CYBERSECURITY CAPACITY REVIEW

Republic of Cyprus

December 2017

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Dr Maria Bada, Dr Ioannis Agrafiotis

Reviewed by: Professor Paul Cornish, Professor William Dutton, Professor Michael Goldsmith, Professor Basie Von Solms, OCECPR

Approved by: Professor Michael Goldsmith

LIST OF ABBREVIATIONS

BCM	Business Continuity Management
CNA	Cyprus News Agency
CE	Computer Engineering
CEF	Connecting Europe Facility
CEO	Chief Executive Officer
CEPOL	European Police College
CI	Critical Infrastructure
CII	Critical Information Infrastructure
3CE	Cyprus Cybercrime Centre of Excellence
CMM	Cybersecurity Capacity Maturity Model
CNI	Critical National Infrastructure
OCECPR	Office of the Commissioner of Electronic Communications and Postal Regulation
OCPDP	Office of the Commissioner for Personal Data Protection
CSIRT	Computer Security Incident Response Team
CPI	Cyprus Pedagogical Institute
CSE	Child Sexual Exploitation
DDoS	Distributed Denial-of-Service
DEFL	Digital Evidence Forensic Laboratory
DESI	Digital Economy and Society Index
DISA	EU Digital Agenda Scoreboard
DITS	Department of Information Technology Services, Ministry of Finance
DNS	Domain Name Server
DRP	Disaster Recovery Plan
ECDL	European Computer Driving Licence
ECTEG	European Cybercrime Training and Education Group
EMAS	Europol Malware Analysis System
EUCTF	European Union Cybercrime Taskforce
EUROJUST	European Union Judicial Cooperation Unit
FBI	Federal Bureau of Investigation
GCSCC	Global Cyber Security Capacity Centre

GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IoT	Internet of Things
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
IXP	Internet Exchange Point
KPI	Key Performance Indicator
MLAT	Mutual Legal Assistance Treaty
NCB	National Central Bureau (Interpol)
NCS	National Cybersecurity Strategy
NIS	Network and Information Systems (Directive)
NGA	Next Generation Access
NGO	Non-Governmental Organisation
OCECPR	Office of the Commissioner of Electronic Communications & Postal Regulation
OCC	Office for Combating Cybercrime, Cyprus Police
PPP	Public Private Partnership
RFID	Radio-Frequency Identification
SIEM	Security Information and Event Management
SIC	Cyprus Safer Internet Centre
SME	Small or medium-sized enterprise
UCLan	University of Central Lancashire Cyprus
UNCRC	United Nations Convention on the Rights of the Child
VCACITF	Violent Crimes Against Children International Task Force
WIPO	World Intellectual Property Organisation

EXECUTIVE SUMMARY

The Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') was invited to undertake a review of the maturity of cybersecurity capacity in the Republic of Cyprus. The review was hosted by the Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR). The objective of the review was to enable the Republic of Cyprus to gain an understanding of its cybersecurity capacity in order to consolidate the revision of the country's national cybersecurity strategy. This revision aims to mirror the requirements of the EU NIS Directive which entered into force in August 2016, requiring Member States to transpose the Directive into national laws within 21 months of its publication.

Over the period 12-14 July 2017, stakeholders from the following sectors participated in roundtable consultations: public sector entities, academia, civil society, criminal justice sector, policy makers, information technology officers from government and the private sector, telecommunications companies, the banking sector, other critical sectors and international organisations.

The consultations were premised on the Capacity Centre's Cybersecurity Capacity Maturity Model for Nations (CMM). The CMM uses specific language to describe a layered taxonomy, beginning with five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cyber Culture and Society*
- *Cybersecurity Education, Training and Skills*
- *Legal and Regulatory Frameworks*
- *Standards, Organisations, and Technologies*

Each dimension comprises a number of *factors* which, taken together, explain what it means to possess cybersecurity capacity. Factors are further subdivided into *aspects* and for each aspect there are *indicators*, setting out those conditions that define the level of *maturity* achieved in any given aspect. There are five *stages* of maturity, ranging from the *start-up* to the *dynamic*. The start-up stage implies an ad hoc approach to capacity, whereas the dynamic stage is indicative of a strategic approach and the ability to adapt or change in response to environmental considerations. The five stages are defined as follows (see also p.5 below)[1]:

- **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 is an absence of observable evidence at this stage.

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

- **Formative:** Some features of the aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply "new". However, evidence of this activity can be clearly demonstrated.
- **Established:** The elements of the aspect are in place, and working. However, there is not 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's or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter 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). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

Figure 1 below provides an overall representation of the cybersecurity capacity in the Republic of Cyprus and illustrates the maturity assessments 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.

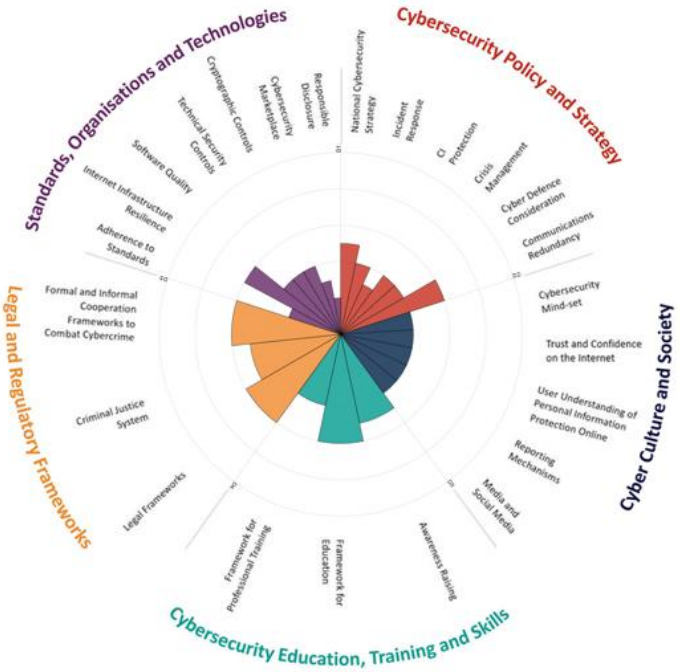

Figure 1: Overall representation of the cybersecurity capacity in the Republic of Cyprus

Cybersecurity Policy and Strategy

Overall, the *policy and strategy dimension* of cybersecurity capacity in Cyprus was gauged to range from *start-up* to *established* stages of maturity.

As far as the National Cybersecurity Strategy (NCS) is concerned, the Republic of Cyprus is at a *formative* tending towards an *established* stage of maturity. Cyprus has had a comprehensive national cybersecurity strategy since March 2013. The mandate for the design, implementation, monitoring and revision of the strategy has been assigned to the Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR). Guiding principles, such as the recognition that a valid strategy must offer multiple levels of security, underpinned the development and implementation of the strategy which highlighted six priority areas, as follows: the creation of a legal framework; the coordination of stakeholders in government; the formulation of technical and organisational measures and procedures; the development of necessary skills in training and awareness; productive collaboration between the public and private sector; and the creation or adaption of necessary structures for incident response. A steering committee comprising stakeholders from the public sector, military, private sector and academia has been formed and is responsible for the design of KPIs to monitor progress on actions and evaluate their impact.

Incident response capacity in Cyprus is at a *formative* stage of maturity. Currently, there is no national computer-related incident response organisation and the authority that serves as the coordinating body for the reporting and management of cybersecurity incidents (only for the government sector) is the government CSIRT (Computer Security Incident Response Team). In addition to this, OCECPR currently receives incident notifications that focus on two key incident types in the electronic communications sector – loss of service availability[2] and breaches of personal data[3]. However, actions are being taken for the development of a National CSIRT, with roles and responsibilities specified as part of a relevant action in the National Cybersecurity Strategy. The country is expected to have an established National CSIRT in the near future (within 2017). The establishment of a National CSIRT would be in line both with the EU NIS Directive and with Action 38 of Pillar III of the Europe 2020 Strategy that incentivises Member States to establish by 2020 a well-functioning, pan-EU network of national-level CERTs. The absence of a national CSIRT in Cyprus means that there is no single entity holding a central registry of national level incidents and that coordination on a national level is ad hoc and depends on personal relations. Currently, OCECPR collects incidents only from electronic communications and internet service providers that are part of Cyprus's critical information infrastructure and from relevant government departments and academic networks.

The protection of Cyprus's critical infrastructure (CI) ranges from *start-up* to *formative* stages of maturity. A list of general critical information infrastructure (CII) assets has been created but has not been disseminated, officially, to all relevant stakeholders, although their

[2] Order 371/2013 on the Notification of breaches of security or loss of integrity of networks and/or services

[3] Order 190/2015 on the Notification of personal data breaches by the operators of publicly available electronic communications networks

designation as CIIs has been communicated to them during the criticality assessment process. Official collaboration with the CIIs will happen in the near future (2017). OCECPR has developed a national level cyber risk assessment methodology based on NIST SP 800-30 and ISO 27005 and guidance from ENISA with additional steps covering the dissemination of information among stakeholders and handling of risk information at the national level. Coordination within CII and between CII owners and the government, in relation to cybersecurity threat and vulnerability disclosure, is currently formal only for the telecommunications sector. For other sectors, such as finance, there are informal channels of communication with scarce reporting of vulnerabilities and incidents. Risk assessment exercises are conducted every two years but do not necessarily include participants from all CII organisations.

National risks and threats have been identified based on a national cyber risk assessment, which was conducted for the first time during 2016. However, the extent to which organisations conduct individual risk assessments or consider cyber threats as part of crisis situations is uncertain. Participants during sessions suggested that CII stakeholders, as well as organisations from the finance sector, hold business continuity plans and depending on the criticality of the system, with exercises being conducted at a local level.

Cyprus's Cyber Defence is at a *formative* stage of maturity. Currently, there is no official cyber defence document although the national defence strategy considers elementary cybersecurity issues. The National Guard handles the military network systems that support the operations of the Ministry of Defence. There is a department in the National Guard that specialises in cyberdefence and is tasked with monitoring activities. The Ministry of Defence is actively seeking collaboration with other countries and specifically with other governmental departments and also foresees an essential collaboration with the National CSIRT that is currently under development.

In the event of a communications disruption, mechanisms are in place to maintain the operational functionality of the national emergency communications network. Current emergency response assets have been identified. Specific CII stakeholders have emergency response assets hardwired into a national emergency plan. ISPs in particular are required to run stress tests frequently.

