incident support. In 2017, all Dutch hospitals had shown to have vulnerabilities in their systems. The most prominent risks were configuration errors and websites running on outdated software[71]. Z-CERT was founded to overcome these IR weaknesses and provide specialised IR services to health care institutions. Z-CERT and National Cyber Security Centre (NCSC) work together by sharing relevant information and data. Today all hospitals (ranging from academic “UMCs”, top clinical “STZ” to “General” hospitals) as well as mental health care institutions ("GGZ") can register with Z-CERT as a participant to the Health Sectoral CSIRT constituency, and can, therefore, benefit from Z-CERT cyber security protection and IR support and knowledge.[72] It appears that the responsibilities and services of Z-CERT will be expanded in the near future. COVID-19-related developments have accelerated Z-CERTs plans to implement Cyber Threat Intelligence Capability as well as other projects to enhance the digital resilience of the Dutch Health Care[73].
Sources
https://www.z-cert.nl/english/ https://www.cybersprint.com/news/cybersprints-study-leads-to-national-investigation-into-Health cares-cyber-security/ https://www.thehaguesecuritydelta.com/partners/partner/663-z-cert https://www.prnewswire.com/news-releases/z-cert-and-eclecticiq-cooperate-to-bring-benefits-of-cti-to-dutch-Health care-sector-301073185.html

The main reasons that seem to have led to the creation of Z-CERT is that Dutch hospitals had shown to have vulnerabilities in their systems[74]. NCSC was only allowed by law to provide services to operators of essential and vital services, as well to the central government. Therefore, without Z-CERT, the Dutch health care would not have access to relevant threat intelligence, which were particularly in face of the increasing number of cyber attacked against the health sector.

3.3 CSIRTS SERVICES

Health Sectoral CSIRTs tend to provide services more adapted to the sector’s specificities and needs in addition to the generic services provided by National CSIRTs.

Depending on their mandate, Health Sectoral CSIRTs appear to offer the same kind of services as the National CSIRTs. However, Health Sectoral CSIRTs seem to provide services that are more fitted to the specificities of the health sector.

According to the information gathered through the survey[75], in comparison to National CSIRTs, the Health Sectoral CSIRT provide the following services, roles or functions:

[71] https://www.cybersprint.com/news/cybersprints-study-leads-to-national-investigation-into-Health cares-cyber-security/
[72] https://www.thehaguesecuritydelta.com/partners/partner/663-z-cert
[73] https://www.prnewswire.com/news-releases/z-cert-and-eclecticiq-cooperate-to-bring-benefits-of-cti-to-dutch-Health care-sector-301073185.html
[74] https://wetten.overheid.nl/BWBR0041520/2021-06-01
[75] Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q8. In your opinion, what are the specific services, roles or functions of the Sectoral CSIRTs in contrast to national, governmental or military CSIRTs? N=15.

- Specialised services to handle sector-specific threats, vulnerabilities and incidents;
- Specific knowledge and expertise on medical devices, medical IT systems, as well as threats and incidents related to the health sector;
- Providing sectoral expertise to the National CSIRT;
- Assisting nonregulated operators in the health sector on incident response;
- Coordination for multi-site compromised systems in the health sector; and
- Vulnerability coordination with vendors of sector-specific systems / devices.

Overall, survey respondents believe that sectoral CSIRTs may offer deeper and more specialised knowledge on sector-specific threats and operational technology, as well as broader networking with sectoral bodies and organisations. Evidently, this observation also depends on the scale and capabilities of the national CSIRT.

Considerations on proactive approach to incident response in the health sector

Incident response in the health sector tends to be often reactive, i.e. aimed at responding to threats or attacks against the CSIRT's systems, rather than proactive, i.e. aimed at preventing incidents and reduce their negative impact when they do occur. This reactive nature appears to be due to an insufficient communication and collaboration across different stakeholders of the vulnerability ecosystem (national/sectoral CSIRTs, end clients, Operators of Essential Services)[76]. To improve the current coordinated IRC to counteract threats, despite their reactive nature and responsibilities, sectoral CSIRTs may be an important player. Sectoral CSIRTs are indeed well placed to facilitate and encourage a more proactive approach to incident response, as they seem to have in-depth knowledge and close relationships with the main sectoral stakeholders at national level. They could also support the streamlining of information sharing, especially with OESs, which would highly benefit from guidance, for instance, in the form of guidelines and trainings, and exchange of knowledge and expertise[77].

Table 3 shows the services provided by the Health Sectoral CSIRTs in the Netherlands in comparison with the National CSIRTs. The services are presented per service categories according to the FIRST CSIRT Services Framework[78]. The service categories considered are the following:

1. **Information security event management**: This category includes monitoring, detection and event analysis services.
2. **Information security incident management**: This category refers to services, such as information security incident report acceptance, information security incident analysis, artifact and forensic evidence analysis, mitigation and recovery procedures, information security incident coordination, and crisis management support.
3. **Vulnerability management**: These services encompass vulnerability discovery / research, vulnerability report intake, vulnerability analysis, vulnerability coordination, vulnerability disclosure, and lastly, vulnerability response.
4. **Situational awareness**: This category consists of the following subtypes: analysis and synthesis and communication.
5. **Knowledge transfer**: It involves awareness building, training and education, exercises, technical and policy advisory.

[76] https://www.jmir.org/2021/4/e21747#figure2
[77] https://www.enisa.europa.eu/publications/csirt-expertise-and-capabilities-development
[78] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Table 3: Case Study – Z-CERT - Specific mandate and services compared with those the National CSIRT

Case study – The Netherlands	
National CSIRT's mandate	**Health Sectoral CSIRT's mandate (Z-CERT)**
The NCSC is the competent national authority for the implementation of the Network and Information Systems Security Act (Wbni), which has been in force since 9 November 2018. The Wbni regulates the statutory tasks of the NCSC in the field of cybersecurity. Organisations in vital sectors are obliged to report serious digital security incidents to the NCSC. Under the Wbni, the NCSC is the designated CSIRT for vital providers and providers of essential services (AEDs).	Z-CERT offers specialised services to health care institutions with regards to optimal cyber security protection and offers support in case an incident has occurred. Z-CERT has in-depth knowledge of medical applications, medical networks and medical devices.
National CSIRT's services	**Health Sectoral CSIRT's services**
Under the Wbni, the services offered by the NCSC include: **Information Security Event Management** - Monitoring incidents at national level, warning providers early and disseminating information about risks and incidents. **Information Security Incident Management** - Carrying out analyses and technical investigations into threats and incidents. **Vulnerability Management** - Responding to incidents that are reported voluntarily or mandatorily and assist AEDs and parts of central government in taking measures to guarantee the continuity of their services. **Situational awareness** - Maintaining cooperative contacts with the private sector. **Knowledge Transfer** - Sharing information with organisations tasked with informing other organisations or the public about threats and incidents, and computer crisis teams.	**Information Security Event Management** - Sending out alerts regarding possible threats and current attacks. - Checking periodically participants' IP addresses and domain names for multiple blacklists (viruses, worms, botnets, etc.). **Information Security Incident Management** - Conducting forensic research into the Modus Operandi, in order to minimize technical and financial damage as well as any reputation risk. **Vulnerability Management** - Immediately informing the participant(s) and offer advice in case viruses, worms, and botnets. - Offering advice on the approach and best resolution method of the incident. **Situational Awareness** - Informing its participants of any vulnerabilities detected in medical devices, medical networks and medical applications. **Knowledge Transfer** - Sharing knowledge with its participants. - Facilitating meetings for its participants, as well as hosts network events and theme sessions.
Sources	
https://www.z-cert.nl/english/ https://www.ncsc.nl/over-ncsc/wettelijke-taak	

The Dutch case seems to confirm the opinion of survey respondents and the desk research findings:

- Z-CERT appears to have **specific knowledge of the risks and threats targeting the health sector**, and is, therefore, better placed to inform sectoral operators of any vulnerabilities detected and provide advice on how best to deal with the situation.
- In addition, as Z-CERT works on a smaller perimeter than the National CSIRTs, it can also **invest more on proactive services**, such as sending out alerts and publishing white papers regarding possible threats and attacks.[79]
- Lastly, Z-CERT appear to have **more direct contact with sectoral operators**, which can, for instance, participle to Z-CERT networks events and theme sessions.[80]

3.4 IR TOOLS AND PROCEDURES

According to the respondents, the main resources and tools in place to support the development of constituents' IRC in the health sector are shared frameworks for incident classification and threat modelling, training and education activities and a network of incident response actors.

