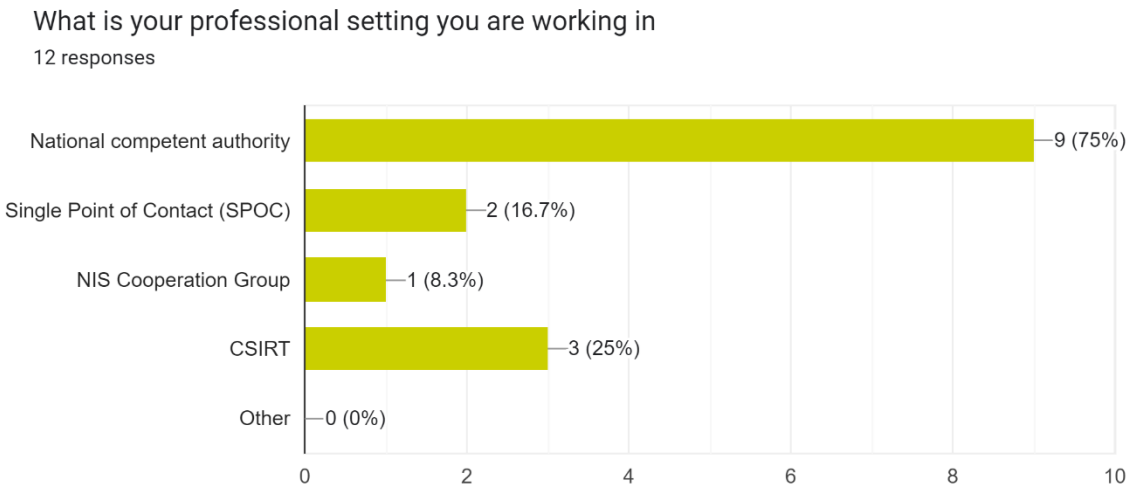
EnCaViBS – Summary Report on Cooperation

The interdisciplinary project EnCaViBS evaluates the implementation of the NIS Directive in the EU Member States. One of our focus points also in terms of the NIS 2.0 Proposal is the assessment of the different cooperation mechanisms introduced by the NIS Directive. In that regard we asked the single points of contact (SPOCs), national regulatory authorities and computer incident response teams (CSIRTs) to respond to a brief questionnaire in order to assess whether and how information sharing improved on a national, inter-institutional level, and international level.

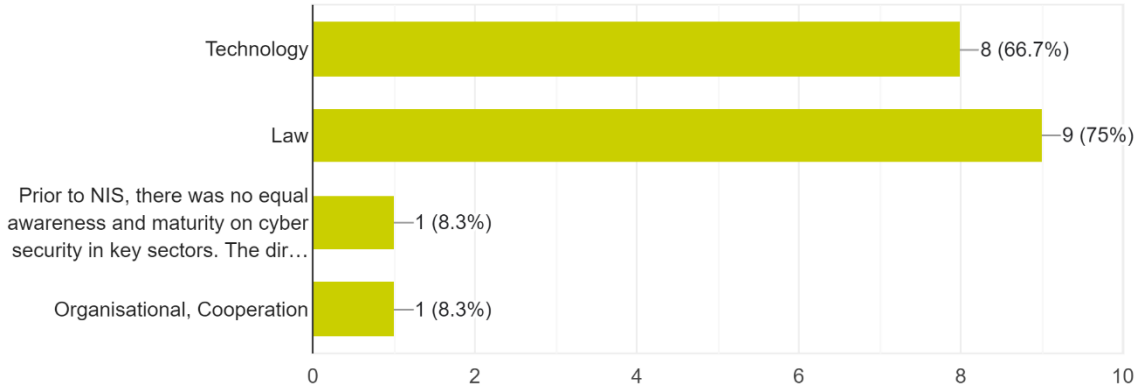
Questions Responses 18 Settings

A. Context data of the expert



How do you consider the relevance of NISD in achieving an overall increased level of cybersecurity?