Cyber Culture and Society

Consultations indicated that Cyprus's national capacity regarding *cybersecurity culture and society* is at a *formative* stage of maturity. The government has recognised the need to prioritise cybersecurity across its institutions. Analysis of risks and threats has influenced the processes and structures across government institutions but in particular in leading agencies. Participants noted that mandatory password update has been introduced, but often lack of personnel leads to shortcuts in security. A general concern was expressed that employees within the public sector do not always follow specific online safety measures such as updating passwords, not sharing passwords etc. The majority of the population use the Internet, but do not understand online risks.

Overall, participating stakeholders accepted that a limited proportion of Internet users critically assess what they see or receive online and consider that they have the ability to use the Internet and protect themselves online. Moreover, a limited proportion of users trust in the secure use of the Internet based on indicators of website legitimacy. Their trust is often blind trust. Although Cypriots are active users of social networks, video calls and online content, they engage in online banking and shopping activities much less than other Europeans. E-government services have been established in Cyprus. The Government continues to increase e-service provision and tax declarations are already being submitted electronically. E-commerce services are fully established by multiple stakeholders.

Users and stakeholders within the public and private sectors have general knowledge about how personal information is handled online but few proactive cybersecurity practices are used, either due to perceived inconvenience or due to the way people weigh up the trade-offs in service and protection of their personal information. Cyprus has adopted and enforced the Processing of Personal Data (Protection of Individuals) Law (N. 138(I)/2001) and is now in the process of implementing the EU General Data Protection Regulation (GDPR). It is expected that the implementation of the new regulation will enhance user awareness and promote understanding of the importance of the protection of personal information online.

In Cyprus both public and private sectors provide some channels for reporting online incidents, but these channels are not coordinated and are used in an ad hoc manner. In 2014 the Office for Combating Cybercrime (OCC) implemented the Cybercrime Reporting Platform and the Cyprus Police Mobile Application that allows the public to report cybercrime online. Additionally, the European CyberSafety project aims to create an awareness platform where stakeholders can find information, resources and tools, as well as share experiences, expertise and good practices. The CyberSafety Hotline 1480 ensures that users can report illegal content. There is ad hoc media coverage of cybersecurity, with some limited information provided and reporting on specific issues that individuals face online, such as cyber-bullying. Social media discussions of cybersecurity are also limited.

Cybersecurity Education, Training and Skills

Cyprus's capacity for *cybersecurity education, training and skills* ranges from a *formative to an established stage of maturity*. Awareness-raising programmes, courses, seminars and online resources are available for target demographics from public and private sectors, academia, and civil society sources. The National Cybersecurity Strategy provides for a systematic approach to cybersecurity awareness, the implementation of which is coordinated by the Office of the Commissioner of Electronic Communications and Postal Regulation. The relevant strategy action includes the development of a national awareness programme, which is under development. Some executives in the private sector may be aware of general cybersecurity issues, but not necessarily how these issues and threats might affect their organisation. Executives in some sectors, such as finance, telecommunications, Internet providers and cloud operators are aware of cybersecurity

risks, and how their organisation deals with cybersecurity issues, but not of the strategic implications.

The need for enhancing cybersecurity education in schools and universities has been identified by leading government, industry, and academic stakeholders. Action 13 of the NCS recognises the need for the development of a suitable workforce, both within and outside the public sector, which will have the necessary technical know-how and experience to implement the provisions of the NCS. A supply of suitably qualified cybersecurity educators is readily available. In Cyprus specialised courses in cybersecurity are offered and accredited at the university level (mainly postgraduate). Universities and other bodies also hold seminars and lectures on cybersecurity aimed at non-specialists. Research and development is an important consideration in education. Universities apply for European and other research funding schemes in order to promote research in the field of cybersecurity. There is a limited budget dedicated to national cybersecurity research. However, participants noted that with the implementation of the NIS directive the budget will be increased.

The need for training professionals in cybersecurity has been documented in Cyprus at a national level. ICT professional certification with some security modules or components is available. Private companies and local chapters of international training and certification organisations such as $(ISC)^2$, ISACA, CISCO, Deloitte, PwC, KPMG and ICIS offer courses on ethical hacking and other topics as well as accreditation. However, at a national level there is currently no strategy for professional qualifications, certification and accreditation. Executive training courses for CEOs or chief financial officers are offered in an ad hoc manner, including topics such as good governance practices related to cybersecurity and risk management.

Legal and Regulatory Frameworks

The *legal and regulatory* frameworks in Cyprus range between *formative* and *established* stages of maturity. The Republic of Cyprus has implemented comprehensive provisions on cybersecurity in its ICT legislative and regulatory frameworks. Specific legislation and regulation related to cybersecurity has been enacted through the following laws: Electronic Commerce Law (156(I)/2004); the Law for the Protection of Confidentiality of Private Communications (92(I)/1996); the Law Regulating Electronic Communications and Postal Services 112(I)/2004, last amended by Law 76(I)/2017; the Legal Framework for Electronic Signatures and for Relevant Matters Law 188(I)/2004 and the Processing of Personal Data Law L.138(I)/2001. The incorporation of the Council of Europe Convention on Cybercrime ("Budapest Convention") into the Republic's national law is also stated in Law 22(III)/2004.

The Processing of Personal Data (Protection of Individuals) Law (N. 138(I)/2001) entered into force in November 2001 to address privacy issues related to collection, storage, processing, dissemination and use of personal data, and was amended by Law N. 37(I)/2003. The Office of the Commissioner for Personal Data Protection (OCPDP) was established in 2002 and deals with the protection of personal information relating to an individual, prohibiting the unauthorised and illegal collection, recording, and further use of such private information.

Comprehensive legislation on the protection of children has been adopted and enforced, through the Law N. 60(I) of 2014 on the Prevention, Fighting against Trafficking in and Exploitation of Human Beings and Protection of Victims. The legal and institutional framework for the protection of children's rights is largely in line with international human rights obligations in this field. In particular, the Fighting of Marketing of Persons and Sexual Exploitation of Minors Law 2000 2(I)/2000 and the Budapest Convention of the Rights of the Child (Ratifying) Law 1990 (No. 243 199) are laws aimed at the protection of children, particularly online.

Comprehensive legislation protecting consumers from business malpractice online has been adopted and is enforced. E-commerce in Cyprus is regulated by the Electronic Commerce Law 156/2004. A lead agency responsible for the protection of consumers online has been designated. The Competition and Consumer Protection Service constitutes one of the divisions of the Ministry of Energy, Commerce, Industry and Tourism. Comprehensive legislation addressing intellectual property (IP) of online products and services has been adopted and is enforced. Cyprus's statutory legislation, regarding Intellectual Property, is based in the English Common Law tradition. Cyprus is also signatory to international conventions relevant to IP.

Substantive cybercrime legal provisions are contained in the general criminal law. The Criminal Code (Ch. 154) comprises a codified version of all main offences and criminal responsibilities. The Criminal Procedure Code is structured to provide support to all significant provisions of the Constitution of the Republic of Cyprus, the European Convention of Human Rights and other international treaties. Cyprus has established agreements with Interpol and Europol on cross-border information sharing. However, the existing legislation does not include specific provisions for incident reporting. The government is working towards the implementation of the NIS Directive and the GDPR in 2018 and as participants noted it is expected that existing gaps in legal and regulatory frameworks will be closed.

Across the criminal justice system in Cyprus, capacities range from a *formative to established* stages of maturity. Digital chain of custody and evidence integrity is established including formal processes, roles and responsibilities. The Office for Combating Cyber Crime (OCC) was established in 2007 based on the Police Order 3/45 and it comprises investigators as well as forensic analysts. Furthermore, the Digital Evidence Forensic Laboratory (DEFL) is under the same administration and is staffed with specialist personnel in the collection of evidence and digital forensic analysis of electronic devices. Within the framework of the Prevention of and Fight against Crime Programme of the European Union, Cyprus was granted funding for the establishment of the Cyprus Cybercrime Centre of Excellence (3CE).

A limited number of specialist cybercrime prosecutors and judges have the capacity to build a case based on electronic evidence, or preside over a cybercrime case. Although training is offered to prosecutors, law enforcement and judges, the uptake of these opportunities is low.

Formal mechanisms of international cooperation have been established to prevent and combat cybercrime. As mentioned above, Cyprus has agreements with Interpol and Europol as well as bilateral agreements with neighbouring countries on cross-border information

sharing. Mutual legal assistance and extradition agreements and mechanisms have been established and are applied to cybercrime cases. The National Cybersecurity Strategy provides scope for using a Public-Private Partnership (PPP) in the prevention of and fight against cybercrime. In addition, informal relationships between government and criminal justice as well as between ISPs and law enforcement exist with clear communication channels enabling the regular exchange of information on cybercrime cases.

Standards, Organisations, and Technologies

The maturity of Cyprus's capacity in *cybersecurity standards, business models and technologies* ranges from *start-up to established stages*. The Republic of Cyprus has established the Cyprus Organisation of Standardisation under the Ministry of Finance. There is a specific branch for information and technology sector standardisation where organisations, both private and public, can turn to for accreditation to ICT standards. The government and the private sector have adopted several ICT security, procurement and software development standards and good practices. However, compliance is not mandatory for all sectors. Regarding the standards related to procurement of hardware, similar conclusions to software procurement can be drawn practices regarding the maturity of the public and private sector.

The maturity of Internet infrastructure resilience was found to be at an established stage of maturity while the security standards in e-services offered by public and private organisations were found to be at a *formative* stage of maturity mostly due to the lack of available resources. Participants indicated that a wide range of e-government services are offered via a system named Ariadni[4]. However, according to DISA[5] the percentage of citizens who interact online with the public sector is one of the lowest in the EU.

Software quality is a matter of concern and requirements in both public and private sectors are identified, but not necessarily in a strategic manner. Focusing on standards in software development, there are guidelines in place in both public and private sectors, but the extent to which these guidelines are related to cybersecurity is not clear.