As per the article 9 of the NIS Directive, CSIRTs are responsible for risk and incident handling in accordance with well-defined process, supported by the adequate resources.[81]

3.4.1 Tools

There are 5 different types of possible tools according to the service they offer within the scope of CSIRTs' responsibilities:

1. **Information security event management tools.** This type includes monitoring, detection and event analysis tools.
2. **Information security incident management tools.** This area involves tools and procedures such as information security incident report acceptance, information security incident analysis, artifact and forensic evidence analysis, mitigation and recovery procedures, information security incident coordination, and crisis management support.
3. **Vulnerability management tools**. These services encompass vulnerability discovery / research, vulnerability report intake, vulnerability analysis, vulnerability coordination, vulnerability disclosure, and lastly, vulnerability response.
4. **Situational awareness tools.** This category consists of the following subtypes: analysis and synthesis and communication.
5. **Knowledge transfer tools.** It involves awareness building, training and education, exercises, technical and policy advisory tools.

The analysis of the CSIRTs through the survey offered the following perspectives:

- On average, half of the respondents indicated that there is a tool operating for each of the service (see Table 4 below).
- In the cases where there is not a tool in place, there is a plan to implement one quarter of the cases.
- Notably, only the crisis management support services underscore compares to this trend (only 33% of organisations have a tool in place).

[79] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report

[80] https://www.z-cert.nl/english/

[81] NIS Directive, Article 9.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Table 4: Uptake of tools per service/function

Service area and Services	Tool in service	Planning to implement one
Service Area 1 – Information security event Management		
Monitoring and detection	60%	27%
Event analysis	47%	33%
Service Area 2 - Information security incident management		
Information security incident report acceptance	67%	7%
Information security incident analysis	60%	27%
Artifact and forensic evidence analysis	53%	20%
Mitigation and recovery	47%	13%
Information security incident coordination	60%	27%
Crisis management support	33%	33%
Service Area 3 - Vulnerability management		
Vulnerability discovery / research	53%	27%
Vulnerability report intake	47%	27%
Vulnerability analysis	40%	27%
Vulnerability coordination	47%	33%
Vulnerability disclosure	40%	27%
Vulnerability response	40%	13%
Service area 4 – Situational awareness		
Data acquisition	53%	27%
Analysis and synthesis	47%	33%
Communication	73%	13%
Service area 5 – Knowledge transfer		
Awareness building	53%	20%
Training & Education	53%	20%
Exercises	53%	20%
Technical and policy advisory	47%	27%

Source: Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q24: Which specific tools does your organisation rely on to conduct the following services? (N=15).

Furthermore, CSIRTs tools may be developed in-house, or a service/tool procured from vendors.[82] As it will be mentioned in section 3.6 on CSIRTs Challenges and Gaps, the use of vendors' solutions comes with its own specific challenges, such as the import of unforeseen vulnerabilities in the tool. They will require additional efforts (on top of those for in-house systems) for updates and patches to guarantee their safety/efficiency.[83] Moreover, it is important to note that organisations that have fewer resources are more likely to look at external tools. This may lead to some type of incidental standardisation of security practices impacting on the overall performance of externalised tools users.

When asked about the specific information exchange tools to enable the notification of incidents, the stakeholders pointed that the most common ones were secure emails, Malware Information Sharing Platform and Threat Sharing (MISP) standard formats and technologies and special government secured networks. This also implies their reliance on internet access, obliging Health CSIRTs to have a minimum of two internet service providers or at least redundant physical connections.[84] Moreover, the stakeholders pointed out that, in the majority of the cases, uptake by the National CSIRTs ensured the broader uptake of these tools and procedures by their constituents.

Finally, according to the survey responses, the main resources and tools in place to support the development of constituents' IRC in the health sector are shared frameworks for incident classification and threat modelling (24% of responses), training and education activities (24%), and a network of incident response actors at a national or sectoral level to exchange good practices about information exchange, capabilities, cooperation (20%).

Table 5: List of tools in service for the five service areas of CSIRTs[85]

Service area	Tool family	Commercial tools	Free tools
Service Area 1 - Information security event Management	**Security informa tion and event management (SIEMs)**	Splunk, Elastic Stack, Arctic Hub	HIDS OSSEC, HAVARO, ADTimeLine, Autoreporter
		Network probes	
	Ticketing		Request Tracker (RT), Request Tracker for Incident Response (RTIR)
	Threat intel sharing		Malware Information Sharing Platform and Threat Sharing (MISP)
Service Area 2 - Information security incident management	**Security Orchestration Automation Response (SOARs)**	OTRS, Splunk	Rocket.chat, DFIR-ORC, RT, RTIR, IntelMQ
	Analysis Tool	Commercial Sandbox	Free Sandbox
Service Area 3 - Vulnerability management	**Vulnerability scanners**	Shodan for vulnerability discovery	Greenbone OpenVAS
	Ticketing		RT, RTIR

[82] https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation pg 14.
[83] https://www.forrester.com/report/Best+Practices+Medical+Device+Security/-/E-RES132003#
[84] https://www.enisa.europa.eu/publications/csirt-capabilities
[85] This list of solutions does exclude in house developed tools, however a number of in house solutions have been reported in the stakeholder consultation carried out for this study.

Service area	Tool family	Commercial tools	Free tools
Service area 4 - Situational awareness	**Security information and event management (SIEMs)**	Mattermost, Splunk, OTRS, MS Teams	OpenCTI
	Free		MISP, RT
	Generic		Cyber Threat Intelligence feeds, conferences, bulletins, training platforms
Service area 5 - Knowledge transfer		Mattermost, TSM, OpenEx, Intranet repository, Slack,	MISP, Wiki, E-mail, GitLab, SMS, Websites, Mailing lists, MS Teams, IRC
			Cyber exercises, YouTube, TV Commercials

Source: Survey for assessing incident response capabilities in the health sector, ENISA, June 2021. Q24: Which specific tools does your organisation rely on to conduct the following services? (N=15).

3.4.2 Procedures

Beyond the existing types of tools in place, there are other variants that should be considered in the analysis to guarantee a successful handling of incidents. The clarity and availability of the procedures in place are key in the course of incident response; procedures for usage of the tools should be always written down.

For instance, after the collection of the incident reported, CSIRTs ought to define and apply some type of information classification[86]. Following the incident classification, there should be a formal document indicating the statistics on how the handled incidents are created and disclosed. [87] Within this context, an over complicated or imprecise plan will deter a swift reaction to a cyberattack on an organisational level or prevent rising awareness on potential vulnerabilities across the sector or cross border.[88]

In this line, more than half of Health Sectoral CSIRTs offer clear procedures. In the consultation process carried out within the scope of this study, the stakeholders stressed that their organisation had standard operating procedures (SOPs) that OESs' teams should follow in case of incident in 67% of the cases. Moreover, 60% of respondents pointed that their organisation made use of an incident notification template, available to all constituents, while only 40% did not. In this context, according to the stakeholders consulted for this study, the most recurrent types of information reported through the different tools are root causes (20% of the cases), the services affected (18% of the cases), and the description of the incident, with the indicators of compromise (IOCs) and the tactics, techniques, and procedures (TTPs) (in 16% of the cases). This information compilation is important, as the use of a template indicates how efficiently and easily the CSIRTs can categorise the information collected.