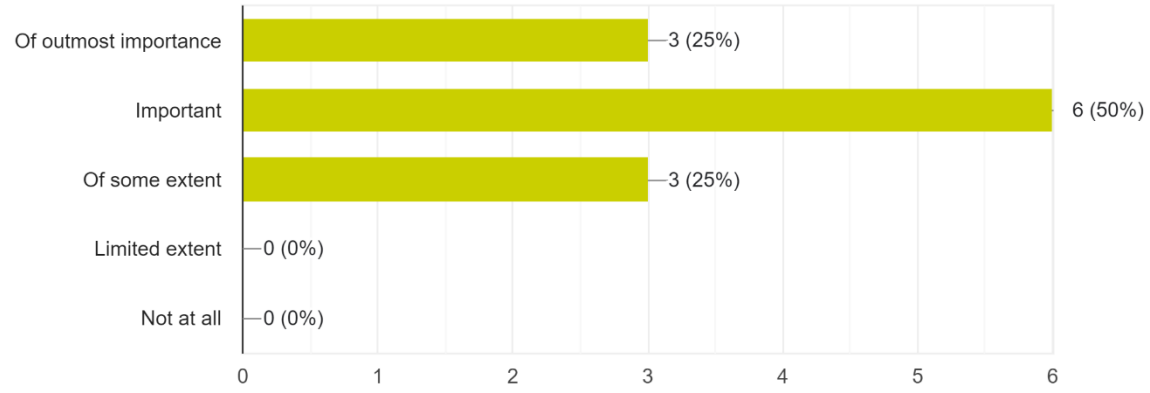
12 responses



B. Impact of the NIS Directive

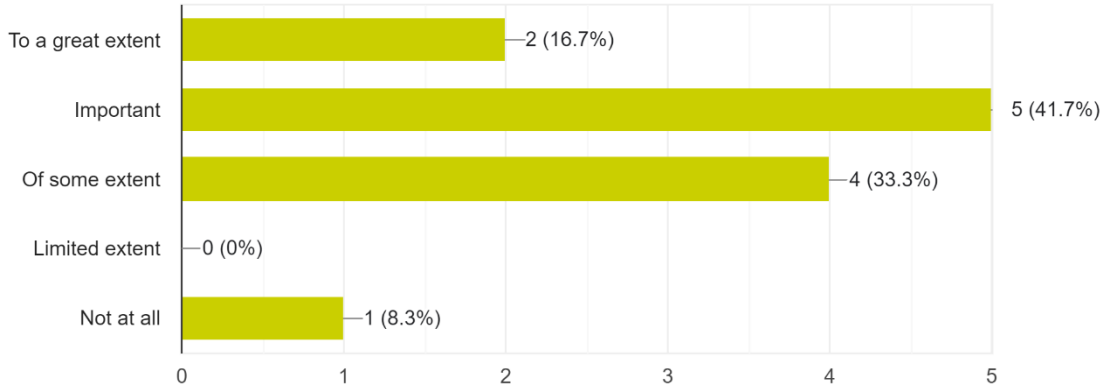
1. How do you consider the relevance of NISD in achieving an overall increased level of cybersecurity?

12 responses



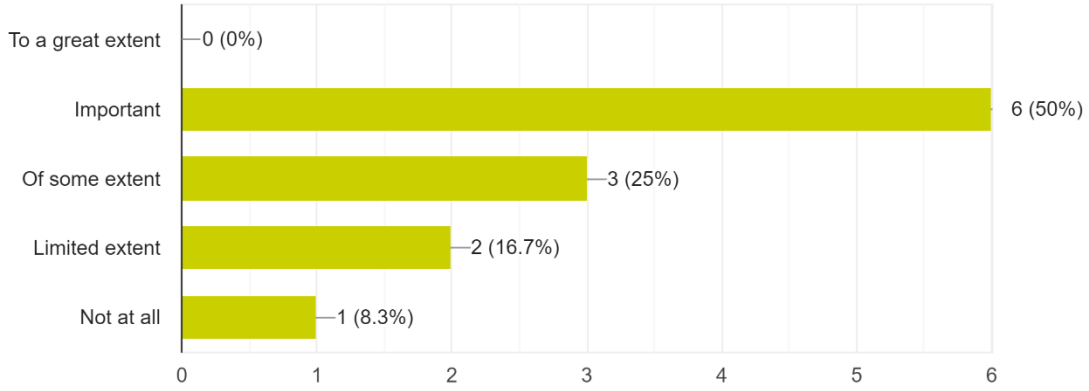
2. Did the NIS Directive (and moreover the national implementation of the Directive) improve the level of cybersecurity in your domain?

12 responses



3. Did you observe an overall increase in level of resilience against cybersecurity threats?

12 responses



4. Which further interventions in the field of cybersecurity to you consider important for achieving a high level of security of NIS within the European Union?