The adoption of technical security controls in the Republic of Cyprus varies across sectors and organisations. The main technical controls which are implemented in almost every government department are the use of back-ups and antivirus services, along with centralised firewalling, filtering and other network protection measures. Guidelines are available to users detailing how to back-up data stored on their personal devices. However, the majority of employees lack the knowledge to recover these back-ups in emergency situations. Participants stated their concerns over the lack of personnel and the absence of training for existing IT employees. Finally, of concern is the complete absence of evaluation metrics for determining the effectiveness of existing technical controls. The use of cryptographic controls also varies across sectors and organisations. Cryptographic controls in

[4] https://cge.cyprus.gov.cy/re/public/

[5] http://digital-agenda-data.eu/

both public and private sectors are applied to data at rest and in a small number of cases to data in transit. Participants were concerned that email exchange is often conducted unencrypted. It was also noted that users may send sensitive official information from their personal devices using non-governmental email clients. A major difficulty in applying cryptographic controls is the legislation that governs how sensitive information is handled. However, some participants mentioned that their organisations are in the process of encrypting all personal devices.

The domestic market for cybersecurity technologies revolves around services. Consultancy firms (such as Deloitte, PwC, EY and KPMG) regularly offer their services in the private sector, whereas some companies also acquire software and utilise security information and event management (SIEM) systems designed locally in Cyprus or in Greece. The cyber insurance market in Cyprus is in its infancy. There is a small range of products on offer and usually these contain restrictions and specify policies that organisations must adhere to be insurable.

A vulnerability disclosure framework is not in place. Stakeholders mainly share technical details of vulnerabilities informally with other stakeholders who can distribute the information more broadly. But this is not common practice. Currently, organisations establish their own processes and mechanisms for receiving, disseminating and sharing information on vulnerabilities, and only some organisations are obliged to report to OCECPR or the Police.

Additional Reflections

This was the 19th country review supported directly by the Global Cyber Security Capacity Centre at Oxford. This review is intended to assist the Government of the Republic of Cyprus to gain insights into the breadth and depth of the country's cybersecurity capacity. While some dimensions are still in the initial stages of development, the Republic of Cyprus has a thorough plan within its current National Cybersecurity Strategy, as well as following the NIS Directive and has begun the process of developing different aspects of cybersecurity capacity across all five CMM dimensions. If existing efforts in different organisations and sectors are linked and coordinated, budget requirements are met and human resources found, these can form the cornerstone for significant advances in capacity in the future.

These changes may render the Republic of Cyprus the "Estonia of the Mediterranean" as some participants argued during the review. This report suggests a number of specific steps by which the Republic of Cyprus's cybersecurity capacity might achieve greater levels of maturity and which might contribute to the development, among other things, of a national CSIRT and collaboration between private-owned and state-owned organisations that are part of the CII.

INTRODUCTION

The Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') was invited to undertake a review of the maturity of cybersecurity capacity in the Republic of Cyprus. The review was hosted by the Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR). The objective of the review was to enable the Republic of Cyprus to gain an understanding of its cybersecurity capacity in order to consolidate the revision of the country's national cybersecurity strategy. This revision aims to mirror the requirements of the EU NIS Directive which entered into force in August 2016, requiring Member States to transpose the Directive into national law within 21 months of its publication.

Over the period 12–14 July 2017, stakeholders from the following sectors participated in a three-day consultation to review cybersecurity capacity in the Republic of Cyprus:

- Public sector entities:
  - Office of the Commissioner of Electronic Communications & Postal Regulation – OCECPR
  - Department of Information Technology Services, Ministry of Finance - DITS
  - Office For Combating Cybercrime, Cyprus Police - OCC
  - Water supply
  - National CSIRT
  - Government CSIRT
  - Academic CSIRT
  - Ministry of Finance
  - Ministry of Justice and Public Order
  - Ministry of Defence
  - Ministry of Foreign Affairs
  - National Security Authority
  - Cyprus Intelligence Service
  - Ministry of Interior
  - Ministry of Education and Culture
  - Ministry of Transportation, Communications and Works
  - Ministry of Energy, Commerce, Industry and Tourism
  - Ministry of Agriculture, Rural Development and Environment
  - Ministry of Labour, Welfare and Social Insurance
  - Ministry of Health
  - Audit Office
  - Internal Audit Service
  - Office of the Commissioner for Personal Data Protection
  - Fire Department
  - Cyprus National Guard
- Private sector
- Electronic Communications companies and ISPs
- Finance sector
- Academia

- Professional Societies
- Internet Governance
- Operators of Critical Information Infrastructures (banks, civil aviation, merchant shipping, health etc.).

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model (CMM)[6] which is composed of five distinct *dimensions* of cybersecurity capacity.
Each dimension consists of a set of *factors*, which describe and define what it means to possess cybersecurity capacity in a specific functional area. The table below shows the five dimensions with the five dimensions together with the factors of which they are comprised:

DIMENSIONS	FACTORS
Dimension 1: Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2: Cyber Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3: Cybersecurity Education, Training and Skills	D3.1 Awareness-raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4: Legal and Regulatory Frameworks	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5: Standards, Organisations and Technologies	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality Protection

[6] See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

D5.4 Technical Security Controls
D5.5 Cryptographic Controls
D5.6 Cybersecurity Marketplace
D5.7 Responsible Disclosure

ANALYSIS OF CYBERSECURITY CAPACITY MATURITY

Each dimension comprises factors which describe what it means to possess cybersecurity capacity in a given functional area. Factors consist of aspects and for each aspect there are indicators which amount to a set of steps and actions that serve as the criteria by which to judge the maturity of a given aspect of capacity. There are five stages of maturity, ranging from *start-up* to *dynamic*. 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 to changing environmental and other circumstances or change against environmental change. 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 is no observable evidence at this stage.
- **Formative:** Some features of the aspects have begun to grow and be formulated, but may be ad hoc, disorganized, poorly defined – or simply "new". However, evidence of this activity can be clearly demonstrated.
- **Established:** The elements of the aspect are in place, and working. However, there is not 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's or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter 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). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

METHODOLOGY - MEASURING MATURITY

The assignment of maturity stages is based upon the evidence and information collected in the course of a CMM review, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff.

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

In order to determine what stage of maturity a nation is currently placed, each aspect has a set of indicators across all five stages of maturity. The implementation of these indicators has either been completed by the nation or not. Therefore, when reading the model, a nation must conclude whether they have implemented all of the indicators for each aspect. If a nation cannot provide evidence for the implementation of all the indicators at one stage, then that nation has not yet reached that stage of maturity.

In order for the participants to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions participants should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised.

The CMM uses a focus group methodology since it has been acknowledged to offer a rich set of data compared to other qualitative approaches[7,8,9]. Like interviews, focus-groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions will emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives[10,11,12]. It is this interaction and tension that offers the advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained[8].

[7] M. Williams. Making sense of social research. Sage Publications Ltd, 2003.
[8] J. Knodel. The design and analysis of focus group studies: A practical approach. Successful focus groups: Advancing the state of the art, 1:35–50, 1993.
[9] R.A. Krueger and M.A. Casey. Focus groups: A practical guide for applied research. Sage, 2009.
[10] J. Kitzinger. The methodology of focus groups: the importance of interaction be- tween research participants. Sociology of health & illness, 16(1):103–121, 1994.
[11] J. Kitzinger. Qualitative research: introducing focus groups. Bmj, 311(7000):299– 302, 1995.
[12] E.F. Fern. 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, pages 1–13, 1982.

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to the data generated from focus groups[13]. The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use"[10].

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study[14]. The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning[15]. Dey explains that this process categorises data as "belonging together" and presupposes a comparison that crystallises the different perceptions[15].

The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is crafted by the key features and variables of the adopted theory[11]. In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly these novel categories that offer a refined perspective may be neglected. This is the reason why we opt for a blended approach in the analysis of our data, which is a mixture of deductive and inductive approach, instead of a deductive approach guided by the indicators of the model.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the final stages of maturity for each factor of the CMM. We adopt a blended approach to analyse focus group data and use the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a Convention on

[13] K. Krippendorff. Content analysis: An introduction to its methodology. Sage Publications, Inc, 2004.
H.F. Hsieh and S.E. Shannon. Three approaches to qualitative content analysis. Qualitative health research, 15(9):1277–1288, 2005.
K.A. Neuendorf. The content analysis guidebook. Sage Publications, Inc, 2002.

[14] S. Elo and H. Kyng¨as. The qualitative content analysis process. Journal of advanced nursing, 62(1):107–115, 2008.
H.F. Hsieh and S.E. Shannon. Three approaches to qualitative content analysis. Qualitative health research, 15(9):1277–1288, 2005.

[15] I. Dey. Qualitative data analysis: A user-friendly guide for social scientists. Routledge, 1993.
P.D. Barbara Downe-Wamboldt RN. Content analysis: method, applications, and issues. Health care for women international, 13(3):313–321, 1992.

personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is 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.

Using the GCSCC CMM methodology, as set out above, this report presents results of the cybersecurity capacity review of the Republic of Cyprus and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in Cyprus. These recommendations are based on the comments collected during the review as well as on the CMM.

CYBERSECURITY CONTEXT IN THE REPUBLIC OF CYPRUS

Internet usage by Cypriots is at 71.9% in 2017[16] according to figures released by European Internet Statistics. According to the same source, Facebook had 800,000 Cypriot subscribers in 2016 a 67.4% penetration rate.

According to the World Economic Forum report[17] Cyprus scores highly in the development of ICT infrastructure (including mobile network coverage, International Internet bandwidth, secure internet servers and electricity production) as well as the availability of digital content. Additionally, Cyprus scores high in the affordability of accessing ICT, either via mobile telephony or fixed broadband internet, as well as in the level of competition in the internet and telephony sectors that determine this cost.

Cyprus ranks 22nd in the European Union in the Digital Economy and Society Index (DESI) 2017[18]. The evidence from DESI are combined with country-specific policy insights in Europe's Digital Progress Report (EDPR) report which shows progress made in terms of digitalisation by each Member State and providing an important feedback loop for policy-making at EU level. Cyprus showed significant progress in connectivity as shown above. In Cyprus mobile broadband uptake is rising. Conversely, while Next Generation Access (NGA) coverage is progressing, the increase in the take up of broadband is slow, as prices are still relatively high. The delivery of online public services is close to the EU average.

Cyprus has one of the highest percentages of social media users in Europe. No less than 94% of Internet users in Cyprus are Facebook users, and three-quarters of the population use the Internet[19]. It is also a lively marketplace. With Cypriot users being the fifth most active of social media subscribers in Europe, there is a hugely promising audience for the companies who market successfully on Facebook and other social media sites.

Although Cypriots are active users of social networks, video calls and online content they engage in online banking and shopping activities much less than other Europeans. Similarly, companies engage in the use of social media and trade online, but are less prone to take up new technologies such as cloud and RFID.