In relation to the incident response in cross-border crisis situations, while half of respondents (47%) declared that there are specific procedures to address cross-border incidents, there is not a clear trend on how those are dealt with: in some cases, there is a sectoral or national procedure, in other cases it is done through a third-party Point of Contact. Some of the specific

[86] According to the NIS Directive, "To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for: (i) incident and risk-handling procedures; (ii) incident, risk and information classification schemes.", which are defined by them.
[87] https://www.enisa.europa.eu/publications/study-on-csirt-maturity
[88] https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation pg 13.

procedures mentioned by the respondents were the organisation of cross-border exercises or the participation of a representative of the other country in the crisis response processes.

Furthermore, these stakeholders stressed that in 60% of the cases, their CSIRTs had specific measures in place to inform the relevant actors (national authorities and OES) in neighbouring countries about an incident that may impact them; 47% percent would inform other stakeholders through a Point of Contact (a trusted third-party) while only 13% would rely on a direct contact (communicating with relevant actors using their direct contact information, without going through an intermediary).

Notably, while these recommendations are universally applicable, each health CSIRT has specific needs, which should be reflected in the tailoring of their tools and procedures. For that reason, each team should have an in-house developer that takes into account the requirements and suggestions that emerge from the team through their experience.[89] Moreover, procedures are dependent on workflows. Thus, they should be designed consequently, for instance with one procedure that fits all incidents reported, or various procedures for different types of incidents.[90]

Lastly, another key element to consider is the usage and maintenance of the CSIRTs solutions: tools and processes should be managed, tested, and updated in order to achieve full protection against attacks, as well as complementary training should be provided for the personnel who use them.[91]

3.5 IR MATURITY DEVELOPMENT

This study found out that the key forces driving CSIRT's IR development are sector-specific clarifications on the security requirements and responsibilities of the organisations, and the exchange of IR related information.

The maturity of a CSIRT is defined as the measurement of its capability in terms of structure, people, processes, and technologies. Its capabilities must guarantee that the organisation can perform its activities and functions consistently, as well as being able to continuously develop these capabilities.[92]

More in detail, ENISA has developed a maturity assessment model that can be used to evaluate the capabilities of CSIRTs.[93] Based on this maturity model, there are three pillars that greatly influence the development of CSIRTs capabilities: the uninterrupted performance of tasks and procedures, a workplace culture of continuous improvement of the CSIRT's capabilities (monitoring of tasks performance, for instance), and education and training continuously provided to the team (to educate and also update the teams expertise). In addition, it is key to put in place policies, procedures and workflows that support the team's goals and tasks, polished through real life application. Lastly, these pillars may only be attainable if the CSIRT fills in the following prerequisites: it must have been operating for a while, have sufficient budget and have a low turn-over rate of staff members.

CSIRTs maturity can be measured and classified in three levels:

- **Basic Maturity Level**: the CSIRT coordinates handling of incidents, has a minimum foundation in terms of their existence (mandate etc.), is easily reachable and has a basic incident handling process in place.

[89] https://www.enisa.europa.eu/publications/csirt-capabilities
[90] https://www.enisa.europa.eu/publications/csirt-capabilities
[91] https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation pg 14
[92] https://www.enisa.europa.eu/publications/csirt-capabilities
[93] https://www.enisa.europa.eu/publications/study-on-csirt-maturity

- **Intermediate Maturity Level**: the CSIRT coordinates the handling of incidents, and also allows additional joint activities (like vulnerability handling), it has a mature foundation, with detail descriptions of all relevant tools, processes, and human aspects.
- **Advanced Maturity Level**: the CSIRT coordinates the handling of incidents, while also reliably supports additional joint activities, such as sharing of threats and early-warning data, vulnerability handling. This implies that the CSIRT has well described, approved, and actively assessed processes, tools, and human aspects.

The assessment model offers a clear image of a CSIRTs maturity. According to this model, the average health CSIRT has achieved the Basic Maturity level and is close to achieve the Intermediate level of maturity, only needing to formalise already existing procedures.[94] Interestingly, more than 90 percent of all National CSIRTs or government teams with national scope reached the Basic Maturity level as well, according to the model, on average being close to reaching the Intermediate Maturity level.[95]

In the frame of the ENISA model, reaching the basic maturity level implies that the CSIRT analysed is operational, with a basic functioning incident handling process in place, its contact information available to other teams, fully functional in its other responsibilities, its services are defined according to the RFC2350, and the team has reached an appropriate level of maturity. These features are essential requirements for capacity building, collaboration with other CSIRTs and to support the national landscape of CSIRT.[96]

However, the consultation carried out for this study revealed that only 40% of Health CSIRTs use a specific CSIRT maturity assessment methodology to support the development of IRC within their sector. Within the 40% of stakeholders that use a specific CSIRT maturity assessment methodology, the majority of them relied on the SIM3 model (Security Incident Management Maturity Model), and to a lesser degree, the National CSIRT maturity tool available in their country. All methodologies are seen as relevant to enhance the maturity of CSIRTs. Moreover, they pointed that the key factors facilitating the maturity development of Health CSIRTs and/or their IR capacities depend mainly on the following:

- The establishment of sector-specific regulations clarifying the security requirements and responsibilities (18% of responses);
- The dissemination of threat intelligence, exchange of good practice and lessons learned (16% of responses); and
- To a lesser extent, the establishment of cooperation agreement between national and sectoral actors (13% of responses).

Unsurprisingly, the survey respondents explained that they seek specific support or guidance from external stakeholders to design and implement sectoral IR capacities in the majority of the cases, mainly through CSIRT communities/peers, national authorities, and industry players. Ultimately, both top-down and peer-to-peer support, in the form of training, tooling, and trusted communication channels, is needed for CSIRTs to reach an intermediate level of maturity, which requires further work on the organisational, human, tooling and process parameters. [97]

[94] In 80% of organisations the scope of responsibility has been defined; In 87% of the cases the classification of the incidents handled by the entities have been defined; Security policies have been stablished in 80% of the cases; The level of offer has been defined in 60% of the cases; The organisation approach to ensure the resilience of its personnel is defined on a 60 % of the cases; 70% of organisations have trainings and only 8% guidelines for the personnel.
[95] TI Accreditation was used as baseline for the Basic Maturity Level. https://www.trusted-introducer.org/processes/accreditation.html
[96] NIS Directive, Annex I (1a, 1c, 1e, 1f, 2a).
[97] https://www.enisa.europa.eu/publications/study-on-csirt-maturity

3.6 CSIRTS CHALLENGES AND GAPS

When it comes down to incident response, this study found out that the main challenges faced by the health CSIRTs are the lack of security culture among OESs, the fact that management (and the security) of OESs IT infrastructure is often outsourced, and the lack of established cooperation tools and channels with OESs incident response teams.

3.6.1 OESs cybersecurity challenges

In general, health care operators face some specific complications in the realm of cybersecurity and IR, due to the nature of their services. Consequently, these barriers also impact the work and efficiency of health CSIRTs in fulfilling their responsibilities. Below, the main challenges faced by health care providers are presented in more detail.