8 responses

- Analyze the level of cyber security maturity of key sectors and Member States to identify common weaknesses and develop a strategic plan to strengthen these areas.
- Strengthening the role of CERT
- this Q is too big to answer here
- Creation of SOCs
- NIS2
- -
- More funding opportunities for capacity development at the national level, and for organisations and businesses
- Education

C. Cooperation at National Level

1. If applicable: Where the competent authority, the single point of contact and the CSIRT ofthe same Member State are separate: Has inter-institutional cooperation and exchange of information at national level improved? Please elaborate.

11 responses

- Forming of working groups at the state level in order to connect people dealing with this issue and to exchange information on cyber threats and incidents, cross-sectoral and inter-institutional cooperation has greatly improved. Also, as part of the EU project, the National CSIRT has developed a central platform for the exchange of information on cyber threats and incidents, to which more and more interested OES's, DSP's and NCA's are joining over time.
- CSIRT is seperate from competent authority and the single point of contact. Cooperation and exchange of information is good.
- It has not improved, but it was already in reasonably good levelyea
- The exchange of information at national level have improved
- The SPOC is an irrelevant nuissance.
- The NIS law gave a better legal foundation for the existing cooperation.
- Yes it has, and the cooperation between the different competent authorities.
- Yes, cooperation improved, we have regular meetings and consultations
- Yes, Through the Grow2CERT project – Increasing the maturity of the National CERT for closer cooperation in the cybersecurity community
- In Cyprus, the Digital Security authority (which is the NIS competent authority and the single point of contact) incorporates the National CSIRT-CY as well. Thus, is a centralized structure.
- The exchange of information has improved due to collaboration meetings with all competent authorities and the Single point of contact.
- As a small country the different actors where already working together before NISD. Not much change there.

2. If applicable: Where sector-specific regulation exists that is lex specialis to the NIS Directive (e.g. PSD2, eIDAS Regulation) with regard to cybersecurity incidents, are there any rules on inter-institutional national cooperation and exchange of information between national authorities?

11 responses

- yes
- National authority according to PSD2 and national authority for banking sector according to NISD is the same body - Central Bank.
- Yes, inter-institutional national cooperation is defined by national law and regulations.
- There is already good national cooperation and exchange of information between national authority and CERT LV.
- -
- Yes
- Yes, we have formed joined national body to deal with that
- Currently, there are specific security requirements only for electronic communication providers, which are under the supervision of the Digital Security Authority as well. There are also MoUs in place between the Digital Security Authority and other supervisory authorities for the exchange of incident-related information, such as with the Central Bank of Cyprus.
- N/A
- The information exchange has been defined.

3. Security incidents which concern also personal data must be reported to the relevant data protection authority (DPA). Is the information sharing between and national competent authority under the national NIS law regulated by law? If not, what is the common practice with regard to cooperation of the relevant authorities?

10 responses

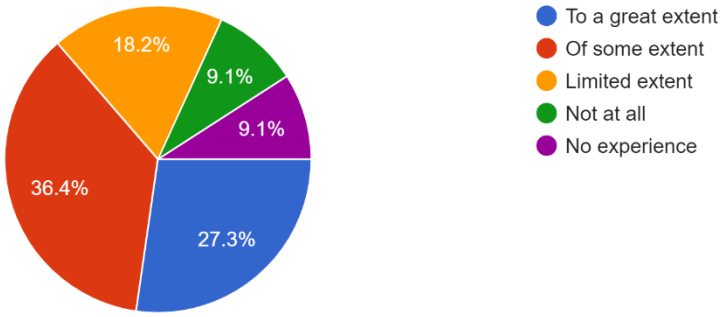
- yes
- Yes, it is regulated by law according to this article: "Competent authorities shall cooperate and exchange relevant information with the personal data protection authority when personal data are compromised due to an incident on the network and information system of the key service operator or digital service provider, or with judicial authorities when such an incident is the result of criminal activity."
- Yes, it is set in national law and institutions have established channels for communication.
- some sharing with telecom regulator. none with the data protection authority
- Yes
- Information sharing if personal data is concerned is regulated by separate law, national NIS law does not deal with that
- According to Article 17 of Law 89(I), the Digital Security Authority has the responsibility to cooperate with the Office of the Commissioner for Personal Data Protection, especially concerning the response to cybersecurity incidents which include personal data breach.
- Yes, it is regulated by law

- Data protection law applies to information exchange.