Despite the fact that internet users engage in a wide variety of online activities, the relatively low level of digital skills risks acting as a brake to the further development of Cyprus's digital economy and society.

Cyprus's government has recognised the importance of revising and implementing the existing National Cybersecurity Strategy. The revision of the NCS demonstrates the government's will to work closely with all stakeholders and help all critical sectors, including the energy and maritime sectors to progress and economic prosperity.

[16] European Internet Statistics, 2017. http://www.internetworldstats.com/stats4.htm#europe

[17] World Economic Forum, 2015. http://reports.weforum.org/global-information-technology-report-2015/economies/#economy=CYP

[18] https://ec.europa.eu/digital-single-market/en/scoreboard/cyprus

[19] https://www.cyprusnewsreport.com/2017/02/cyprus-has-highest-percentage-of-facebook-users-in-eu-cyprus-is-infographic/

During the GCSCC CMM review, participants often referred to regulations, laws, activities, processes which are recommended as a significant part of Cyprus' work on the revision of the Strategy as well as the implementation of the GDPR[20] and the NIS Directive[21]. These developments are expected to ensure a high level of network and information security preparedness in Cyprus.

[20] http://www.eugdpr.org/
[21] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

REVIEW REPORT

In this section, we provide an overall representation of cybersecurity capacity in the Republic of Cyprus. Figure 2 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.

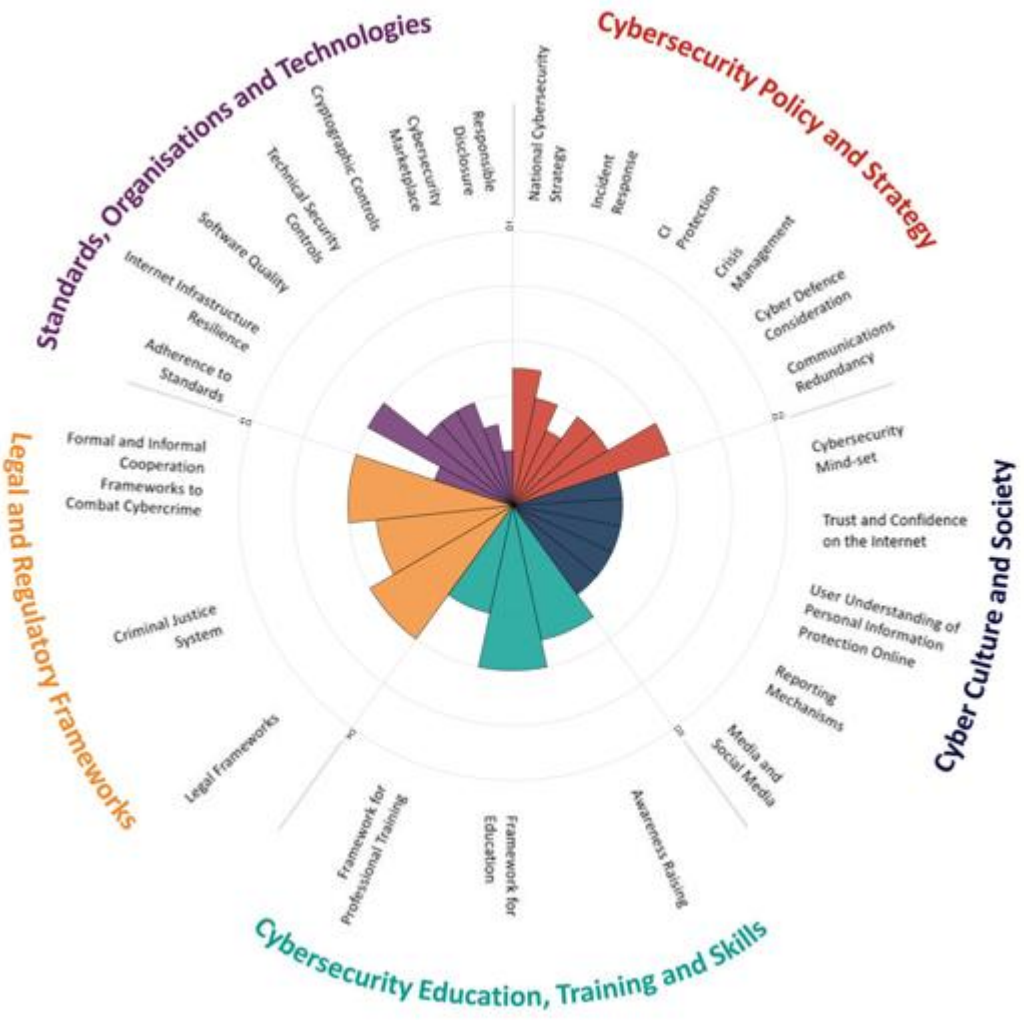

Figure 2: Overall representation of the cybersecurity capacity in Republic of Cyprus.

The CMM methodology requires all the indicators for a certain stage to have been met before that stage of maturity can be completed. Maturity in cybersecurity is assessed and attributed according to the highest completed stage. In the case where a large set of factors for a higher maturity level are met but the maturity stage is not yet complete, we describe this state in between stages (i.e., start-up to formative).

The Appendix presents a summary of the results for each factor, including links to key policy and strategy documents, laws and secondary resources. The Appendix also presents a total of 152 recommendations regarding the enhancement of the existing capacity for each factor.

DIMENSION 1
CYBERSECURITY POLICY AND STRATEGY

The factors in Dimension 1 gauge Cyprus's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. This dimension considers policies aiming to advance national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace increasingly vital for government, international business and society in general.

D1.1 NATIONAL CYBERSECURITY STRATEGY

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

Stage: Formative to Established

The Republic of Cyprus published a comprehensive national cybersecurity strategy in March 2013[9]. The central vision of the strategy was "the operation of information and communications technologies in Cyprus with the necessary levels of security, to the benefit of every user"[22]. To achieve this vision, the strategy identified clear objectives, inter alia, the development and preservation of safe and secure electronic business environments, the development of e-government services and the mitigation of effects of threats from cyberspace. Guiding principles, such as the recognition that a valid strategy must offer multiple levels of security, underpinned the development and implementation of the strategy which highlighted six priority areas. These were:

- *The creation of a legal framework*

[22]https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-cyprus/view

- *The coordination of governmental stakeholders*
- *The formulation of technical and organisational measures and procedures*
- *The development of necessary skills in training and awareness*
- *Productive collaboration between the public and private sector*
- *The creation or adaption of necessary structures for incidence response*

A total of 17 actions were detailed in the strategy; these were categorised in actions achievable in the immediate future, taking into account budgetary restrictions, and long-term actions which - according to the strategy - will be executed once the necessary organisational restructuring has taken place following the adoption of the NIS Directive[9]. The NCS actions were intended to build capacity in all priority areas. Some actions were applicable horizontally and concerned all stakeholders, while others focused vertically on specific parts of the cybersecurity 'spectrum': preparedness, incident response, mitigation, recovery.

Responsibility for the design, implementation, monitoring and revision of the strategy was assigned to OCECPR[23]. CMM review participants concurred that despite the financial crisis, which has affected Cyprus for the last five years, significant progress has been observed in certain aspects of the implementation of the strategy. A steering committee comprising stakeholders from the public sector, military, private sector and academia has been formed and is responsible for the design of KPIs to monitor progress on actions and evaluate the impact of these actions. As participants noted, the steering committee is gathering information on what has been achieved thus far regarding legal and policy requirements, as well as evaluation information from measurable targets for specific actions. KPIs that refer to general progress in the implementation of the strategy, as well as in estimating overall costs for the full implementation of the strategy, are absent.

National risks and threats have been identified based on a national cyber risk assessment. This assessment was conducted for the first time during 2016. It is the intention of the steering committee that the results of this assessment will inform the objectives of the revised strategy. It should be noted that the revised content of the strategy will be aligned to the NIS Directive[24], a comprehensive and thorough framework which details measures for a common and high level of security of network and information systems across EU. The current plan, as described in Cyprus's strategy, requires revisions of the strategy every three years.

An area of concern for all participants that might hinder progress in cybersecurity initiatives is the availability of financial resources to implement the long-term actions. These actions are of paramount importance for the successful implementation of the strategy since they concern the creation of the national CSIRT and the orchestration of formal communication between multiple stakeholders of the strategy. Participants suggested that due to the mandatory adoption of the NIS Directive, the revised strategy will provide the legal grounds for organisational restructuring and will ensure the availability of sufficient funds. It was mentioned that governmental approval has been given to establish a dedicated structure for

[23] http://www.ocecpr.org.cy/
[24] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

network and information security and cybersecurity under the supervision of the Commissioner and to hire adequate personnel for the formation of the national CSIRT. Ministerial approval will also be sought for the adoption of the NIS Directive, the creation of the CSIRT and the National NIS Authority, and the enhancement of the cyber awareness strategy. Once these actions are fulfilled, the parliament will be officially informed. We emphasise that it is the lack of formal coordination between multiple stakeholders and the absence of a national CSIRT, rather than the substantive content of the strategy, that prompts a relatively low assessment (from formative to established) of the maturity of this factor. Once the necessary funding is available it is probable that significant progress will be made, affecting all other dimensions of the model.

D1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify the characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Formative

There are four main authorities that are responsible for different parts of incident response in Cyprus. The Ministry of Transport and Communications and Works (*Υπουργείο Μεταφορών, Επικοινωνιών και Έργων*)[25], through OCECPR, is handling incidents related to the network and information security, the Ministry of Defence (*Υπουργείο Άμυνας*)[26] is responsible for cyber defence while the Ministry of Foreign Affairs (*Υπουργείο Εξωτερικών*)[27] handles diplomatic incidents that may emerge from cyber events. Finally, the Ministry of Justice and Public Order (*Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως*)[28], in coordination with the Cyprus Police and the OCC, is in charge of cybercrime incidents.

Currently, there is no national computer-related incident response organisation and the authority that serves as the coordinating body for the reporting and management of cybersecurity incidents for the government sector, is the government CSIRT. It was established in 2015, when the necessary equipment was bought, including forensic software for data loss recovery, and staff were trained by ITU over one period of just two weeks. Budgetary and other resource restrictions, however, prohibit the CSIRT's operational ability. Participants noted that the CSIRT is operational only up to a certain time in the evening (5-6 pm) during working days and its employees work part-time; they are employed to support other operations of the Department of Information Technologies and if an incident occurs they will leave their regular duties to contribute to the incident response process.