Equipment: legacy systems and lack of cybersecurity by design

Traditional sectors, including health care, are more vulnerable to cyberattacks health care operations and equipment have a long-lasting lifetime (15 years on average), they were not conventionally designed to deal with malicious acts from the beginning of the product life cycle[98], while at the same time the Information Technology cycles have continuously shorten in the past decades.[99]

These have resulted in a constant growing number of vulnerabilities founded in digital device providers and hardware manufacturers, forcing hospitals to update and adapt their systems in a very short span of time, accumulating vulnerabilities as a result of the IT layer obsolescence through their lifecycle. Hence, the pace of updates is quickly outrun by the pace of IT technology evolution. Moreover, this vendor dependence is accentuated by the IoT device adoption taking place in health care providers, leading to an endpoint complexity that expands greatly the areas that can be attacked.[100] The fact that this array of devices is closely interconnected only exacerbates the risk and potential impact of the threats. At the same time, practitioners usually circumvent security in order to deliver better care to patients.[101]

In this line, some recurrent problems are inappropriate encryption configurations, and the incapacity for safe health information sharing and exchange with third-party and cross-border partners (there are no sophisticated data security tools in the health industry).[102]

Organisational complexity meets incident reporting

Closely linked to the previous section, organisational complexity challenges the cybersecurity of health providers. The large supply chain of the health care ecosystem involves many stakeholders, which leads to potential cascade effects in the middle of a crisis. Concretely, existing organisational silos as well as excessive disparities among members of the hospital are recurrent risks.[103]

Moreover, the coordination of an incident response is highly affected by this complexity. In the course of an incident, overcomplicated response plans that involve many stakeholders delay the effectiveness of the procedure, as each team member is not always aware of their role in the process. As a result, the health sector tends to have a time lag between an attack and its detection.[104]

[98] https://www.jmir.org/2018/5/e10059?utm_source=TrendMD&utm_medium=cpc&utm_campaign=JMIR_TrendMD_0
[99] https://www.forrester.com/report/Best+Practices+Medical+Device+Security/-/E-RES132003#
[100] https://www.forrester.com/report/Best+Practices+Medical+Device+Security/-/E-RES132003#
[101] https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025
[102] https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7
[103] https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-r
[104] https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

Exchange of information

This study found out there is a lack of exchange of information and best practices on a sectoral level and across countries. It is noteworthy to mention again the H-ISAC, as it facilitates knowledge transfer across the world through educational summits, webinars, workshops and white papers, supporting in this way the exchange of information and the building of relationships that may contribute to make the health sector more resilient and proactive in the face of future cyberattacks. [105] However, while H-ISAC has shifted its focus towards an international approach in 2018[106], effort is still needed to increase and maintain the exchange of information across health care stakeholders.

Lack of expertise

There is a lack of sufficiently skilled experts in the health care industry.[107] In general IT security experts are hard to find,[108] while dealing with an incident can be challenging if the team is not mature or does not know how to best use a tool.[109] For instance, buying the most protective equipment will not shield an operator from cyberattacks if it is used inadequately due to the fact that the personnel has not been trained.

Lack of security awareness

There is low awareness on cyber risks in the health sector, and its potential impact on the organisation.[110] Concretely, health practitioners are not aware of the consequences of cyber risky behaviour, due to the lack of policies and reinforcement of secure behaviour. Through the pandemic, while digitalisation increased in all sectors, there were no increase on cybersecurity procedures, or guidance on revised procedures and technologies. This lack of awareness is partly due to an inadequate board-level risk communication in the hospitals.[111]

Uninterrupted functioning systems

It is challenging to implement certain cybersecurity procedures in real time in the health sector, without shutting down the equipment. And continuous monitoring coverage or shutdowns of the systems are not easily implemented. For instance, few health care IT infrastructures could be shut down without serious impact on the patients' life (and hence the functioning of the hospitals or health care facilities).[112]

3.6.2 Health CSIRT Challenges

Within this landscape, the Health CSIRTs consulted for this study stressed that the main challenges faced when collaborating with OESs in the health sector are usually the following, in order of importance:

- Lack of security culture among operators of essential services;
- The management and the security of operators of essential services IT infrastructure is often outsourced;
- Lack of established cooperation tools and channels with operators of essential services incident response teams;
- No 24/7 coverage / capabilities; and
- Resources or expertise issues.

Unsurprisingly, all the challenges listed by the consulted Health CSIRTs are closely linked to or referred directly to the challenges faced by the OESs themselves.[113] To a lesser extent, supply

[105] https://h-isac.org/
[106] https://www.prnewswire.com/news-releases/nh-isac-changes-name-to-health-isac-h-isac-300706786.html
[107] https://www.jmir.org/2021/4/e21747#figure2
[108] https://www.jmir.org/2021/4/e21747#figure2
[109] https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1/language-en
[110] https://www.jmir.org/2021/4/e21747#figure2
[111] https://www.jmir.org/2018/5/e10059?utm_source=TrendMD&utm_medium=cpc&utm_campaign=JMIR_TrendMD_0
[112] https://www.jmir.org/2021/4/e21747#figure2
[113] https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7

chain management and confidentiality issues were also listed by the consulted stakeholders as particular challenges.

Notably, 60% of consulted stakeholders pointed to the absence of a specific Health Sectoral CSIRTs, hence in these cases there are no overlaps between the responsibilities and services offered by the National CSIRTs, and the ones offered by Health Sectoral CSIRTs. Only 13% of interviewees pointed to an existing overlap between National and Health Sectoral CSIRTs.

In parallel to the overlaps, they also referred to the gap between the responsibilities and services offered by the National CSIRTs and the responsibilities and services offered by Health Sectoral CSIRTs: the stakeholders stressed that “the main gap is that National CSIRT have more coordination functions and they have a different constituency”. Particularly, the Health CSIRTs address all potential victims of cyberattacks from the health care industry, including non-essential services such as social health care. Other stakeholders pointed to the gap of information, as Health CSIRTs can only share information in its industry across the National one, creating delays or even under informing the other Health CSIRTs stakeholders.

Regarding the internal work of the CSIRTs, respondents to the consultation also explained that recurrent personnel-related challenges in the context of incident response teams include lack of knowledge and skills and high personnel rotation, while organisational-related challenges in the context of incident response activities usually involve also lack of personnel, and of formal definition of responsibilities and duties.

3.7 CSIRTS LESSONS LEARNED

73% of stakeholders who participated on the survey stressed the support received from groups/forums to exchange with peers IR information, good practices, and experience in the health sector. These types of information are key for the enhancement of sectoral IR capacity-building. Some stakeholders suggested that they often communicate with the EU institutions, bodies, and agencies to share information. Some other forums mentioned are international groups such as the CSIRTs Network Members.

In the same line, the respondents suggested that existing capacity-building initiatives implemented at European level related to information sharing tools, and awareness raising actions in relation to security incidents, are very useful for improving the effectiveness of the Health CSIRTs, particularly their IR capacities. Moreover, the stakeholders also pointed to more guidance on the use of vendor health care systems.

Regarding specific tools/ processes in place in their organisation that would help improve the effectiveness of sector IR capacities in other Health CSIRTs, respondents to the survey pointed to the following:

- Policy and procedure trainings and exercises;
- Vulnerability response tools; and
- Information sharing actions.

Finally, stakeholders pointed towards the creation of public-private-partnership programs, that would help create a common vision among OESs and CSIRTs, minimising the lack of trust among players.

4. RECOMMENDATIONS

4.1 INTRODUCTION

Overall, this study has found that Health sectoral CSIRTs are still scarce in a landscape where health OESs need specialised support in their incident response activities. Moreover, the insights shared by the consulted parties stressed the great potential of Health CSIRTs in offering this support, in particular, in information sharing initiatives.

