CYBERSECURITY CAPACITY REVIEW

Republic of Cyprus

September 2021

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Dr Ioannis Agrafiotis, Dr Louise Axon

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Dr Jamie Saunders, Professor Federico Varese, Professor Basie Von Solms

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*29/10/2021*	*Full draft by leading researchers submitted to the GCSCC Technical Board*
2	*17/11/2021*	*Second draft submitted to Cyprus DSA*
3	*02/02/2022*	*Third draft submitted to Cyprus DSA addressing their comments*
4	*31/03/2022*	*Final Version*

LIST OF ABBREVIATIONS

3CE	*Cyprus Cybercrime Centre of Excellence for Training, Research and Education*
CAB	*Conformity Assessment Body*
CC	*Common Criteria*
CEPOL	*European Union Agency for Law Enforcement Training*
CERT	*Computer Emergency Response Team*
CI	*Critical Infrastructure*
CISO	*Chief Information Security Officer*
CMM	*Cybersecurity Capacity Maturity Model for Nations*
CSIRT	*Computer Security Incident Response Team*
CSIRT-CY	*National CSIRT of Cyprus*
CTF	*Capture the Flag*
CyCLONe	*EU Cyber Crises Liaison Organisation Network*
CYCLOPS	*Cyprus Centre for Land, Open-seas, and Port Security*
CYNET	*Cyprus Research and Academic Network*
CYS	*Cyprus Organisation for Standardisation*
CYTA	*Cyprus Telecommunications Authority*
DDoS	*Distributed Denial of Service*
DEFL	*Digital Evidence Forensic Laboratory*
DESI	*Digital Economy and Society Index*
DITS	*Department of Information Technology Services*
DORA	*EU Digital Operational Resilience Act*
DR	*Disaster Recovery*
DSA	*Digital Security Authority*
eIDAS	*Electronic Identification and Trust Services*
ENISA	*European Union Agency for Cybersecurity*
EUCTF	*EU Cybercrime Task Force*
EUROJUST	*EU Judicial Cooperation Unit*
FIRST	*Forum of Incident Response and Security Teams*
GCSCC	*Global Cyber Security Capacity Centre*
GDPR	*General Data Protection Regulation*
GUN	*Governmental Unified Network*
IOC	*Indicator of compromise*
ISACA	*Information Systems Audit and Control Association*

(ISC)²	*International Information System Security Certification Consortium*
ISO	*International Standards Organisation*
ISP	*Internet Service Provider*
ITIL	*Information Technology Infrastructure Library*
ITU	*International Telecommunication Union*
KPI	*Key performance indicator*
LAN	*Local area network*
MISP	*Malware Information Sharing Platform*
MPLS	*Mathematical Physical and Life Sciences*
MSSP	*Managed Security Service Provider*
MoU	*Memorandum of Understanding*
NCCA	*National Cybersecurity Certification Authority*
NCS	*National Cybersecurity Strategy*
NCSC	*National Cyber Security Centre (UK)*
NGA	*Next Generation Access*
NGO	*Non-governmental organisation*
NIS	*Network and Information Systems (Directive)*
NISD2	*NIS 2 Directive*
NIST	*National Institute of Standards and Technology*
NSA	*National Security Authority*
OAS	*Organisation of American States*
OCC	*Office for Combating Cybercrime*
OCECPR	*Office of Electronic Communications & Postal Regulation*
OCPDP	*Office of the Commissioner for Personal Data Protection*
OSCE	*Organisation for Security and Co-operation in Europe*
PCI DSS	*Payment Card Industry Data Security Standards*
QTS	*Qualified Trust Services*
QWAC	*Qualified Website Authentication Certificate*
R&D	*Research and Development*
RSIT WG	*Reference Security Incident Taxonomy Working Group*
SCADA	*Supervisory control and data acquisition*
SIC	*Safer Internet Centre*
SIEM	*Security Information and Event Management*
SME	*Small or medium-sized enterprise*
SOC	*Security Operations Centre*

STEM	*Science, Technology, Engineering and Mathematics (subjects)*
TI	*Trusted Introducer*
TSP	*Trust Service Provider*
WIPO	*World Intellectual Property Organisation*

EXECUTIVE SUMMARY

At the invitation of, and in collaboration with, the Digital Security Authority, the Global Cyber Security Capacity Centre (GCSCC, or "the Centre") undertook a review of the maturity of cybersecurity capacity in Cyprus. The objective of this review was to enable Cyprus to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period 21 to 24 September 2021, the following stakeholders participated in round-table consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the Cyprus Government and the private sector (including financial institutions), telecommunications companies, and the banking sector as well as international partners. These sessions took place in person, in Cyprus.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *Dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cybersecurity Culture and Society*
- *Building Cybersecurity Knowledge and Capabilities*
- *Legal and Regulatory Frameworks*
- *Standards and Technologies*

Each Dimension contains a number of *Factors* which describe what it means to possess cybersecurity capacity. Each Factor presents a number of *Aspects* grouping together related *Indicators*, which describe steps and actions that, once observed, define the stage of maturity of that Aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an *ad-hoc* approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in Cyprus, and illustrates the maturity estimates in each Dimension. Each Dimension represents one fifth of the graphic, with the five stages of maturity for each Factor extending outwards from the centre of the graphic; "start-up" is closest to the centre of the graphic and "dynamic" is placed at the perimeter.

[1] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition," February 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

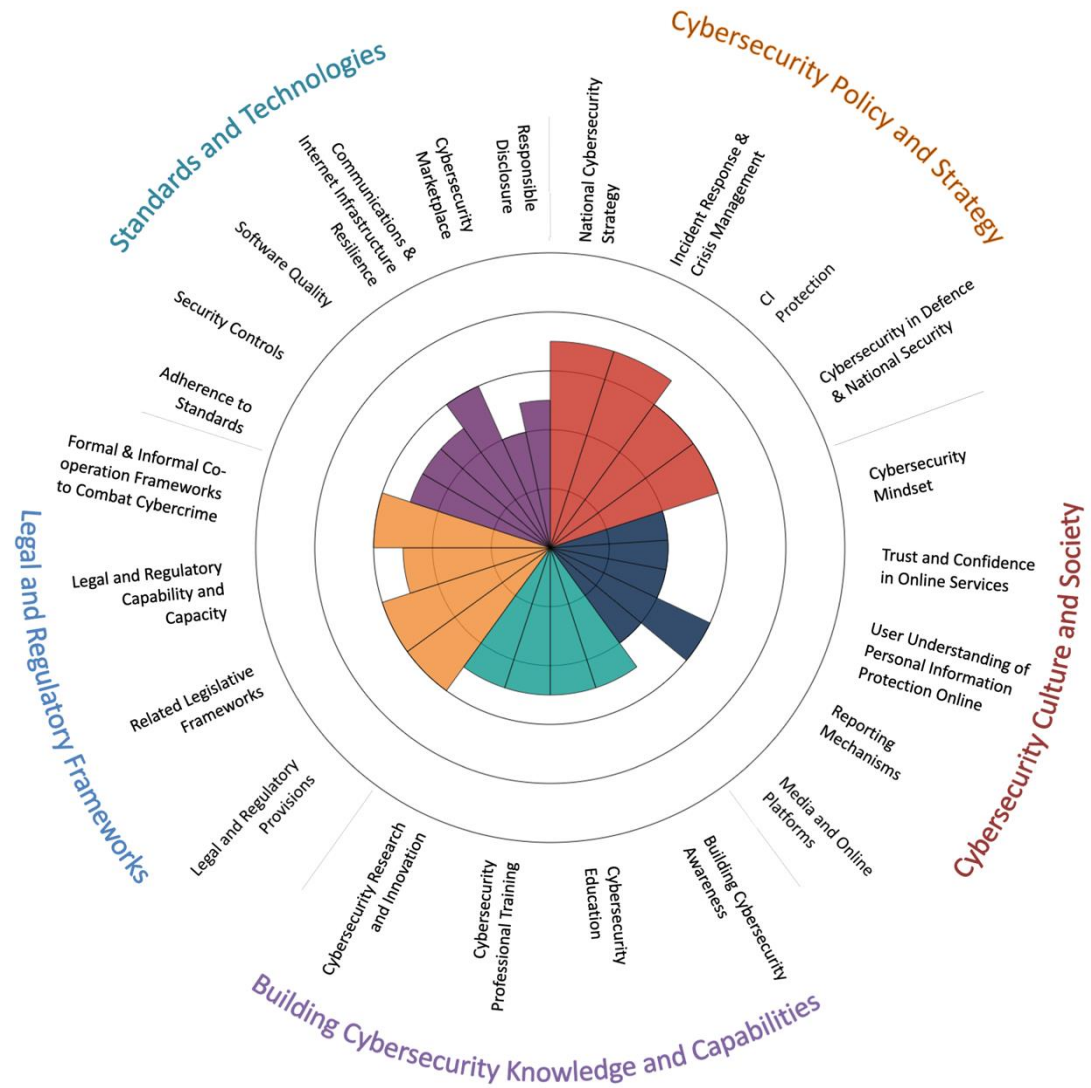

Figure 1: Overall representation of the cybersecurity capacity in Cyprus – CMM review 2021

This was the second CMM review of Cyprus, following the first in 2017. Figure 2 below shows the overall representation of the cybersecurity capacity in Cyprus presented in the 2017 CMM report. The CMM was revised in 2021 to reflect the continuously changing cybersecurity risk and control landscape, and the changing operational environment in which nations have to deliver cybersecurity. There are, therefore, some differences between the CMM used in the 2017 review and that in the 2021 review; differences in the structure of Dimensions and phrasing of Factor names can be seen from the graphs.

Comparing Figure 1 and Figure 2 indicates the extent to which cybersecurity capacity in Cyprus has changed during the last four years. Significant progress has been made in terms of cybersecurity maturity in Dimension 1: *Cybersecurity Policy and Strategy*, and Dimension 5: *Standards and Technologies* in particular. The maturity score for the *Cybersecurity Education* Factor has decreased since the 2017 review (from Established to Formative-Established). This is a result of requirements added during the CMM 2021 revision that must be met in order for nations to reach the Established stage; in particular, the need for nations to have well-funded programme review processes and outcome-oriented metrics in place, to be able to review the supply and demand for cybersecurity courses.

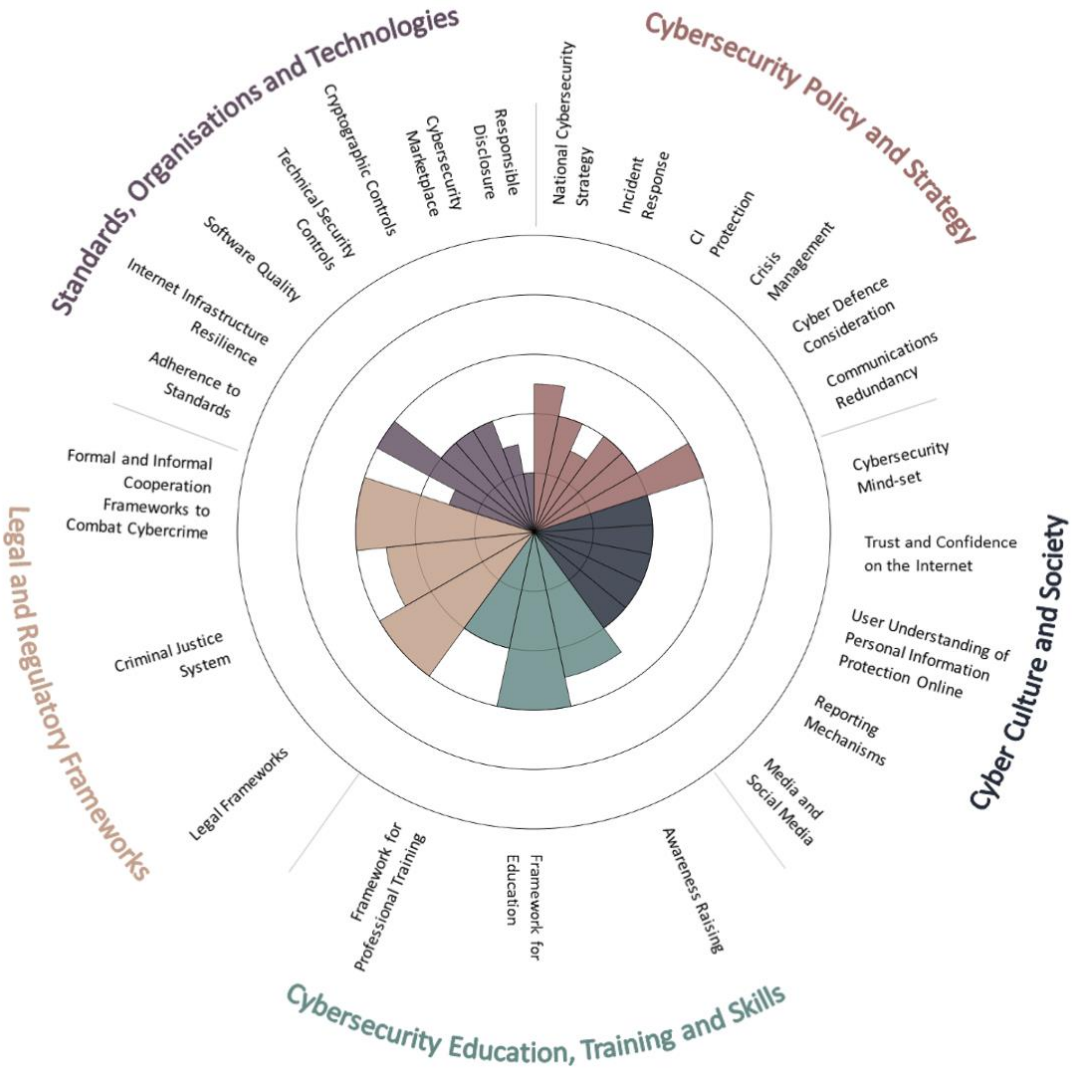

Figure 2: Overall representation of the cybersecurity capacity in Cyprus – CMM review 2017

Table 2 provides a summary overview of capacity developments for all factors assessed both in 2017 and 2021.

	Maturity Stage‡		Capacity Changes*
Factors based on CMM 2017	**2017**	**2021**	
D1 Cybersecurity Policy and Strategy			
D1.1 National Cybersecurity Strategy	Formative to Established	Established to Strategic	+ +
D1.2 Incident Response	Formative	Established to Strategic	+ +
D1.3 Critical Infrastructure Protection	Start-Up to Formative	Established	+ +
D1.4 Crisis Management	Formative	Established	+ +
D1.5 Cyber Defence	Formative	Established	+ +
D1.6 Communications Redundancy	Established	Established	o
D2 Cybersecurity Culture and Society			
D2.1 Cybersecurity Mind-Set	Formative	Formative	o
D2.2 Trust and Confidence on the Internet	Formative	Formative	o
D2.3 User Understanding of Personal Inf.	Formative	Formative	o
D2.4 Reporting Mechanisms	Formative	Establish	+ +
D2.5 Media and Social Media	Formative	Formative	o
D3 Cybersecurity Education, Training, and Skills			
D3.1 Awareness Raising	Formative to Established	Formative to Established	o
D3.2 Framework for Education	Established	Formative to Established	-
D3.3 Framework for Professional Training	Formative	Formative to Established	+
D4 Legal and Regulatory Frameworks			
D4.1 Legal Frameworks	Established	Established	o
D4.2 Criminal Justice System	Formative to Established	Established	+
D4.3 Formal and Informal Cooperation Fra.	Established	Established	o
D5 Standards, Organisations, and Technologies			
D5.1 Adherence to Standards	Start-Up to Formative	Formative to Established	+ +

‡ For reasons of backward compatibility, this overview presents maturity levels observed in the 2021 CMM assessment in the framework of a previous version of the CMM that had served as the basis for the CMM review of Cyprus conducted in 2017.

* Factors that have advanced to the next maturity stage have received the mark «+ +». Factors that have seen improvements in some of its indicators but not sufficient progress to warrant an upgrade in the next maturity stage have been marked «+». Factors without notable progress have been registered with the neutral mark «o». Any regression, if observed, would have been marked «- -»/«-», correspondingly.

D5.2 Internet Infrastructure Resilience	Established	Established	o
D5.3 Software Quality	Formative	Formative to Established	+
D5.4 Technical Security Controls	Formative	Formative to Established	+
D5.5 Cryptographic Controls	Formative	Formative to Established	+
D5.6 Cybersecurity Marketplace	Start-Up to Formative	Formative	+ +
D5.7 Responsible Disclosure	Start-Up	Formative to Established	+ +

Table 1: Capacity developments comparing CMM assessments of Cyprus in 2017 and 2021

Cybersecurity Policy and Strategy

Since the 2017 CMM report, Cyprus has implemented a number of structural reforms, resulting in a significant increase in the maturity of the country's policy and strategy. The national strategy has been reviewed and renewed, with the current published strategy positioning Cyprus as a pioneering country in cybersecurity. The revision of the strategy entailed a consultation process which included numerous stakeholders from diverse sectors. The new strategy consists of fifteen thematic areas which cover the needs of a variety of crucial actors, many of which are often overlooked by other countries. Each thematic area includes detailed actions which trigger projects that contain working groups, clear milestones, delivery plans and metrics for effective implementation. A single authority, the Digital Security Authority (DSA), is responsible for the co-ordination of the implementation of the strategy and it monitors all actions, and has processes in place to identify emerging actions and reprioritise projects in case of changes in the threat-landscape. As the national vision is for Cyprus to become a reference point in the region, international co-operation is a key priority. One of the strategy's dedicated thematic areas encourages cyber diplomacy, and the participation of public and private entities in international forums.

The national Computer Security Incident Response Team (CSIRT) of Cyprus, namely CSIRT-CY, was formed with the Council of Ministers Decision No. 81/477 and participants in the review consistently reported that it had fulfilled its role well. Since its development, CSIRT-CY has provided a platform for communication for critical infrastructures (Cis), is considered to be a hub of cyber threat intelligence, assists CIs in incident handling, and has established communication channels with other countries. The categorisation of incidents by CIs follows the taxonomy set by the European Union Agency for Cybersecurity (ENISA); the national database of incidents is maintained by CSIRT-CY, and lessons learned from incident handling inform strategic and policy decisions. Although Cyprus has achieved significant progress with structural reforms in the area of incident handling and reporting, monitoring and detection practices are lagging behind. The national CSIRT has developed sensors in collaboration with academia, which are applied to critical government networks, to bridge this gap. However, it is critical that a dedicated governmental security operations centre (SOC) is developed and that it is operational 24/7. The governmental SOC should be complemented with the creation

of sectorial SOCs or Computer Emergency Response Teams (CERTs) to supervise CIs which remain oblivious to monitoring and detection best practices. As far as national crisis management is concerned, cybersecurity is fully integrated and hybrid threats inform national security strategy and exercises. A decisive step in deciding how to respond to crisis situations is the development of a national cyber-range platform, which will be delivered by the DSA, in conjunction with academia, in the near future.

The establishment of the national risk assessment provides an up-to-date and frequently reviewed inventory of all CI stakeholders, who have acknowledged their role by signing Memorandums of Understanding (MoUs) with the DSA. The activity of CSIRT-CY has institutionalised the practice of incident disclosure for all CIs, ensuring compliance with the Network and Information Systems (NIS) Directive. The current incident notification legislation, and processes for CIs to report cybersecurity incidents to the DSA, have ensured that this practice is formalised. The DSA has legislated a list of security requirements that apply horizontally to all CIs. This framework is designed to ensure that key service operators will undertake all appropriate measures to prevent and mitigate the impact of cyber attacks on systems that provide essential services. To ensure compliance with the newly regulated framework, a novel audit framework, requiring dedicated personnel for each sector, is being developed. Thus far, only the telecommunications sector has been audited for compliance at regular intervals. However, the first audits of the other CI sectors are due to be conducted in late 2021.

Cyprus has adopted a national strategy for security and defence which, as participants attested, is informed by cybersecurity elements and hybrid threats. It was further mentioned in the focus groups that rules of engagement described in the strategy abide with international humanitarian law. Civil defence co-ordination and co-operation is formally described in the strategy and has been implemented by specific MoUs signed by the Civil Defence and the DSA. National Guard has recently developed a specialized Cyberdefence Unit hosting a military CERT for the protection of its information networks. The military CERT is fully operational and has established bilateral agreements for the exchange of cyber threat intelligence. High-level cybersecurity training is also provided to military personnel in general, in an effort to increase cybersecurity awareness. At an operational level, there is dedicated infrastructure for co-operation during national incidents, specifically by sharing access to facilities, which is evidence of a commitment to effective civil-defence co-ordination.

Cybersecurity Culture and Society

The degree to which cybersecurity is prioritised and embedded in the attitudes and practices of stakeholders in Cyprus varies across sectors and demographics. In the private sector, particularly in large organisations in regulated industries such as Finance and Electronic Communications, there is a strong awareness of cybersecurity risks and a prioritisation of safe cybersecurity practices. While the cybersecurity mindset is less prevalent in small and medium-sized enterprises (SMEs), on the whole, the mindset across the private sector appears to be improving, with reports that this is evidenced by the number of requests for, and the improving results of, penetration tests, for example.

Participants expressed the view that cybersecurity awareness and prioritisation of cybersecurity in government departments was mixed. However, it was stated that this has been improving, with a growing awareness of the risks from phishing, for example. Furthermore, a recruitment process is in progress for a government Chief Information Security Officer (CISO) and this, along with the impending cybersecurity regulation overseen by the DSA, should help improve the cybersecurity mindset and adherence to cybersecurity best practices in government.

In terms of the cybersecurity mindset of the general public, participants in the focus groups felt that there are stark differences between generations, with senior citizens being less aware, while younger people generally have a stronger level of awareness (due in large part to significant cybersecurity awareness-raising initiatives that target the younger generation). The same generational difference is present when it comes to trust and confidence in online services. According to participants, only a limited proportion of Internet users are able to critically assess what they see or receive online, and identify possible risks, or protect themselves from misinformation online; this view is supported by the European Commission's Digital Economy and Society Index (DESI) 2020 report. Online disinformation is cited as an offence in Cyprus's criminal code.

A limited but growing number of e-government and e-commerce services exist. Legislation is in place that deals with identification and trust for electronic transactions, including the use of digital signatures in government services and applications. The existing e-government services are widely used for processes such as handling tax. E-commerce services are increasingly used for services such as online food delivery and clothing purchases, with usage accelerated by the COVID-19 pandemic. The review team was not made aware of surveys or metrics to assess users' trust and confidence online, or their trust in e-government or e-commerce services.

Statistics from the CYberSafety Helpline (a cybersecurity awareness initiative in Cyprus) show that the public has some awareness of the need to protect personal information online and attempts to do so. Participants expressed the view that the risks around personal information online, and the need to protect it, tends to be included in awareness-raising campaigns and materials, and this had led to the citizens of Cyprus gradually becoming more aware of how to protect themselves online. However, there are still many cases of people posting sensitive content on social media. The EU General Data Protection Regulation (GDPR), supplemented by local data-protection laws, has been a driver over the last few years in improving cybersecurity mindset (particularly around data privacy and protection) and practice across organisations.

A number of platforms exist for reporting cyber harms and concerns in Cyprus, covering most of the incident-reporting requirements of the population. The Cyprus Police runs a Cybercrime Reporting Platform and a mobile reporting application that can be used by Internet users and organisations; the CYberSafety Helpline and Hotline are available; the former provides support to children, adolescents and their families on issues relating to the safe use of the Internet, while the latter enables Internet users in Cyprus to report illegal content or actions online. These channels are promoted, particularly via social media, and statistics show that there is reasonable level of uptake. Participants expressed the view that some organisations may be reluctant to report cybersecurity incidents for fear of reputational harm, especially given the potential difficulty of remaining anonymous in a relatively small country.

On the whole, there was a view that the representation of cybersecurity issues in the media and on online platforms is becoming more regular, and that the public is being kept better informed about cybersecurity incidents than a few years ago. This is largely due to the efforts of the DSA and the Cybercrime Unit of the Cyprus Police, both of which issue regular announcements via social media. Some cybersecurity information is disseminated *ad-hoc* via the mainstream media: participants stated that cybersecurity incidents and data breaches tend to be covered on television and on radio news channels, and in (online) newspaper articles. The perception was expressed that the mainstream media lacks sufficient cybersecurity knowledge to report as completely or effectively about the subject as one might hope, nor create continuous media campaigns that help raise cybersecurity awareness. It is unclear to what extent whistleblowers would be accepted as playing a positive role, but legislation is in development to protect them.

Building Cybersecurity Knowledge and Capabilities

A national programme for raising cybersecurity awareness, covering all users of electronic systems, does not yet exist although significant and co-ordinated awareness-raising efforts are ongoing for specific target demographics. There has been particular focus on awareness-raising for children, teachers and parents, according to the National Strategy for a Better Internet for Children in Cyprus, including input from government, the private sector, academia and civil society through the CYberSafety campaign. For other demographics, the effort has been less co-ordinated, so far, although parties including the Cyprus Police and the DSA have various initiatives that target other demographics. Awareness-raising for business and government leaders is an area that requires further attention.

The Government recognises the need to expand the existing awareness-raising provision, to create co-ordinated national awareness-raising programmes that cover all users of electronic systems. This is reflected in Thematic Unit 9 of the National Cybersecurity Strategy (NCS; *Creation of Security Culture*). A competence centre is currently being established to promote the safe use of digital technology and the Internet across demographics in Cyprus, and it is envisaged that this centre will play an important role in raising cybersecurity awareness across a wider range of demographics.