D. Cross-Border Cooperation

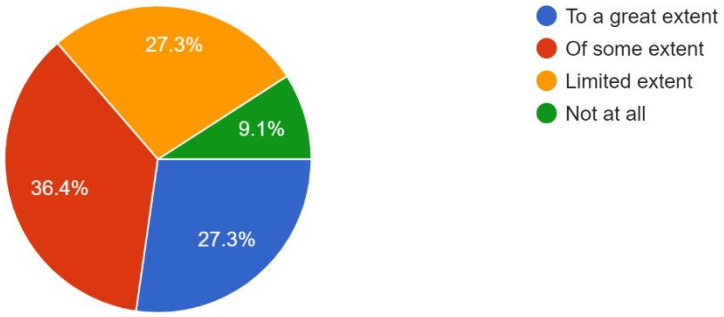
1. From your personal experience, did cross-border cooperation increase?

11 responses



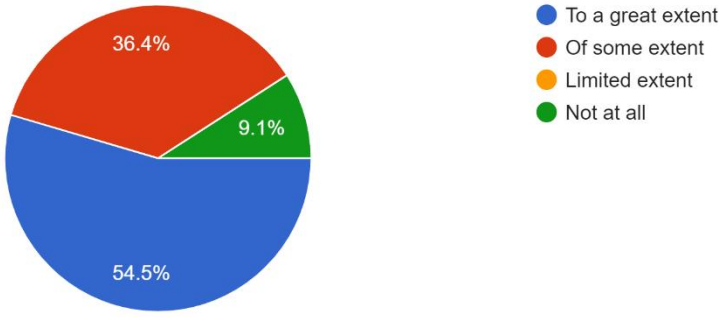
2. Did the set-up of the NIS Cooperation Group improve cooperation?

11 responses



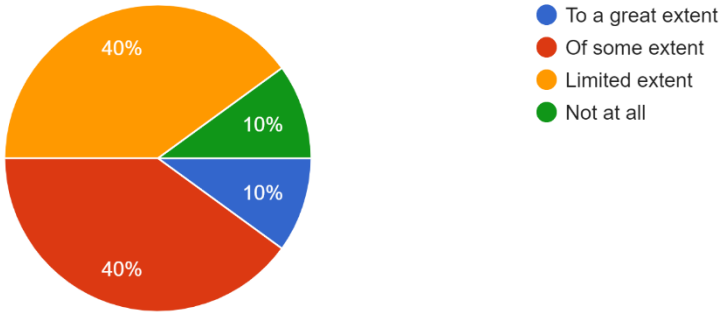
3. Did the set-up of the CSIRTs network improve cooperation?

11 responses



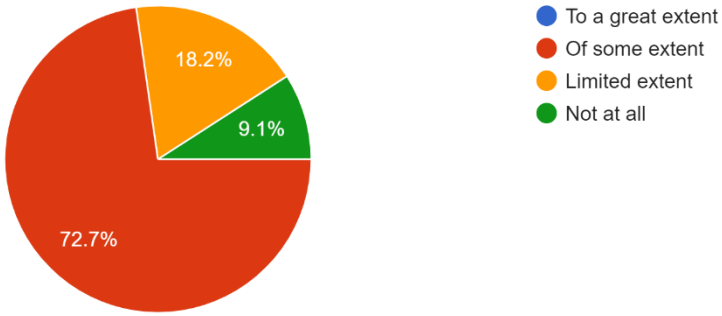
4. Is there an increase in cooperation between competent authorities of different Member States?

10 responses



5. Are cybersecurity risks related to cross-border dependencies sufficiently addressed?

11 responses



6. Has cross-border cooperation become more effective and/or efficient since the introduction of the cooperation mechanisms (NIS Cooperation Group, CSIRT network, and national point of contact)? Please elaborate.

10 responses

- According to the information available to us, the mentioned bodies have developed their own procedures and tools for the efficient exchange of information, which has facilitated and accelerated the process of information sharing. Note: We do not participate directly in the work of these bodies, so it is difficult to give a relevant answer to this question.
- Yes
- of some extent
- It completed the map. There already was good csirt cooperation between a limited set of countries.
- Yes
- Somewhat, because it is difficult to classify information as non-sensitive regarding national security, so most of the actors play it on safe side...
- It's much better.
- Yes, through cross-border cooperation mechanisms, national competence authorities have the opportunity to exchange ideas, develop new initiatives and collaborations, and address existing and new challenges.
- N/A
- The CSIRT Network is strengthin cooperation and exchange of information on a daily basis between members CSIRTs.