Based on this key area of opportunity, and the needs expressed by the OESs, the following recommendations have clearly emerged across the study:

4.2 RECOMMENDATION 1: ENHANCE AND FACILITATE THE CREATION OF HEALTH SECTORAL CSIRTS

While there is a trend in developing sectoral CSIRTs and sector-wide CSIRTs collaborations by the health OESs, still few governments have Health CSIRTs or intend to create one. In general, incident response capabilities are handled by the main OESs and supervised by the national/governmental CSIRT, leaving the IR coordination and information sharing activities to parties with less expertise on this niche: the intersection between cybersecurity and health care.

Active efforts should be placed in facilitating funding, guidance - in relation to capacity building, information sharing, awareness raising - and cooperation to guarantee the creation of Health Sectoral CSIRTs.

Recommendation aimed at: National Cybersecurity Authorities.

4.3 RECOMMENDATION 2: CAPITALISE ON THE EXPERTISE OF THE HEALTH CSIRTS FOR HELPING OESS DEVELOP THEIR IR CAPABILITIES

OESs stressed the need for guidance, direction and capability building when it comes down to incident response; one concrete challenge is that incident response in the health sector tends to often rely more on reactive services rather than proactive ones, due to a lack of a coordinated incident response capacity to counteract threats. Concretely, OESs need help identifying lessons learned from past incidents within the sector. At the same time, the lack of sector-specific knowledge of the National CSIRT prevents them from executing this coordination role to the best of the health OESs interest, leaving an unfulfilled role that Health CSIRTs can take on.

For these reasons, **Health CSIRTs should be empowered to gain the role of supporting OESs w.r.t. incident response, encouraging the organisation and pool of incident response capabilities, and facilitating a more proactive approach to incident response in general**.

Recommendation aimed at: National Cybersecurity Authorities, Sectoral and/or National CSIRTs.

Ideally, this role would include the following responsibilities: promotion of specialised services to handle sector-specific threats, vulnerabilities and incidents; dissemination of specific knowledge and expertise on medical devices, medical IT systems, as well as threats and incidents related to the health sector in real time; provide sectoral expertise to the National CSIRT; assist nonregulated operators in the health sector on incident response; coordination for multi-site compromised systems in the health sector; and vulnerability coordination with vendors of sector-

specific systems / devices. These activities address the core challenges of both health OESs and CSIRTs. Furthermore, the fulfilment of these activities will require strong efforts from the Health CSIRTs, as well as development of expertise and cooperation with national/international CSIRTs.

In order to achieve this, the following measures may enhance health CSIRTs capabilities: establishing sector-specific regulations clarifying the security requirements and responsibilities (such as guidelines and requirements for reporting and management of incidents); the establishment of cooperation agreement between national and sectoral actors (through the appointment of a liaison officer, sharing of know-how, expert advice or tailored training); establishing a direct and fluent communication channel with the OESs; and the use of public-private partnerships, which can accelerate the maturity of Health CSIRTs and OESs IR capabilities. Linked to this, this study found that Health CSIRTs have an opportunity to reach an Intermediate Maturity Level on its IR capabilities by formalising their existing procedures.

4.4 RECOMMENDATION 3: EMPOWER HEALTH CSIRTS ROLE ON INFORMATION SHARING ACTIVITIES

In the same line, the last recommendation stresses the importance of empowering Health CSIRTs on the information sharing across OESs.

The organic emergence of Health CSIRTs, such as the Health Information Sharing and Analysis Centre (H-ISAC), points towards OESs' strong need for information exchange, bypassing national centralised systems that do not have sector-specific knowledge and that may create unnecessary extra steps in the information sharing process.

Health CSIRTs could have a role in breaking down the barriers associated to incident information sharing, which are specially complicated in the health care industry. Concretely, **Health CSIRTs should be supported on the development of this information exchange activities, which among others should include: dissemination of threat intelligence (both ex-ante and ex-post incident information), exchange of good practice and lessons learned, and information regarding trainings and exercises for the capacity building of OESs**.

Recommendation aimed at: National Cybersecurity Authorities, CSIRTs Network, Sectoral and/or National CSIRTs.

5. BIBLIOGRAPHY

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., & Flahault, A, *Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks, BMC Medical Informatics and Decision Making*, BioMed Central Ltd 20(1), 1-10, 2020. Available: https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7

Check Point, *The 2020 Cybersecurity Report*, Check Point Online, 2020. Available: https://research.checkpoint.com/2020/the-2020-cyber-security-report/

CYBERSPRINT, *Study Leads to National Investigation Cyber Security Health care*, CYBERSPRINT Online, 2019. Available: https://www.cybersprint.com/news/cybersprints-study-leads-to-national-investigation-into-Health cares-cyber-security/

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, OJ L 194/1,19.7.2016, Brussels. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

Dyrda, Laura, *Inside UVM Medical Center's ransomware attack: 11 details*, Becker's Health care Online, 2020. Available: https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html

EclecticIQ, *Z-CERT and EclecticIQ Cooperate to Bring Benefits of CTI to Dutch Health care Sector*, Cision, 2020. Available: https://www.prnewswire.com/news-releases/z-cert-and-eclecticiq-cooperate-to-bring-benefits-of-cti-to-dutch-Health care-sector-301073185.html

ENISA, *CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs,* European Union Agency for Network and Information Security, 2016. Available: https://www.enisa.europa.eu/publications/csirt-capabilities

ENISA, *Strategies for incident response and cyber crisis cooperation,* European Union Agency for Network and Information Security, 2016. Available: https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

ENISA, *CSIRT maturity assessment model*, European Union Agency for Network and Information Security, 2019. Available: https://www.enisa.europa.eu/publications/study-on-csirt-maturity

ENISA, *Strategies for incident response and cyber crisis cooperation*, European Union Agency for Network and Information Security, 2016. Available: https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

ENISA, *Study on CSIRT landscape and IR capabilities in Europe 2025*, European Union Agency for Network and Information Security, 2019. Available: https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025

ENISA, *EU Member States incident response development status report,* European Union Agency for Network and Information Security, 2019. Available: https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report

ENISA, *CSIRT maturity assessment model*, European Union Agency for Network and Information Security, 2019. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

ENISA, *Sectoral CSIRTS Capabilities,* European Union Agency for Network and Information Security, 2020. Available: https://www.enisa.europa.eu/publications/sectoral-csirt-capabilities-energy-and-air-transport

ENISA, *PSIRT Expertise and Capabilities Development,* European Union Agency for Network and Information Security, 2021. Available: https://www.enisa.europa.eu/publications/csirt-expertise-and-capabilities-development

He, Y., Aliyu, A., Evans, M., Lu,o C., *Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review*, JMIR Publications, 2021. Available: https://www.jmir.org/2021/4/e21747#figure2

ICF, CEPS and Wavestone, *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665*, 2020. Available: https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1

Interpol, *Cybercriminals targeting critical health care institutions with ransomware*, The International Criminal Police Organization, 2020. Available: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-health care-institutions-with-ransomware

Jalal, Mohammad S., Kaiser, Jessica P., Cybersecurity in Hospitals: A Systematic,Organizational Perspective, JMR Publications, 2018. Available: https://www.jmir.org/2018/5/e10059?utm_source=TrendMD&utm_medium=cpc&utm_campaign=JMIR_TrendMD_0

KPMG, *Complying with the European NIS Directive. Cybersecurity for critical infrastructures*, KPMG, April 2019. Available: https://assets.kpmg/content/dam/kpmg/nl/pdf/2019/advisory/complying-with-the-eu-nis-directive.pdf

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, 05.04.2017, Brussels. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R0745

Reuters staff, *Prosecutors open homicide case after hacker attack on German hospital,* The Guardian, 2020. Available: https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital

Sherman, C., Schiano, S., *Best Practices: Medical Device Security - Control Your Hospital's Expanding Device Risk Exposure*, Forrester, May 2019. Available: https://www.forrester.com/report/Best+Practices+Medical+Device+Security/-/E-RES132003#

Staff Working Document 345 final, Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 16.12.2020, Brussels. Avalable: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345

The Dutch Security Cluster, *Z-Cert, Online*. Available: https://www.thehaguesecuritydelta.com/partners/partner/663-z-cert (Accessed 04.08.2021).