There are various university-level cybersecurity courses offered in the Republic of Cyprus. A number of universities offer master's degrees in Cybersecurity but there are no dedicated bachelor degrees offered in the subject, although cybersecurity is a compulsory part of some Computer Science courses; various specific Cybersecurity-related elective modules, such as cybercrime and legal concepts, are also offered within Computer Science degrees. The universities reported collaboration with industry and the Government in the development and updating of cybersecurity curricula. There are also a few Doctoral-level students in the field of cybersecurity. However, the view was widely expressed that that number is not high enough and that this impacts on the supply of cybersecurity educators and makes recruitment challenging. Currently, there are few internship programmes and little industry involvement in university projects that might enable students to gain cybersecurity industry experience during their degree programmes.

Part of the CYberSafety project has been focused on the school curriculum, and this has led to new curricular units on cyber-safety and cyber-bullying being offered at primary-school level,

and sections of relevant courses such as Information Technology, covering key cybersecurity concepts, at secondary school level. It was reported that some private schools offer more extensive cybersecurity education, including hackathons. Cyprus participates in international Capture-the-Flag competitions and runs its own in-country competitions, which contribute towards establishing a cadre of cybersecurity experts who not only have technical skills but who also understand how to co-operate within the field of cybersecurity.

Professional training programmes in cybersecurity are offered primarily by the Cyprus chapters of the international cybersecurity professional training and certification bodies, the International Information System Security Certification Consortium (ISC)[2] and Information Systems Audit and Control Association (ISACA). A range of training courses and certifications are offered by some private companies, including certifications from software providers Cisco and Check Point. There is no evidence that formal documentation of the national cybersecurity training requirements has been produced yet. It was noted by some government participants that a greater training offering for government personnel would be beneficial, and the NCS includes actions to address this. A shortage of people qualified to run cybersecurity professional-training courses in Cyprus was reported. This is rooted in a cybersecurity workforce shortage; to address this, there is a need to continue to encourage the study of science, technology, engineering and mathematics (STEM) subjects in schools; promote cybersecurity careers to students; and implement initiatives that will encourage cybersecurity experts to remain in the country after training.

An initiative is underway, led by the Deputy Ministry of Research, Innovation and Digital Transformation, to build a Digital Academy (similar to the academy that exists in Greece). This will enable self-study on courses in digital technology and cybersecurity provided by various vendors. The Cyprus Centre for Land, Open-seas, and Port Security (CYCLOPS) is in development: it is a forward-looking joint initiative between the US and Cyprus for a regional security (including cybersecurity) training hub, located in Cyprus, that will support capacity-building in the region. Members of the international community participating in the review expressed the view that many countries are excited about the prospect of collaborating with CYCLOPS.

Cybersecurity research and development (R&D) activities have been established in Cyprus and are indicated in Thematic Unit 11 (*Research and Innovation*) of the NCS. A specific cybersecurity R&D strategy is not in place but one might be beneficial as it would enable stakeholders to identify R&D requirements necessary to meet the national need. Cybersecurity research laboratories have been established at a number of universities in Cyprus and there is active international collaboration in R&D projects, including participation in research consortia with EU partners, such as the EU's Erasmus programme.

The public sector also collaborates with university cybersecurity R&D programmes. One such is the Cyber Sensors for Critical Infrastructure Protection and Large Scale Cyber Range Training Environment (CY SENTINEL) project, which is run as a collaboration between the Open University of Cyprus and the DSA and which has delivered a cyber-range platform that will be used to run national-level cybersecurity exercises. Most R&D projects at universities are funded by EU schemes such as Horizon 2020 and Erasmus. It was reported that the Government has considered how to allocate funds to cybersecurity R&D, but this has not yet been delivered. No evidence was provided of any metrics in place to measure R&D performance in Cyprus.

Legal and Regulatory Frameworks

Cyprus has diligently implemented EU Regulations and Directives into Cypriot law. There is an umbrella of different laws on substantive cybercrime legislation covering illegal access to, interferences on, and the interception on devices, computer systems and data. Furthermore, Cyprus has completed all the necessary legal requirements for the establishment of an entity – the DSA – to create frameworks for CIs, and the mandatory sharing of information, with defined rules that CIs need to adhere to and will be subject to strict penalties if they do not conform to their obligations. The complete legal framework for the DSA, including detailed security measures and incident notification obligations, has already been published and is in force.

The umbrella of laws that the cybercrime unit has at its disposal provides it with comprehensive provisions for the investigation of cybercrime and evidentiary requirements. All the necessary EU legislation, as well as international treaties, have been ratified and there is consistent monitoring through various units of the implementation of emerging treaties and EU legislation in national law. Apart from the DSA's legal unit, which is tasked with monitoring cybersecurity-related developments in legislation, Counsels and prosecutors follow developments in case law closely, at local, EU and international level. Human rights considerations are at the heart of every piece of Cypriot legislation, as Article 5 of the Constitution of the Republic of Cyprus states, that the Republic of Cyprus will secure the human rights and fundamental freedoms of everyone under its jurisdiction.

In the case of related legislative frameworks, Cyprus has fully implemented the NIS Directive, along with Articles 40 and 41 of the European Electronic Communications Code related to the security of electronic communications providers. Cyprus has also implemented the EU's General Data Protection Regulation (EU, 2016/679). The country's recent legislation builds on a number of previous legislative efforts regarding the processing of personal data. Evidence of the importance of child protection online in Cyprus can be found in the national strategy, as there are dedicated actions for this area. Participants mentioned that the main cybercrime offences that are prosecuted in Cyprus involve child pornography, with specific laws applying to such cases. There is comprehensive legislation for protecting consumers in online environments. Furthermore, there is a consumer protection service entity, under the Ministry of Energy, Commerce and Industry, with dedicated helplines and portals for lodging complaints. The website provides information about fraudulent websites that pretend to be the official websites of Cypriot organisations, online scams, and phishing emails. Participants mentioned that there are pending actions concerning qualified trust services and electronic identities, which may boost further consumers' confidence in e-commerce. Intellectual property law is effective in Cyprus, in accordance with best practice and EU legislation. Comprehensive intellectual property (IP) legislation exists for online products and services, based on Common Law. Cyprus is signatory to numerous international conventions relevant to IP, to ensure that the Cypriot law will remain informed by international developments.

The NCS recognises the need to continue to build capacity to combat cyber offences. In terms of the capacity of the prosecution and the courts, Cyprus has reached an Established stage of maturity. The Cybercrime Unit of the Cyprus Police is responsible for the investigation of cybercrime and is composed of the Office for Combating Cybercrime (OCC) and the Digital Evidence Forensic Laboratory (DEFL), which is staffed by specialised officers for the collection

and forensic analysis of electronic devices, and the presentation of expert scientific evidence to the courts. The Cybercrime Unit has grown significantly since its inception in 2007, when it had five staff; in 2021, it had 22 staff across the OCC and DEFL.

It was reported that, wherever possible, cybercrime cases are assigned to prosecutors and counsels who have expertise in that field. In general, participants believed that over the last few years, a reasonable level of expertise has been reached within law enforcement, and among prosecutors and judges, due to experience gained by handling increasing numbers of cybercrime cases, and because of the various training efforts both within Cyprus, particularly through the Cyprus Cybercrime Centre of Excellence for Training, Research and Education (3CE) project, and at a European level. However, it was noted that there is still room for improvement, and that increased training might be beneficial.

The DSA has established its role as the cybersecurity regulator for the CIs in Cyprus, in line with the developed regulatory framework. The relevant regulatory requirements came into force in 2020, and the legal bases and specifics for auditing are being developed by the DSA's Regulatory, Strategy and Supervision Team, in consultation with the Attorney General's office and other legal entities. Since the audits have not yet taken place, the resources and capabilities of the DSA as the regulator have not yet been fully tested.

The NCS recognises the need to continue to strengthen co-operation at an international level for the investigation of cross-border cyber offences, and between the public and private sectors. Cyprus' co-operation with foreign law-enforcement counterparts is advanced, achieving elements of the CMM's highest maturity level, Dynamic. For international exchange of information in relation to cybercrime investigations, Cyprus co-operates with the EU and also with non-EU countries on the basis of bilateral and multilateral agreements; some of these agreements have already been tested and been shown to work effectively during cross-border investigations of cyber-incidents.

The OCC is integrated into and co-operates closely with a number of international networks, including Europol and Interpol. Representatives from Cyprus are participating in EU initiatives to address challenges around delays in mutual legal assistance, which can significantly disrupt the investigation of cross-border cybercrime cases. There is also Cypriot representation within the Council of Europe Protocol Drafting Plenary for drafting the Second Additional Protocol to the Convention on Cybercrime.

Law enforcement follows specified procedures to obtain digital evidence from organisations; this is the manner in which law enforcement and the private sector co-operate. There is close and effective co-operation between the DSA and the Cybercrime Unit, according to both the DSA and law-enforcement representatives. A formal relationship is established between the two entities, with a Memorandum of Understanding in place for information exchange, extending to CSIRT-CY. There is also co-operation between the DSA and the Law Office, with a representative of the Law Office who participates in the steering committee that monitors the implementation of the NCS; this enables the legal service to develop its cybersecurity in alignment with the NCS.

Standards and Technologies

Since the 2017 CMM review, Cyprus has achieved significant structural reforms that will pave the way for the adoption of security standards by all CIs and the Government. The Cyprus Organisation for Standardisation (CYS), to which both private and public organisations can apply for accreditation to ICT standards, is now complemented with new capabilities offered by the DSA. It has been given the mandate to act as the National Cybersecurity Certification Authority (NCCA), aligning with the certification practices provided by the EU Cybersecurity Act. There is a stark difference between the public and private sector approaches regarding the application of ICT standards. In the public sector, participants noted that despite efforts by the Department of Information Technologies (DITS), the Government does not comply with internationally-recognised standards, relying instead on minimal security requirements across all departments. Participants suggested that the new structure of the Government will provide an opportunity to break silos between ministries, and enforce horizontal security standards on the Government. The DSA framework, which is mandatory for all Cis, will be another decisive step in improving the public sector's cybersecurity approach.

The private sector is much more advanced regarding the design, adoption and audit of standards for ICT security. The rate of adoption differs between sectors but the majority of CI organisations comply with internationally-recognised standards, such as International Organisation for Standardisation (ISO) 27001 and NIST Cybersecurity. The DSA, in line with the NIS Directive, has constructed a baseline of security controls based on best practice and international standards and this newly developed DSA framework, which is prescribed in legislation, must be followed by all CIs. The DSA framework has the potential to institutionalise adherence to standards in all CIs, including the Government. Additional vertical 'plugin' guidelines need to be developed by the DSA that will incorporate security requirements into standards tailored for every sector.

Regarding standards in procurement, there are strict standards in the public sector, with scarce reference to security requirements. These strict standards add to bureaucratic strains and time-consuming processes, forcing staff to circumvent them in many cases by buying personal IT-related gadgets and hardware which, in turn, complicates the IT environment that needs to be secured. By contrast, the private sector and CIs in particular have developed standards that consider security with specific outsourcing guidelines for cloud services. The EU Cybersecurity Act is the cornerstone by which cybersecurity certification schemes for products and services can be created. Such schemes created by ENISA, with the assistance of *ad-hoc* working groups comprising experts in the field, will entail references to standards and provide guidelines based on best practice. Therefore, as Cyprus is a pioneer in the exploration of how the Cybersecurity Act will be implemented, it will be in a unique position to lead the way on adherence to standards for the provision of products and services.

The degree of adoption of security controls in Cyprus resembles the adherence to standards situation, meaning it varies across sectors and organisations. Participants suggested that the implementation of security controls in government bodies – despite recent improvements following initiatives from DITS – is elementary and inconsistent across ministries. Constraints in budget, mismanagement of human resources, and a lack of appropriate organisational structure are the main reasons why the Government lags significantly in its cybersecurity status. Participants recommended the urgent development of a Government SOC to monitor

it. In the private sector, there is an understanding that organisations which are enlisted as Cis must implement appropriate security controls tailored to the services they offer. There are also organisations that have decided to outsource security to third parties, particularly for supervisory control and data acquisition (SCADA) systems or essential services. Participants warned, however, that outsourcing such services should be considered with caution as the perception of transferring IT risk to a third party is that it is wrong. It was mentioned in the meetings that there are protocols in place, defining service levels agreements that are appropriate for the security and continuation of services. The use of cryptographic controls is evident in both the public and private sectors, with encryption controls applied in critical systems both for data in transit and data at rest.

There is also evidence that organisations in both the public and private sectors try to develop inventories of secure software. Most mature organisations will routinely perform vulnerability scans and patching. For organisations that are not part of a CI, participants noted that controls for patching rarely exist and *ad-hoc* lists of secure software are scarce. Particular attention should be paid to IT companies which provide services for critical infrastructure stakeholders. Turning to software development, the majority of the participants noted that their organisations depend heavily on software purchased from multinational companies. There are cases where software is developed in house, however, that is mainly for internal use rather than for customer-facing applications. When software is purchased, many organisations reported that they have internal procedures for checking software security during the procurement phase.

Participants estimated that the infrastructure of the Internet in Cyprus is stable, with reliable services that are widely used. More than 80 percent of households in Cyprus have a fixed broadband service,making Cyprus a country with one of the highest take-up rates in Europe. Speeds offered to households are average – Cyprus is one the last countries in EU to have households (less than 10 percent) that have broadband speeds of at least 100 Mbps. Mobile broadband is developing fast and is considered complementary to fixed broadband – Cyprus has more than 120 subscriptions per 100 people. Participants mentioned that in general, Internet service providers (ISPs) undergo strict audit controls and also need to comply with EU legislation concerning telecommunications. Internet Exchange Points therefore exist which guarantee resilience of the Internet service, redundancy systems for continuity, and detailed policies on handling incidents.

The domestic market for cybersecurity technologies is rather limited. Participants explained that Cyprus is a small country and the majority of cybersecurity products that organisations use derive from well-established multinational organisations, which are very hard to compete with. It is difficult for a Cypriot company to offer cybersecurity products locally as there is limited trust in their capabilities. By contrast, consultancy firms regularly offer cybersecurity services to the private and public sectors. Furthermore, Cyprus has accredited Trust Service Providers which offer electronic signatures, timestamps, and qualified website authentication certificates; however, their up-take is extremely low. Participants believe that there will be government initiatives for public-private partnerships to encourage the cybersecurity market in Cyprus, as there are dedicated thematic areas with specific actions and budgets within the national cybersecurity strategy.

Where Cyprus is leading initiatives and has acquired expertise is in the area of cybersecurity certification schemes. Such schemes may become vehicles for accelerating developments in

the cybersecurity market, as Cyprus will have the opportunity to offer conformity assessment body (CAB) services in the EU market, for all future EU schemes. Regarding the outsourcing of services, participants mentioned that in the private sector, there are risk assessment processes in place, with specific focus on assessing the need for cloud services. In the public sector, participants mentioned that there are considerations regarding the transfer of services to the cloud. Many employees are of the opinion that they transfer risk at the same time which, according to participants, is erroneous. Finally, since the 2017 review, there have been small improvements to the cyber insurance market in Cyprus,. Participants mentioned that there are products provided by foreign insurance companies but they suggested that these are not adaptive to emerging threats and the dynamic nature of incident response.

Since the inception of CSIRT-CY, sharing of information on vulnerabilities amongst CIs has significantly improved in Cyprus. There are formal agreements with all the constituencies that participate in CSIRT-CY's cyber-threat intelligence network, mandating the disclosure of incidents and vulnerabilities, as per the NIS Directive. The CSIRT-CY has developed incident disclosure practises, as well as protocols to address incidents within given timeframes, according to their severity. Furthermore, at an EU level, there are multilateral agreements for information-sharing and Cyprus is an active member of the EU CSIRT network, and in Europe's information-sharing for cyber crisis management (CyCLONe – Cyber Crisis Liaison Organisations Network). In the matter of responsible disclosure of security flaws, participants acknowledged that many organisations provide incentives for bug detection, using bug bounties to encourage disclosure. For the public, there is a hotline and a website where incidents can be reported, but legal protections for whistleblowers are still lacking. Participants mentioned that this will be addressed soon as there is legislation pending in the House of Representatives.

INTRODUCTION

At the invitation of, and in collaboration with, Cyprus's Digital Security Authority (DSA), the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of the cybersecurity capacity of Cyprus. The objective of this review was to enable Cyprus to determine areas of capacity in which the Government might strategically invest, so that it may improve its national cybersecurity status.

Over the period 21 to 24 September 2021, a three-day consultation process took place in Cyprus. This was preceded by a desk-research phase in which the GCSCC researchers gathered information from documents available online and provided by the DSA, and a number of planning meetings between the GCSCC and DSA. Stakeholders from the following organisations participated in person in the consultations:

- Public-sector entities:
    - Digital Security Authority (DSA)
    - National CSIRT of Cyprus (CSIRT-CY) (part of the DSA)
    - Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR)
    - Deputy Ministry of Research, Innovation and Digital Policy
    - Department of Information Technology Services (DITS)
    - Treasury of the Republic of Cyprus
    - Department of Electromechanical Services
    - Customs & Excise Department
    - Department of Civil Aviation
    - Civil Defence Department
    - Deputy Ministry of Maritime and Shipping
    - Cyprus Agricultural Payments Organisation
    - Cyprus Police Cybercrime Unit
    - Cyprus Ports Authority
    - Cyprus Organisation for Standardisation (CSY)
    - Law Office of the Republic of Cyprus
    - Members of Parliament
    - Ministry of Defence
    - Office of the Commissioner for the Protection of Personal Data
    - Ministry of Foreign Affairs
    - National Security Authority
    - Cyprus Intelligence Service
    - Cyprus Army
    - Embassy representatives from Poland and the UK
- Universities
- Professional societies
- Telecommunications service providers and Internet service providers (ISPs)
- Broadcasting corporations

- Operators of Critical Infrastructures (Cis; Finance sector, Oil and Gas sector, Electricity sector, Transport sector)
- Academic CSIRT
- Cybersecurity technology and service providers
- Consultancy firms
- Certification companies

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM),[2] which is composed of five distinct *Dimensions* of cybersecurity capacity (see Figure 3).

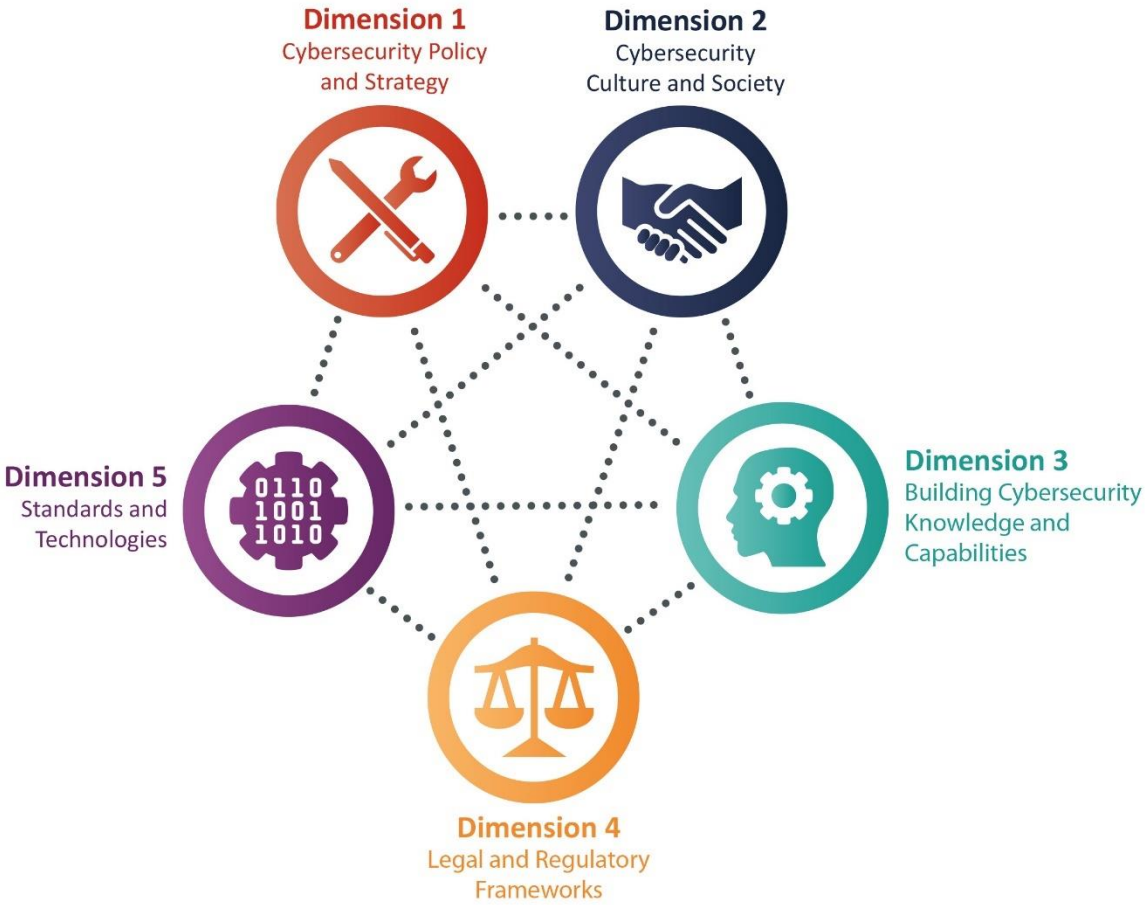

Figure 3: Dimensions of CMM.

[2] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 Edition," March 2021, https://gcscc.ox.ac.uk/the-cmm#/.

Each *Dimension* consists of a set of *Factors*, which describe and define what it means to possess cybersecurity capacity therein. Table shows the five *Dimensions* together with the *Factors* which each presents:

DIMENSIONS	***FACTORS***
Dimension 1 ***Cybersecurity Policy and Strategy***	D1.1 Strategy Development D1.2 Incident Response and Crisis Management D1.3 Critical Infrastructure (CI) Protection D1.4 Cybersecurity in Defence and National Security
Dimension 2 ***Cybersecurity Culture and Society***	D2.1 Cybersecurity Mindset D2.2 Trust and Confidence in Online Services D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Online Platforms
Dimension 3 ***Building Cybersecurity Knowledge and Capabilities***	D3.1 Building Cybersecurity Awareness D3.2 Cybersecurity Education D3.3 Cybersecurity Professional Training D3.4 Cybersecurity Research and Innovation
Dimension 4 ***Legal and Regulatory Frameworks***	D4.1 Legal and Regulatory Provisions D4.2 Related Legislative Frameworks D4.3 Legal and Regulatory Capability and Capacity D4.4. Formal and Informal Co-operation Frameworks to Combat Cybercrime
Dimension 5 ***Standards and Technologies***	D5.1 Adherence to Standards D5.2 Security Controls D5.3 Software Quality D5.4 Communications and Internet Infrastructure Resilience D5.5 Cybersecurity Marketplace D5.6 Responsible Disclosure

Table 2: the Dimensions *and their* Factors *that are considered in CMM.*

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each *Dimension* contains a number of *Factors* which describe what it means to possess cybersecurity capacity. Each *Factor* presents a number of *Aspects* grouping together related *Indicators*, which describe steps and actions that, once observed, define the stage of maturity of that *Aspect*. There are five *Stages* of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an *ad-hoc* approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five *Stages* are defined as follows:

- **Start-up:** at this *Stage*, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There may be an absence of observable evidence at this *Stage*;

- **formative:** some features of the *Aspect* have begun to grow and be formulated, but may be *ad hoc*, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated;

- **established:** the Indicators of the *Aspect* are in place, and evidence shows that they are working. There is not, however, well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the *Aspect*. But the *Aspect* is functional and defined;

- **strategic:** choices have been made about which parts of the *Aspect* are important, and which are less important for the particular organisation or nation. The strategic *Stage* reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances; and

- **dynamic:** at this *Stage*, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology of the threat environment, global conflict, or a significant change in one area of concern (e.g. cybercrime or privacy). There is also evidence of global leadership on cybersecurity issues. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this *Stage*.

The assignment of maturity stages is based upon the evidence collected, including the general or consensus view of accounts presented by stakeholders, desktop research and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Cyprus and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN CYPRUS

According to European Internet statistics, 84.4 percent of the population of the Republic of Cyprus were Internet users in December 2020.[3] Cyprus ranks above the EU average on mobile broadband take-up, but well below the EU average on take-up of fast broadband, according to the European Commission's Digital Economy and Society Index (DESI) 2020.[4] The same report states that almost an eighth of Cypriots have never used the Internet, around half of Cypriots lack basic digital skills, and the supply of ICT specialists is below the EU average.

In terms of Cyprus' readiness to exploit the opportunities offered by digital technologies, the Network Readiness Index 2020 ranked Cyprus 36th out of the 134 countries it includes, with fairly consistent ranking across the four pillars: Technology, People, Governance and Impact.[5] In terms of overall digital performance and competitiveness, Cyprus ranked 24th out of 28 EU Member States in the European Commission's DESI 2020. The report notes that Cyprus has improved its results on all DESI dimensions compared to data collected prior to the COVID-19 pandemic.

In terms of social media usage in Cyprus, in late 2020, approximately 73 percent of the Cypriot population subscribed to Facebook,[6] and 83 percent to social networks in general.[7] Cyprus had the third-highest social media participation rate among EU Member States in 2020, according to European Commission statistics.[8]

The ITU's Global Cybersecurity Index 2020 ranked Cyprus 41st out of the 182 participating countries, and 26th out of 46 European countries.[9] Legal Measures were highlighted as an area of relative strength, while Capacity Development was highlighted as an area of potential growth.