[25] http://www.mcw.gov.cy/mcw/mcw.nsf/index_gr/index_gr?OpenDocument
[26] http://www.mod.gov.cy/mod/mod.nsf/index_en/index_en?OpenDocument
[27] http://www.mfa.gov.cy/mfa/mfa2016.nsf/index_en/index_en?OpenDocument
[28] http://www.mjpo.gov.cy/mjpo/mjpo.nsf/index_en/index_en?OpenDocument

Despite current adverse economic conditions, the government CSIRT has established clear processes for handling different types of communications-related challenge. Through their system (all government departments are connected internally), the CSIRT maintains an inventory of hardware in governmental infrastructures. There is a help-desk set-up which is responsible for the first level response, mainly concerning email issues and PC malfunctioning. Problems related to applications are forwarded to second-level response teams while major issues that cannot be handled at these levels are escalated to the appropriate technical teams. Participants emphasised that it is the dedication and the commitment of CSIRT employees that has kept the operational levels of the CSIRT at decent levels.

Participants considered the level of staffing to be inadequate, however. No more than two officials are on call to resolve any immediate problems as they arise. Staffing levels are not sufficient to resolve common IT problems and most staff members are expected to deal with problems on multiple levels of severity concerning a wide range of hardware and software types (from horizontal applications and directory files to emails and help desk). CMM participants considered it imperative either to increase the number of employees involved in incident response or to outsource certain parts of the incident handling to other organisations.

Institutions operating in the energy, telecommunications and banking sectors have developed incident response strategies. There are legal requirements in place for the electronic communications sector (in particular ISPs) to provide details of incidents to OCECPR, emergency services and the police, once a stated threshold of severity is crossed. These thresholds are based on adjustments of EU discussions (e.g. the Article 13 Working Group) and CMM participants considered them sufficient. Participants also noted that in certain cases where low-impact incidents might affect other organisations, ISPs will often share threat intelligence on these issues informally. With the valuable coordination of OCECPR, police and telecommunication operators have improved their collaboration in identifying offenders, in providing information to support prosecution of cyber criminals and in blocking malicious websites.

In terms of the banking sector, the Central Bank of Cyprus has adopted means of exchanging information about incidents with supervised institutions, through its regulatory and supervisory framework. Participants also reported that communication channels are established between law enforcement agencies and the finance sector.

Due to the absence of a national CSIRT, there is no single entity holding a central registry of national level incidents. Therefore, as CMM participants observed, coordination on a national level is currently ad hoc and depends on personal relations. The government CSIRT collects incidents from government departments only. There is a library of these incidents, providing details of their nature and severity. Participants advised that there is dedicated software to collect this information and that the overall process is partially automated.

In the course of the CMM review it was evident that informal channels for information sharing within various sectors prevail. As was explained, it is faster to escalate events, request information or act on incidents through personal contacts due to time-consuming

bureaucratic processes that act to delay formal channels of communication. Formal channels are in use only for major national incidents. Participants concurred that in such circumstances, formal processes are in place and that points of contact are identified. In the case of a widespread incident, the Ministry of Transport, Communications and Works will coordinate the crisis response and, depending on the impact of the attack, will involve the Ministry of Finance and the Ministry of Defence, Ministry of Justice, Ministry of Interior, or any other relevant agencies in the response process.

A national CSIRT is long overdue in Cyprus and participants theorised that it would fill most of the gaps observed in the incident response strategy. The setting up of a national CSIRT would be in line with the NIS Directive, as well as with Action 38 of Pillar III of the Europe 2020 Strategy that encourages Member States to establish a well-functioning network of national CERTs by 2020. The European Commission has also invited Member States to strengthen cooperation between existing national CERTs and to expand existing cooperation mechanisms such as the European Government CERTs Group.

A project is in place to expand the incident reporting obligation to other sectors and the platform currently used with the telecommunication sector will be upgraded to facilitate this process. Other plans involve the re-establishment of the academic CSIRT, which ceased to operate due to budgetary restrictions some years ago. Legislation through the NIS Directive will require organisations that are part of the national critical infrastructure to share threat-intelligence information, as well as incident reports. For its part, the private sector has already realised the benefits of voluntarily participating in such schemes.

The vision for the national CSIRT is to provide a platform for better communication between the Ministry of Foreign Affairs, the Ministry of Defence, Ministry of Justice and law enforcement agencies, as well as all critical information infrastructure operators, to offer direct support to incident handling in the critical national infrastructure and to establish communication channels with other countries. Participants anticipated the CSIRT to be operational on a '24/7' basis and to provide preventive capabilities and early warning for incidents, neither of which are currently provided by the government CSIRT. Additionally, a semi-automated system will provide threat-intelligence to those stakeholders that collaborate and share information with the national CSIRT.

There is close collaboration with ITU experts from Geneva and Lithuania to evaluate the approach and identify key principles for an effective collaboration. Training is scheduled for the future employees of the National CSIRT and of the academic CSIRT. This training will take place during November 2017 for the basic functionalities of CSIRT. Further training will be provided in mid-2018 in forensic analysis and collaboration with other CSIRTs.

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This factor assesses the government's capacity to identify critical infrastructure assets and the risks associated with them, engage in response planning and critical assets protection, facilitate effective interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

Stage: Start-up to formative

Until recently, the concept of cybersecurity in national critical infrastructure was in its infancy in the Republic of Cyprus. However, significant progress is now being achieved. The OCECPR has developed a national risk assessment methodology based on NIST SP 800-30[29] and ISO 27005[30] and guidance from ENISA[31] with additional steps concerning the dissemination of information between stakeholders. A national risk assessment was conducted recently and as a consequence the main CII stakeholders have been identified. The list of stakeholders has been officially approved by the Council of Ministers; those who comprise the list have been informed although their obligations have not yet been detailed to them. The list also describes the criticality of specific systems that organisations have in place and includes domestic and foreign companies.

In relation to cybersecurity threat and vulnerability disclosure, formal coordination within CII owners and between CII owners and the government is established only for the Electronic Communications sector. Formal mechanisms have been put in place for incident disclosure with mandatory reporting of such incidents. For other sectors, such as finance, there are informal channels of communication with scarce reporting of vulnerabilities and incidents. Participants suggested that these processes could become institutionalised as a result of the adoption of the NIS directive. Nevertheless, exchange of information on cybersecurity between CII sectors has not yet begun and a formal and/or regular process of interaction on cybersecurity issues between all CII owners has not yet been established.

Participants reported that in every sector, companies which are part of CII have the basic capacity to detect, respond and recover from cyber attacks. It is problematic, however, that risk assessment exercises which include cybersecurity aspects are not necessarily conducted by every CII; possibly because there is a lack of incentive to do so in the public sector and across the boards of private companies. A characteristic example is the replacement of an archaic Supervisory Control and Data Acquisition (SCADA) system that took place not because of risks identified by assessments but because the contract with the provider of the SCADA system expired and the new provider demanded an immediate update of the system due to cybersecurity issues. On the other hand, participants provided examples where public and private organisations have been assisted by consultancy companies to conduct risk

[29] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[30] https://www.iso.org/standard/44375.html
[31] https://www.enisa.europa.eu

assessments, while certain institutions have taken part in national exercises. The example of EY was given, where the consultancy firm ran risk assessments on the online taxation system (TAXISNET[32]) in which cybersecurity was deemed of paramount importance.

Participants noted that the novel national risk assessment methodology provides a holistic understanding of the gaps in critical information infrastructure. They considered it to be a high level exercise with critical analysis of the interdependencies between different stakeholders that are part of CII. Information from this exercise can be visualised to better reveal issues and problems. Information was drawn from critical infrastructure systems, the national user base and from government systems. Military networks were, however, excluded from the risk assessment, with other (classified) military projects handling risk assessment for military networks. The development of a national contingency plan is in progress and it will be based on (BCM)/DRP standards, while the next iteration of the risk assessment may be extended to non-critical areas.

Although it is reasonable to conduct the national risk assessment every two years, it was noted that there are processes in place to monitor for developments that may require an update of the CII list before the next iteration of the risk assessment. For example, a new health IT system has been designed and is expected to be delivered soon. There are plans to include this system in the CII list for the next iteration of the risk assessment. However, due to the criticality of the system, it may be considered appropriate to set security requirements and request compliance to security standards equivalent to those followed by CII stakeholders.

D 1.4 CRISIS MANAGEMENT

Crisis management planning encompasses specialised needs assessments, training exercises and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation and budgetary allocations.

Stage: Formative

It was not possible to obtain a clear picture regarding crisis management in the course of the CMM review. The extent to which organisations consider cyber threats as part of crisis situations is uncertain. Participants noted that certain CII stakeholders, as well as organisations from the finance sector hold business continuity plans and depending on the criticality of the system, exercises are conducted on a local level. The situation is different in the Electronic Communications sector, as there are distinct instructions for ISPs and

[32] https://taxisnet.mof.gov.cy/displayWelcome.do

Electronic Communications operators to run drills and simulations of cyberattacks, as well as an obligation to maintain a certain degree of availability for roaming.

OCECPR has been appointed as an exercise planning authority and as such has participated in cyber exercises organised by ENISA and based on the NIS Directive. Participants pointed out that the ENISA exercises were hosted in the newly developed facilities (ZENON[33]) in the Republic of Cyprus, facilities that serve both national and European purposes. A national exercise, however, focusing on cyber incidents has not been conducted yet. OCECPR is in the process of developing a national contingency plan, in collaboration with stakeholders from CIIs and private sector, think tanks, academia and military. These plans will define measures and techniques that require testing and will set objectives to evaluate exercises. Participants mentioned that national exercises will be conducted regularly and the ZENON facilities will be hosting them.

D 1.5 CYBER DEFENCE

This factor concerns the government's capacity to design and implement a cyber defence strategy and then to lead its implementation, including through a designated cyber defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Formative

The Cyprus National Guard handles the military networks that support the operations of the Ministry of Defence. Review participants noted that military systems are end-to-end encrypted and isolated, with strict security procedures in place. Hence, the CMM review was restricted to assessing the maturity of non-military networks.

Cyber defence capacity in the Republic of Cyprus is at a *formative* stage. Currently, there is no official cyber defence document, although the national defence strategy does consider elementary cybersecurity issues. It was noted that existing plans are intended to adjust the national cybersecurity strategy developed by OCECPR to form the basis of the cyber defence strategy. The cyber defence strategy is expected to correspond closely with the overarching national strategy and to adopt the risk assessment methodology developed by OCECPR.