WEBSITES OF NATIONAL AND SECTORAL CSIRTs

Austria, Computer Emergency Response Team Austria. Contact: cert.at

Belgium, Belgian Federal Cyber Emergency Team. Contact: cert.be

Bulgaria, CERT Bulgaria. Contact: govcert.bg

Croatia, Croatian National CERT. Contact: cert.hr

Cyprus, National CSIRT-CY. Contact: csirt.cy

Czech Republic, CSIRT.CZ. Contact: csirt.cz/

Denmark, Centre for Cyber Security (formerly Danish GovCERT). Contact: govcert.dk/

Denmark, CSIS.DK. Contact: csis.dk/

Denmark, Danish Computer Security Incident Response Team. Contact: cert.dk

Estonia, CERT Estonia. Contact: cert.ee/

European Union, CERT-EU. Contact: cert.europa.eu

France, CERT-FR. Contact: cert.ssi.gouv.fr

France, CERT Santé, https://esante.gouv.fr/securite/cert-sante

Finland, National Cyber Security Centre Finland. Contact: viestintavirasto.fi/en/cybersecurity.html

Germany, CERT-Bund. Contact: bsi.bund.de/EN/TheBSI/thebsi_node.html

Greece, Greek National Authority Against Electronic Attacks. Contact: cert.gov.gr

Hungary, HUN-CERT. Contact: cert.hu/hun-cert/index.html

Hungary, National Cyber Security Center of Hungary. Contact: nki.gov.hu

Iceland, Computer Incident Response Team Iceland. Contact: cert.is

Ireland, National Cyber Security Centre (IE) (formerly NCSC (IE)). Contact: ncsc.gov.ie/CSIRT/

Italy, Computer Security Incident Response Team – Italia. Contact: csirt.gov.it/

Latvia, Information Technologies Security Incident Response Institution (CERT.LV). Contact: cert.lv/

Lithuania, National Cert of Lithuania - CERT-LT. Contact: nksc.lt/en/

Luxembourg, HealthNet-CSIRT (formerly HealthNet). Contact: healthnet.lu

Luxembourg, Governmental CERT of Luxembourg. Contact: govcert.lu

Luxembourg, Computer Incident Response Center Luxembourg. Contact : circl.lu/

Malta, CSIRTMalta. Contact: maltacip.gov.mt/en/CIP_Structure/Pages/CSIRTMalta.aspx

Netherlands (The), Nationaal Cyber Security Centrum. Contact: ncsc.nl

Netherlands (The), CSIRT-DSP. Contact: csirtdsp.nl/

Netherlands (The), Z-CERT. Contact: z-cert.nl

Poland, CERT POLSKA. Contact: cert.pl/

Poland, The Governmental Computer Security Incident Response Team of Poland. Contact: csirt.gov.pl/

Poland, CSIRT-MON. Contact: csirt-mon.wp.mil.pl/pl/index.html

Portugal, Servico de Coordenacao Nacional da Resposta a Incidentes de Ciberseguranca. Contact: cncs.gov.pt/

Romania, Romanian National Computer Security Incident Response Team. Contact: cert.ro

Slovakia, SK-CERT (formerly GovCERT-SK). Contact: sk-cert.sk

Slovakia, Computer Security Incident Response Team Slovakia (formerly CERT-SK). Contact: csirt.gov.sk/

Slovenia, Slovenian Computer Emergency Response Team. Contact: cert.si/

Spain, INCIBE-CERT. Contact: incibe-cert.es/

Sweden, CERT-SE (formerly SITIC). Contact: cert.se

A ANNEX: SURVEY – QUESTIONNAIRE

ABOUT YOUR ORGANISATION

Name: ……

Incident Response Team Full Time Employees: ……

What type of organisation are you part of? *(*Mandatory)*

☐ **National CSIRT**

☐ **Government or Military CSIRT**

☐ **Regulatory organisation, body or Ministry**

☐ **Sectoral CSIRT**

☐ **OES Incident Response Team**

☐ **Other. Please specify: ……**

If pertinent, please select relevant sub-sector *(*Conditional)*

☐ **Health care services and facilities**

☐ Manufacturer of medical devices, equipment, and hospital supplies

☐ Other. Please specify: ……

Comments

CSIRT INCIDENT RESPONSE CONTEXT

1. **What are the services and associated functions provided by the sectoral CSIRTs or sector-specific IR capabilities in your sector[114]?** *(*Mandatory)*

Service Area 1 – Information security event management

☐ Monitoring and detection

- Log and sensor management
- Detection use case management
- Contextual data management

☐ Event analysis

- Correlation
- Qualification

Service Area 2 - Information security incident management

☐ Information security incident report acceptance

- Information security incident report receipt
- Information security incident triage and processing

☐ Information security incident analysis

- Information security incident triage
- Information collection
- Detailed analysis coordination
- Information security incident root cause analysis
- Cross-incident correlation

☐ Artifact and forensic evidence analysis

- Media or surface analysis
- Reverse engineering
- Run Time or dynamic analysis
- Comparative analysis

☐ Mitigation and recovery

- Response plan established
- Ad-hoc measures and containment
- System restoration
- Other information security entities support

☐ Information security incident coordination

- Communication
- Notification distribution
- Relevant information distribution
- Activities coordination
- Reporting
- Media communication

Service Area 3 - Vulnerability management

☐ Vulnerability discovery / research

- IR vulnerability discovery
- Public source vulnerability discovery
- Vulnerability research

☐ Vulnerability report intake

- Vulnerability report receipt
- Vulnerability report triage & processing

☐ Vulnerability analysis

- Vulnerability triage
- Vulnerability root cause analysis
- Vulnerability remediation development

☐ Vulnerability coordination

- Vulnerability notification/reporting
- Vulnerability stakeholder coordination

☐ Vulnerability disclosure

- Vulnerability disclosure policy & infrastructure maintenance
- Vulnerability announcement / communication
- Post-vulnerability disclosure feedback

☐ Vulnerability response

- Vulnerability detection/scanning
- Vulnerability remediation

Service area 4 – Situational awareness

☐ Data acquisition

- Policy aggregation, distillation, and guidance
- Asset mapping to functions, roles, actions and key risks
- Collection
- Data processing and preparation

[114] See the FIRST CSIRT framework for details: https://www.first.org/education/csirt_service-framework_v1.1

☐ Crisis management support

- Information distribution to constituents
- Information security status reporting
- Strategic decisions communication

☐ Communication

- Internal and external communication
- Reporting and recommendations
- Implementation
- Dissemination / integration / information sharing
- Management of information sharing
- Feedback

Service area 5 – Knowledge transfer

☐ Awareness building

- Research & information aggregation
- Reports and awareness materials developed
- Information dissemination
- Outreach

☐ Training & Education

- Knowledge, skill, and ability requirements gathering
- Educational and training materials development
- Content delivery
- Mentoring
- CSIRT staff professional development

☐ Analysis and synthesis

- Projection and inference
- Event detection
- Information security incident management decision support
- Situational impact