Since the last CMM review conducted by the GCSCC in 2017, the Digital Security Authority (DSA) has been established as a new national competent authority to enforce the security measures of the Network and Information Security (NIS) Directive, and incident-reporting obligations across the CI. The Computer Security Incident Response Team (CSIRT) of Cyprus, namely CSIRT-CY, has also been established as part of the DSA. Furthermore, the National Cybersecurity Strategy (NCS) has been fully updated: the new NCS was published and adopted in 2020.

[3] internetworldstats.com/stats4.htm#europe
[4] https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020
[5] https://networkreadinessindex.org/wp-content/uploads/2020/11/NRI-2020-V8_28-11-2020.pdf
[6] internetworldstats.com/stats4.htm#europe
[7] https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020
[8] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20210630-1
[9] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Throughout the in-person discussions held with a wide range of stakeholders, this review gained a picture of a generally positive trust relationship with the DSA, one in which stakeholders appear to feel supported and well informed. These strong relationships appear to be reaping positive results, with stakeholders understanding the benefits of co-operating with the DSA rather than simply “complying”.

As an EU Member State, the impacts of the EU General Data Protection Regulation (GDPR) and the NIS Directive were clear throughout the review, and Cyprus participates in many EU-level Cybersecurity activities and networks. EU-level developments, as well as developments being made in-country, are driving a high level of activity that is leading to higher levels of cybersecurity maturity in Cyprus.

REVIEW REPORT

OVERVIEW

This section provides an overall representation of the cybersecurity capacity in Cyprus. Figure 4 below presents the maturity estimates in each *Dimension*. Each *Dimension* represents one fifth of the graphic, with the five stages of maturity for each *Factor* extending outwards from the centre of the graphic; start-up is closest to the centre of the graphic and dynamic at the perimeter.

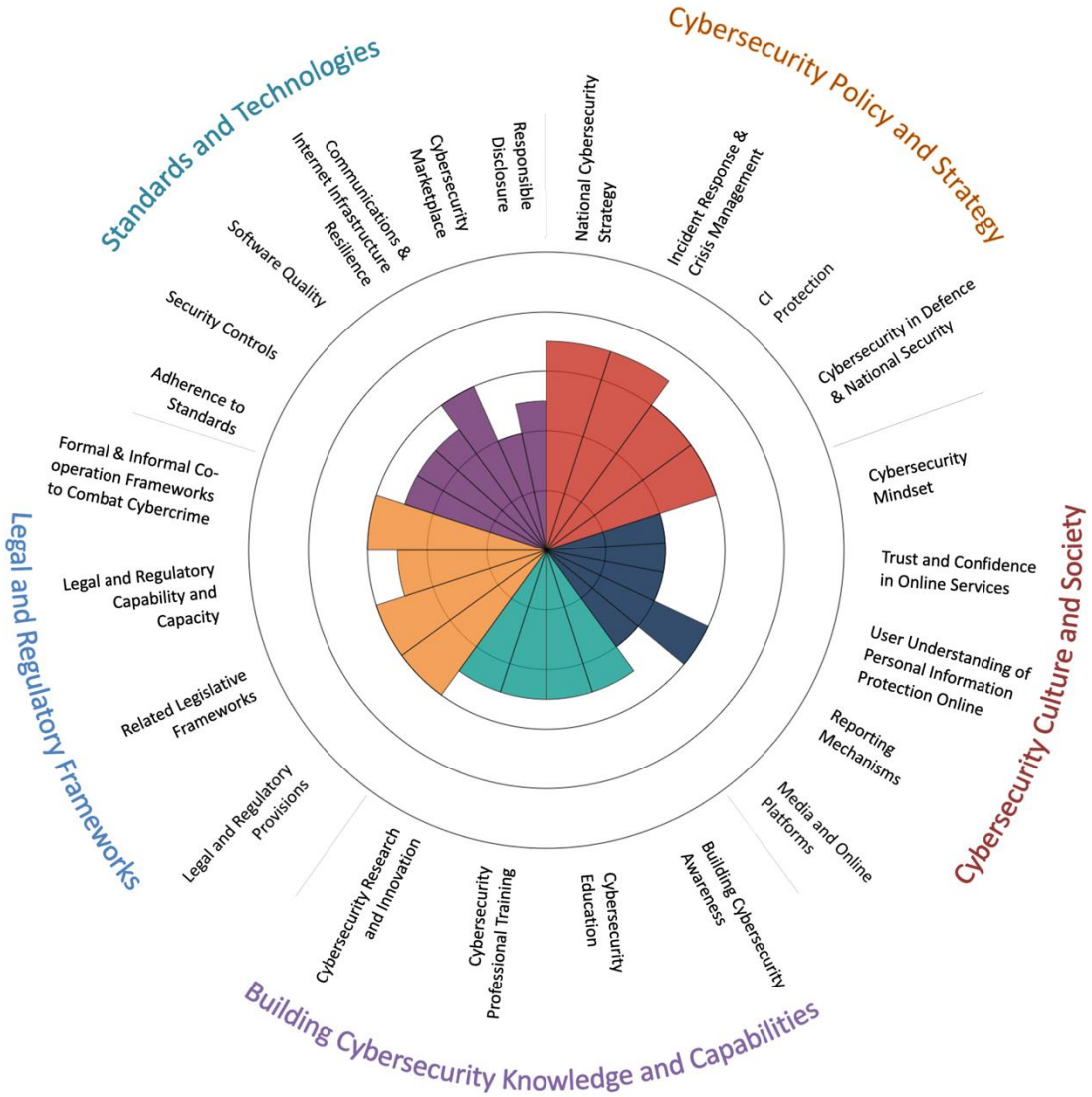

Figure 4: Overall representation of the cybersecurity capacity in Cyprus – CMM review 2021

This was the second CMM review of Cyprus, following the first in 2017. Figure 2 below shows the overall representation of the cybersecurity capacity in Cyprus as presented in the 2017 CMM report. The CMM was revised in 2021 to reflect the continuously changing cybersecurity risk and control landscape, and the changing operational environment in which nations have to deliver cybersecurity. There are, therefore, some differences between the CMM used in the 2017 review and in the 2021 review; differences in the structure of dimensions and phrasing of *Factor* names can be seen from the graphs.

A comparison of Figure 1 and Figure 2 indicates the extent to which cybersecurity capacity in Cyprus has changed during the last four years. Significant progress has been made in terms of cybersecurity maturity in Dimension 1: *Cybersecurity Policy and Strategy*, and Dimension 5: *Standards and Technologies* in particular. The maturity score for the Cybersecurity Education factor has decreased since the 2017 review (from Established to Formative-Established). This is a result of requirements added during the CMM 2021 revision that must be met in order for nations to reach the Established stage; in particular, the need for nations to have well-funded programme review processes and outcome-oriented metrics in place, to review the supply and demand for cybersecurity courses.

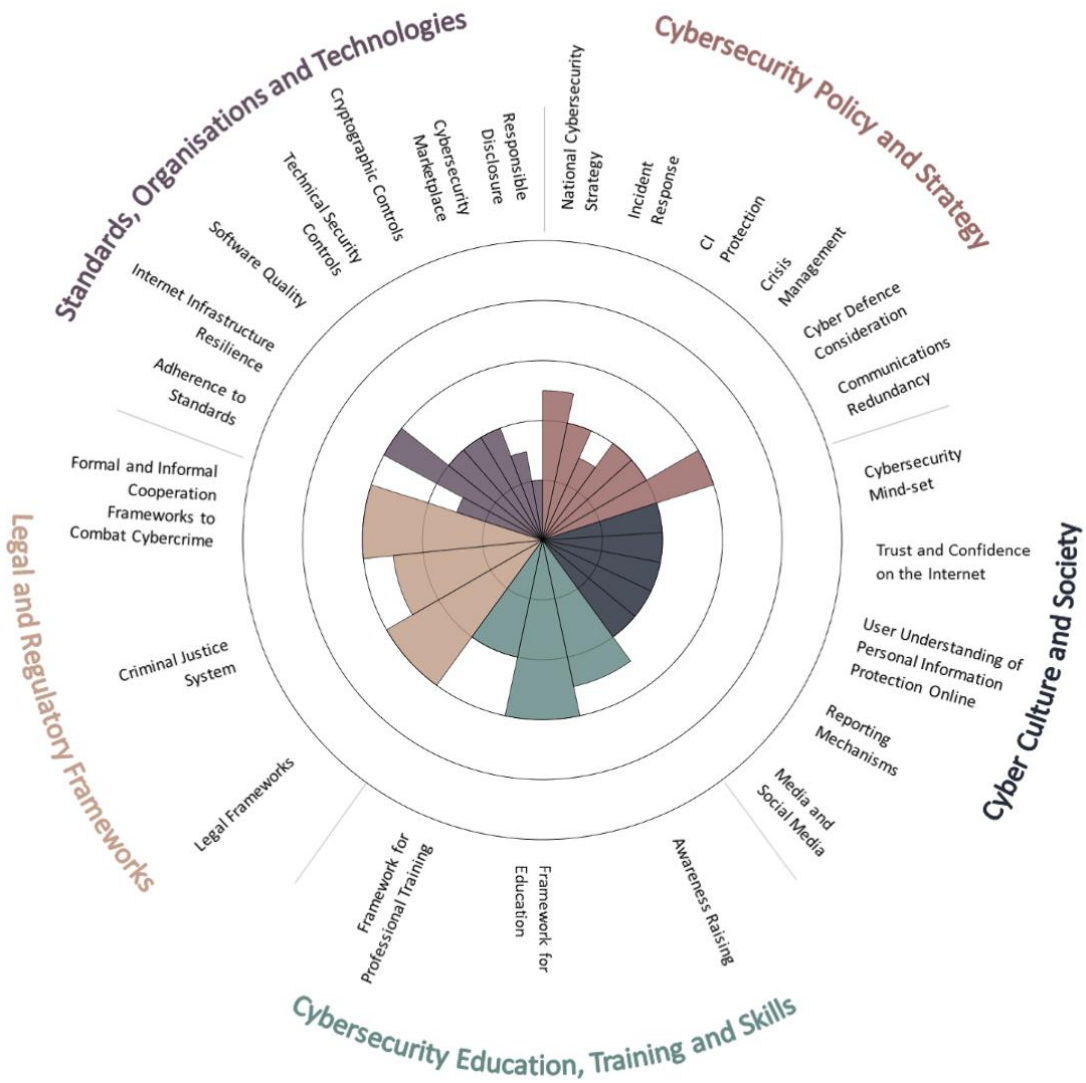

Figure 5: Overall representation of the cybersecurity capacity in Cyprus – CMM review 2017

Table 3 provides a summary overview of capacity developments for all *Factors* assessed in both 2017 and 2021.

Factors based on CMM 2017	Maturity *Stage*‡		Capacity Changes*
	2017	2021	
D1 Cybersecurity Policy and Strategy			
D1.1 National Cybersecurity Strategy	Formative to Established	Established to Strategic	+ +
D1.2 Incident Response	Formative	Established to Strategic	+ +
D1.3 Critical Infrastructure Protection	Start-up to Formative	Established	+ +
D1.4 Crisis Management	Formative	Established	+ +
D1.5 Cyber Defence	Formative	Established	+ +
D1.6 Communications Redundancy	Established	Established	o
D2 Cybersecurity Culture and Society			
D2.1 Cybersecurity Mindset	Formative	Formative	o
D2.2 Trust and Confidence on the Internet	Formative	Formative	o
D2.3 User Understanding of Personal Info	Formative	Formative	o
D2.4 Reporting Mechanisms	Formative	Establish	+ +
D2.5 Media and Social Media	Formative	Formative	o
D3 Cybersecurity Education, Training, and Skills			
D3.1 Awareness Raising	Formative to Established	Formative to Established	o
D3.2 Framework for Education	Established	Formative to Established	-
D3.3 Framework for Professional Training	Formative	Formative to Established	+
D4 Legal and Regulatory Frameworks			
D4.1 Legal Frameworks	Established	Established	o
D4.2 Criminal Justice System	Formative to Established	Established	+
D4.3 Formal and Informal Co-operation Frameworks	Established	Established	o
D5 Standards, Organisations, and Technologies			
D5.1 Adherence to Standards	Start-up to Formative	Formative to Established	+ +
D5.2 Internet Infrastructure Resilience	Established	Established	o
D5.3 Software Quality	Formative	Formative to Established	+

‡ For reasons of backward compatibility, this overview presents maturity levels observed in the 2021 CMM assessment in the framework of a previous version of the CMM that had served as the basis for the CMM review of Cyprus conducted in 2017.

* Factors that have advanced to the next maturity stage have received the mark «+ +». Factors that have seen improvements in some of its indicators but not sufficient progress to warrant an upgrade in the next maturity stage have been marked «+». Factors without notable progress have been registered with the neutral mark «o». Any regression, if observed, would have been marked «- -»/«-», correspondingly.

D5.4 Technical Security Controls	Formative	Formative to Established	+
D5.5 Cryptographic Controls	Formative	Formative to Established	+
D5.6 Cybersecurity Marketplace	Start-up to Formative	Formative	+ +
D5.7 Responsible Disclosure	Start-up	Formative to Established	+ +

Table 3: Capacity developments comparing CMM assessments of Cyprus in 2017 and 2021

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

This *Dimension* explores Cyprus's capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience through improving its incident response, cyber defence and critical infrastructure protection capacities. This *Dimension* considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general, as depicted in Figure 6.

Figure 6: Factors and aspects examined in Dimension 1.

D1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

***Stage*: Established to Strategic**

The first National Cybersecurity Strategy (NCS) in the Republic of Cyprus was published in 2013. It was a decisive step to enable relevant actors in the country to understand the threat landscape and develop the necessary structure and agencies for a cyber-secure environment. In December 2020, a new NCS[10] was published and adopted. The review process incorporated lessons learnt from the implementation of the first strategy, inputs from the EU Cybersecurity Strategy[11] and NIS Directive,[12] including the imminent updated NIS Directive,[12] recommendations from the European Union Agency for Cybersecurity (ENISA) through its online tool, good practice guides from the International Telecommunication Union (ITU)[13] and Organisation for Security and Co-operation in Europe (OCSE),[14] and the results of the GCSCC's 2017 CMM review of the Republic of Cyprus.[15]

The central vision of the new strategy aims to render Cyprus "a pioneering country in cybersecurity, by ensuring the protection of Critical Infrastructure (CI) and the society at large, and by creating an attractive environment for the development and dissemination of services in areas which Cyprus excels and holds a leading role globally, such as maritime and finance'. The new strategy envisions a pivotal role in cybersecurity for Cyprus, in contrast with the vision of the old strategy, which focused more narrowly on securing systems for the benefit of the users. The striking difference in how Cyprus envisages its long-term role in the region depicts the significant progress that was achieved in cybersecurity during the last four years.

Several stakeholders with diverse backgrounds were involved in the development of the new strategy, including Government, CIs, the private sector and Small Medium Enterprises (SMEs), academia and non-governmental organisations (NGOs). Rounds of consultation, where stakeholders actively provided feedback and proposals, resulted in more than 250 recommendations being collected. This inclusive consultation approach ensured that the current strategy covers dedicated thematic areas and the needs of a variety of crucial actors, many of which are often neglected by countries, such as civil society.

The strategy comprises fifteen thematic areas, each one with dedicated actions to ensure that new threats can be addressed dynamically as they emerge. At the core of the thematic areas

[10] https://dsa.cy/images/pdf-upload/csrc-2020.pdf
[11] https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
[12] https://digital-strategy.ec.europa.eu/en/policies/nis-directive
[13] https://www.itu.int/en/Pages/default.aspx
[14] https://www.osce.org/
[15] https://dsa.cy/en/strategy/ccr-2017/

is the promotion of human rights, with emphases on child protection, online privacy and equality. The fifteen thematic entities described in the strategy are: governance, regulation for the co-operation of appropriate public sector entities, legislative, regulative and policy frameworks, national framework for cybersecurity, risk assessment and management, incident handling and crisis management, capacity building and design or participation in exercises, situational awareness, awareness, education, research and innovation, public-private partnership, security for all, international collaboration and cybercrime.

Every thematic area introduces a number of actions, which provide implementation details. The strategy uses a structured project methodology for every action, identifying responsible co-ordinating parties and working groups, deliverable plans and specific milestones, as well as Key Performance Indicators (KPIs) and indications of cost, with the necessary flexibility to update budgets based on emerging threats. The steering committee for the NCS meets monthly to check for delays and issues, records progress and submitted deliverables, and sets actions for co-ordinators to implement, thus ensuring the effective implementation of every action. There is a three-year plan for the budget that is controlled by the steering committee. Participants noted that since the publication of the strategy, the budget has been reprioritised and novel actions have been introduced to respond to emerging threats, providing evidence of agile and adaptive capabilities.

While the steering committee has access to a wide range of KPIs, these have generally been developed to track progress on individual projects and actions within the implementation progamme. They do not necessarily provide an holistic view of whether the overall strategic outcomes of the NCS are being achieved. It is therefore important to ensure that project-level KPIs are complemented by programme-level KPIs to enable the steering committee to determine whether the cumulative effect of the various implementation projects is sufficient to meet Cyprus's overall needs. In particular, to enable the steering committee to answer the question, "is the NCS succeeding in reducing Cyprus's overall exposure to cyber risks?".

The DSA is responsible for the co-ordination of the implementation of the NCS, as stated in Law 89(I)/2020.[16] It monitors developments in the EU and ensures the smooth implementation of EU legislation and policy related to cybersecurity. The DSA has formed a team to assist ministries in the implementation of the strategy, advising on policy issues and enabling policy-making without delays. Furthermore, Memorandums of Understanding (MoUs) have been signed with all the necessary stakeholders to ensure their active participation in the implementation of the strategy. Participants deemed that the current governmental structure, with the formation of the new Deputy Ministry for Research, Innovation and Digital Policy,[17] will provide political leverage and empower the DSA with the necessary tools to fulfil its mandate. While the DSA is generally seen to have the resources it needs to carry out its role effectively, there remain shortfalls in cyber expertise elsewhere in Government, which, in turn, is leaving its systems relatively unprotected – it is essential that this issue is addressed if Cyprus is to fully achieve the objectives of the NCS.

Participants highlighted the essential role played by the DSA in the recent developments in cybersecurity, as it acts as the national competent authority for the implementation of the NIS Directive in Cyprus, and the single point of contact for the purposes of the NIS Directive,

[16] https://dsa.cy/images/pdf-upload/DSA-Law-89-I-2020.pdf
[17] https://www.dmrid.gov.cy/dmrid/research.nsf/home_en/home_en?opendocument

incorporates the National CSIRT-CY[18] and acts as the National Cybersecurity Certification Authority (NCCA) under the EU Cybersecurity Act.[19] Finally, the DSA is responsible for conducting the national risk assessment. The first national-level risk assessment was conducted in 2017 and led to the establishment of the DSA to enforce NIS security measures and incident-reporting obligations across the CI, along with the establishment of the national CSIRT-CY. The national risk assessment defines national impact levels across five *Dimensions*: National Security, National Economy, Health and Safety, and Social Wellbeing, of people and environmental impacts.

Instead of focusing on the infrastructure of every CI, the risk assessment correctly emphasises the services these CIs offer, and, more importantly, on the dependencies of these services. Risk information is gathered from all identified CIs and a high-level analysis considers the impact on Cyprus if such services become unavailable. Individual in-depth risk assessments for all CIs have not been performed yet. There is legislation in place to mandate such exercises (DSA Law 89(I)/2020 and Decision 389/2011) and the first results are expected by the end of 2021. Conducting such exercises regularly for all CIs, especially through standardised risk assessment methodologies, will provide a more accurate depiction of the threat landscape, allowing better-informed decisions at the strategic level. Despite the absence of risk assessment exercises for CIs, the national risk assessment resulted in a risk register, which is utilised by the Government to support risk-management decisions in the area of cybersecurity and CI protection. Recommendations for managing each risk are also included in the risk register, together with recommendations of changes to existing CI legislation.

The strategy establishes a revision process which will be performed periodically, every four years. Documents from the implementation of the current strategy will shape the direction of the revision process, which also includes foreseeable changes in EU legislation and in the threat landscape. The DSA is an observer to ENISA's threat landscape working groups, to ensure that the latest emerging threat information (including threats from emerging technologies) is always considered, while meetings with regional observers include discussions about the emerging threats.

Participants expressed a preference for the next strategy to be designed with more agile elements, considering a dynamic set of generic actions rather than a rigid list which may be adapted at a later stage. They deemed that the next revision, which is planned for 2024, is a good milestone as the updated NIS Directive will have been finalised and there will be a better understanding of EU initiatives in certification. Furthermore, the legislated DSA cybersecurity framework, which provides horizontal regulation of security controls for all CIs, will have been applied to all CIs for more than two years, allowing useful lessons to be drawn that will inform certain actions in the revision process.

It was further recommended that the next steps of the cybersecurity strategy and policy in Cyprus should focus on implementing forward-looking initiatives. Examples underway, which were mentioned by participants, included the joint US-Cyprus Cyprus Center for Land, Open-seas, and Port Security (CYCLOPS) security-training hub, and the threat-intelligence and vulnerability-disclosure approaches being developed in collaboration with academia. Such projects can identify the pioneering role of Cyprus and pave the way for other countries to

[18] https://csirt.cy/

[19] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

follow. Emphasis was also given by the participants to developing cybersecurity expertise in the maritime sector, to enable Cyprus to lead developments in this area.

The national vision is for Cyprus to become a reference point in cybersecurity expertise in the region; international co-operation is therefore a main priority within the NCS. A dedicated thematic area in the strategy encourages cyber diplomacy and the participation of public and private entities to international forums. The NCS mentions that Cyprus needs to set long-term goals for international co-operation and to identify the key entities and organisations at national, European and international level. It further defines Cyprus's contribution to the international dialogue on setting norms and defining rules for a secure cyberspace as a goal. Actions identified by the NCS focus on continuing Cyprus's activities at European and International levels. Cyprus is actively involved in dedicated cybersecurity activities organised at an EU level (from exchange of cyber-threat intelligence to capacity-building activities and mitigation of cybercrime). Bilateral relations through MoUs on cybersecurity issues with countries in the region (e.g., Israel) have been formed and have resulted in streamlined exchanges of cybersecurity expertise. Participants mentioned that Cyprus collaborates with African countries and the Organisation of American States (OAS) regarding educational efforts, as well as with Greece and the Middle East for cybersecurity defence purposes.

In order for Cyprus to achieve broader international leadership in cybersecurity policy and to realise the strategy's vision, there is a need for further resources to become available. Some participants reported budget constraints for actions listed in the strategy that may result in delays in implementation, and prohibit Cyprus from reaching its full potential in the cybersecurity area.

D1.2 INCIDENT RESPONSE AND CRISIS MANAGEMENT

This Factor *addresses the capacity of the Government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the Government's capacity to organise, co-ordinate, and operationalise incident response, and whether cybersecurity has been integrated into the national crisis management framework.*

***Stage*: Established**

In the 2017 CMM review, participants hoped that the creation and establishment of the national CSIRT-CY would provide a platform for communication between the CI stakeholders, act as a hub for cyber threat intelligence for CI operators, and offer direct support to incident handling for CI while establishing communication channels with other countries. Since its inception due to Council of Ministers Decision No. 81/477, CSIRT-CY, operating under the DSA, has consistently reported that it has fulfilled its role well and is recognised by ENISA as the fastest developing CSIRT in Europe. Within a short period of time, the CSIRT-CY has developed capabilities to be certified as "Advanced maturity" in ENISA's CSIRT Maturity Assessment,[20]

[20] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

and it is pioneering in the development of internal processes and cybersecurity services by following the Information Technology Infrastructure Library[21] (ITIL) framework.

To demonstrate the high level of expertise acquired by the CSIRT-CY team, participants underlined that ENISA recommended members of CSIRT-CY, who are certified as SIM3[22] auditors, to participate in future peer review assessments of other EU countries' CSIRTs. Thus far, CSIRT-CY employs and regularly trains sixteen staff, who ensure that it remains operational 24/7. Recruiting plans aim to increase this number to 36 by early 2022. Regarding international co-operation, the CSIRT-CY is a full member of the Forum of Incident Response and Security Teams (FIRST)[23] and has been a part of the CSIRTs Network[24] that operates under the NIS Directive since its inception in 2017.

For the categorisation of incidents, CSIRT-CY has adopted ENISA's eCSIRT.net incident taxonomy, created by the Reference Security Incident Taxonomy Working Group (RSIT WG) with the aim of enabling the CSIRT community to reach a consensus on security incident references. The eCSIRT.net taxonomy is adopted by all CIs in Cyprus which, in line with MoUs agreed with the DSA, can notify CSIRT-CY of incidents through more than one channel: hotlines, email, or *via* a portal. Reported incidents are investigated by CSIRT-CY, in discussion with constituents. There are clear procedures for handling incidents, which are divided into three categories that classify severity and risk. Response times and escalation processes are defined for every category and reports are available once incidents have been addressed. Participants identified the critical role of CSIRT-CY in maintaining a national database of incidents and capturing lessons learnt from reporting incidents, which inform strategic and policy decisions. They further recommended that escalation processes should be extended to include plans at a ministerial/political level, and it was suggested that the EU's Cyber Crises Liaison Organisation Network (CyCLONe)[25] should be emulated.