There is a department in the National Guard, specialised in cybersecurity, which is tasked with monitoring activities. There are also exercises in cybersecurity which are conducted jointly with Greece.

[33] http://www.mod.gov.cy/mod/CJRCC.nsf/cjrcc45_en/cjrcc45_en?OpenDocument

The Ministry of Defence and the National Guard are very clearly determined not only to seek collaboration with other countries but also – and most importantly – to work with other government departments. Participants suggested that assigning a dedicated structure under the Commissioner, as the responsible authority of the NIS, is considered to be the best practice to be followed since it is adopted by most European countries. It was noted that there are strong informal channels of communication between the Ministry of Defence and OCECPR and that military personnel are invited to receive advanced training offered by OCECPR. Also, the Ministry of Defence recently organised a one-day seminar concerning internet security, which was attended by high-level public sector employees.

Participants agreed that formal collaboration with the national CSIRT is imperative. Good cooperation will result in effective analysis of incidents and in timely threat intelligence sharing which will inform both parties of imminent threats. It was noted that a decisive step for an efficient communication would be the identification of the types of information that should (and should not) be shared. For example, it was agreed that information from military systems was not appropriate for cross-governmental sharing.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Established

It was not possible to obtain a clear picture regarding communications redundancy in the course of the CMM review. Specific CII stakeholders have emergency response assets hardwired into a national emergency plan. In particular, ISPs are required to run stress tests frequently and have clear obligations set by legislation. These obligations are audited annually. Review participants noted that there are obligations on the operators' side for dealing with crisis management issues and that there are legal obligations for all services to be offered by at least two different operators.

RECOMMENDATIONS

With respect to the maturity of Cybersecurity Policy and Strategy (Dimension 1 of the Cybersecurity Capacity Maturity Model), the following set of recommendations for

extending capacity are offered for consideration by the Republic of Cyprus. Recommendations are grouped by CMM factor.

NATIONAL CYBERSECURITY STRATEGY

R 1.1 Develop general KPIs to monitor progress of the implementation of the strategy.

R 1.2 Allocate budget to ensure the implementation of cybersecurity strategic plans. Strategic plans must consider the implementation of the NIS and GDPR Directives.

R 1.3 Design a methodology to analyse the results of the national cyber risk-assessment and incorporate lessons learnt from this exercise in the revision of the strategy.

R 1.4 Expand the key stakeholder group (steering committee), which is involved in the revision of the national cybersecurity strategy, to include the financial sector, the private sector (including SMEs) that might be considered part of CII in the near future, and international partners.

R 1.5 Enhance collaboration with ENISA and the NIS Cooperation Group regarding the revised strategy and seek advice on the effective implementation of the NIS Directive.

R 1.6 Design and disseminate coordinated cybersecurity programmes. Strengthen and promote inter-departmental cooperation in cybersecurity to ensure full implementation of the cybersecurity programmes.

R 1.7 Design and conduct regularly scenario and real-time cyber exercises that provide a contemporary picture of national cyber resilience.

INCIDENT RESPONSE

R 1.8 Develop an operational central registry of national-level cybersecurity incidents and designate an entity to be responsible for maintain the list (it is recommended that the national CSIRT must have this role).

INCIDENT RESPONSE

R 1.9 Establish a national CSIRT with clear processes, defined roles and responsibilities. Draft legislation that will allocate responsibilities to the national CSIRT. According to NIS Directive, the national CSIRT should:

- ensure high levels of availability and business continuity,
- monitor incidents at a national level,
- provide early warning, alerts, announcements and disseminate threat intelligence to relevant stakeholders,
- respond to incidents,
- provide risk and incident analysis,
- establish relationships with the private sector in Cyprus and in other countries.

R 1.10 Establish metrics to monitor and evaluate progress on implementing the CSIRT.

R 1.11 Establish metrics to monitor and evaluate CSIRT's effectiveness. Enhancing collaboration with ITU and ENISA will be beneficial for this recommendation.

R 1.12 Establish regular training for the CSIRT's employees and design metrics to assess the results of this training.

R 1.13 Create a system for national cyber incident response detailing when and how organisations should report incidents. Reach consensus among stakeholders on architecture, interfaces and standards for information exchange. Common standards promoted by the EU are STIX[34] and TAXII[35].

R 1.14 Identify and document key incident response processes highlighting when and how different Ministries should be involved.

R 1.15 Enhance collaboration with other EU CERTs by establishing formal channels of communication and agreeing on specific standards for threat intelligence sharing.

R 1.16 Develop coordination and information/cybersecurity threat sharing mechanisms between the private and public sectors, as well as within the cybersecurity community at national, regional and international levels.

[34] https://stixproject.github.io
[35] https://taxiiproject.github.io

INCIDENT RESPONSE

Ensure the appropriate involvement of the financial sector in incident response.

R 1.17 Enhance the operational ability of the government CSIRT either by increasing the number of employees involved in incident response or by outsourcing certain parts of incident handling to other organisations and reinstate the academic CSIRT.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R 1.18 Perform regular, detailed audits of CII assets with regards to cybersecurity and disseminate CII asset audit lists to relevant stakeholders. Inform CII stakeholders of their responsibilities.

R 1.19 Mandate the design and implementation of appropriate regular cyber risk assessments for all CII stakeholders, in line with recommendations from the NIS Authority and identify the required information to be shared. Design cyber risk assessments for all CNI CII stakeholders based on the national risk assessment approach.

R1.20 Establish a mechanism for regular vulnerability disclosure and information sharing between CII asset owners and the government. Establish regular dialogue between tactical and strategic/executive levels regarding cyber risk practices and encourage communication among CII operators. Ensure that the financial sector is involved in the discussions.

R 1.21 Ensure GDPR guidelines are adhered to in the sharing of threat-intelligence information.

R 1.22 Identify internal and external CII communication strategies with clear points of contact.

R 1.23 Establish information protection and risk management procedures and processes within CII, supported by adequate technical security solutions which inform the development of a response plan for cyber incidents.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R 1.24 Establish common processes to measure and assess the capability of CII asset owners to detect, identify, respond to and recover from cyber threats.

CRISIS MANAGEMENT

R 1.25 Design a cybersecurity needs assessment of measures and techniques for crisis management. The involvement of key stakeholders and other experts, such as think tanks, academics and civil society leaders should be sought.

R 1.26 Participate more actively with more personnel in all exercises organised by ENISA.

R 1.27 Develop a national business continuity / disaster recovery / contingency plan.

R 1.28 Organise national cyber security exercises, identify metrics to evaluate the success of the exercises and ensure that lessons will inform the decision-making process for future exercises. Plan the exercises by engaging relevant participants, outlining their role in the exercise, and articulating the benefits of, and incentives for participation.

CYBER DEFENCE

R 1.29 Develop an official cyber defence document based on the national strategy developed by OCECPR. This document should consider the threats to national security that might emerge from cyberspace.

R 1.30 Develop a cyber risk assessment methodology (for defence). Evaluate if the national risk assessment designed by OCECPR is appropriate for military use.

R 1.31 Create a CSIRT for the National Guard.

CYBER DEFENCE

R 1.32 Establish formal communication channels with the forthcoming national CSIRT and the NIS authority in Cyprus.

R 1.33 Establish training programmes for employees and develop awareness campaigns.

R 1.34 Develop a communication and coordination framework for cyber defence in response to malicious cyber-attacks on military information systems and critical infrastructure.

R 1.35 Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.

COMMUNICATIONS REDUNDANCY

R 1.36 Test the interoperability and function of emergency response assets under compromised communications scenarios to inform strategic investment in future emergency response assets.

R 1.37 Allocate resources to hardware integration, technology stress testing, personnel training and crisis simulation drills.

R 1.38 Establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response asset communications and authority responsibilities.

R 1.39 Connect all emergency response assets into a national emergency communications network with isolated but accessible in emergency situations backup systems.

R 1.40 Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of protocols for communications redundancy tailored to the roles and responsibilities of

each organisation in the emergency response plan.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies encompass a wide array of actors, including Internet users. All actors, including Internet users, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of all users and other actors in achieving greater capacity for cybersecurity, but also seeks to avoid conventional tendencies to blame users for the challenges facing cybersecurity. Instead, cybersecurity experts need to build user-friendly operating systems and programs that can be incorporated in everyday practices online.

This dimension reviews elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This factor also entails the existence of mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this factor reviews the role of mass media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D2.1 CYBERSECURITY MIND-SET

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 mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Maturity Stage: Formative

The government has recognised the need to prioritise cybersecurity across its institutions. Also, aspects of governmental processes and institutional structures have been designed in response to risks to cybersecurity, but primarily in particular leading agencies.

According to review participants, awareness-raising efforts about risks and threats exist but there is a general lack of knowledge on the specific actions that are necessary for various actors to take. A programme for training and education for public services on IT and cybersecurity is already being applied. However, this training programme is not mandatory for all employees. Another concern noted by participants is a lack of coordination across these programmes, and strategies for ensuring that they are sustainable over the long term to ensure that employees will retain the knowledge they acquire.

A general concern was expressed that there is no top management commitment regarding safety measures while employees within the public sector do not always follow specific online safety measures, such as locking their computer, updating passwords, or not sharing passwords. Participants noted that mandatory password update has been introduced. However, a shortage of personnel leads often to employees taking shortcuts in security. Review participants noted that many employees tend to share their passwords with co-workers. There is a general habit to consider IT personnel as responsible for security and, therefore, although a cybersecurity mind-set exists, it does not always translate into employees routinizing secure behavior.

Representatives from CII organisations noted that there are different policies in place, such as concerning password updates, and there is an awareness campaign conducted every two years. Moreover, Performance Assessment Tests are carried out every year and that helps bring pressure to the management teams.

Leading firms within the private sector have begun to place more priority on a cybersecurity mind-set by identifying high-risk practices. Programmes and materials have been made available to train and improve cybersecurity related practices. Specifically, the finance sector is organising training programmes for employees. However, participants noted that the private sector needs to ensure trust in their services to customers, when many Small and Medium Enterprises (SMEs) do not have the resources of large organisations to allocate towards cybersecurity.