☐ Exercises

- Requirements analysis
- Format and environment development
- Scenario development
- Exercise execution
- Exercise outcome review

☐ Technical and policy advisory

- Risk management support
- Business continuity and disaster recovery planning support
- Policy support
- Technical advice

Comments

2. How many incidents related to the health sector do you handle per year? *(*Mandatory)*

☐ 0-10

☐ 10-50

☐ 50-100

☐ 100+

☐ Other. Please specify: ……

☐ I do not know

3. **What is the scope of your Incident Response?** *(*Mandatory)*

☐ Company-level

☐ City-level

☐ National-level

☐ International-level

☐ I do not know

☐ Other. Please specify: ……

4. **How long has your organisation been in place in years?**

Comments

CREATION OF SECTORAL CSIRT/IR CAPABILITIES

5. **Do you know if the health sector has, or is going to have a dedicated CSIRT in your country of operation?** *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If <u>yes</u>, please specify in the comment box the status of CSIRT establishment: existing, under development, development process to be launched in 2021, plans for the coming years, no plans yet. Please also specify whether the CSIRT is/are listed, accredited or certified.**

Comments

6. **What are the key reasons to create such sector-specific IR capacities?** *(*Mandatory)*

☐ The implementation of the NIS Directive

☐ The lack of sector-specific knowledge or capacity of the National CSIRT

☐ Lessons learned from past incidents

☐ The difficulties in managing the cybersecurity incidents in the NIS Directive sectors

☐ The complexity of managing the high number of OES in some of the NIS Directive sectors

☐ The need to facilitate incident handling cross-borders

☐ I do not know

☐ Other. Please: specify: ……

7. **What impact(s) do you think the NIS Directive had on your activity?** *(*Mandatory)*

Comments

8. **In your opinion, what are the specific services, roles or functions of the sectoral CSIRTs in contrast to national, governmental or military CSIRTs?** *(*Mandatory)*

Comments

9. **Based on your experience, is there any overlap between the responsibilities and services offered by the National CSIRTs and the responsibilities and services offered by Health Sectoral CSIRTs?** *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

☐ Not applicable – absence of health sectoral CSIRT

If yes, could you specify which overlaps? *(Conditional question)*

Comments

10. **In your opinion, is there any relevant gap in the responsibilities and services offered by the National CSIRTs and the responsibilities and services offered by Health Sectoral CSIRTs? If yes, could you specify which ones?** *(*Mandatory)*

Comments

11. **Based on your experience, what are the key factors facilitating the development of sectoral CSIRTs and/or IR capacities?** *(*Mandatory)*

☐ The lessons learned from past incidents

☐ The establishment of sector-specific regulations clarifying the security requirements and responsibilities

☐ Recommendations from a previous audit and certification programmes

☐ Requests from stakeholders or participating organisations/future members

☐ The establishment of cooperation agreements between national and sectoral actors

☐ Access to funding and support of IR capability development through the Connecting European Facility (CEF) programme

☐ Access to funding and support of IR capability development through other funding

☐ The establishment of public-private partnerships. Please specify the nature of these PPPs: ……..

☐ The dissemination of threat intelligence, exchange of good practices and lessons learned

☐ I do not know

☐ Other. Please specify:
……

Comments

12. What specific resources and tools are in place to support the development of constituents' incident response capabilities (IRC) in the health sector? *(*Mandatory)*

☐ Appointment of local or sectoral counsellors advising OES on the development of their IRC

☐ Training and Education activities

☐ A network of IR actors at a national or sectoral level to exchange good practices about information exchange, capabilities, cooperation

☐ Methodological baselines and tools to support IR (e.g.: specific software tools, risk assessment methodologies, best practices, frameworks)

☐ Shared framework for incident classification and threat modelling

☐ Certification by cybersecurity companies providing reliable services and products

☐ I do not know

☐ Other. Please specify……

Comments

13. Does your organisation need / have you asked for any specific support or guidance from external stakeholders to design and implement sectoral IR capacities? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If <u>yes</u>, please specify from who:**

☐ European Union entities
☐ International authorities
☐ National authorities
☐ Professional associations
☐ CSIRT communities/peers
☐ Industry players

☐ Other. Please specify: ……..

Comments

14. Does your organisation use a specific CSIRT maturity assessment methodology to support the development of IR capabilities within your sector(s)? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If <u>yes</u>, which one?**

☐ SIM3 (Security Incident Management Maturity Model)[115]

☐ ENISA CSIRT maturity assessment[116]

☐ Your National CSIRT maturity tool

☐ A CSIRT maturity assessment methodology from the private sector (please specify in comments)

☐ Other (please specify in comments)

Comments

ORGANISATION AND PERSONNEL

15. Has the scope of responsibility of your entity in regard to Incident Response activities been defined? *(*Mandatory)*

☐ Not defined

☐ Informally defined

☐ Formally defined

☐ I do not know

(Conditional question) **If <u>informally</u> or <u>formally defined</u>, could you please provide more information on the scope of responsibility of your entity in regard to Incident Response activities?**

Comments

16. Has the classification of the incidents handled by your entity been defined? *(*Mandatory)*

☐ Not defined

☐ Informally defined

[115] https://opencsirt.org/csirt-maturity/sim3-and-references/
[116] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

☐ Formally defined

☐ I do not know

(Conditional question) **If <u>informally</u> or <u>formally defined</u>, how do you classify the incidents handled by the entity?**

Comments

17. Has a security policy for operations been established by your organisation, and to which extent is it respected? *(*Mandatory)*

☐ Not defined

☐ Informally defined

☐ Formally defined

☐ I do not know

(Conditional question) **If <u>informally</u> or <u>formally defined</u>, could you please provide more information on the security policy for operations, and to which extent it is respected?**

Comments

18. Has your organisation formalised the level of services that it offers in its intervention scope?[117] *(*Mandatory)*

☐ Not defined

☐ Informally defined

☐ Formally defined

☐ I do not know

(Conditional question) **If <u>informally</u> or <u>formally defined</u>, could you please provide more information on the level of services that it offers in its intervention scope?**

Comments

19. How does your organisation approach the need to ensure the resilience of its personnel? *(*Mandatory)*

☐ Not tackled

☐ Informal approach

☐ Formal approach

☐ I do not know

[117] ENISA CSIRT maturity assessment model. See page 15. https://www.enisa.europa.eu/publications/study-on-csirt-maturity

(Conditional question) **If informal or formal approach, could you please provide more information on how your organisation approach the need to ensure the resilience of its personnel?**

Comments

20. How many people are involved with incident-response activities in your organisation? *(*Mandatory)*

☐ 1 - 3

☐ 4 - 10

☐ 11 - 15

☐ 16 - 20

☐ More than 20 – Please specify

☐ I do not know

21. How does your organisation ensure the training of staff internally? *(*Mandatory)*

☐ In-person trainings

☐ Online trainings

☐ Guidelines

☐ Other. Please specify:……

22. Based on your experience, what are the most recurrent personnel-related challenges in the context of incident response teams? *(*Mandatory)*

Comments

23. In your opinion, what are the most recurrent organisational-related challenges in the context of incident response activities? *(*Mandatory)*

Comments

INCIDENT RESPONSE CAPABILITY DEVELOPMENT IN THE SECTORS

24. Which specific tools[118] does your organisation rely on to conduct the following services? Please tick the right answer: *(*Mandatory)*