Apart from handling incident management for the CIs in critical cases, CSIRT-CY acts as a cyber-threat intelligence (CTI) hub, provides malware analysis and forensics services, as well as vulnerability analysis of CI systems through penetration testing services. A distribution of threat notifications and advice for prevention is sent daily to all CI operators through automated emails. Participants deemed that notifying CIs daily with cyber-threat intelligence has significantly contributed to the prevention of attacks. CIs are increasingly aware of the importance of acting rapidly when the intelligence is received. Mandating CIs to perform the recommended actions to further encourage this practice, while necessarily reporting the successful implementation of the prevention guidelines to CSIRT-CY, is advised. Given the key role of the DSA and CSIRT-CY in Cyprus's cybersecurity developments, it is important to ensure that the steering committee has a mean of independently evaluating their operational effectiveness – this will help inform strategic decisions around resourcing and capability development.

[21] https://www.axelos.com/certifications/itil-service-management

[22] https://opencsirt.org/csirt-maturity/sim3-and-references/

[23] https://www.first.org/members/teams/csirt-cy

[24] (https://csirtsnetwork.eu/)

[25] https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

Although Cyprus has made significant progress with structural reforms in the area of incident handling and reporting, monitoring and detection practices are lagging behind. CSIRT-CY has developed sensors in collaboration with academia, which are applied to critical government networks to bridge this gap. However, the development of a governmental Security Operational Centre (SOC), operational 24/7, is highly recommended. It is further recommended that the government SOC covers the Parliament network. More details about the public sector's current status are provided in *Dimension* 5.

The government SOC should be complemented with raising awareness amongst CIs about the importance of following best practice in the detection of incidents. Participants mentioned that a small number of CIs lack knowledge and expertise in monitoring and detection practices. A possible solution could be to create sectorial SOCs or Computer Emergency Response Teams (CERTs) to supervise CIs, especially those which remain oblivious to monitoring and detection best practices. Furthermore, sectorial CERTs may offer cyber threat intelligence services to non-CIs and SMEs which currently do not benefit from these services. At the moment, there are two sectorial CERTs in operation: the academic CERT[26] and the military CERT. The former is a Full Member of FIRST, a Trusted Introducer (TI) Accreditation Candidate, and a provider of incident response and cybersecurity services to universities, research institutes and educational networks that are members of the Cyprus Research & Academic Network (CYNET). The latter is fully implemented and on the verge of becoming operational. The military SOC has already formed bilateral agreements for the exchange of cyber threat intelligence specific for military systems, and it develops training courses for SOC analysts. More details on the current status in the private sector are provided in *Dimension* 5.

It is common practice for organisations that have immature detection and monitoring processes to be uninvolved in incident-sharing practices. Despite the fairly poor monitoring and detection practices observed in the government networks and in a handful of CIs, participants acknowledged that CSIRT-CY has fostered trust with all critical stakeholders. This resulted in the rise in incident reports over the last four years, which should be considered as a positive sign. This rise indicates that CIs are becoming capable of detecting attacks and have confidence that CSIRT-CY can handle these when necessary, or will inform all the constituents with intelligence. Incident-sharing practices will be further improved with platforms, equivalent to the MISP project, an open-source threat-intelligence platform[27] that will automatically report incidents, analyse intelligence and provide early warnings. The development of such a project is was concluded recently by CSIRT-CY, in co-operation with academia, and its successful implementation was said to be of paramount importance.

Cybersecurity is fully integrated into the national crisis management process. Hybrid threats inform national security strategy and exercises. Participants mentioned that a national catastrophe exercise was once interrupted by a real cyber attack resulted in a hybrid type of exercise that will be enacted periodically. There are national crisis plans in place that may be triggered by cybersecurity incidents, as well as dedicated facilities to ensure the continuation of cybersecurity services in times of crisis. A decisive step in deciding how to respond to crisis situations is the development of a national cyber-range platform, which will be delivered by the DSA, in conjunction with academia, in the near future; participants mentioned that a

[26] https://cynet.ac.cy/csirt/

[27] https://www.misp-project.org/

prototype has already been demonstrated. Such a platform will be able to host national-level exercises from 2022, as well as regional ones. It is worth mentioning that Cyprus has extensive experience in exercises as the DSA and CSIRT-CY actively participate in international exercises, especially those organised at an EU level by ENISA (i.e., Cyber Europe). Such exercises include assessing the strategic, operational and technical levels, and may involve the military.

D1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This Factor *studies the Government's capacity to identify CI assets, the regulatory requirements specific to the cybersecurity of CI, and the implementation of good cybersecurity practice by CI operators.*

***Stage*: Established**

Since the 2017 CMM review, significant regulatory and structural reforms have enabled Cyprus to improve the protection of CIs and to lay the ground to streamline further enhancements. The establishment of the national risk assessment provides an up-to-date and frequently reviewed inventory of all critical infrastructure stakeholders, who have acknowledged their role with legal decisions sent by the DSA, as the 89(i)/2020 Law dictates. The risk assessment has further identified dependencies between various CI services across all relevant sectors.

The activity of CSIRT-CY has institutionalised the practice of incident disclosure for all CIs, ensuring compliance to the NIS Directive. The current incident notification legislation and processes for CIs to report cybersecurity incidents to the DSA ensures that this practice is formalised. The proposed creation of sectorial CERTs, which will provide specialised intelligence pertinent to a specific sector, will streamline sharing of information within sectors. Because sectorial CERTs have the ability to send information pertinent to systems commonly used in this sector, this practice will contribute to a deeper understanding of root causes of incidents per sector, enable better incident response and a faster return to normal operations.

Furthermore, the DSA, through Law 89(I)/2020 on Network and Information Systems Security,[28] has legislated a list of security requirements that apply horizontally to all CIs. The Decision 389/2020 "DSA Security Measures Framework for adoption of cybersecurity standards[29]" provides a national framework that mandates the implementation of a series of controls, encapsulating those in ISO 27001 and National Institute for Standards and Technology (NIST) 800-53, and controls documented by the NIS Co-operation Group. This framework should have the potential to ensure that key service operators will undertake all appropriate measures to prevent and mitigate the impact of cyber attacks on systems that provide essential services.

[28] https://dsa.cy/wp-content/uploads/DSA-Law-89-I-2020.pdf
[29] https://dsa.cy/wp-content/uploads/dsa__security_measures_framework_v1.0_consultation.pdf

Participants mentioned that as Cyprus is a small country, a centralised approach with respect to the NIS 2 Directive (NISD2) is optimal. Therefore, the DSA already supervise all sectors, including telecommunications, and will be responsible for identifying possible new CIs following new provisions in NISD2. Given the different security requirements for each sector, vertical security measures will complement the horizontal security controls and working groups with specialised knowledge of each sector will be formed. For example, members specialised in supervisory control and data acquisition (SCADA) systems will be responsible for setting up requirements for energy, water or healthcare but for the energy sector in particular, where new systems will be adopted to respond to the energy market needs, an assessment of security controls is pertinent. Another example of vertical measures is the telecommunications sector, where legislation specialising in 5G security has already been published to respond to the threat landscape of this emerging technology.

To ensure compliance with the newly regulated framework, a novel audit framework, requiring dedicated personnel for each sector, is being currently developed. So far, only the telecommunications sector has been audited at regular intervals but first audits of the other CI sectors will be conducted in late 2021. Participants recommended that these should assess compliance with security controls without exercising fines as prescribed in law under certain cases, their reasoning being that if a strict assessment with heavy fines is chosen, certain CIs may become reluctant to co-operate or share incidents in the future.

The framework provided by the DSA obliges CIs to conduct regular risk assessments. Risk management practice is an area that remains problematic in Cyprus as risk assessment exercises, with emphasis on cybersecurity aspects, have not necessarily been conducted by every CI in the past. However, CIs are now mandated by law to perform such assessments. Participants mentioned that the situation may drastically improve as, late in 2021, certain CI organisations will submit their risk assessments for the first time, formally verifying compliance with the DSA's framework through audits. To facilitate the reporting process for CIs, a stakeholder-management platform has been developed for centralised cyber-risk management and monitoring at the national level. CIs and operators of essential services will be able to submit documents relating to their compliance with the relevant security-measures legislation, and submit incident notifications, electronically, and a new risk-aggregation methodology across CI sectors has been developed as part of this platform. The methodology can combine cyber risks at the sectoral or national level, to give an understanding of national-level cyber risk based on the status risks of the CIs. This is expected to be tested through selective use early in 2022, and to be used fully for national-level risk aggregation thereafter.

D1.4 CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

This Factor *explores whether the Government has the capacity to design and implement a strategy for cybersecurity within national security and defence. It also reviews the level of cybersecurity capability within the national security and defence establishment, and the collaboration arrangements on cybersecurity between civil and defence entities.*

***Stage*: Established**

Cyprus has adopted a national strategy for security and defence which is informed by cybersecurity elements and hybrid threats. Participants mentioned that rules of engagement described in the strategy abide with international humanitarian law. Civil defence co-ordination and co-operation is formally described in the strategy and has been implemented by specific MoUs signed by the Ministry of Defence and the DSA. The reviewers were unable to review the strategy as it is a confidential document but it may be beneficial to consider an in-depth review of the cyber elements in it, to ensure these are sufficient. A competent party (an ally) could review the strategy, to ascertain whether adequate resources are available and verify that the necessary capabilities are identified.

National Guard has recently developed a fully operational CERT, which has already established bilateral agreements for the exchange of information, and particularly for intelligence on threats that target military organisations. It has also conducted exercises dedicated to cybersecurity and has invited DSA, Governmental organizations and the private sector to actively participate. Moreover, the military CERT participates in several tactical cybersecurity exercises that are organised at a European level. The training next year will be facilitated by the national cyber range platform, which will be launched soon and which will also be available to military personnel. High-level cybersecurity training is provided to military personnel in general, to increase cybersecurity awareness focusing on the modern cyber threat landscape.

In the 2017 CMM review, participants agreed that formal collaboration between the military and the national CSIRT would be imperative. They further deemed that good co-operation would result in effective analysis of incidents and in timely threat intelligence-sharing. During the 2021 focus groups, it was evident that CSIRT-CY and the military CERT collaborate closely and effectively. An MoU describes the processes that enable this effective collaboration, and plans are in place for times of crisis. On an operational level, there is dedicated infrastructure in place for co-operation during national incidents, specifically that each side shares access with the other side.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Cyprus. These recommendations provide advice and steps aimed at increasing existing cybersecurity capacity in line with the considerations of the GCSCC's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each *Factor*.

NATIONAL CYBERSECURITY STRATEGY

R1.1.1 Ensure review and renewal processes for the next NCS in 2024 are formally in place. These processes should describe how to identify lessons learnt from the current implementation of the strategy;

R1.1.2 ensure that metrics and KPIs, which have generally been developed to track progress on individual projects and actions within the implementation programme, can provide an holistic view of whether the overall strategic outcomes of the NCS have been achieved. If necessary, complement project-level

KPIs and metrics with programme-level ones to enable the steering committee to determine if the cumulative effect of the various implementation projects is sufficient to meet Cyprus's overall needs. Furthermore, ensure that these metrics are used to refine action plans of the NCS;

R1.1.3 it is imperative that the framework designed by the DSA is implemented in full. Ensure that the various change programmes underway (e.g., in the energy sector) identify the importance of cybersecurity and are subject to risk assessments. Given the emerging 5G technology in the telecommunications sector, identify the risk of these technologies and the impact of a cyber attack within critical infrastructure and the wider economy;

R1.1.4 ensure that the appropriate budget is available for the implementation of the NCS, and that the Government is manned with the necessary human resources;

R1.1.5 continue pioneering work in cybersecurity certification schemes and assist other countries in building capacity in this area;

R1.1.6 conduct risk assessment exercises in all CIs and ensure that the results can be incorporated into the national risk assessment;

R1.1.7 develop tools to automatically obtain information from the CIs' risk assessments and to better monitor vulnerabilities and impact at a national level; and

R1.1.8 continue to involve a wide range of stakeholders in the implementation of the actions described in NCS.

INCIDENT RESPONSE AND CRISIS MANAGEMENT

R1.2.1 Create a federated SOC for government that will be operational 24/7 and will cover the Parliament's network. Ensure that the Government is brought up to standard with resources, and that the requirements indicated in D5 are met;

R1.2.2 consider the design of sectorial CERTs, especially for the sectors that are critical, based on the national risk assessment, and promote SOC services to those CIs that do not currently possess an in-house SOC nor employ such services. Ensure that the detection processes of CIs follow best practice;

R1.2.3 ensure the planned hiring process in CSIRT-CY will be successfully concluded, and offer training to CSIRT-CY as often as possible;

R.1.2.4 create cyber threat intelligence associations for each sector, and across sectors, and motivate non-CIs and SMEs to participate actively in sharing incidents. If necessary, CSIRT-CY should consider ways of protecting the wider Cypriot economy by extending access to cyber threat intelligence beyond CI and into non-CI and SME sectors;

R1.2.5 routinely analyse insights from national level incidents to establish lessons learnt and inform broader cybersecurity policy and strategy;

R1.2.6 create an evaluation framework to ensure the steering committee has a means of independently evaluating the operational effectiveness of DSA and CSIRT-CY; and

R1.2.7 create scenarios and exercises specifically for cybersecurity and run these frequently in the newly developed cyber range platform. Lessons learnt from these exercises could inform national crisis management policy and the NCS's implementation plan.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.3.1 Ensure that the list of CI assets can adapt to shifts in the technical and the socio-economic environment;

R1.3.2 consider adding the Parliament to the list of CI assets;

R1.3.3 ensure the DSA's horizontal security requirements are implemented by all CIs. It is imperative to start auditing CIs for compliance with these requirements. Develop vertical security requirements for sectors where emerging technologies are introduced, or for sectors that have poor cybersecurity posture;

R1.3.4 create platforms so that incidents can be shared *inter* and *intra* sectors automatically (such as MISP), and also a platform to share risk assessment results from Cis;

R1.3.5 Regarding audits, the DSA needs to ensure that CIs will be compliant with best practice in detection and monitoring processes, either by utilising SOC services (in-house or outsourced) or by other means;

R1.3.5 organise cybersecurity exercises where CIs will actively partake, and establish these periodically; and

R1.3.6 develop a platform to analyse incidents and automatically provide early warnings to all CIs.

CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

R1.4.1 Consider a more in-depth review of the cyber elements of the defence strategy, to ensure it is sufficient. It may be valuable to have it reviewed by a competent party who can test its validity and verify that adequate resources are available;

R1.4.2 engage defence in cyber-range exercises and continue the training on scenarios that involve hybrid threats; and

R1.4.3 regularly test the national plans that involve cyber-incidents and update as necessary.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

This *Dimension* reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this *Dimension* explores the existence of reporting mechanisms that function as channels for users to report cybercrime. In addition, this *Dimension* reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.

Figure 7: Factors and aspects examined in Dimension 2.

D2.1 CYBERSECURITY MINDSET

This Factor *evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large. A cybersecurity mindset consists of values, attitudes and practices – including habits of individual users, experts, and other actors – in the cybersecurity ecosystem that increase the capacity of users to protect themselves online.*

***Stage*: Formative**

Participants felt that cybersecurity awareness and prioritisation of cybersecurity in the government departments was not uniformly prominent. The government stakeholders present in focus group sessions expressed the view that employees in government departments generally do not follow best practices in cybersecurity because of a lack of education and awareness, a perception that following these practices may conflict with the need to deliver, and due to a lack of oversight that ensures best practice.

A gradual improvement in government cybersecurity mindset was described, nonetheless. Some increased awareness of the risks of phishing, for example, is being driven by information on incidents distributed by the DSA to raise awareness, and by informative emails about phishing sent out by the Department of Informatics Services (DITS). Some departments are more mature in terms of priority and awareness of cybersecurity than others: some described compliance with security standards such as ISO 27001, and of having carried out phishing exercises, for example.

DITS is responsible for the IT of government departments; however, it is not sufficiently resourced to handle cybersecurity and only offers some services, such as *ad-hoc* distribution of information. The government departments (some of which do not have IT personnel) are largely left to implement cybersecurity measures and practices with very limited support or guidance, particularly when it comes to tailoring cybersecurity requirements and measures to match their context, and requirements are not currently enforced. DITS recommends (but does not oversee or have the power to enforce) policies such as regular password changes for employees of government departments, and some government departments described their enforcement of such policies.

There is an ongoing effort to set up a cybersecurity directorate within government and a recruitment process for a government Chief Information Security Officer (CISO) took place earlier this year. This first recruitment attempt was unsuccessful, but there is confidence that the role will be filled in the near-future, that a government security team will follow, and that the structures planned should help improve the government's cybersecurity mindset and adherence to best practices in cybersecurity. Furthermore, the government departments, like the rest of the CI, will be obliged to start working towards compliance with the DSA's CI cybersecurity regulation under the NIS Directive in the near future (with cybersecurity risk assessments due in late 2021). This should also elevate cybersecurity best practices, mindset and deployment of controls within government.

It was noted that education and awareness are hugely important, since an approach that relied solely on the enforcement of new policies (i.e., a compliance-focused approach) could lead to government employees following insecure practices to circumvent security measures they perceive to be inconvenient. An example was given of perceived inconveniences already caused by policies involving access to certain websites *via* the Government's local area network (LAN).

The fact that cybersecurity is intended to have a central role in government is a positive step; however, difficulties with recruitment indicate the lack of resources and skills that participants mentioned in the focus groups. The public sector in particular was reported to be experiencing challenges around attracting personnel with cybersecurity skills, as they often opt to work in the private sector, where there are more competitive salaries.

Based on the focus group discussions, there appear to be two main reasons for the current, relatively weak cybersecurity mindset and practice in government departments. First, some participants felt that the organisation of DITS is not efficient. For example, it was stated that the department currently has around 200 personnel but only a small proportion of these are in the central IT team that runs the central services; the others provide support to individual departments.

Second, it was stated that there is a lack of resources and funding to support the implementation of a secure digital environment in government, and for running the training and awareness schemes necessary to achieve the necessary cybersecurity mindset. There is a need to find a way to increase the level of cybersecurity resourcing for the public sector, including the DSA. It was highlighted that the issue stems from the prioritisation of the national budget by the Ministry of Finance: while participants, including the DSA, felt that parliament generally understands the importance of cybersecurity and approves cybersecurity legislation put to it, some of the necessary changes are blocked earlier in the budget-approval stage. It is therefore important to seek to improve the way in which cybersecurity requirements are presented to those deciding the national budget, and to specifically seek to improve the cybersecurity awareness and mindset of the relevant departments, and the Ministry of Finance in particular.

Participants in the focus groups felt that the private sector generally has a stronger cybersecurity mindset than the public sector, particularly when it comes to private CI and large organisations. The also felt that improvements over the last five years are evidenced by the results of penetration tests. Larger organisations in regulated sectors such as banking and electronic communications were perceived to have a high level of cybersecurity maturity with associated strong cybersecurity mindset within the organisation. It was reported that some organisations (telecommunications service providers, for example), cover cybersecurity best practices in their induction training for new employees.

As in the case of public-sector CI, the private-sector CI are required to comply with the DSA's CI regulation, which includes a requirement to have a CISO, which should further improve practice and mindsets. It was noted by participants that a ground-up approach is also needed, so that company leaders are aware of the need rather than just being forced to comply with legislation. It is therefore important that continued focus is placed on awareness-raising for company leadership. It is important that focus is placed on improving cybersecurity mindsets across businesses, not just the CIs covered by the DSA's regulation. This need is reflected in Thematic Unit 9 of the NCS (Creation of Security Culture).

The cybersecurity mindset (and cybersecurity maturity in general) is not as strong in SMEs, as is broadly the case worldwide. There is a feeling that this is improving to some extent, with a new, more cybersecurity-aware generation of leaders starting to join the market. Some SMEs were reported to be running annual cybersecurity awareness training for their employees, and participants noted that, ten years ago, only large organisations in the banking and telecommunications sector would request penetration tests. Today, penetration tests are conducted more widely, including some SMEs.

It was noted that many of the SMEs in Cyprus are very small – ten to fifteen staff, making resourcing for cybersecurity an issue – and they are falling victim to distributed denial-of-service (DDoS) and ransomware attacks; they need support to implement cybersecurity best practices and controls to mitigate these risks. There was some discussion about whether a relatively basic security guideline or standard for SMEs, one that they could certify against (like the UK Cyber Essentials, as one example), might be beneficial.

It was noted that the evolving threat landscape has been driving improvements to the awareness of risks and the implementation of cybersecurity practices across all types of organisations. The ransomware threat to organisations, including SMEs, was cited as having pushed organisations to prioritise cybersecurity more due to the fear of, or experience of, being compromised, rather than seeing cybersecurity as an unnecessary cost.

In order to improve cybersecurity mindsets across organisations in the private sector, there is a need for focused efforts (awareness-raising) to make company leaders aware of the need for cybersecurity professionals. Plans were cited in different sessions for cybersecurity professionals and also owners of businesses in various market areas to raise awareness around cybersecurity risks that companies might be facing now, and in the near future. It was suggested that a relative lack of awareness of the need to have a cybersecurity mindset and to hire cybersecurity experts in business stems from a relatively low level of digital literacy. It was also noted that starting to educate people about the importance of cybersecurity from an early school age is important in order to ensure the right mindset is fostered; the strong cybersecurity awareness-raising efforts at school level are therefore well-placed to affect positive change.

The perception was expressed during multiple focus groups that the mindset of Cypriot businesses is to some extent influenced by broader Cypriot culture. In particular, Cyprus is a relatively small island that is home to a relatively small community of organisations, many of which know each other. Companies may be reluctant to perform audits or attempts to certify, due to the impossibility of doing so “anonymously”: there is a mentality of not wanting to be exposed to the closely-linked network of other businesses.

The DSA has recently run a survey gathering information from businesses on factors including their perceptions of cybersecurity and needs for training, as well as questions to help evaluate their cybersecurity-awareness levels and the cybersecurity controls in place. A report is being produced and results will inform actions taken by the DSA which aim to elevate the levels of cybersecurity in businesses.

In terms of the cybersecurity mindset of the general public, participants in the focus groups felt that there are stark differences between generations, with senior citizens being less

aware, while younger people generally have a better level of awareness (which, of course, reflects the situation worldwide). It was noted that the awareness of younger citizens has been improved particularly by the efforts of the Ministry of Education, which has targeted schools with significant cybersecurity awareness-raising initiatives. However, few if any direct surveys of the public exist to document these impressions.

D2.2 TRUST AND CONFIDENCE IN ONLINE SERVICES

This Factor *reviews critical skills, the management of disinformation, the level of users' trust and confidence in the use of online services in general, and of e-government and e-commerce services in particular.*

***Stage*: Formative**

Similar to the presence of a cybersecurity mindset, Internet users' digital literacy and skills differ starkly between generations, with the younger generation being more competent and confident online. This is in part a result of a continuous focus on educating children about digital literacy and cybersecurity, with the initiatives rooted in the "National Strategy for a Better Internet for Children in Cyprus" in particular.[30]

The European Commission's DESI 2020 states that almost an eighth of Cypriots have never used the Internet, and around half of Cypriots lack basic digital skills.[31] Correspondingly, only a limited proportion of Internet users are able to critically assess what they see or receive online and identify possible risks, or are able to protect themselves from misinformation online. The effort being put into programmes that will ensure children have a high level of digital literacy and understanding of cybersecurity is extremely positive. Embedding these skills at a young age is of course important, but older generations may require more attention than is presently provided when it comes to digital literacy and a basic awareness of online risks.

According to DESI, the number of Cypriot respondents using online services is below the EU average. However, DESI does report a steady increase over the last few years in the use of online services, including banking and shopping. Participants verified that online services are becoming more popular, particularly as a result of the restrictions in place during the COVID-19 pandemic, which acted as a digital accelerator. Legislation is in place regarding identification and trust for electronic transactions, including the use of digital signatures in government services and applications: Law 55(I)/2018, on the Implementation of Regulation (EU) No. 910/2014, on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. Law 60(I)/2021) is the 2021 amendment to this law.

[30] https://www.esafecyprus.ac.cy/ethniki-stratigiki

[31] https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020

Disinformation (such as inciting public mistrust) is dealt with as an offence under the criminal code and as such, it is a matter for the Cybercrime Unit of the police. There have, reportedly, been incidents of disinformation in Cyprus and some *ad-hoc* awareness initiatives about disinformation have been put in place. For example, public advisories from the DSA have warned about fake websites relating to the COVID-19 pandemic. Participants in the focus groups felt that a limited number of, but not most, citizens have the capacity to identify disinformation and fake news, and that more structured initiatives to raise public awareness about how to identify disinformation would be beneficial.

A few e-government services are available *via* the recently created Ariadni Government e-services portal for individuals and organisations.[32] The portal requires user authentication, with some physical authentication to create an account. Participants expressed the view that users use the services that are available; the tax process can only be carried out online, for example. This suggests that users have a reasonable level of trust in e-government services. In cases where a breach of government services affects the security or privacy of personal data or credentials, under the terms of GDPR, there would be an obligation to inform users; it was noted that incidents have not, so far, affected the public.

There are also a few e-commerce services, and they are growing steadily. The International Trade Administration reported that in 2021, web-based trade in Cyprus was relatively small but growing, with most companies having websites and a social media presence.[33] The report notes that while previously, individuals and companies were more sceptical about using e-commerce services, the COVID-19 pandemic has accelerated the use of such services for online food deliveries and clothing purchases, for example, as well as online financial transactions. Foreign e-commerce sites such as Amazon, eBay and Alibaba are in widespread use. This CMM review was not made aware of surveys or metrics to assess users' trust and confidence online, or of their trust in e-government or e-commerce services.