A limited but growing proportion of Internet users have begun to place a higher priority on cybersecurity, such as by identifying risks and threats. Most (94%) Internet users in Cyprus are on Facebook, and three-quarters of the population use the Internet. Nevertheless, according to participants, the majority of users do not understand the risks associated with being online. Participants noted that it is likely that the majority of Internet users in the country have never received any advice or training on such simple issues as updating their password. Users generally have only one password that they rarely ever change. A reason cited by participants is that users tend to place more priority on convenience than security. However, this is not inevitable. For example, people in Cyprus place a high priority on security when using their credit cards online. In line with this, Internet users in Cyprus tend to worry more on sharing their information online when it is associated with financial exchanges, and seem to have less stake or understanding of the value of how personal data can be gathered and used online.

D2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Maturity Stage: Formative

Overall, participating stakeholders believe that a small proportion of Internet users critically assess what they see or receive online. Similarly, few believe that they have the skills to use the Internet and to protect themselves online. Moreover, a limited proportion of users trust in the secure use of the Internet and are not aware of ways to determine the legitimacy of a website.

Internet users in Cyprus simply have a high level of trust in the security of the Internet without basing that trust on a critical assessment, such as of the credibility of a website. Their trust is too often "blind" trust. People like the convenience of online services and either do not understand what secure browsing is, for instance, nor do they fully understand the risks that are associated with insecure Internet provision.

As mentioned above, according to DESI (2017),[36] Cyprus has one of the highest percentages of social media users in Europe, such as illustrated by the take-up of Facebook. With Cypriot users being the fifth most active in the use of social media across Europe, this means that the country provides a promising audience for the companies who market successfully on Facebook and other social media. That said, although Cypriots are active users of social networks, video calls and online content, they tend to engage less in online banking and shopping activities than other Europeans. Similarly, companies engage in the use of social media and trade online, but are less prone to the take up new technologies, such as cloud computing and RFID. As noted above, while Internet users trust the security of the Internet in general, they are more wary when it comes to online banking and other services involving financial transactions.

Internet service providers in Cyprus have developed programmes to promote trust in online services but have not routinely implemented them. Participants informed us that they offer online payment services, and more services will be offered within the next year. However, a limited number of customers use them due to a lack of adequate skills in Internet use.

E-government services have been established in Cyprus, and the number of e-government users has been growing. However, improvements in the delivery of these services have stalled.

The e-government Strategy of the Republic of Cyprus covers the period 2014-2020. It applies to all ministries, departments and services of the Cypriot government, focusing on technical,

[36] https://ec.europa.eu/digital-single-market/en/scoreboard/cyprus

operational and organisational aspects of the provision of electronic services (eServices) to citizens and businesses. The objectives of the e-government strategy are to enhance public sector capacity while reducing operational costs. The strategy also foresees major strategic interventions such as the provision of advanced electronic identification and electronic signature functionalities, now in preparation.

The Government continues to increase e-service provision and tax declarations are already being submitted electronically. Participants informed us that the Parliament tried to legally require online tax submission, but the skills of citizens were not adequate to justify this move. Currently, citizens need to fill in certain forms physically in order to be able to access e-government services for the first time. So this is an area of promise if the services can be offered in more user-friendly and accessible ways.

The government but also other stakeholders and users recognise the need for the application of security measures to establish greater trust in these services. However, participants noted that users trust in e-government services ''by default'' as they do for other government services. Moreover, the use of e-government services is currently not being actively promoted. Another concern expressed by participants was the fact that local government need more assistance, such as looking to the central government for tools for providing e-government services.

E-commerce services are fully established by multiple stakeholders in a secure environment. Security solutions are updated and reliable payment systems have been made available. A growing proportion of users trust in the secure use of e-commerce services. E-commerce is considered to be one of the top priorities of the Ministry of Energy, Commerce, Industry and Tourism. A scheme has been prioritised within Cyprus' digital strategy action plan for the period 2014-2020 and will be implemented in the first quarter of 2017 with the objective of encouraging SMEs to transform E-commerce opportunities into commercial advantages. National legislation has also been amended to comply with the E-commerce Directive and will be proposed for adoption by parliament. Participants noted that generally, online-banking and other commercial services from local suppliers are being used but foreign services are used and trusted more than local services.

D2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Maturity Stage: Formative

Users and stakeholders within the public and private sectors have general knowledge about how personal information is handled online but cybersecurity practices are either not proactively used, either due to perceived inconvenience, or due to the way people weigh up the trade-offs in service and the protection of their personal information. Participants noted that personal information is shared through social media, for example, but users do not necessarily perceive that information as sensitive personal information that should be private.

Cyprus has adopted and enforced the Processing of Personal Data (Protection of Individuals) Law (N. 138(I)/2001) in order to address privacy issues related to the collection, storage, processing, dissemination, and use of personal data, and was amended by Law N. 37(I)/2003 (see Section D4.1). This Law is compliant to the European Directive 95/46/EC on Data Protection.

Issues concerning Internet safety and protection of personal data are addressed in Part 14 of The Regulation of Electronic Communications and Postal Services Law 112(I)/2004. Moreover, the Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007 regulates the terms under which the retention of personal data for the purpose of crime investigation, detection and prosecution is legal.

Also, Cyprus is in the process of implementing the EU General Data Protection Regulation (GDPR). It is expected that the implementation of the new regulations will promote a greater awareness of cybersecurity on the part of users and promote more understanding of the importance of protecting personal information online.

D2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning 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.

Maturity Stage: Formative

In Cyprus, the public and private sectors are providing some channels for reporting online incidents, but these channels are not coordinated and are used in an ad hoc manner. Participants were not aware of the existing reporting mechanisms in the country especially related to incidents such as phishing emails. Promotion of the existing reporting channels has not yet begun or is ad hoc.

Detailed reporting and notification mechanisms lie within the mandate of the NIS authority and the National CSIRT.

Citizens and companies report online card fraud offences to the police except when the cases concern small sums of money. In such cases they prefer to cooperate with the banks to solve the problem. Moreover, the O.C.C. implemented in 2014 the Cybercrime Reporting Platform[37] and the Cyprus Police Mobile Application[38] that allows the public to report cybercrime online.

According to Law 112(I)/2004 all ISPs are supervised by OCECPR. Furthermore, Law 187(I)/2007 obliges the ISPs to keep traffic and user identification data for a period of six months. Moreover, pursuant to Article 11 of the Law 91(I)/2014, the police and courts can order the ISPs to block access, remove content or take down web pages. Although existing legislation facilitates the protection of citizens, users seem not to be aware of the existing reporting mechanisms or they find that these mechanisms are not useful to them in reporting incidents. Participants noted that communication links have not been established between the police and the finance sector, although some initial meetings have taken place with a view to formalise such links, and the National CSIRT currently under development does not yet have the resources to take up this role.

The European CyberSafety[39] project aims to create an awareness platform where stakeholders can find information, resources and tools, as well as share experiences, expertise and good practices. The CyberSafety Hotline 1480 ensures that users can report illegal content and actions related to illegal child pornography, racism and xenophobia.

[37] https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm
[38] http://mobile.cypruspolicenews.com/landing/Desktop#.WYI-Fojys2x
[39] http://www.cybersafety.cy/

Events are promptly forwarded to the appropriate authority for further investigation and action.

D2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Maturity Stage: Formative

Media coverage of cybersecurity is ad hoc, with limited information provided and reporting on specific issues that individuals face online, such as cyber-bullying, but not consistently and broadly covering the full range of issues. Overall, discussions on social media about cybersecurity are also limited. Review participants noted that due to reputational harm, incidents within the private sector are often not disclosed and therefore under-reported.

Social media platforms such as YouTube, Facebook, Twitter, and international blog hosting services are freely available and are used by a large part of the population[40]. If there is an announcement by police like the 'WannaCry ransomware', then media promote it and get the public attention. Most of the times they report things but they do not provide best practice, such as informing Internet users about what they can do.

In 2016 the website of the Central Bank of Cyprus briefly came under cyber attack, days after a hacking collective said it conducted a similar attack on the Greek central bank's site. Traditional media and social media such as Cyprus Mail[41], Cyprus News Agency (CNA)[42] and Reuters[43] reported about this attack and they also provide updates on the international cybercrime scene. Incidents reported in media certainly raise the general public awareness. However, participants noted that journalists often do not necessarily understand cybersecurity issues and might misinform the public by creating fear.

[40] https://www.cyprusnewsreport.com/2017/02/cyprus-has-highest-percentage-of-facebook-users-in-eu-cyprus-is-infographic/
[41] http://cyprus-mail.com/2017/06/28/major-cyber-attack-disrupts-businesses-around-world/
[42] http://www.cna.org.cy/webnews-en.aspx?a=da94a22f8d9b4a539c07c6e286ae5d74
[43] http://www.reuters.com/article/us-cyprus-cyber-cenbank-idUSKCN0XX1NQ

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cyber Culture and Society*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Republic of Cyprus. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

CYBERSECURITY MIND-SET

R 2.1 Enhance efforts at all levels of government, especially officials, and the private sector to employ cybersecurity good (proactive) practices. Design systems that enable users across society to embed secure practices more easily into their everyday use of the Internet and online services.

R 2.2 Develop coordinated training programmes for employees in the public sector.

R 2.3 Routinize cross-sectorial cooperation and information sharing among private and public sector organisations on cybersecurity risks and good practice.

R 2.4 Identify vulnerable groups and high-risk behaviour across the public, in particular young people, to inform targeted, coordinated awareness campaigns, as recommended in R3.1.

TRUST AND CONFIDENCE ON THE INTERNET

R 2.5 Establish programmes for all ISPs to promote trust in their services based on measures of effectiveness of these programmes.

R 2.6 Promote use of e-government services and trust in these services through a coordinated programme, including the compliance to web standards that protect the anonymity of users.

TRUST AND CONFIDENCE ON THE INTERNET

R 2.7 Implement feedback mechanisms for use to ensure that e-services are continuously improved and trust is strengthened among users.

R 2.8 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R 2.9 Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R 2.10 Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online.

R 2.11 Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

R 2.12 Promote the compliance to web standards that protect the anonymity of users.

R 2.13 Promote privacy by default as a tool for transparency.

R 2.14 Develop user-consent policies designed to notify practices on the collection, use or disclosure of sensitive personal information.

REPORTING MECHANISMS

REPORTING MECHANISMS

R 2.15 Develop programmes to promote the use of the existing reporting mechanisms by public and private sectors for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

R 2.16 Encourage different stakeholders (public-private sector, Police, CSIRT) to coordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms.

R 2.17 Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.

MEDIA AND SOCIAL MEDIA

R 2.18 Encourage media and social media providers to further extend the coverage beyond threat reporting and focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts.