Service area and Services	Tool in service	Planning to implement one	Out of scope or perimeter	I do not know	Please specify
Service Area 1 – Information security event Management					
Monitoring and detection	☐	☐	☐	☐	
Event analysis	☐	☐	☐	☐	
Service Area 2 - Information security incident management					
Information security incident report acceptance	☐	☐	☐	☐	
Information security incident analysis	☐	☐	☐	☐	
Artifact and forensic evidence analysis	☐	☐	☐	☐	
Mitigation and recovery	☐	☐	☐	☐	
Information security incident coordination	☐	☐	☐	☐	
Crisis management support	☐	☐	☐	☐	
Service Area 3 - Vulnerability management					
Vulnerability discovery / research	☐	☐	☐	☐	
Vulnerability report intake	☐	☐	☐	☐	
Vulnerability analysis	☐	☐	☐	☐	
Vulnerability coordination	☐	☐	☐	☐	
Vulnerability disclosure	☐	☐	☐	☐	
Vulnerability response	☐	☐	☐	☐	
Service area 4 – Situational awareness					
Data acquisition	☐	☐	☐	☐	
Analysis and synthesis	☐	☐	☐	☐	
Communication	☐	☐	☐	☐	
Service area 5 – Knowledge transfer					
Awareness building	☐	☐	☐	☐	
Training & Education	☐	☐	☐	☐	
Exercises	☐	☐	☐	☐	
Technical and policy advisory	☐	☐	☐	☐	
Other Service area: Please specify	☐	☐	☐	☐	

[118] Example: Cyber Threat Intelligence system, Request tracker for Incident Response (RTIR), or equivalent, Open Technology Real Services, or equivalent, osTicket, or equivalent, dedicated alerting & reporting dedicated portal, Active & passive monitoring tools, Use of public, semi-public, or commercial feed, Digital forensic tools, Security assessment tools)

25. Does your organisation have standard operating procedures (SOPs) that OES' teams should follow in case of incident? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If yes, could you please provide details for which services or functions?**

Comments

26. Does your organisation make use of an incident notification template? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If yes, could you please provide additional information on who has (or will have) access to the notification template? (e.g., constituents, participating organisations, LEA, third-party organisations, CSIRT peers)**

Comments

(Conditional question) **If yes, could you please indicate the nature of the information reported?**

☐ Description of the incident and IOCs and TTPs ☐ Root cause

☐ Services affected ☐ Severity

☐ Cross border impact ☐ Lessons learned

☐ Indicators to measure the nature and impact in addition to those of the NIS Directive.

☐ Current situation of the incident (actions taken or needed, investigation status etc.)

☐ I do not know

☐ Other. Please specify.

Comments

27. Does your organisation have specific information exchange tools to enable the notification of incidents? *(*Mandatory)*

☐ Secure emails (e.g., PGP encrypted) ☐ MISP standard formats and technologies

☐ A special government secured network ☐ via an ISAC (Information Sharing and Analysis Center)

☐ I do not know

☐ Other. Please specify:
……

28. How does your organisation ensure the uptake of these tools and procedures by constituents? *(*Mandatory)*

☐ Obligation stipulated in legislature ☐ Code of conduct

☐ Promotion by National CSIRT ☐ Post-attack measures implemented by National CSIRT

☐ I do not know ☐Other. Please specify.

Comments

29. Based on your experience, what are the main challenges related to sectoral CSIRTs' tools and procedures? *(*Mandatory)*

Comments

INCIDENT RESPONSE COOPERATION AND OPERATIONAL MODELS WITHIN THE SECTORS

Cooperation with OES/Critical Infrastructure (in particular from the private sector)

30. In case of an incident, does your organisation have: *(*Mandatory)*

☐ Specific cooperation agreements between the national cybersecurity authorities and the IR teams of OES (in particular for private companies)

☐ Specific consultation process involving OES' incident response capabilities (in particular for private companies)

☐ Specific process allowing OES to request operational assistance from the national, governmental or military CSIRT

☐ Specific process to share lessons learned among national and sectoral CSIRT after a crisis (e.g.: after incident standard report, meetings etc.)

☐ I do not know

Comments

31. What are the main challenges faced when collaborating with OES in the health sector? *(*Mandatory)*

☐ Confidentiality issues
☐ Cross-border related issues
☐ Commercial issues
☐ Regulatory issues
☐ GDPR-related issues
☐ Resources or expertise issues
☐ No 24/7 coverage / capabilities
☐ Supply chain management
☐ Lack of security culture among OES
☐ The management (and the security) of OES IT infrastructure is often outsourced
☐ Lack of established cooperation tools and channels with OES IR teams
☐ Cross-sector interdependencies and cooperation
☐ I do not know
☐ Other. Please specify: …….

Comments

Incident response in cross-border crisis situations

32. Does your organisation have specific procedures to address cross-border incidents within the sector? *(*Mandatory)*

☐ Yes, there are such procedures at a national level
☐ Yes, there are such procedures at a sectoral level
☐ Yes, indirectly (through a trusted third-party Point-of-Contact such as governmental CSIRT, LEA)
☐ No, but these are planned to be implemented
☐ No, it is not planned at the moment
☐ I do not know

Comments

33. What is the nature of these procedures? *(*Mandatory)*

☐ Bilateral agreement with the other MS
☐ Designation of a Point of Contact at national or sectoral level to facilitate cross-border cooperation in case of incident
☐ Participation of representative of the other country in the crisis response process

☐ Organisation of cross-border exercises

☐ Information sharing platform (existing or about to be implemented)

☐ I do not know

☐ Other. Please specify: ……

34. Does your organisation have specific measures in place to inform the relevant actors (national authorities and OES) in neighbouring countries about an incident that may impact them? *(*Mandatory)*

☐ Yes, direct contact (communicating with relevant actors using their direct contact information, without going through an intermediary).

☐ Yes, indirectly (through a Point of Contact, a trusted third-party)

☐ No, but it is planned to establish some

☐ No, it is not planned at the moment

☐ I do not know

(Conditional question) **If yes directly or indirectly, please specify.**

Comments

GDPR COMPLIANCE AND DATA BREACH MANAGEMENT

35. Does your organisation have an appointed "privacy champion"? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If yes, could you please detail his/her functions and tasks (full time or part time, exclusively or partially dedicated to privacy related issues)?** *(*Mandatory)*

Comments

36. Does your organisation provide awareness training in GDPR? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If yes, could you please describe the training policy (frequency, percentage of the team that has been trained, regular updates)? If not, where can you receive guidance related to GDPR matters?**

Comments

(Conditional question) **If no, could you please provide information on how or where can you receive guidance related to GDPR matters?**

Comments

37. Does your organisation's Incident Response Policy specify how to identify a Data Breach, as defined by the GDPR (articles 33 & 34)? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

Comments

38. Does your organisation's Incident Response Management Process indicate the information of the Data Protection Officer (DPO), or any other person or institution in charge of the privacy/GDPR compliance concerns? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

Comments

39. Does your organisation have a forensics manual or guidelines to handle evidence related to a Personal Data Breach? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

Comments

LESSONS LEARNED AND RECOMMENDATIONS

40. Do you use groups/forum to exchange with peers IR information, good practices, and experience in your sector with peers? *(*Mandatory)*

☐ Yes

☐ No

☐ I do not know

(Conditional question) **If yes, could you please specify which group?**

Comments

41. In your opinion, what possible measures undertaken by European Institutions, international or national authorities, or private body in a specific sector, would help improve the effectiveness of the health sector IR capacities? *(*Mandatory)*

Comments

42. What specific tools or processes in place in your organisation would help improve the effectiveness of sector IR capacities? *(*Mandatory)*

Comments

43. Do you have any other inputs about your work or about the IR capacities within the health sector in your country you would like to share with us?

Comments

END OF QUESTIONNAIRE

TP-07-21-067-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-542-5
DOI: 10.2824/201143