D2.3 USER UNDERSTANDING OF PERSONAL INFORMATION

This Factor *looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protecting personal information online, and whether they are sensitive of their privacy rights.*

***Stage*: Formative**

Helpline statistics show that the public has some awareness of the need to protect personal information online and that citizens attempt to do so: for example, eight percent of the calls made by the public to the CYberSafety Helpline in the first quarter of 2021 concerned the protection of personal data.[34]

[32] https://eservices.cyprus.gov.cy/EN/Pages/Home.aspx
[33] https://www.trade.gov/country-commercial-guides/cyprus-ecommerce
[34] https://cyprus-mail.com/2021/04/30/over-half-of-calls-to-cyber-safety-helpline-were-about-covid/

Participants felt that the risks around, and the need to protect, personal information online tend to be included in awareness-raising campaigns and materials, and this had led to citizens of Cyprus gradually becoming more aware of how to protect their online personal information, and be more careful with the content they post on social media. It was noted there are still plenty of cases of people posting sensitive or problematic content on social media, such as photographs of their children. It was suggested that awareness-raising initiatives should focus more on educating Internet users about the tools available to protect their personal information, and how to use them, rather than focusing on advising users to avoid social media and posting online.

As an EU Member State, Cyprus has implemented GDPR and participants noted that over the last few years, it has been a driver in improving cybersecurity mindsets (particularly around data privacy and protection) and practices across organisations. The Regulations are supplemented by local data protection law to further regulate certain issues. Data protection officers for the public and private sectors have had GDPR training and audits are performed to assess the level of compliance. There was some concern that this could be creating a compliance-driven culture and as an alternative, many expressed a preference for data protection to be rooted in a clear understanding across organisations of the need to prioritise the protection of personal data.

D2.4 REPORTING MECHANISMS

This Factor *explores the existence of reporting mechanisms that function as channels for users to report Internet-related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.*

***Stage*: Established**

A number of platforms exist for reporting cyber harms and concerns. Participants expressed a view that the reporting mechanisms in place cover most of the incident-reporting requirements of the population of Cyprus.

In January 2014, the Cyprus Police implemented its Cybercrime Reporting Platform, CyberAlert.cy,[35, 36] and the Cyprus Police Mobile Application,[37] both of which enable the public and organisations to report cybercrime online. These channels are promoted *via* social media. Police representatives stated that around 1,200 reports are received per year *via* these platforms; most involve computer-related fraud, child sexual exploitation, and attacks on information systems.

The CYberSafety Helpline[38] is run as part of the CYberSafety campaign and is aimed at children, adolescents, and their families, providing support on issues related to the safe, responsible

[35] https://cyberalert.cy/
[36] https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm
[37] http://mobile.cypruspolicenews.com/landing/Desktop#/VbclTfmm2jw
[38] https://www.cybersafety.cy/helpline-en

and ethical use of the Internet. The CYberSafety campaign also runs a hotline[39] for Internet users in Cyprus to report illegal online content or actions (including on websites, chat rooms, social media, and *via* mobile and email communication), such as illegal child sexual abuse material, hacking, cyber fraud, and hate speech.

Trained operators run the hotline and make a preliminary assessment of the legal nature of the content before forwarding to the relevant body for action. This includes informing the host provider of content assessed as child pornography and monitoring its take-down. Incidents can be reported to both the helpline and the hotline by telephone, by email, *via* an online form or by Internet chat. The helpline and hotline cases are managed using a software platform called Case Management Platform and Tools, which records essential data, administers cases as appropriate, monitors the status of cases, and reports on data analytics. Both co-operate closely with the Cybercrime Unit of the Cyprus Police, forwarding incidents as necessary. The hotline co-operates with a network of other hotlines and connects to the relevant EU platforms.

Reportedly, the CYberSafety Helpline receives reports about concerns that focus primarily around extortion, cyber-bullying, and data privacy. It was reported that in the first quarter of 2021, the helpline received calls from 683 individuals (but half of these were about COVID-19 and not cybersecurity), and that there was an increase in complaints of sexual harassment online.[40] In that quarter, a majority (61.46 percent) of cybersecurity-related calls were from girls or women and were mainly (93.75 percent) from adults. Electronic crimes such as hacking and electronic fraud were the subject of the largest proportion of calls (27.4 percent), followed by calls concerning cyber-bullying, which had increased in proportion since the previous year.

There appears to be less clarity about how government departments should report incidents: some cited a lack of understanding about how to report events such as phishing emails. The organisation of cybersecurity-reporting mechanisms within government may require improvement or clarification. It was noted that there are measures in place (a reporting email address) but not all relevant parties are aware of it.

The view was expressed that some organisations may still be reluctant to report cybersecurity incidents for fear of reputational harm; particularly given the closeness of the network of organisations in a relatively small country which, it is perceived, makes it difficult to remain anonymous. An example of a ransomware incident that was not reported a few years ago was cited. Participants noted that reporting is essential for increasing awareness of the current risk landscape in the country, and encouraging parties at all levels to prioritise cybersecurity, and find ways to remove any barriers to reporting, is important.

[39] https://www.cybersafety.cy/hotline-en

[40] https://cyprus-mail.com/2021/04/30/over-half-of-calls-to-cyber-safety-helpline-were-about-covid/

D2.5 MEDIA AND ONLINE PLATFORMS

This Factor *explores whether cybersecurity is a common subject of discussion across mainstream media, and an issue for broad discussion on social media. Moreover, this* Factor *looks at the role of media in conveying information about cybersecurity to the public, thus shaping citizens' cybersecurity values, attitudes and online behaviour.*

***Stage*: Formative**

Generally, there was a view that the representation of cybersecurity issues in the media and on online platforms has been becoming more regular, and the public is being kept better informed about cybersecurity incidents than was the case a few years ago. This is largely due to the efforts of the DSA and the Cybercrime Unit of the Cyprus Police, both of which issue regular announcements *via* social media. Their announcements include reports of cybersecurity incidents and risks, and also guidance and tips in line with relevant incidents and awareness-raising needs. These were regarded favourably by participants, who felt they make a positive contribution to the cybersecurity culture of Cyprus and lead to public discussion of cybersecurity issues.

Some cybersecurity information is disseminated *ad hoc via* mainstream media: participants stated that cybersecurity incidents and data breaches tend to be covered on television and radio news channels, and in print and online newspaper articles. The perception was expressed that the mainstream media lacks sufficient specialist cybersecurity knowledge to report completely and effectively on the subject (for example, to take the opportunity to educate the public about actionable cybersecurity measures they could take to protect themselves against possible similar incidents in the future), or to create continuous media campaigns that contribute to raising awareness about cybersecurity.

At present, it is unclear to what extent whistleblowers would be accepted as playing a positive role. There is, however, legislation is in development to protect them. At the time this report was written, a draft law for the protection of whistleblowers had been submitted to parliament, where it was under discussion.

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *Cybersecurity Culture and Society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity in line with the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MINDSET

R2.1.1 Seek to increase the level of awareness of cybersecurity risks and the prioritisation of cybersecurity across all government agencies and private-sector firms, through awareness-raising and training;

R2.1.2 seek to increase the number of Internet users within society that have an awareness of cybersecurity risks, and prioritise cybersecurity, with a particular focus on groups that may not yet have received as much attention as others (noting that substantial efforts are already being made around awareness-raising for children);

R2.1.3 implement and publish the results of surveys that evaluate knowledge of cybersecurity within the nation;

R2.1.4 enhance focused awareness-raising efforts to raise the cybersecurity mindset of leaders in the public and private sectors. In particular, these initiatives should raise awareness of the need for safe cybersecurity practices within government departments and businesses, and of the need to employ cybersecurity professionals. These efforts should extend to those responsible for making resourcing decisions at a national level, to ensure that sufficient priority is given to cybersecurity; and

R2.1.5 consider developing a basic cybersecurity framework or standard for SMEs (the UK's Cyber Essentials is an example).

TRUST AND CONFIDENCE IN ONLINE SERVICES

R2.2.1 Develop programmes to raise the level of digital literacy in Cyprus, including improving the ability of citizens to protect themselves against misinformation online and to critically assess what they see and receive online;

R2.2.2 ensure that programmes developed to support digital and media literacy skills cover all necessary demographics within the population. There may be a need to focus particularly on groups that have not yet received as much attention as others;

R2.2.3 continue to expand the range of secure e-government services;

R2.2.4 public authorities should routinely publish information on privacy and security initiatives in e-government services, as well as publishing their policy on breach disclosure, to increase the trust of users in these services;

R2.2.5 continue to expand the range of secure e-commerce services, ensuring that they use up-to-date security solutions, and that certification schemes and trust marks for these services are in place; and

R2.2.6 implement and publish the results of surveys and metrics to evaluate users' trust and confidence online, in e-government services, and in e-commerce services.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.3.1 Seek to further improve the population of Cyprus's understanding of how to protect personal information online. This might involve awareness-raising initiatives that focus on educating Internet users about how to use the tools available to protect their personal information; and

R2.3.2 seek to ensure, through awareness-raising efforts, that businesses have a strong understanding of the importance of protecting personal information online, and to ensure that their actions have a strong basis in understanding and are not rooted solely in compliance with GDPR and associated regulations.

REPORTING MECHANISMS

R2.4.1 Enhance promotion of reporting mechanisms within the public and private sectors and for the general population, to ensure all parties are aware of how to report cybersecurity incidents. In particular, the organisation and promotion of cybersecurity-reporting mechanisms for government may require improvement;

R2.4.2 develop processes for routinely feeding back metrics from reporting mechanisms, to inform the revision and promotion of cybersecurity policies and the NCS; and

R2.4.3 ensure ISPs collaborate with organisations that control reporting mechanisms so that phishing and fraudulent websites can be blocked instantly.

MEDIA AND ONLINE PLATFORMS

R2.5.1 Encourage providers of mainstream media to extend their coverage of threats and incidents, and to use the opportunity to inform the public about proactive and actionable cybersecurity measures, as well as economic and social impacts;

R2.5.2 consider running cybersecurity awareness-training initiatives for media providers, to create cybersecurity expertise within the media that enables more effective and informed reporting; and

R2.5.3 continue to run and enhance the cybersecurity-awareness campaigns on social media. As part of these campaigns, seek to foster broad discussion on social media about cybersecurity, and encourage individuals to use social media to share online experiences.

DIMENSION 3
BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

This *Dimensio*n reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the Government, the private sector and the population as a whole, and relates to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes.

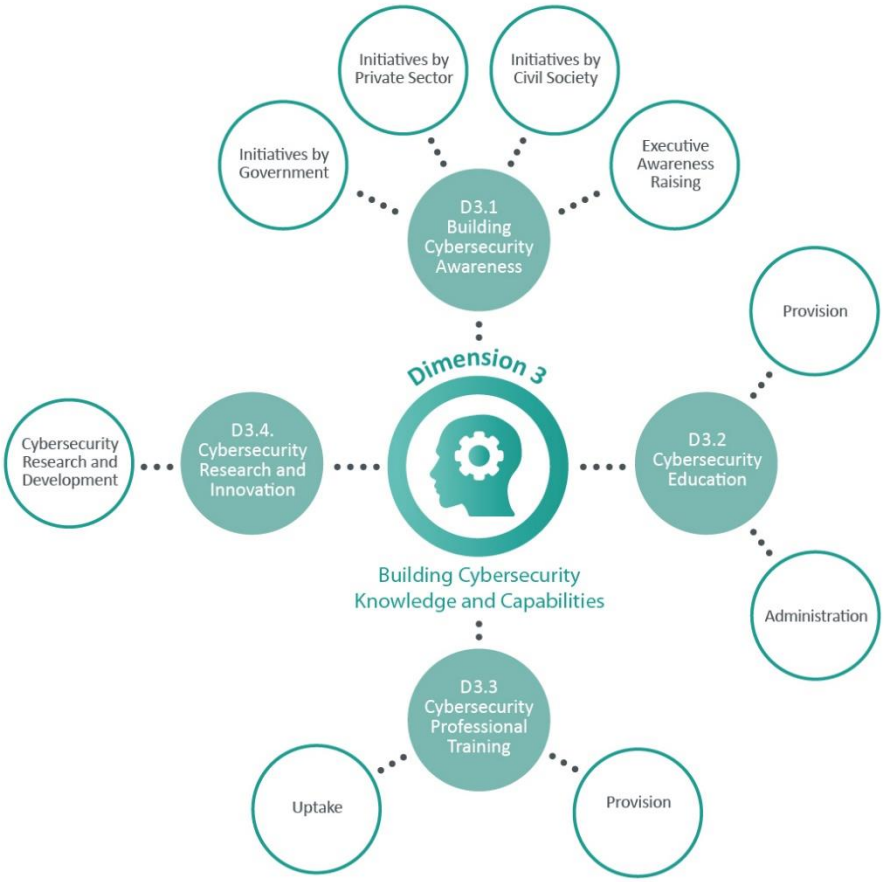

Figure 8: Factors and aspects examined in Dimension 3.

D3.1 BUILDING CYBERSECURITY AWARENESS

This Factor *focuses on the availability of programmes that raise cybersecurity awareness throughout the country, concentrating on cybersecurity risks and threats, and ways in which to address them.*

***Stage*: Formative to Established**

A national programme for raising cybersecurity awareness that covers all users of electronic systems does not yet exist, although significant and co-ordinated awareness-raising efforts are ongoing for specific target demographics (particularly children, teachers and parents). The Government recognises the need to expand the existing awareness-raising provision to create a co-ordinated programme and this is reflected in Thematic Unit 9 of the NCS ("Creation of Security Culture").

For children, teachers and parents, Cyprus has very strong awareness-raising efforts involving the collaboration of the public and private sectors, and civil society. On behalf of the Ministry of Education and Culture, the Cyprus Pedagogical Institute co-ordinates and oversees awareness-raising initiatives for this demographic at the national level. There is a published strategy – the "National Strategy for a Better Internet for Children in Cyprus"– which is concerned with raising the cybersecurity awareness of students, teachers and parents and encourages them to develop a culture of safe use of the Internet.[41] This is in alignment with the Actions of the NCS.

The Cyprus Safer Internet Centre (SIC) – CYberSafety has been in operation since 2018, as part of the EU's Better Internet for Kids project,[42] with closely related activities under CyberEthics projects having been run since at least 2006. The Cyprus SIC comprises eight partners, including the Cyprus Pedagogical Institute, the Ministry of Education, Culture, Sports and Youth, the DSA (and CSIRT-CY), universities (University of Cyprus and Cyprus University of Technology), civil society (the Pancyprian School for Parents and the Cyprus Neuroscience and Technology Institute), and telecommunications providers (CYTA and Epic Ltd). Events such as talks and workshops are run for children and parents.

Participation in the European Safer Internet Day is also co-ordinated by the Cyprus SIC, and includes activities that run throughout the month of February.[43] This includes a conference aimed at students and teachers, and a video contest for students. Schools are encouraged to organise school-based activities for Safer Internet Day, and TV shows host speakers who can inform viewers about Internet safety and promote cybersecurity reporting mechanisms, including the CYberSafety Helpline.

[41] https://www.esafecyprus.ac.cy/ethniki-stratigiki
[42] https://www.betterinternetforkids.eu/en-GB/sic/cyprus
[43] https://www.saferinternetday.org/en-GB/in-your-country/cyprus

Both the CYberSafety portal[44] and the portal of the Pedagogical Institute for Internet Safety[45] are focused on the safety of children on the Internet. The CYberSafety portal, for example, provides general information about Internet safety, and advisory material that is aimed at students, teachers and parents in particular. It also hosts information about the CYberSafety Helpline, and a Youth Panel which allows young people to exchange knowledge and experiences concerning digital technologies and how to stay safe online.

For other demographics, the effort has so far been less co-ordinated, although various initiatives targeting other demographics do exist. The DSA and NSA have run awareness training for civil servants and users of government information systems. CSIRT-CY runs campaigns for the operators of CI, to raise their cybersecurity awareness and teach preventive and response actions. The Office for Combating Cybercrime, Cyprus Police (OCC) is responsible for raising awareness in the field of cybercrime. It has undertaken activities such as preparing video material relating to cyber-bullying, which has been disseminated on TV and on the Internet.[46]

ASPIS (INFORMATION SECURITY), a joint cybersecurity-awareness campaign between the DSA, the OCC, the Central Bank of Cyprus and the Cyprus Banking Association, began in September 2021. It involves the dissemination of information *via* social media, TV and radio. Its aim is to raise the cybersecurity awareness of the general public, particularly in relation to access to personal data, online communications and bank accounts, and online fraud.[47] The DSA and OCC have both been using social media posts to disseminate cybersecurity-awareness information for a few years, and multiple stakeholders expressed positive views about these posts.

The European Cybersecurity Awareness month takes place each October; in October 2021 specific groups were targeted in Cyprus.[48] This included (among others) a collaboration between the European University of Cyprus and the DSA to run awareness-training for older citizens with less technological awareness, and for SMEs.

In summary, while various awareness-raising events have taken place for demographics other than children, there is a need to raise the level of these and to co-ordinate them in the same way. This includes awareness-raising for the wider public (including more senior citizens), SMEs, and the government.

In terms of choosing which campaigns to run, there was some discussion about the interplay that exists between the DSA and CSIRT-CY and other parties such as universities, and their understanding of the priorities for the nation. This should continue as the demographics targeted expand. This may currently be somewhat *ad hoc*, and some participants, including some universities which run awareness campaigns according to their own understanding of what the community needs, noted that it would be beneficial to have an overarching

[44] https://www.cybersafety.cy/awareness-en

[45] https://internetsafety.pi.ac.cy/

[46] https://www.police.gov.cy/police/police.nsf/All/671EB91BDCAA303EC22584000041D696?OpenDocument

[47] https://www.stockwatch.com.cy/el/article/emporika-nea/oloi-mazi-na-prostateytoyme-apo-tis-ilektronikes-apates

[48] https://cybersecuritymonth.eu/countries/cyprus

programme from which the various stakeholders can gain a clear understanding of priorities and of how their various awareness-raising efforts can align and address the national need and the threat landscape.

A specific group that requires attention is executives. There was frequent mention throughout the review of the need for business leaders to have a higher level of cybersecurity awareness in general, so that cybersecurity is prioritised in organisational budgets and dedicated security teams are created within organisations. Action 14 of the NCS states the need to include awareness-raising campaigns aimed at business executives as part of the developing national awareness-raising programme.

There is also a need to ensure that awareness-raising efforts extend to the top levels of government, to support their own security and practice in protecting the sensitive data they handle, and so that those responsible for national, strategic and budgetary decision-making have a strong understanding that can support well-informed decisions around cybersecurity policy and budget. This includes educating and raising the awareness of those responsible for passing legislation (Parliament), and of those responsible for the national budget (Ministry of Finance). Budget and a lack of uptake were cited as barriers to running awareness training for government personnel.

A "competence centre" is currently being established to promote the safe use of digital technology and the Internet across demographics in Cyprus, based on Action 14b of the NCS, which resulted from the suggestions of stakeholders from Cypriot society. The creation of this centre has already been approved by the Council of Ministers; plans are in development and funding is being sought. It is envisaged that this centre will play an important role in raising cybersecurity awareness, and also in cybersecurity education and training, research and innovation. The competence centre will target students first, but there are plans to expand its reach, targeting, for example, prosecutors, lawyers, and SMEs. Programmes will be developed and implemented in collaboration with academia.

D3.2 CYBERSECURITY EDUCATION

This Factor *addresses the availability and provision of high-quality cybersecurity education programmes and having sufficient qualified teachers and lecturers. Moreover, this* Factor *examines the need to enhance cybersecurity education at national and institutional levels, and the collaboration between government and industry to ensure that educational investments meet the needs of the cybersecurity education environment across all sectors.*

***Stage*: Formative to Established**

There are various university-level cybersecurity courses offered in the Republic of Cyprus. A number of universities offer master's degrees in Cybersecurity, including distance-learning

Masters.[49,50] These cover topics such as network security; cryptography; risk analysis and management; cybersecurity operations; cybersecurity policy, governance and law; cyber warfare; ethical hacking; and digital forensics. There are no dedicated bachelor degrees in Cybersecurity but the subject is a compulsory part of some Computer Science courses,[51] and various specific Cybersecurity-related elective modules are offered within Computer Science degrees, such as cybercrime and legal concepts.[52]

It was reported by the universities present that there are also a few Doctoral-level students in the field of Cybersecurity. However, the view was widely expressed that the number of people in Cyprus qualified at this level, in this subject, is not high enough, and that this affects the supply of cybersecurity educators and makes recruitment challenging. It was noted that this is not only a problem in cybersecurity, but in many disciplines; there is a lack of people qualified to teach at a university level.

Participants noted that funding is an issue in attracting PhDs in Cybersecurity, and there is a need for universities to offer funded PhDs in order to attract post-graduate students and people working in industry. There was discussion during the sessions of whether an approach such as doctoral-training centres for Cybersecurity might be beneficial, to increase the opportunities for Cybersecurity doctorates, if funding were available.

This review found no evidence of cybersecurity educational offerings for non-specialists, such as cybersecurity risk-awareness modules offered as part of other university courses, nor any seminars or lectures aimed at non-specialists, on the subject of cybersecurity issues.

The universities reported collaboration with industry in the development and updating of cybersecurity curricula; this was done *via* industrial advisory boards including representatives from $(ISC)^2$, ISACA and other cybersecurity bodies and companies, and with a particular focus on updating curricula in line with emerging technologies and threats. They also reported running sessions with invited speakers from industry to provide information to students about trends in cybersecurity and certification options, for example. Universities also reported co-operation with the Government in terms of receiving information about cybersecurity trends from them, and government participation in university advisory boards, which are involved in developing and updating curricula. It may be beneficial to create more formal approaches to ensure cybersecurity educational offerings are aligned with the national need; for example, by creating a body that can certify university degrees to show that they meet the national need.

As part of the CYberSafety project, the Ministry of Education has focused efforts on the school curriculum. As a result, new curricular units on cyber-safety and cyber-bullying are being offered at primary school level. At the secondary school level, sections of relevant courses such as Information Technology refer to key cybersecurity concepts. Both the academic CSIRT run by CYNET and the Cyprus Pedagogical Institute reported visits to schools to give hands-on cybersecurity training to students, to increase interest in the subject and awareness of risks.

[49] https://www.uclancyprus.ac.cy/postgraduate-course/msc-cybersecurity/
[50] https://euc.ac.cy/en/programs/master-cybersecurity/
[51] https://www.uclan.ac.uk/undergraduate/courses/computer-science-bsc
[52] https://euc.ac.cy/en/programs/bachelor-computer-science/#tab-program-of-study

It was reported that some private schools have other cybersecurity educational offerings, including hackathons.

Participants expressed the view that it is important to encourage students to pursue science, technology, engineering and mathematics (STEM) subjects, to educate children about cybersecurity, and to clarify and promote the many possible routes to becoming a cybersecurity professional. The efforts being put into cybersecurity within school curricula, reflected in the NCS Thematic Unit 10 ("Education and Training"), which recognises the need to "promote school programmes that raise awareness and encourage students' interest in network and information security issues and inform them about career opportunities in cybersecurity", are a positive step towards this.

Cyprusparticipates in international Capture-the-Flag (CTF) competitions and runs in-country competitions, which contribute towards establishing a cadre of cybersecurity experts who not only have technical skills but also understand how to co-operate in cybersecurity. Cyprus participates in both the European and International Cyber Security Challenges run by the EU,[53] and it has also organised national competitions for qualification. A significant growth in the number of Cypriot students participating in the national competition was reported, from around ten at its inception to around 150 this year; Cypriot participants qualified for the European team for the International Challenge, and the Cypriot team has placed well in the recent European Challenge. It was suggested that running more regular and widespread CTF competitions might be an area that would benefit from attention from the Ministry of Education.

A topic that arose many times during the stakeholder discussions was the lack of internship programmes for students to gain cybersecurity industry experience during their degree programmes. Similarly, there is a lack of industry involvement in university projects such as dissertations at master's degree level. Participants felt that it might be difficult to resolve this issue, given that Cyprus is a relatively small country with relatively few companies that could offer these opportunities. A number of private-sector representatives expressed the view that companies may have trust-related concerns about taking on interns, particularly given the need to handle sensitive information, and that they may also perceive internships as something of a burden. This appears to be an area in which consideration of solutions is needed: this might involve incentives for the private sector to offer internships, or financial support from the Government, for example.

This review found no evidence of programme review processes or outcome-oriented metrics in place to review the supply and demand for cybersecurity courses.

[53] https://ccsc.org.cy/

D3.3 CYBERSECURITY PROFESSIONAL TRAINING

This Factor *addresses and reviews the availability and provision of affordable cybersecurity professional training programmes to build a cadre of cybersecurity professionals. Moreover, this* Factor *reviews the uptake of cybersecurity training, and horizontal and vertical cybersecurity knowledge and skills transfer within organisations, and how this transfer of skills translates into a continuous increase of cadres of cybersecurity professionals.*

***Stage*: Formative to Established**

Professional training programmes in cybersecurity are offered primarily by the Cyprus chapters of the international cybersecurity professional training and certification bodies: $(ISC)^2$,[54] and ISACA.[55] Representatives of these bodies reported that they seek to provide training sessions for professionals in cybersecurity every few months, and that the uptake of cybersecurity certification courses is increasing. A range of training courses and certifications are offered by some private companies, including certifications from Cisco and CheckPoint.[56] Cyprus does not have its own accreditation programmes for cybersecurity professionals.

A shortage of people qualified to run cybersecurity professional-training courses in Cyprus was reported. This is rooted in a cybersecurity workforce shortage. Some participants expressed the view that this is part of the reason for an overall shortage of cybersecurity training opportunities in Cyprus.