7. In practice, have you experienced an increase in exchange of information among Member States, notably in situations involving cross-border elements? Please elaborate.

10 responses

- At regular monthly meetings of cybersecurity working bodies and other channels of communication we use, the designated CSIRT regularly informs us and sends alerts about cyber threats and other relevant information received from the CSIRT Network community.
- Yes, especially in the context of changed threat environment
- no
- yes, but the cross-border element is overrated.
- No, not at my level.
- Not really and when it happens, it's usually too late...
- Yes, cooperation is much better.
- Yes, information concerning emerging cross-border threats and incidents is provided to Member States, through cooperation mechanisms as well as by ENISA.
- N/A

- Yes, the CSIRt Network is actively collaboration and exchanging information even in cases that are not explicitly cross-border.

8. Has cooperation at national and international level contributed to an improved preparedness for cybersecurity incidents? Please elaborate.

10 responses

- Yes, it has. During major cyber attacks and/or threats (eg WannaCry, NotPetya, Log4j, sector specific attacks, DDoS attacks, etc.), national bodies and Member States with more technical knowledge are helping by exchanging information on attack indicators, mitigation measures and tools which helps everyone to protect their information systems quickly and in a timely manner.
- Yes, especially in the context of changed threat environment
- very limited extent
- yes. e.g. tool sharing
- Yes
- Yes, even if information is not timely, it raises awareness, which drives preparedness...
- Not necessarily, but it contributed to a better understanding.
- Yes, the information provided concerning emerging cross-border threats and incidents, as well as the national and international cybersecurity exercises which are conducted on a regular basis, lead to an improved level of preparedness for cybersecurity incidents.
- Perhaps cooperation between entities on a national level has contributed to some extent.
- Strengthening the relation between member states and the different national authorities improves preparedness and readiness.

9. Which cybersecurity needs of cross-border cooperation are currently not addressed by the NIS Directive and the national implementation of the Directive in your country?

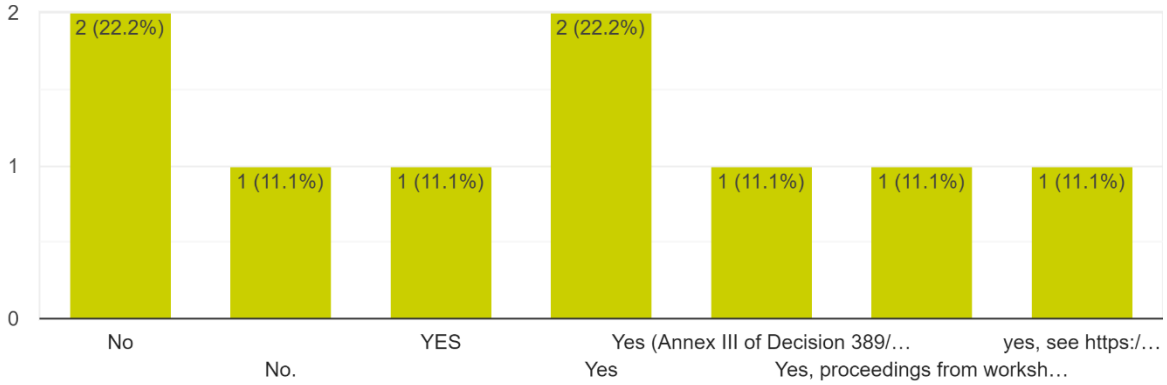
7 responses

- N/A
- Nothing to add here.
- -
- Timely exchange of classified information
- All essential elements are covered
- Exchange mechanisms for classified information.
- -

E. Technical Guidance by National Authorities/Regulator/etc.

1. Has your institution issued any technical guidance to OESs or DSPs?

9 responses



2. If not, is there any guidance that is actively promoted by your institution?

6 responses

- Additional guidance is publicly available at national CSIRT website.
- No
- We also promote "best practices" guidance from CSIRTs
- Yes, guidance of ENISA and other organizations is distributed to OES on a regular basis
- Yes

F. Incidents Reports

1. If you are the national competent authority designated to receive mandatory incident reports, how many incident reports have you received last year?

8 responses