An initiative is underway, led by the Deputy Ministry of Research, Innovation and Digital Transformation, to build a Digital Academy (similar to the academy in Greece[57]). This will enable self-study on courses provided by various vendors and on a range of topics, from basic digital training (e.g., how to set up a website) to professional training for cybersecurity. This academy is reported to be currently under development and has an allocated budget.

The Government recognises the need to align the provision and promotion of cybersecurity professional training with the needs of society and industry; this is reflected in Thematic Unit 10 of the NCS but there is no evidence that formal documentation of the training requirements has been produced yet. The DSA recently invited businesses in Cyprus to answer a questionnaire, one of the aims of which was to identify needs for training; the responses may therefore help identify national training needs.

It was noted by some government participants that a greater training offering for government personnel would be beneficial, and that this might need to be tailored towards the threats and risks most relevant to the various different departments. The NCS Thematic Unit 10 ("Education and Training") includes an Action aimed at integrating relevant cybersecurity certifications into cybersecurity-related public-sector projects and ensuring opportunities for

[54] https://www.isc2cyprus.com/
[55] https://engage.isaca.org/cypruschapter/home
[56] https://www.aktina.com.cy/category/certifications/
[57] https://nationaldigitalacademy.gov.gr/

development in cybersecurity for public-sector personnel. This is an approach that might help address the issues noted around the topic of retention of cybersecurity personnel in the public sector. CSIRT-CY trains its own personnel and CI operators, seeking to build capacity through regular training programmes.

There is no evidence of training programmes being made available for non-cybersecurity professionals to learn basic cybersecurity skills. The transfer of knowledge from cybersecurity-trained employees to untrained employees may happen on an *ad-hoc* basis but not generally through established mechanisms.

The Cyprus Center for Land, Open-seas, and Port Security (CYCLOPS) is under development.[58] This regional security-training hub (which will focus on cybersecurity as well as aspects of national security such as customs and exports control, and port and maritime security, for example) is a forward-looking joint initiative between the US and Cyprus; located in Cyprus, with financial and implementation support from the US, it will support capacity-building in the region. Trainers will be provided by both countries and the centre will include a mobile cybersecurity training lab for cybersecurity technical training, enabling regional partners to learn best practices for securing CIs and to engage in cross-border cyber investigations. Training will also be offered to specialised cybersecurity professions, e.g., SOC analysts.

The aim is to develop synergies between CYCLOPS and similar international centres including the European Security and Defence College,[59] and the European Centre of Excellence for Countering Hybrid Threats.[60] Members of the international community participating in the review expressed the view that many countries are excited about the prospect of collaborating with CYCLOPS.

Many participants expressed the view that there is a shortage of cybersecurity professionals in Cyprus. This, it was suggested, begins at the school level, where there is a shortfall in the number of children studying STEM subjects (as is broadly the case worldwide). There may also be a gap between people being interested in cybersecurity careers (through education and competitions, for example) and people actually taking up a cybersecurity career, which is having a negative impact on the cybersecurity workforce. It was suggested that there is not enough promotion of information about the paths to a cybersecurity career aimed at potentially interested parties. This includes parties from a range of disciplines: those with legal and political backgrounds, for example, not just technical ones. The lack of cybersecurity internships for students, and of graduate schemes, were also cited as possible blockers.

It was noted that it can be challenging to create an adequate cybersecurity government workforce, particularly given the financial incentives that encourage cybersecurity experts (e.g., those graduating from cybersecurity courses at universities) to join private-sector organisations. It was noted that it can even be challenging to create an adequate private-sector cybersecurity workforce, given the financial incentives that encourage graduates to work in the finance industry and foreign-exchange market. Participants suggested that more organised discussion between the Government, private-sector cybersecurity organisations,

[58] https://mfa.gov.cy/press-releases/2021/01/04/groundbreaking-cyclops-04012021-remarks/
[59] https://esdc.europa.eu/
[60] https://www.hybridcoe.fi/who-what-and-how/

students and graduates, would be valuable, to understand the issues and identify ways of retaining cybersecurity experts in the cybersecurity workforce.

The DSA noted that it has ongoing discussions with the UK's National Cyber Security Centre (NCSC) about how to retain a skilled cyber workforce in government and within the country. Government initiatives to incentivise cybersecurity experts to stay in the country after training are not yet in place, however. The need for incentives and competitions was discussed, as well as the need for further input from industry to discuss opportunities, for example with students at universities, to seek to address this issue of workforce retention. A collaborative effort will be needed with the relevant stakeholders coming together to assess the needs of industry and the current offer from universities, and a discussion needs to be had about how to adapt the offerings and enhance promotion of cybersecurity careers to meet the national demand.

The requirement for greater public-private partnership on cybersecurity was noted. To enhance collaboration and the mutual understanding of needs, it may be beneficial to offer secondments from the private sector to public-sector cybersecurity roles. It was also suggested that, while a cybersecurity private-sector advisory group to the Government already exists, more informal meetings would be beneficial to enable private-sector representatives to voice their needs and ideas, and enable to the Government to better represent them in its provisions and policy-making.

D3.4 CYBERSECURITY RESEARCH AND INNOVATION

This Factor *addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges, and to advance the building of cybersecurity knowledge and capabilities in the country.*

***Stage*: Formative to Established**

Cybersecurity R&D activities have been established in Cyprus and are indicated in Thematic Unit 11 ("Research and Innovation") of the NCS. The Actions listed in the Strategy state that R&D activity should be "directly related to the needs identified within Cyprus and at European and international level and be able to support the objectives of this Strategy". The actions also focus on the "evaluation and creation of cybersecurity ecosystems in areas where the Republic of Cyprus pioneers or presents increased activity, such as merchant shipping, financial services or energy". A specific cybersecurity R&D strategy is not in place but such a strategy may be beneficial as it would enable stakeholders to identify R&D requirements to meet the national need.

Cybersecurity research laboratories have been established at a number of universities in Cyprus[61,62] and there is active international collaboration in R&D projects. This includes participation from Cypriot universities in research consortia with EU partners. An example is

[61] https://www.unic.ac.cy/centres/centres-established-through-the-university/defence-and-security-research-institute-dsri/d-open-seas-and-port-security/

[62] https://www.uclancyprus.ac.cy/academic/dr-eliana-stavrou/

the REWIRE project which is funded by the EU's Erasmus programme and has partners from around Europe which have joined forces to build a European Cybersecurity Skills Strategy, which aims to address the gap between industry requirements and training provisions.[63]

The public sector also collaborates with universities, to operate cybersecurity R&D programmes. An example is the Cyber Sensors for Critical Infrastructure Protection and Large Scale Cyber Range Training Environment (CY SENTINEL) project, which is run as a collaboration between the Open University of Cyprus and the DSA and which aims to develop systems to protect the CI from cyber threats, as well as deliver a cyber-range platform for cybersecurity training.[64] The cyber-range is complete and has been demonstrated and there are plans to run national-level cybersecurity exercises using the platform from 2022. Other universities also reported having submitted research proposals in collaboration with the DSA in the past.

In terms of resources, most R&D projects at universities are funded by EU schemes such as Horizon 2020 and Erasmus. It was reported that the Government has considered how to allocate funds to cybersecurity R&D, but this has not yet been delivered.

No evidence was provided of there being any metrics in place to measure R&D performance in Cyprus. The DSA reported that it continues to try to identify approaches and incentives that will encourage stakeholders, particularly industry stakeholders, to participate in cybersecurity research and innovation.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Building Cybersecurity Knowledge and Capabilities*, the following set of recommendations are provided to Cyprus. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

BUILDING CYBERSECURITY AWARENESS

R3.1.1 Assign a dedicated body , for example the Cyprus Safer Internet Centre (SIC) or any other relevant body, to take responsibility for the co-ordination of all Cybersecurity Awareness activities in Cyprus;

R3.1.2 task this dedicated body to adopt a centralised approach to awareness campaigns, for example a national cybersecurity awareness-raising programme, from which the various stakeholders can ensure that their efforts contribute to a cohesive awareness-raising effort that meets national demand. This programme should continuously take account of the national need and shifts in the threat landscape;

[63] https://rewireproject.eu/

[64] The cyber-range is complete and has been demonstrated; exercises have not yet been run using it, but national-level exercises are planned from 2022.

R3.1.3 task the dedicated body, working with relevant stakeholders, to extend the cybersecurity awareness-raising strategy for children to cover a wider range of target groups, or develop additional standalone strategies for cybersecurity awareness-raising in other target groups including, for example, older citizens and SMEs;

R3.1.4 task the dedicated body, working with relevant role players, to increase awareness-raising initiatives for leaders – business executives, and leaders in government responsible for making national policy and budgetary decisions;

R3.1.5 seek to exploit the "competence centre" at regional and European levels, as a training, education and research and innovation hub for cybersecurity (as suggested in Action 14 of the Strategy). Here, Cyprus has the opportunity to make a strong international offering and contribute to building capacity in the region;

R3.1.6 create programme review processes and outcome-oriented metrics to measure the effectiveness of awareness campaigns (and the developing national cybersecurity awareness-raising programme); and

R3.1.7 develop a national portal for all cybersecurity awareness initiatives. Such a portal could be a national point of contact, providing information about all initiatives relating to cybersecurity awareness including courses, lectures and more. Consider whether the CYberSafety portal or the portal of the Pedagogical Institute for Internet Safety could be expanded to perform this role.

CYBERSECURITY EDUCATION

R3.2.1 Task the Ministry of Education, or another suitable Ministry, to take responsibility for the implementation of the Recommendations below;

R3.2.2 seek to incorporate cybersecurity awareness modules as part of non-cybersecurity university courses;

R3.2.3 run seminars or lectures on cybersecurity issues for non-specialists, led by universities or other bodies;

R3.2.4 identify ways of further clarifying and promoting cybersecurity career paths to students at school and university levels, to ensure that a lack of awareness of the career options is not a blocker to the creation of an adequate cybersecurity workforce;

R3.2.5 consider running more regular and widespread CTF competitions in Cyprus, to help increase the cadre of cybersecurity experts;

R3.2.6 create cybersecurity internships in industry for students, with financial support from the Government;

R3.2.7 create incentives for the private sector to participate in cybersecurity master's degrees and offer projects for dissertations;

R3.2.8 create multidisciplinary master's degrees in cybersecurity, and encourage people from non-Computer Science degrees (or STEM degrees) to undertake courses in cybersecurity;

R3.2.9 consider establishing doctoral-training centres in Cybersecurity, to increase the number of PhD graduates. Ensure that funding is made available by the Government;

R3.2.10 create a body that can certify cybersecurity university qualifications (e.g., master's degrees) to show that they meet the national need; and

R3.2.11 implement programme review processes and outcome-oriented metrics to review the supply and demand for cybersecurity courses as well as the supply and demand for cybersecurity graduates in the country.

CYBERSECURITY PROFESSIONAL TRAINING

R3.3.1 Task the Ministry of Research, Innovation and Digital Transformation, or another suitable Ministry, to take responsibility for the implementation of the Recommendations below;

R3.3.2 create a programme of measurements and metrics to assess the supply and demand for cybersecurity-skilled workers in both public and private environments in Cyprus. Use collected data to influence decisions made;

R3.3.3 seek to ensure the provision and promotion of cybersecurity professional training is aligned with the needs of society and industry, including creating formal documentation of training requirements. Use the data compiled through the metrics system (see Recommendation 3.3.2) for this;

R3.3.4 identify and implement initiatives to address the gap that may exist between parties interested in cybersecurity, and those actually taking it forward as a

career. This may require more co-operation from industry to disseminate information about, and promote, cybersecurity careers;

R3.3.5 ensure government funding is made available to support cybersecurity graduate schemes and internships;

R3.3.6 enhance training offerings for government personnel. This may include creating opportunities for personnel working on cybersecurity projects in the public sector to undertake cybersecurity certification;

R3.3.7 create initiatives to enhance the transfer of knowledge from cybersecurity-trained employees to untrained employees in both the public and private sectors;

R3.3.8 develop training programmes for non-cybersecurity professionals;

R3.3.9 develop job-creation cybersecurity initiatives within organisations, to encourage employers to train staff to become cybersecurity professionals;

R3.3.10 develop initiatives that will encourage trained cybersecurity professionals to stay in the country, and specifically, to retain skilled professionals in government;

R3.3.11 seek to enhance public-private partnership in the area of cybersecurity. It may be beneficial to offer secondments from the private sector to public-sector cybersecurity roles. It may also be beneficial to run informal meetings, to enable private-sector representatives to voice their needs; and

R3.1.12 develop a national portal for all cybersecurity professional training initiatives. Such a portal could be a national point of contact, providing information about all initiatives relating to cybersecurity professional training, such as certification opportunities, lists of certified professionals, and more.

CYBERSECURITY RESEARCH AND INNOVATION

R3.4.1 Task the Deputy Ministry of Research, Innovation and Digital Transformation, or another suitable Ministry, to take responsibility for implementation of the Recommendations below;

R3.4.2 implement metrics for measuring cybersecurity R&D performance and outputs, to improve the cybersecurity R&D capability of the country;

R3.4.3 develop a cybersecurity R&D strategy that, with relevant stakeholders, identifies and selects cybersecurity R&D projects beneficial to national interests;

R3.4.4 ensure that R&D projects identified and selected in 3.4.3 are assigned to students in universities; and

R3.4.5 allocate national funds to cybersecurity R&D projects that will improve the cybersecurity capability of Cyprus.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This *Dimension* examines the Government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation, and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this *Dimension* observes issues such as formal and informal co-operation frameworks to combat cybercrime.

Figure 9: Factors and aspects examined in Dimension 4.

D4.1 LEGAL AND REGULATORY PROVISIONS

This Factor *addresses various legislation and regulatory provisions relating to cybersecurity, including legal and regulatory requirements, substantive and procedural cybercrime legislation, and human rights impact assessment.*

***Stage*: Established**

Cyprus has diligently implemented EU Regulations and Directives into Cypriot law. There is an umbrella of different laws on substantive cybercrime legislation covering illegal access to, interferences on and the interception on devices, computer systems and data. Law 22(III)/2004,[65] which was modified in 2013, ratifies the Budapest Convention on Cybercrime, defining computer data and systems, as well as computer crimes, crimes related to content such as child pornography or racism and fraud. It further empowers courts to express an opinion on such crimes and defines the penal articles that are relevant for such crimes.

Further legislation that is substantive for cybercrime includes:

- Law 147(I)/2015,[66] which considers attacks on information systems, describing specific penalties for crimes;
- the Regulation of electronic communications and postal services Law 112(I)2004[67];
- the Retention of Telecommunication data for the investigation of serious offences Law 183(I)/2007[68];
- Law 25(I)/2018[69] which describes the protection of individuals from the processing of personal data;
- the Processing of Personal Data with Law 138(I)/2001;
- Law 112(I)/2004 which contains provisions for issues concerning internet security and protection of personal data and was modified in 2020[70];
- Law 26(III)/2004[71] which refers to the criminalisation of acts of a racist and xenophobic nature committed through computer systems;
- Law 2011 134(I)/2011[72] which adds to the aforementioned expressions of xenophobic nature.

Finally, there are provisions for fake news, with specific penalties for those who engage in spreading misinformation.

[65] http://www.cylaw.org/nomoi/arith/2004_3_022.pdf
[66] http://www.cylaw.org/nomoi/arith/2015_1_147.pdf
[67] https://ocecpr.ee.cy/sites/default/files/ec_law_generallaw_en_l-112-1-2004_09-03-2017_kv__0.pdf
[68] http://www.cylaw.org/nomoi/arith/2007_1_183.pdf
[69] http://www.cylaw.org/nomoi/arith/2018_1_125.pdf
[70] http://www.cylaw.org/nomoi/arith/2020_1_090.pdf
[71] http://www.cylaw.org/nomoi/indexes/2004_3_26.html
[72] http://www.cylaw.org/nomoi/indexes/2011_1_134.html

Since the 2017 review, Cyprus has completed all the necessary legal requirements for the inception of an entity (DSA) to create legally binding frameworks for CIs, the mandatory sharing of information with defined rules to which CIs need to adhere, and strict penalties if CIs do not conform to their obligations. Details are provided in Law 89(I) 2020,[73] as well as Decisions 389/2020, 218/2019 and 408/2020. There are also specific provisions for certification schemes in cybersecurity, however, participants mentioned that the law will be complemented to fully support the Cybersecurity Act. It is worth noting that the DSA has a dedicated policy-making unit and legislation that deals with cybersecurity. Therefore, Cyprus's current legal requirements for cybersecurity show initial indicators of a strategic maturity, which can inform future regulation.

The umbrella of laws that the cybercrime unit has at its disposal set out evidentiary requirements and provide comprehensive provisions for the investigation of cybercrime. All the necessary EU legislation, as well as international treaties, have been ratified and various units carry out consistent monitoring of the implementation of emerging treaties and EU legislation into national law. Apart from the legal unit of the DSA, which is tasked with monitoring cybersecurity-related developments in legislation, developments in case law at local, EU and international levels are closely followed by counsels and prosecutors. They participate in the e-evidence Working Group in Brussels, where the European Commission's proposal for the adoption of a regulation creating the European Production Order[74] and the European Preservation Order[75] is discussed at a technical level allowing, in essence, the exchange of cybercrime information between EU countries. They further participate in the Council of Europe Protocol Drafting Plenary for the drafting of Second Additional Protocol to the Convention of Cybercrime. Finally, regular meetings with the police and representatives of various ministries are organised to discuss problems and amendments in the legislation of cybercrime.

Human rights are at the heart of every piece of Cypriot legislation; Article 5[76] of the Constitution of the Republic of Cyprus states that the Republic of Cyprus shall secure for everyone within its jurisdiction, human rights and fundamental freedoms comparable to those set out in Section I of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Protocol to that Convention. Cyprus ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1995, and the Universal Declaration of Human Rights of the United Nations General Assembly and the International Charter of Human Rights, protecting the right to freedom of speech and expression. All human rights are recognised in laws related to cybersecurity and participants mentioned that frequent impact assessments of substantive and procedural cybercrime legislation are conducted by an independent authority.

[73] https://dsa.cy/wp-content/uploads/DSA-Law-89-I-2020.pdf

[74] The European production order will allow a judicial authority in one EU country to obtain electronic evidence (such as emails, messages in applications) directly from a service provider, or its legal representative in another EU country.

[75] The European Preservation Order will allow a judicial authority in one EU country to request that a service provider, or its legal representative in another EU country, preserves specific data in view of subsequent request to produce this data via mutual legal assistance.

[76] http://www.kypros.org/Constitution/English/appendix_a.html

D4.2 RELATED LEGISLATIVE FRAMEWORKS

This Factor *addresses the legislative frameworks relating to cybersecurity, including data protection, child protection, consumer protection, and intellectual property.*

***Stage*: Established**

Cyprus has fully implemented the EU's General Data Protection Regulation (EU, 2016/679) with Law 125(I)/2018.[77] The recent legislation builds on a number of previous legislative efforts involving the processing of personal data under Law 138(I)/2001,[78] which was a response to the European Directive 95/46/EC on Data Protection.[79] In 2002, Cyprus established The Office of the Commissioner for Personal Data Protection (OCPDP),[80] which is an independent authority for data protection. An issue that has not yet been addressed at EU level is the privacy considerations when cloud providers are based in the US, or are US companies with branches in the EU. Particular attention of this should therefore be drawn to users of such cloud services.

The importance of child protection online in Cyprus is evidenced in the national strategy, as there are dedicated actions for this area. Participants mentioned that the main cybercrime offences that are prosecuted in Cyprus involve child pornography, and the law that applies is the Prevention and Combating of Sexual Abuse, Child Sexual Exploitation and Child Pornography (91 (I)/2014).[81] This law deals with general child protection, including measures for online activity, and is complemented by Law 60(I)/2014 on human trafficking and the protection of victims. Participants mentioned that in the regular meetings conducted for the effectiveness of legislation between the police and the Law Office, it had been recommended that the law should also cover the use of abusive language online, and that the scope of online providers should be widened to include social media. These are pending proposals that are currently before the House of Representatives.

Consumers in online environments are protected by a comprehensive raft of legislation. E-commerce is regulated by Law 156/2004,[82] implementing the Directive 2000/31/EC of the European Parliament and the Council of the European Union. The law draws on certain legal aspects of information society services, in particular, electronic commerce in an Internal Market. Law 156(I)/2004 specifies the free movement of information society services between the Republic of Cyprus and EU/EEA Members, and regulates the following online activities: online information services; online advertising and marketing; online selling of products and services; and online entertainment services. There is a consumer protection service entity, under the remit of the Ministry of Energy, Commerce and Industry, with

[77] http://www.cylaw.org/nomoi/arith/2018_1_125.pdf
[78] http://www.cylaw.org/nomoi/arith/2001_1_138.pdf
[79] http://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:31995L0046
[80] http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument
[81] http://www.cylaw.org/nomoi/enop/non-ind/2014_1_91/full.html
[82] http://www.cylaw.org/nomoi/arith/2004_1_156.pdf

dedicated helplines and portals for lodging complaints. The website provides information about the latest fraudulent websites pretending to be official websites of Cypriot organisations, online scams, and phishing emails.

Cyprus has recently legislated additional laws which provide better protection for consumers online. The first is Law 51(I)/2021,[83] which is an implementation of the European Parliament and the Council of the European Union law, 2019/713. The law deals with criminal offences of fraud and impersonation when monetary transactions do not include cash and provides ways to deter such criminal activities and support actions for victims of fraud. Law 61(I)2021[84] aims to mitigate the legitimisation of profits from illegal activities and Law 60(I)2021[85] deals with services pertinent to electronic authentication and services for trust in electronic transactions. Participants mentioned that there are pending Actions concerning qualified trust services and electronic identities, which may boost consumers' confidence in e-commerce further.

Intellectual property (IP) law is effective in Cyprus, in accordance with best practice and EU legislation and there is also comprehensive IP legislation for online products and services based on Common Law. Some general principles of the aforementioned legislation are: the Intellectual Property Law 59/76, as amended by Law 63/77 and Law 18/93; the Trade Marks Laws CAP.268, as amended by Law 63/62, Law 69/71 and Law 206/90; the Patents Law, 16(1)/98, and the Partnerships and Trade Names Law, CAP 116. Cyprus has recently modified the law on IP rights *via* the newly legislated law 56(I)/2020.[86] International overview of IP legislation and how it informs changes to Cypriot law falls under numerous international conventions relevant to IP of which Cyprus is a signatory; they include, *inter alia*, the European Community Trademarks, the Convention Establishing the World Intellectual Property Organisation (WIPO), the Madrid Agreement Concerning the International Registration of Marks (the "Madrid Agreement") and Protocol to the Madrid Agreement, the Patent Cooperation Treaty, the Berne Convention for the Protection of Literary and Artistic Works, and the Paris Convention for the Protection of Industrial Property.

A common element in child protection online, consumer protection and IP legislation is the lack of monitoring units to assess the effectiveness of legislation in these areas. There are informal initiatives in place which should be enhanced to ensure that further amendments or policy initiatives in these areas are informed by monitoring practices and lessons learnt.

[83] http://www.cylaw.org/nomoi/arith/2021_1_051.pdf
[84] http://www.cylaw.org/nomoi/arith/2021_1_061.pdf
[85] http://www.cylaw.org/nomoi/arith/2021_1_060.pdf
[86] http://www.cylaw.org/nomoi/arith/2020_1_056.pdf

D4.3 LEGAL AND REGULATORY CAPABILITY AND CAPACITY

This Factor *studies the capacity of law enforcement to investigate cybercrime, the prosecution's capacity to present cybercrime and electronic evidence cases, and the court's capacity to preside over cybercrime cases and those involving electronic evidence. Finally, this* Factor *reviews the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.*

***Stage*: Formative to Established**

The NCS (Action 23) recognises the need to continue to build capacity to combat cyber offences. In terms of the capacity of the prosecution and the courts, Cyprus has reached an Established *stage* of maturity. The capacity of Regulatory Bodies is at a Formative *stage* as cross-sector regulation of the cybersecurity of the CI has been established since 2020, but the capability and resources of the Regulatory Body to undertake this role have not yet been fully tested, with the first audits planned to take place in 2022.

The Ministry of Justice and Public Order, together with the Cyprus Police, is responsible for combating cybercrime in Cyprus. The Cybercrime Unit of the Cyprus Police, established in 2020 and previously called the Cybercrime Subdivision, is responsible for the investigation of cybercrime.[87] The Office for Combating Cybercrime (OCC) is part of this Unit and was established in 2007, under Police Order No. 3/45, to implement Law 22(iii)/2004 (which ratifies the Budapest Convention on Cybercrime).

According to Police Order No. 3/45, the OCC is responsible for investigating crimes committed *via* the Internet or *via* computers. It is also responsible for investigating all offences that violate the rules laid down in Law 22(iii)/2004. The police reported investigation of cases of attacks on information systems and child exploitation.

The Digital Evidence Forensic Laboratory (DEFL) is also part of the Cybercrime Unit and supports the work of the OCC. It was established in 2009 and is responsible for the effective examination of electronic evidence. It is staffed with specialist officers who manage the collection and forensic analysis of electronic devices, and the presentation of expert scientific evidence in the courts. The Cybercrime Unit has grown significantly since its inception in 2007, when it had five staff; in 2021, it was formed of 22 staff working across the OCC and the DEFL. The latter has a formal framework that is aligned with international practice prescribing specific procedures for the collection and treatment of electronic evidence and maintaining the integrity of evidence.

Participants reported a reasonable capacity within the DEFL, with specialised tools and staff but it was noted that more cybersecurity training may be needed for field officers. The police academy runs several cybersecurity-related programmes, including serious-crime investigation courses for officers. Materials from the Cyprus Cybercrime Centre of Excellence

87 https://www.police.gov.cy/police/police.nsf/All/671EB91BDCAA303EC22584000041D696?OpenDocument

for Training, Research and Education (3CE) project[88] have been incorporated into training programmes that are followed by all police officers. This project also provided specialised cybercrime-related training for public- and private-sector participants, and developed modules for judges, prosecutors and law enforcement officers. It is being extended as part of the new "competence centre", which is currently under development. It was noted that while training materials are currently available, finding the resources to implement training is a challenge, and also that there is a need to encourage greater uptake.

Law enforcement officers also participate in training organised by the European Union Agency for Law Enforcement Training (CEPOL), relating to cybercrime investigation. It was reported that the Cyprus police force also provides some cybercrime-investigation training to other European countries, *via* CEPOL. The DSA has also been involved in providing training for audiences including international law enforcement, on aspects of cybersecurity such as CI protection, *via* the European Security and Defence College.[89]

Currently, there is no centralised unit responsible for the investigation of computer-related fraud. Such investigations are the responsibility of district crime-investigation departments, not the Cybercrime Unit, and some participants believed that information is being lost when computer-related fraud relates directly to other types of offence and is investigated as such (for example, phishing attacks used to obtain personal data that is later used in other offences). It was noted that there is a need for a centralised overview of all computer-related fraud cases in Cyprus, and a dedicated organisation responsible for the investigation of computer-related fraud may be needed.

In terms of procedures for cybercrime investigation, in order to gather intelligence, the police must obtain a court order to obtain telecommunications data, or a search warrant to obtain access to suspects' digital devices. Authorisation is given by a counsel, who represents the Attorney General under the Data Retention Law. In October 2021, in response to issues identified in this area, the state legal service offered training to police officers about how to apply successfully to court for search warrants and access to telecommunication data. If sufficient evidence is obtained, the case is filed in court and presented either by a prosecutor or a counsel of the Law Office, according to the seriousness.

Based on the evidence presented during the review, the focus is currently on the reactive investigation of cybercrime. In order to make progress towards the "Strategic" level of the CMM, attention should be given to developing law-enforcement strategies that include proactive cybercrime-prevention measures, including the use of intelligence to support proactive investigation.

It was reported that, to the greatest extent possible, cybercrime cases are assigned to prosecutors and counsels who have gained expertise in that area. Cybercrime is a subject that is included in training activities offered at national and European level, in which counsels and prosecutors take part. This includes training is organised by the European Judicial Training Network, and prosecutors take part either online or in person. There is also training organised

[88] https://euc.ac.cy/en/3ce-eu-funded-project-on-cybercrime-prevention-concluded-successfully/amp/

[89] https://goalkeeper.eeas.europa.eu/course/details.do;jsessionid=iQ9UOjxN9SNDXKzSCYhc2lnpYCTqo6psRTO63Z2Vng6msNQDtf3n!-1134091793?id=532

bilaterally with other countries. A senior counsel has recently been assigned to organise and co-ordinate training activities for the counsels and prosecutors of the Criminal Law Department. Not many training events have been co-ordinated so far, due to the restrictions imposed by the COVID-19 pandemic, but some training has been conducted online.

Training for the judiciary was carried out as part of the 3CE project,[90] and it was reported that these activities will be extended and run by the "competence centre", when it is up and running. It was noted that while judges have attended training events (as part of the 3CE project), and are gaining experience through handling increasing numbers of cybercrime cases, there is a need to provide more regular training and to find ways of encouraging uptake, particularly given the continuing rise in the number of cybercrime cases.

In general, participants believed that a reasonable level of expertise across law enforcement, prosecutors and judges has been reached during the last few years as a result of the various training efforts, and of experience gained through handling increasing numbers of cybercrime cases. It was noted that there is still room for improvement, however, and increased training might be beneficial. Furthermore, in order to guide the allocation of sufficient resources to operational cybercrime units and to the development of human and technological capacity across law enforcement, the prosecution and the courts, it may be beneficial to implement quantified risk assessments of the levels of cybercrime in, and the key risks to, the country.

The DSA has established its role as the cybersecurity regulator for the CI in Cyprus, in line with the developed regulatory framework, and regulatory requirements came into force in 2020. The DSA's Regulatory, Strategy and Supervision Team is working, in consultation with the office of the Attorney General and other legal entities, on developing the legal bases to confirm implementation of the relevant legislation by the CIs. A new audit framework for this is being developed, with public consultation. Since the audits have not yet taken place, the resources and capabilities of the DSA as the regulator have not yet been fully tested.

D4.4 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This Factor *addresses the existence and function of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.*

***Stage*: Established**

The NCS recognises the need to continue to strengthen co-operation at an international level, for the investigation of cross-border cyber offences, and between the public and private sectors.

[90] https://euc.ac.cy/en/3ce-eu-funded-project-on-cybercrime-prevention-concluded-successfully/amp/

Cyprus' co-operation with foreign law enforcement counterparts is relatively advanced. For international exchange of information in relation to cybercrime investigations, Cyprus co-operates with the EU and also with non-EU countries on the basis of agreements that are bilateral (with Israel, for example[91]) and multilateral (between Cyprus, Israel and Greece, for example[92]). It was noted that some of these agreements have already been tested and shown to work effectively during cross-border investigations of cyber-incidents. The DSA cited the importance of building more of these relationships and is co-operating with the Ministry of Foreign Affairs, to create further bilateral agreements.

The OCC is integrated into and co-operates closely with international networks, including Europol, Interpol, the EU Cybercrime Task Force (EUCTF), ENISA, the EU Judicial Cooperation Unit (EUROJUST), and CERT-EU. This includes access to Europol resources such as large file-exchange systems for uploading materials that require decryption.

It was reported that there are challenges around delays in mutual legal assistance, which can significantly disrupt the investigation of cross-border cybercrime cases. These challenges are mainly encountered at the investigation phase, which is carried out by the police, and it was noted that these challenges are experienced by most countries. A solution is being developed at EU level *via* the e-Evidence Working Group, the forum where the European Commission's proposal for the adoption of a regulation creating the European Production order (which will allow a judicial authority in one EU country to obtain electronic evidence directly from a service provider or its legal representative in another EU country) and the European Preservation Order (which will allow a judicial authority in one EU country to request that a service provider or its legal representative in another EU country preserves specific data in view of a subsequent request to produce this data via mutual legal assistance) is discussed at a technical level.

Counsels and prosecutors from Cyprus participate in this e-Evidence Working Group, and also in the Council of Europe Protocol Drafting Plenary, on the drafting of the Second Additional Protocol to the Convention on Cybercrime. A counsel has been designated to participate in the European Judicial Cybercrime Network, which aims to facilitate the exchange of expertise and best practice, enhancing co-operation between competent judicial authorities when dealing with cybercrime.

In terms of cooperation between law enforcement and the private sector to combat cybercrime, there is no structured procedure in place for formal cooperation of the police with the ISPs and the banks. Banking institutions are obliged to report suspicious activity to the National Unit for Combating Money Laundering, which is separate from the police. The National Unit for Combating Money Laundering transmits the information to the police for handling if needed. Law enforcement officers follow specified procedures (obtaining court orders or search warrants under Data Retention Law) to obtain digital evidence (telecommunications data; digital devices) from organisations. This approach enables the private sector, including ISPs, to co-operate with law enforcement to some extent, although no evidence was provided of assessment of the effectiveness of such collaborative processes, or of any update to take account of new technologies or emerging forms of cybercrime.

[91] https://dsa.cy/en/mou-dsa-incd/

[92] http://www.xinhuanet.com/english/2018-12/21/c_137688022.htm

There is close and effective co-operation between the DSA and the Cybercrime Unit, according to both the DSA and law enforcement representatives. A formal relationship is established, with a Memorandum of Understanding in place for information exchange, which extends to CSIRT-CY. The Cybercrime Unit is not currently directly connected with the threat-intelligence platforms of CSIRT-CY, and there is no automated exchange of threat information; however, the DSA is reportedly seeking to implement a platform that would enable this. A representative of the Law Office participates in the steering committee that monitors the implementation of the NCS. The Law Office gains valuable information on national and international developments in cybersecurity through this participation, enabling alignment of the development of the legal service in this area. Regular assessments of the collaboration between the Government and the criminal justice sector would be beneficial, to ensure their effectiveness.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to Cyprus. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL AND REGULATORY PROVISIONS

R4.1.1 Ensure that the legal team of the DSA continues to monitor international and regional trends, as well as good practices in relevant legal provisions;

R4.1.2 ensure continuous monitoring of emerging technologies, and consider how legislation needs to be adapted for cybercrime and procedural legislation;

R4.1.3 conduct regular impact assessments on how human rights are observed in cybersecurity legislation, and ensure that emerging technologies are considered; and

R4.1.4 legislate on the matter of whistle blowing, and consider how cybersecurity practices can assist in promoting human rights.

RELATED LEGISLATIVE FRAMEWORKS

R4.2.1 Ensure emerging technologies, or the use of services from cloud providers that are not EU companies, do not infringe GDPR; and

R4.2.2 ensure there exist monitoring units to assess the effectiveness of legislation regarding child protection online, consumer protection and IP.

LEGAL AND REGULATORY CAPABILITY AND CAPACITY

R4.3.1 Implement quantified risk assessments, and analyse statistics of cybercrime and law-enforcement interventions, and their impact on harm reduction. Use this information to inform strategy and guide long-term allocation of resources to operational cybercrime units, and to the development of human and technological capacity across law enforcement, the prosecution and the courts;

R4.3.2 increase capacity and resources for the provision of training for law enforcement officers, prosecution lawyers, and judges, and seek to build comprehensive institutional capacity for each. Promote training offerings to increase uptake;

R4.3.3 consider whether there is a need to clarify the responsibility for dealing with computer-related fraud, to ensure that all necessary information is gathered and is accessible, as necessary. Implementing a dedicated organisation responsible for the investigation of all computer-related fraud in Cyprus is a possible solution;

R4.3.4 ensure the DSA has the capabilities and resources necessary to deliver its new cross-sector regulatory role for the CI. Continuously evaluate its resources and capabilities, and use the results to implement improvements and allocate resources;

R4.3.5 develop a mechanism that enables the exchange of information and good practices between prosecutors and judges, to ensure efficient and effective prosecution of cybercrime cases;

R4.3.6 develop law-enforcement strategies for cybercrime-prevention measures alongside enforcement measures. Use intelligence to support proactive investigation; and

R4.3.7 implement frequent reviews of the institutional capacity of the court system to conduct cybercrime cases, to inform necessary revisions.

FORMAL AND INFORMAL CO-OPERATION FRAMEWORKS TO COMBAT CYBERCRIME

R4.4.1 Develop and regularly assess the effectiveness of frameworks for collaboration between law enforcement and the private sector. This should include regular

reassessment and adaptation, to take account of new technologies and emerging forms of cybercrime;

R4.4.2 implement regular assessments of the relationship between government actors, prosecutors, judges and law enforcement, and use the results to enhance the effectiveness of these relationships; and

R4.4.3 continue to build bilateral and multilateral agreements of co-operation in relation to cybercrime investigation. Also, continue to participate in international initiatives to develop improved international co-operation mechanisms.

DIMENSION 5
STANDARDS AND TECHNOLOGIES

This *Dimension* addresses the effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The *Dimension* specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

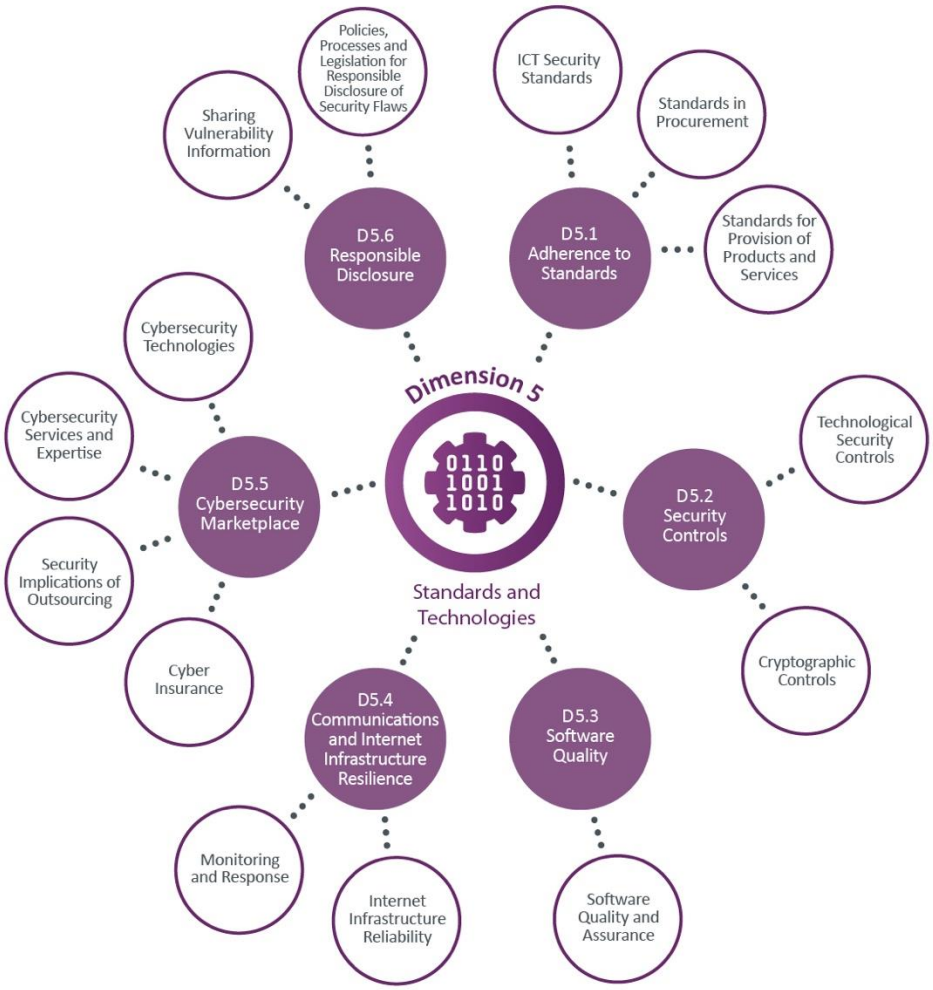

Figure 10: Factors and aspects examined in Dimension 5.

D5.1 ADHERENCE TO STANDARDS

This Factor *reviews the Government's capacity to promote, assess implementation of, and monitor compliance with international cybersecurity standards and good practices.*

***Stage*: Formative to Established**

Since the 2017 CMM review, Cyprus has achieved significant structural reforms that will pave the way for the adoption of security standards in all CIs and the Government. The Cyprus Organisation of Standardisation (*Κυπριακός Οργανισμός Τυποποίησης*),[93] where both private and public organisations can refer to for accreditation to ICT standards, is now complemented with new capabilities offered by the DSA.

Through legislation, the DSA has been given the mandate to act as the national cybersecurity certification/accreditation authority (NCCA), aligning with the certification practices described in the EU Cybersecurity Act. The DSA has started a pioneering project named B4C, which aims to build up the cybersecurity certification capabilities of Cyprus, with a focus on the newly published EU cybersecurity certification scheme on Common Criteria. Next year, three cloud pilots will enable the project to further test the EU cloud certification scheme, which is still under development. For the purpose of B4C, a dedicated Conformity Assessment Body (CAB) from Cyrus has already been certified to offer cybersecurity certification services and has partnered with a French laboratory.

As EU cybersecurity certification schemes are a novel endeavour by the EU, to change the market needs for cybersecurity products and services, Cyprus is one of the pioneers gaining experience in EU certifications. Experts from Cyprus transfer knowledge acquired from the B4C project, by assisting other countries to create the required structural entities and obtain certification capabilities. Participants acknowledged that as a small country, Cyprus does not usually lead activities in Europe nor assist other countries. Such an experience, therefore, highlights Cyprus's potential in cybersecurity, as the forecaster of changes in the certification arena, and this pioneering work in providing EU certificates may place Cyprus in a unique position to respond to the EU's market needs.

Regarding the application of ICT standards, there is a stark difference between the public and private sectors. In the public sector, participants noted that despite efforts from DITS, the Government does not comply with internationally recognised standards. Minimal security requirements exist across all departments, with guidelines that focus on password security, Active Directory usage and anti-virus protection. These minimal controls, which form a basic standard, follow ISO 27001 to a certain extent but are not applied uniformly to all ministries. Participants painted a rather bleak picture, as the tailored ICT security standards are only recommended and advertised by DITS; they are not mandatory. Consequently, many ministries tend to implement them as they see fit, resulting in varying degrees of compliance across government. The lack of accountability for employees in cases of policy misuse,

[93] http://www.cys.org.cy/el/

financial constraints, as well as limited human resources, are the main reasons for the poor cybersecurity posture of the public sector. Participants suggested that the new structure of the Government will provide an opportunity to break silos between ministries, and enforce security standards horizontally across government. The DSA framework, which is mandatory for all CIs, will be another decisive step in improving the public sector's cybersecurity posture.

The private sector is much more advanced regarding the design, adoption and audit of standards for ICT security. The rate of adoption varies between sectors, but the majority of CI organisations comply with internationally recognised standards, such as ISO 27001 and NIST Cybersecurity. Companies operating in the finance sector, as well as ISPs, are considered to be the most mature in compliance with ICT standards, as there exist strict legal and regulatory security requirements in these sectors. In the banking sector, there are frequent audits for compliance conducted by the Central Bank, which holds the role of regulator. There is a combination of international standards, such as the Payment Card Industry Data Security Standards (PCI DSS)[94] for data security, and others imposed by MasterCard[95] and Visa,[96] which are strictly followed by banks. The newly developed EU Digital Operational Resilience Act (DORA) is another legislative proposal to which the banking sector will need to adjust. The ISPs follow regulations and standards that derive from EU legislation, as well as ISO 27001 and standards on business continuity. The introduction of 5G poses ISPs with a significant challenge as new regulatory requirements to secure such critical services have already been published. Cyprus, through the DSA, has participated in ENISA's efforts to develop guidelines for 5G and closely monitors developments in this field.

Other sectors such as energy, water supply and aviation comply with the standards and EU regulations pertinent to their sector, some of which contain elements of ICT security. However, participants recognised that CIs in these sectors should try to comply with international security standards. Furthermore, all CIs need to comply with Decision 389/2020, which includes 70 specific measures inspired by international standards such as ISO 27011 and NIST cybersecurity framework. The legislation includes a detailed mapping of the 70 measures to the international standards. Regarding non-CIs and SMEs, the recent ransomware attacks which have affected numerous companies in Cyprus have resulted in better awareness of the need to comply with ICT security standards. However, as participants mentioned, the driving force for adherence to standards is market demand and business needs. As they lack motivation and skills to identify which standards are appropriate to their needs, the majority of non-CIs and SMEs still do not, therefore, follow ICT security standards strictly.

The DSA, following the NIS Directive, has constructed a baseline of security controls based on best practice and international standards. The newly developed DSA framework must be followed by all CIs, as prescribed in legislation, and it has the potential to institutionalise adherence to standards in all CIs, including the Government. As the DSA acts as the Government entity that assesses the use of standards across private and public sectors, all structural reforms are in place. Participants were hopeful that once audits have been conducted by the DSA, all those members of CIs and government who currently lack the

[94] https://www.pcisecuritystandards.org

[95] http://www.mastercard.com/sea/consumer/standard-mastercard.html

[96] https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf

experience and incentive to apply ICT standards within their organisation will be forced to comply.

Vertical guidelines need to be developed by the DSA that will incorporate security requirements into standards tailored for each sector. There are some sectors, such as energy and telecommunications, for example, where recent market developments (changes in energy retailing, with smaller companies acting as brokers and energy providers) or emerging technologies (5G), have led to the introduction of new software and hardware that need to be secured. It was further mentioned that a lighter version of the DSA framework, equivalent to UK's Cyber Essentials scheme, will provide guidance to SMEs and non-CIs. The DSA has the capacity to bridge the gap in ICT security standards, by providing standards that are tailored to SMEs and which raise awareness of the necessity to adhere to them.

Regarding procurement, there are strict standards in the public sector, but with scarce reference to security requirements. These strict standards add to bureaucratic strains and time-consuming processes, causing staff to circumvent them, in many cases, by buying personal IT-related gadgets and hardware, which further complicates the IT environment that needs to be secured. On the other hand, the private sector, and CIs in particular, have developed standards that consider security and which have specific outsourcing guidelines for cloud services. Regarding software, there were only scattered references to organisations that have developed in-house software. In most cases, there was a lack of standards and policies for the secure development and monitoring of software.

The EU Cybersecurity Act is the cornerstone for the creation of cybersecurity certification schemes for products and services. Such schemes, created by ENISA with the assistance of *ad-hoc* working groups comprising experts in the field, will entail references to standards and provide guidelines based on best practice. Therefore, as Cyprus is a pioneer explorer in the implementation of the Cybersecurity Act, it will be in a unique position to lead the adherence to standards for the provision of products and services. Currently, participants suggested that there exist core activities and methodologies for quality assurance and general guidelines for the provision of cloud services.

D5.2 SECURITY CONTROLS

This Factor *reviews evidence regarding the deployment of security controls by users and public and private sectors, and whether the technological cybersecurity control set is based on established cybersecurity frameworks.*

***Stage*: Formative to Established**

It comes as no surprise to learn that the degree of adoption of security controls in Cyprus resembles the adherence to standards situation, therefore, it varies across sectors and organisations. Participants suggested that the implementation of security controls in

government bodies, despite recent improvements following initiatives from DITS,[97] is elementary and inconsistent across ministries. Constraints in budget, mismanagement of human resources and the lack of appropriate organisational structure, are the main reasons why government lags significantly in cybersecurity posture.

In co-operation with third parties, DITS has recently developed a Governmental Unified Network (GUN),[98] to offer an air-gapped environment for all ministries. The GUN is well-monitored with SIEM tools, vulnerability scanning occurs frequently, and secure configurations are propagated across the network. Furthermore, DITS informs ministries about which secure procedures they need to adhere to. Most departments utilise the services offered by DITS, however, as each ministry possesses its own IT team, following DITS recommendations (i.e., on Active Directory, password policy) is at the discretion of the ministries. Participants admitted that in certain cases, the GUN is made impractical because of restrictions in the types of applications that can be used, or the websites that can be visited. Therefore, in order to continue their working routine, employees try to circumvent the GUN and the security controls offered by DITS, introducing risk to the whole government infrastructure. Furthermore, there are laptops and Internet of Things (IoT) devices that are plugged into the government network without being registered, rendering any effective inventory of devices and software impossible.

Participants raised concerns about the current organisation of government structure, which impedes DITS from obtaining situational awareness, allows employees with their current practices to introduce vulnerabilities and lowers the effectiveness of the security measures of the GUN. They further opined that the parliamentary network – it is not currently considered a CI – is vulnerable to attacks. Moreover, they were of the opinion that a government SOC, which could also monitor the Parliament's network, is long overdue; DITS may monitor for incidents but its detection capabilities are limited. Finally, CSIRT-CY informs DITS and other governmental CIs of vulnerabilities, but the other ministries' IT departments (that are not currently considered critical) do not have access to the same information.

If applied appropriately, the security framework developed by the DSA, and mandatory for all CIs, will ensure that the cybersecurity posture of the public sector will mature. Moreover, participants were optimistic that with the new structure, where all cybersecurity services of the Government are under a single (deputy) ministry, structural issues that create siloed approaches to security with varying degrees of compliance to controls, will cease to exist. However, they admitted that acquiring people with the appropriate skills to equip the newly developed ministry is a rather difficult task, given that the public sector cannot offer competitive salaries. As an example, they pointed to the recently established position of CISO within the Government which remains vacant. It is worth noting that the presence of three members of the Parliament in the review process demonstrates the political will to enhance Cyprus's maturity in cybersecurity, especially in government, by supporting all necessary legislative and structural reforms.

Regarding the training of employees, participants mentioned that in the last few years, newly recruited employees have received basic training in cybersecurity. A limited number of

[97] https://dits.dmrid.gov.cy/dmrid/dits/dits.nsf/home/home?opendocument
[98] https://solutions.logicom.net/news-events/governmental-unified-network-project/

phishing campaigns were run by DITS, to raise awareness, but due to procurement technicalities, such services are difficult to acquire. Similar issues prevent DITS from procuring appropriate penetration-testing services. Of particular concern is the lack of evaluation metrics for determining the effectiveness of the existing security controls. This is due to the fact that monitoring practices, which might allow such evaluation, are elementary; also, penetration testing is not performed regularly, and detection capabilities are limited. Finally, participants recognised that DITS relies on a handful of people for IT and security requirements, and these people are overwhelmed by their daily tasks; many IT employees, meanwhile, are misplaced in different roles across the ministries.

Finally, the Government is currently considering the acquisition of a number of cloud services. Participants voiced concerns that decisions are made without a clearly defined framework to assess the risks of such a migration of services, nor clear SLAs. They believed that the current mindset considers outsourcing of services to the cloud as transferring the risk from cyber-attacks to the cloud provider. This perception is flawed, and any outsourcing decision should be driven by risk assessments and clear protocols that will ensure that oversight of all services, and that data remains within the Government.

In the private sector, there is an understanding that most organisations that are enlisted as CIs implement appropriate security controls tailored to the services they offer. The finance sector and ISP companies were reported to be the most mature, with SOCs developed in-house, specialised personnel monitoring networks, and strict security policies for their staff. The SOCs offer 24/7 coverage and run frequent vulnerability and configuration scans. Most organisations adopt practices for monitoring the effectiveness of controls, following guidance from the SANS Institute[99] for their KPIs. In the banking sector in particular, companies are obliged to adhere to specific standards (e.g., PCI DSS), which enforce strict security controls. Participants suggested that over the last ten years, the banking sector has been transformed, increasing its maturity in security so as not to be excluded by the market. The telecommunications sector, due to EU legislation, has also implemented appropriate security controls, greatly improving its security posture. All ISPs are in a position to protect customers by applying DDoS prevention measures and provide clients of interest with reports regarding vulnerabilities in their infrastructure. Due to the development of 5G networks, there are specific controls that need to be applied and participants deemed that Cyprus, given its contribution to the ENISA's toolkit on 5G, is well-equipped to secure such systems.

There are also organisations that have decided to outsource security to third parties, especially for SCADA systems or essential services. Such cases exist in the water supply sector, and in aviation. Participants warned, however, that outsourcing such services should be considered with caution, as the perception of transferring IT risk to a third party through outsourcing is wrong. It was mentioned in the consultations that there are protocols in place which define SLAs that are appropriate for the security and continuation of services. Regarding the energy sector in particular, the current SCADA systems are deemed secure and well-protected. However, recent developments in the energy market, with the introduction of small companies that act as brokers, or offer energy to consumers, and the new metering systems required, will require that sector to identify appropriate security controls. It is alarming that certain companies in this sector, although they employ SIEM tools, lack the

[99] https://www.sans.org/blog/cis-controls-v8/

expertise to use such tools to their full potential. Therefore, particular vertical frameworks should be developed by working teams, as well as specialised training in cybersecurity for IT employees and security analysts.

Participants concurred that during the last ten years, the majority of organisations in the private sector, including SMEs, have improved their cybersecurity posture. This positive change is driven in part by legislation, but the main driving force has been the ransomware attacks that started to target Cypriot companies in 2015 and which have been increasing in frequency and impact since then. Organisations, and especially SMEs, which have experienced cyber-attacks realise that security is not an unnecessary cost and have invested in basic security controls. To understand the current level of cybersecurity posture, the DSA has conducted a survey, gathering information from several organisations on the perceived risks that they face from cyber-attacks, the impact that these attacks may have on their services, and the investments in controls that they have made. Results of the survey are not finalised yet, but a large number of organisations declared that they need guidance in applying security controls, rendering the creation of a set of baseline controls that they could easily follow a priority. In consultations during the review, participants verified these preliminary findings, adding that there is lack of cybersecurity expertise in most companies and a shortage of skilled personnel in the market. They deemed that awareness campaigns should target younger generations, in an effort to attract young talent into Mathematical Physical and Life Sciences (MPLS) related studies.

The use of cryptographic controls is evident both in the public and private sectors. In the public sector, cryptographic controls are applied to data at rest and, in a number of cases, to data in transit (as in the GUN, for example). There is updated legislation on how to handle sensitive information, with provisions for cyberspace, which has improved the way in which employees process sensitive documents online. We were not able to establish if communications between different departments that occur outside the GUN are encrypted. The practice of evading the GUN, as well as of purchasing laptops outside the procurement frameworks for work-related purposes, may result in unencrypted devices and back-up systems being used. Regarding the private sector, encryption controls are applied in critical systems both for data in transit and data at rest. Certain sectors have their back-up systems encrypted as well. We were not able to establish if organisations follow best practice and encrypt all devices in their inventory.

D5.3 SOFTWARE QUALITY

This Factor *examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this* Factor *reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the critical nature of services.*

***Stage*: Formative to Established**

There is evidence that organisations in both the public and the private sectors try to develop an inventory of secure software. In the public sector, there are white-listed applications and softwares that are allowed to access the GUN. Such a security measure is the reason why, in several cases, employees will try to circumvent the GUN by using WiFi options from other Internet providers. The Government remains ignorant of software run on personal laptops or devices that are not connected to the GUN. Regarding patching, software updates are performed automatically through DITS, which centralises and provides the executable files. For certain servers and systems in ministries, however, local IT administrators are responsible for ensuring software is up to date. There is not, therefore, an holistic picture of systems that run vulnerable versions of software within the Government network.

In a similar vein, participants explained that private organisations maintain up-to-date inventories of white-listed software and applications. Most mature organisations will routinely perform vulnerability scans and patching. For organisations that are not part of the CI, participants deemed that controls for patching rarely exist and *ad-hoc* lists of secure software are scarce. Particular attention should be paid to IT companies that provide services to CI stakeholders. It was not clear from the review whether such stakeholders are included in the list of critical providers, nor if they follow software quality and assurance best practice.

Focusing on software development, the majority of the participants noted that their organisations depend heavily on software purchased from multinational companies. There are cases where software is developed in-house, but it is mainly for internal use rather than customer-facing applications. When software is purchased, many organisations reported that during the procurement phase, they use internal procedures to check the security of software. There were participants who described a different situation in certain critical sectors, such as energy and water supply. Despite the acquisition of critical software from energy and water companies, there were no specific procedures in place to assess the security of these systems, and companies perform penetration tests retrospectively. Therefore, guidance from the DSA is needed to develop the appropriate procedures for software assurance. Regarding the in-house development of software, even though it is mainly for internal use, participants mentioned that in the private sector, there are strict procedures for software development which include security requirements. Conversely, in the public sector, there are references for software development without clear secure polices or practices on secure software design. There is a ticketing system for employees to report bugs and malfunctions that occur in in-house software. It is important that the public sector, and especially organisations in the energy sector, implements clear processes for secure software development.

D5.4 COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

This Factor *addresses the existence of reliable Internet services and infrastructure in the country, as well as rigorous security processes across private and public sectors. Also, this* Factor *reviews the control that the Government might have on its Internet infrastructure and the extent to which networks and systems are outsourced.*

***Stage*: Established**

Participants estimated that the Internet infrastructure in Cyprus is stable, with reliable services which are widely used. Cyprus's ISPs offer 100 percent coverage of broadband in a variety of major technologies (FTTP, FWA, LTE and satellite), according to the DESI connectivity report.[100] Cyprus is one of the leading countries in the EU in offering Next Generation Access (NGA) technologies, which deliver download speeds of at least 30 Mbps. However, when Very High-Capacity Network (VHCN) is considered, Cyprus does not fare well, providing only ten percent coverage. Regarding households with fixed broadband, more than 80 percent use such services, rendering Cyprus a country with one of the highest take-up rates in Europe. Speeds offered to households are average, as Cyprus is one the last countries in EU to have households with speeds of at least 100 Mbps (less than ten percent). Mobile broadband is developing fast and is considered complementary to fixed broadband, and Cyprus has more than 120 subscriptions per 100 people.

Regarding 5G, according to the DESI report,[100] Cyprus did not assign any 5G spectrum, nor did it run any exercises until March 2020. However, the 5G spectrum license was concluded in January 2021 by the Department of Electronic Communications, and the 2 largest mobile operators are already offering 5G services. Recently published legislation regarding 5G cybersecurity[101] features specific, strict requirements for implementing related standards. Any 5G provider, including those offering 4G technologies, must comply with standards that relate to equipment as well as services.

A national-level risk assessment has been carried out on the cybersecurity of 5G networks in Cyprus and an Action Plan is prepared. Under this Plan, legislation for 5G cybersecurity has been developed and released, and actions are assigned for the implementation of the EU Toolbox of Risk Mitigating Measures for the Cybersecurity of 5G Networks. Providers must submit declarations of conformity to these standards to the relevant authority, and periodically, at intervals not exceeding two years. Participants mentioned that ISPs in general undergo strict audit controls and also need to comply with EU legislation on telecommunications. Therefore, there exist Internet Exchange Points (IXPs) that guarantee resilience of the Internet service, redundancy systems for continuity, and detailed policies for handling incidents. Such polices were tested a few years ago, when one of the three cables providing Internet access to the nation was taken offline. Given the seriousness of the incident, only a small number of households experienced unavailability of services for a short

[100] https://digital-strategy.ec.europa.eu/en/policies/desi-connectivity
[101] https://dsa.cy/wp-content/uploads/Decision-408-2020.pdf

period of time, before they returned to normal. Participants further mentioned that ISPs offer protection from DDoS, and certain customers are offered vulnerability scans of their systems.

D5.5 CYBERSECURITY MARKETPLACE

This Factor *addresses the availability and development of competitive cybersecurity technologies, cyber-insurance products, cybersecurity services and expertise, and the security implications of outsourcing.*

***Stage*: Formative**

The domestic market for cybersecurity technologies is rather limited. Participants explained that Cyprus is a small country and the majority of cybersecurity products that organisations use derive from well-established, multinational organisations, which are very hard to compete with. There are a handful of Cypriot organisations which offer SIEM tools (participants mentioned Odyssey[102] and ADITESS[103]), which are fairly popular in Middle Eastern countries. It is difficult for a Cypriot company to offer cybersecurity products locally, as there is limited trust in their capabilities. A characteristic example is the CYNET academic CSIRT, which has developed tools for universities. Despite offering these tools free of charge, stakeholders showed limited interest in assessing or using these tools in their networks.

On the contrary, cybersecurity services are regularly offered to the private and public sectors by consultancy firms ("the Big Four"[104]). Such services usually entail risk management and penetration tests. There are also companies which acquire services from Managed Security Service Providers (MSSPs), thus relying on third parties to monitor and detect cyber attacks on their networks. Such cases were reported in the energy, aviation and water supply sectors. Furthermore, Cyprus has accredited Trust Service Providers (TSPs) which offer electronic signatures, timestamps, and qualified website authentication certificate (QWAC); however, take-up of these is extremely low. With the exception of stock market exchange, where the use of qualified trust services (QTSs) was mandated, and rare cases in the banking sector, where organisations voluntarily apply them, there are no other actors which benefit of QTSs. Participants suggested that there will be developments with all eIDAS-related[105] services through legislative action.

Finally, Cyprus provides an increasing number of e-government services (mainly tax declaration and social insurance transactions through the Ariadne portal[106]) and participants referred to Greece as an example to follow. They explained that within a short timeframe, Greece has managed to rapidly increase the number of e-services it offers, has created a

[102] https://www.odysseycs.com/
[103] https://aditess.com/main/
[104] The 'Big Four' are Deloitte, KPMG, Ernst & Young and PriceWaterhouseCoopers.
[105] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
[106] https://eservices.cyprus.gov.cy/EN/Pages/Home.aspx

dedicated website equivalent to “gov.uk”, and has taken advantage of the COVID-19 restrictions to increase the uptake of all of these services. Finally, participants mentioned that Cyprus has not yet got an electronic ID which, once it is introduced, may facilitate the uptake of online services.

Participants deemed that there will be government initiatives to incentivise the cybersecurity market in Cyprus, as there are dedicated thematic areas with specific actions and budget in the national cybersecurity strategy through public private partnerships (see, for example, the CYberSafety project, which includes both public and private sector partners[107]). Given the concerns that participants voiced on budget restrictions, and the hesitance of local organisations to utilise local technologies, it will be challenging to motivate the market towards sovereign tools that can be used in essential services. Recent examples, such as the development of sensors for monitoring networks, a project undertaken by CSIRT-CY in collaboration with academia, the cyber-range platform for national exercises and the early-warning platform that will automate vulnerability sharing amongst CIs, may create the impetus needed for more projects to follow.

Cyprus is leading initiatives and has acquired expertise in the area of cybersecurity certification schemes. Such schemes may become vehicles for accelerating developments in the cybersecurity market, as Cyprus will have the opportunity to offer CAB services in the EU market for all future EU schemes. The DSA has closely followed developments in the certification area, based on the Cybersecurity Act, and has participants contributing to working groups that develop the future EU cybersecurity certification schemes. Cyprus has already adopted its certification structure to capture Cybersecurity Act requirements and participates in a pilot project exploring how the new certification scheme, namely EU CC, will be deployed and implemented in EU. The certification authority has identified the necessary CABs that will handle certification requests and will be in a position to evaluate EU CC services and products in collaboration with local or external accredited laboratories. There are plans in place to collaborate on cloud schemes and, potentially, 5G, with Ireland and the accreditation of current CABs with 17065 standard.

Regarding the outsourcing of services, participants mentioned that in the private sector, there are risk assessment processes in place, with specific focus on assessing the need for cloud services. There are strict procurement procedures in place and cloud providers need to comply with security requirements. In the public sector, participants mentioned that there the transfer of services to the cloud is being considered. Many employees are of the opinion that they transfer risk at the same time which, according to participants, is erroneous. Further concerns were raised regarding the visibility of data from DITS, and also the possibility of creating a future government SOC because cloud providers consider data held on their servers as theirs, making it difficult to monitor that data.

Small improvements have been made to the cyber insurance market in Cyprus since the 2017 review. Participants mentioned that there are products provided by foreign insurance companies; however, they suggested that these products are not adaptive to emerging threats and the dynamic nature of incident response. They further noted that the premium prices are unaffordable, especially since the COVID-19 pandemic. Finally, they mentioned that there are no reductions in premiums if a company demonstrates a cybersecure behaviour over a period of time. The majority of the cyber policies are therefore purchased by banks and ISPs.

[107] https://www.cybersafety.cy/partners-en.

D5.6 RESPONSIBLE DISCLOSURE

***Stage*: Formative to Established**

This Factor *explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors, and whether there is sufficient capacity to continuously review and update this framework.*

Since the inception of CSIRT-CY, sharing information about vulnerabilities amongst CIs has significantly improved in Cyprus. There are formal agreements with all the constituencies that participate in CSIRT-CY's cyber-threat intelligence network which mandate the disclosure of incidents and vulnerabilities, as per the NIS Directive. CSIRT-CY has developed incident-disclosure practises, as well as protocols to address incidents within given timeframes, according to their severity. Furthermore, there are multilateral agreements at an EU level for sharing information, and Cyprus is an active member of the EU CSIRT network, as well as an active participant in the sharing of information for cyber crisis management within Europe. The DSA has also signed bilateral agreements[108] on information-sharing with a number of countries such as Israel, Romania and Poland.

CSIRT-CY endeavours to instil a culture of trust amongst all CIs and acts as a hub for cyber-threat intelligence. Emails containing indicators of compromise (IOCs), advice on how to address vulnerabilities, and security alerts are sent on a daily basis to all its constituents. Participants indicated that CSIRT-CY relies on the organisations to act and does not have the mandate to oversee if the vulnerabilities are addressed. It was recommended that CSIRT-CY be enabled to set thresholds on how fast organisations should respond to its security advice, and to follow up where critical recommendations for the security of systems are neglected. Currently, the DSA is co-operating with academia to design a new threat-intelligence platform that will automate vulnerability disclosure practices, and will provide early-warning alerts. Such a system has the potential to inform future EU cybersecurity certification schemes about vulnerabilities (the main requirements in all new EU schemes will be vulnerability disclosure and patching), and to increase cybersecurity hygiene for related products and services. Participants further suggested that the creation of sectorial CERTs will boost vulnerability sharing and ensure that information critical for specific sectors will be available to all the appropriate constituents, without flooding organisations that operate in other sectors with unnecessary information.

Considering responsible disclosure of security flaws, participants acknowledged that many organisations provide incentives for bug detection by offering bug bounties that encourage disclosure. For the public, there are channels to report incidents to the police, and the CYberSafety hotline, but legal protections for whistleblowers are still absent. Participants mentioned that this gap will be addressed in the following months, as there is legislation pending in the House of Representatives.

[108] https://dsa.cy/en/mou-dsa-incd/

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Standards and Technologies*, the following set of recommendations are provided to Cyprus. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1.1 Create a standard for the Government and enforce its compliance, or ensure that international standards are followed. The standard can be similar to the DSA's framework;

R5.1.2 monitor compliance with the DSA's standard for CIs through regular audits, and enable regulators so they can request adherence to specific standards for sectors that are less mature (i.e., energy, water, health);

R5.1.3 develop vertical standards for every sector, with emphasis on those where emerging technologies are introduced and novel systems are implemented in essential services;

R1.5.3 develop standards for non-CIs and SMEs that will provide guidelines for implementing basic cybersecurity controls. These standards may be adjusted to form a certification scheme;

R5.1.4 consider the development of standards in procurement that will include security requirements, and ensure that staff will not circumvent current policies;

R5.1.5 develop security standards for outsourcing of products and services;

R5.1.6 consider the development of standards for software development that is created in-house;

R5.1.7 ensure Parliament is part of the CI list so that it adheres to the DSA standard; and

R5.1.8 create procurement processes that will allow the Government to conduct the appropriate penetration testing and run awareness campaigns.

SECURITY CONTROLS

R5.2.1 Consider developing SOCs in CIs that currently do not employ such services, or encourage CIs to outsource such services;

R5.2.2 develop an SOC for the government network, and ensure it covers the Parliament networks.

R5.2.3 develop sectorial CERTs (maritime, in particular) and request that SMEs and non-CIs participate in sharing threat intelligence in some capacity;

R5.2.4 consider collaborating with EU countries, to create joint SOCs;

R5.2.5 design controls for sectors where emerging technologies are introduced;

R5.2.5 design metrics to assess the effectiveness of controls provided by the DSA framework;

R5.2.6 develop a lightweight version of baseline controls for SMEs to follow, and design metrics to assess the effectiveness of these controls;

R5.2.7 develop guidelines for assessing security controls in the public sector;

R5.2.9 develop cybersecurity exercises where CIs from different sectors can participate; and

R5.2.10 create a framework with cloud providers and third parties, for use by SLAs, for all services offered in CIs.

SOFTWARE QUALITY

R5.3.1 Develop a framework for monitoring software quality both in the public sector and in Cis;

R5.3.2 develop standards for procuring software for critical sector; and

R5.3.3 ensure CSIRT-CY has a good overview of the vulnerability scanning of CIs, including systems and software acquired by third parties.

COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

R5.4.1 Create exercises at a national level, for ISPs, and include 5G technologies;

R5.4.2 ensure that legislation for 5G is adhered to by ISPs; and

R5.4.3 create metrics for the assessment of controls for 5G.

CYBERSECURITY MARKETPLACE

R5.5.1 Establish risk assessments for outsourcing of services, and create SLAs to guide this process;

R5.5.2 create business continuity processes for the Government;

R5.5.3 create R&D projects in cybersecurity through public private partnerships, with an emphasis on creating tools that can be utilised by CIs and CSIRT-CY to monitor networks and detect attacks;

R5.5.4 start testing security tools developed by local organisations, for adoption by sensitive services, to ensure the sovereignty of those tools;

R5.5.5 promote the use of qualified trust services, especially in Cis;

R5.5.6 develop e-government services, consider a national electronic identity, and enable the adoption of eIDAS services to boost the cybersecurity market; and

R5.5.7 continue to monitor EU cybersecurity schemes and provide certificates for the EU marker, when EU schemes become available.

RESPONSIBLE DISCLOSURE

R5.6.1 Create awareness on the channels provided for responsible disclosure;

R5.6.2 legislate provisions for whistleblowers; and

R5.6.3 enable CSIRT-CY to follow up vulnerability issues discovered in Cis, and ensure that patching is implemented when available.

ADDITIONAL REFLECTIONS

The level of stakeholder engagement in the review was good, and the representation and composition of stakeholder groups was, overall, balanced and broad. This enabled the review team to collect comprehensive evidence to support this CMM review.

APPENDICES

METHODOLOGY - MEASURING MATURITY

Deploying the CMM involves data-gathering both through in-country stakeholder consultation (typically over the course of three days) and remotely through desk research. It is designed to produce an evidence-based report which is submitted to the government representatives for the country being studied and will include recommendations to:

- benchmark the maturity of a country's cybersecurity capacity;
- provide a detailed a set of pragmatic actions to contribute towards the advancement of cybersecurity capacity
- identify maturity gaps; and
- identify priorities for investment and future capacity-building.

During the review of a country, specific dimensions are discussed with relevant groups of stakeholders. Each group of stakeholders is asked to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 'Cybersecurity Culture and Society' and Dimension 3 'Building Cybersecurity Knowledge and Capabilities' of the CMM.

Data collection

The Review Team gathers the evidence necessary to identify the stages of maturity across the CMM through desk research, in-depth interviews, and modified-focus group discussions, utilising the CMM Structured Field Coding (SFC) Tool to capture the results. The functions of the Review Team include that of a facilitator to lead the group sessions, and a note-taker.

The CMM uses a **modified focus-group discussion methodology** that elicits data that complements and helps validate in-depth interviews and desk research.[109] As with interviews, focus-group discussions are an interactive methodology with the advantage that during the process of collecting data, diverse viewpoints and conceptions can emerge as participants follow the discussion. Rather than posing questions to specific participants, the researcher(s) facilitate a discussion among the participants, encouraging them to adopt, defend or explain different perspectives.[110] It is this interaction that offers advantages over other

[109] Williams, M. (2003). Questionnaire design. In *Making sense of social research* (pp. 104-123). SAGE Publications, Ltd, https://www.doi.org/10.4135/9781849209434; Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 35-50). SAGE Publications, Inc., https://www.doi.org/10.4135/9781483349008; Richard A. Krueger, R. A., & Mary Anne Casey, M. A., (2009) Focus-groups: A Practical Guide for Applied Research. SAGE Publications, London.

[110] Kitzinger, J. (1994). The methodology of focus groups: the importance of interaction between research participants. Sociology of health & illness, 16(1), 103-121. https://doi.org/10.1111/1467-9566.ep11347023;

methodologies, making it possible for the participants to reach a mutual understanding and to raise everyone's awareness of cybersecurity practices and capacities.[111] During CMM reviews, the Review Team leads the discussion to get onto all the aspects within the relevant dimensions.

To determine the level of cybersecurity capacity maturity, each *Aspect* has a set of indicators corresponding to all five stages of maturity. A consensus method is used to drive the discussions within sessions, for the stakeholders to provide evidence on how many indicators have been implemented by the country and to determine the maturity level of every aspect of the model. During focus-group discussions, researchers use semi-structured questions to keep discussions around relevant indicators. The discussion among stakeholders provides evidence regarding the implementation of indicators. In gauging the maturity level, if there is no evidence for all the indicators being met at a particular stage, then that country has not yet reached that stage of maturity.

Inconsistencies between stakeholders will inevitably occur. Equally, information known to a stakeholder in one sector might not be familiar in other sectors. Accordingly, it will fall to the Review Team to perceive these information gaps and then investigate them.

Desk research and modified focus groups inevitably raise some additional questions and possible inconsistencies. For this reason, and to a gain more in-depth understanding of key and sometimes unique policies and practices, a set of in-depth interviews are also conducted during and on some occasions following the field research.

Data analysis

With the prior consent of participants, all sessions are recorded. Individual responses are treated as confidential with the Chatham House Rule applied in reporting our results.[112] After conducting a country review, the **data collected during consultations** with stakeholders and the notes taken during the sessions are used to find evidence and **define the stages of maturity** for each *Aspect* of the CMM. The CMM report aggregates this information and determines the maturity for each Factor of the CMM.

In the course of the review further desk research is undertaken to bridge any gaps that emerge during the in-country data-collection process and to validate the evidence provided. While drafting the **CMM report**, further desk research and interviews are often necessary to address any missing information, and to validate and verify the results. For example, stakeholders might not always be aware of recent developments in their country, or if the country has signed a particular convention on personal data protection policy. Therefore, official government or ministry websites, annual reports of international organisations, university websites, in-depth interviews, etc. can be used as supplementary sources for information. This type of additional research helps to ensure that the report accurately reflects the Host

Kitzinger, J. (1995). Qualitative research: introducing focus groups. Bmj, 311(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299; Fern, E. F. (1982). The use of Focus Groups for Idea Generation: The Effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality. Journal of Marketing Research, 19(1), 1–13. https://doi.org/10.1177/002224378201900101

[111] Kitzinger, J. (1995). Qualitative research: introducing focus groups. *Bmj*, *311*(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299

[112] https://www.chathamhouse.org/about/chatham-house-rule

Country's cybersecurity capacity. In each case, the team does not privilege any particular source of information but seeks to reach a consensus on the most valid status of each indicator of the model.

Developing recommendations

For each *Dimension*, **recommendations** are provided for the next steps to be taken for the country to enhance its cybersecurity capacity. If a country's capacity for a certain *Aspect* is, for example, at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders. The recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the CMM. The recommendations are provided specifically for each *Factor.*

After a review by the GCSCC Technical Board, the draft report is submitted to the Local Host to secure feedback. If new evidence arises, the draft report is revised and the maturity stages of each *Aspect* and *Factor* in the CMM are updated correspondingly. Once all parties approve the draft report, the Local Host will take the lead in the publication process. Publication approval rests with the Host Country and if this is agreed the Local Host is encouraged to publish it via an official government portal or other outlet.

Data management and ethical considerations

Focus-group discussions are conducted online on Microsoft Teams™ and Zoom™ platforms. *(depending on platforms preferred by each nation)* The discussions are recorded using external recorders to guarantee confidentiality of the data and information collected, and for future transcription for the purpose of writing the CMM report. The recordings remain anonymised. The findings from the desktop study, in-depth interviews, and focus group discussions are consolidated during the analysis.

Global Cyber Security Capacity Centre

Department of Computer Science, University of Oxford

Wolfson Building, Oxford OX1 3QD,

United Kingdom

Tel: +44 (0)1865 287434

Email: cybercapacity@cs.ox.ac.uk

Websites: https://gcscc.ox.ac.uk/home-page#/ www.oxfordmartin.ox.ac.uk/cyber-security