R 2.19 Encourage a frequent discussion about cybersecurity on social media.

R 2.20 Ensure that the debate in social and mainstream media and the attitudes expressed inform policymaking.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Maturity Stage: Formative to Established

A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) which addresses a wide range of demographics is yet to be established. Such a programme is under development under Action 14 of the NCS, as detailed below.

The National Cybersecurity Strategy provides for a systemic approach on cybersecurity awareness, the implementation of which is coordinated by the Office of the Commissioner of Electronic Communications and Postal Regulation. Action 14 of the Strategy refers to awareness and a committee and several sub-committees have been established to bring all national efforts into a shared vision. Action 14 aims at the development of a comprehensive national awareness programme for cybersecurity matters, covering all users of electronic systems, from governmental workers to ordinary citizens. In this context, an open invitation was sent for all stakeholders interested in being involved and the committee established

under Action 14 is in the process of developing a national awareness and education strategy that will accommodate all existing measures and provide opportunities for new ones.

The department responsible for Safe Internet issues is the Cyprus Pedagogical Institute (CPI). The CPI collaborates with the education department in outlining policies and running programmes that have to do with the critical and responsible use of the Internet. The actions related to the safe Internet area include the following: inclusion of Safe Internet in the school curriculum; provision of school-based workshops for pupils, teachers and parents; presentations in conferences and other events; sustaining school programmes supported by the Cyprus Pedagogical Institute (such as the Safe School for the Internet, the Production of short videos by students competition, Young Coaches for the Internet, eSafety Label etc. mentioned above); participation in nationwide implementations of Safe Internet European supported programmes such as the Safer Internet Programme by the Connecting Europe Facility (CEF).

CyberEthics[44], was a project that has been operating since 2006 with co-funding from the EU through the Safer Internet and CEF Programmes, and it comprised of an awareness node, hotline and helpline. CyberEthics was the National Representative of Cyprus at the European Network of Awareness Centres and Helplines – Insafe and of the Worldwide Association of Hotlines for reporting illegal content on the Internet - Inhope. This project has now been replaced by other initiatives.

The Cyprus Safer Internet Centre (SIC), CyberSafety[45], brings together major national stakeholders in order to create a safe internet culture, empowering creative, innovative and critical citizens in the digital society. CyberSafety aims to provide an awareness platform where actors can find resources and tools, share experiences, expertise and good practices. The operation of the Helpline[46] ensures that all actors get advice and support by trained supporters/helpers on issues related to their use of online technologies. The CyberSafety Hotline[47] line 1480 ensures that users can report illegal content and actions related to illegal child pornography, racism and xenophobia. The Cyprus SIC consortium consists of 7 partners (Cyprus Pedagogical Institute - Ministry of Education and Culture, Office of the Commissioner for Electronic Communications and Postal Regulation, University of Cyprus, Pancyprian School for Parents, Office for Combating Cybercrime (Cyprus Police), Cyprus Telecommunications Authority (Cyta) and MTN Cyprus Ltd).

The Awareness Centre aims to create a culture among children, parents and teachers to take advantage of the affordances of the Internet with safe, responsible and ethical use. Awareness will continue the existing work that is taking place in Cyprus, update and enrich the digital content and resources already developed, enhance existing services and tools deployed and extend collaborations and synergies among stakeholders. An evaluation survey on the impact of the awareness activity is conducted, providing evidence for planning the next steps as well as feedback at the European level.

[44] http://www.cyberethics.info/
[45] http://www.cybersafety.cy/
[46] http://cybersafety.cy/helpline
[47] http://cybersafety.cy/hotline

Success programmes of the Centre include the eSafe[48] school programme which aims to introduce schools into an action process to promote safe use of the internet in the school environment. Moreover, the Young Coaches for the Internet programme[49] aims to involve students in the training of others for the safe use of the Internet. With the guidance of their school teachers and the support of specialists in the subject, small trainers are invited to develop an action plan for their school unit and to design and implement actions to inform on Internet issues. Another success programme of the Centre is the annual Short Videos by Students competition[50].

Another initiative is the CYberSafety Youth Panel[51] which aims to engage children and young people from different demographic groups in an interactive participation and active contribution on the creative and responsible use of the internet. Computer Science university students act as mentors for the younger ones by providing a role model, while members of the Cyprus Children's Parliament, the Commissioner for Children's Rights Young Advisors and the Young Coaches for the Internet are part of the Youth Panel.

Hope For Children UNCRC Policy Center[52] has a consistent and inspirational approach to protecting and promoting the rights of the child and to supporting the active participation of children and youth in society. The aim is to advocate and to protect children's rights based on the standards and principles of the UN Convention on the Rights of the Child and European Union law, regardless of a child's background. The programmes and activities that the Center operates related to the prevention of cybercrime include the European Helpline for Children and Adolescents, 116111, which provides direct psychological support to children and adolescents for free, the "Beat Bullying" programme that aims to raise public awareness of bullying incidents, the ONE in Five Campaign on sexual violence against children, the development of the mobile application "HFCBeatBullying" as a tool to prevent and tackle bullying.

A study conducted by the EU Kids Online survey[53] and United Nations Convention on the Rights of the Child (UNCRC) on grooming has shown that Cyprus was classified as 'higher use, some risk' country. The average age of first Internet use is 10 and around a third of the Cypriot children visit chat rooms, share files, blog and spend time in a virtual world. Most children in Cyprus go online on a computer in their own bedroom, while parents in Cyprus are not aware of what their child may be encountering when online. The study has shown that the vast majority of Cypriot children have a social networking profile and even though they keep their profile private, they still accept invitations from strangers while at the same time displaying abundant information about themselves.

[48] http://esafeschools.pi.ac.cy/
[49] http://youngcoaches.pi.ac.cy/
[50] http://internetsafety.pi.ac.cy/competitions
[51] http://cybersafety.cy/youth-panel
[52] http://uncrcpc.org.cy/gr/
[53] http://uncrcpc.org.cy/index.php?id=47

Additionally, the Cyprus Research and Academic Network (CyNet)[54] prepares and presents an informative movie on Internet dangers and particularly about viruses, worms and bots.

Participants informed us that awareness actions are also planned in 2017, such as role model visits to schools and universities, by important ICT industry figures to explain the importance of ICT professionals in the future. In the second half 2017, an awareness campaign addressing all citizens will be launched in order to publicise what Cyprus is doing for the digital economy and society. The objective is raising the use of ICT and trust in ICT (i.e. E-Banking, E-Commerce); raising the level of online culture and use of electronic services offered by public administration (E-government). The awareness campaign in preparation is also including non-users of Internet as targets in order to encourage them to access digital public services. Another action that the government is planning to take is the establishment of a National Cybersecurity Awareness and Education Centre. This Centre will not only provide education to different demographics but also act as the coordinating body for awareness raising at a national level.

Cyprus has established Safer Internet Day[55] in February and this day aims to raise awareness about online safety issues and to promote safer and more responsible use of the internet and technologies, especially among children and young people.

Because no (known) major incidents have occurred in Cyprus and additionally reporting of incidents is not mandatory for the private sector there is limited motivation for executives to be aware of risks and threats online. Some executives might be aware of general cybersecurity issues, but not necessarily, how these issues and threats might affect their organisation. Executives of some particular sectors, such as finance, telecommunications, Internet providers and cloud operators are aware of cybersecurity risks, and how their organisation deals with cybersecurity issues, but not of the strategic implications. Participants noted that interest of CEOs in receiving training in cybersecurity often depends on the resources of the organisation.

[54] www.cynet.ac.cy/stayalert/

[55] http://internetsafety.pi.ac.cy/saferinternetday

D3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Maturity Stage: Established

The need for enhancing cybersecurity education in schools and universities has been identified by leading government, industry, and academic stakeholders. Action 13 of the NCS recognizes the need for the development of a suitable workforce, both within and outside of the public sector, which will have the necessary technical know-how and experience to implement the provisions of this Strategy. As such, the government will support activities in Cypriot higher education institutions in the area of network and information security, through the inclusion of electronic security topics in their curricula and the institution of related research programmes.

Qualifications for and supply of educators are readily available in cybersecurity. In Cyprus specialised courses in cybersecurity are offered and accredited at the university level. The University of Nicosia[56] offers a Bachelor Degree in Computer Engineering (CE) and in Computer Science as well as a Master Degree in Cybersecurity.

The University of Central Lancashire Cyprus (UCLan)[57] offers Bachelor degrees in Computing and Master Degrees in Computing, Cybersecurity and Data Analytics. The specialised MSc programme in cybersecurity includes modules in Ethical Hacking, Digital Forensic Investigation, Information Security Management, Cyber Warfare and Cyber Defence.

Cyprus Open University[58] offers a Master Degree in cybersecurity, which includes modules in Forensics, Cryptography, Communication Networks and Risk Management. The programme includes virtual labs and penetration testing, password cracking and ethical hacking. Cyprus Open University offers also a Master Degree in Social Information Systems and a Doctoral Degree in Information and Communication Systems and there are considerations regarding the provision of undergraduate degrees in cybersecurity as well.

The European University Cyprus[59] offers a Master Degree in cybersecurity which includes modules in Communications and Network Security, Cryptography, Cybersecurity Policy, Governance, Law and Compliance, Cybersecurity Risk Analysis and Management,

[56] https://www.unic.ac.cy/el
[57] http://www.uclancyprus.ac.cy/en/
[58] http://www.ouc.ac.cy/
[59] http://www.euc.ac.cy/en/home

Cybersecurity Architecture and Operations as well as Ethical Hacking and Data Privacy. Moreover, Doctoral Degrees in cybersecurity are offered.

Universities collaborate with Industry mostly unofficially for student supervision. And students may get job opportunities in the organisation that supervises their work.

Universities and other bodies hold seminars/lectures on cybersecurity issues aimed at non-specialists as well. Participants noted that the interest of young people with regards to cybersecurity has been underestimated. Universities run practical activities such as password cracking and hacking seminars and young people are willing to participate. Participants from academia noted that every year there is a big increase of students registering for such courses, mainly students from Greece, Cyprus and other countries.

Research and development is an important consideration in education. Universities apply for European and other research funding schemes in order to promote research in the field of cybersecurity. There is a limited budget dedicated to national cybersecurity research. However, participants noted that with the implementation of the NIS directive the budget will be increased.

D3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Maturity Stage: Formative

The need for training professionals in cybersecurity has been documented at the national level and training programmes in cybersecurity are offered for the public and private sector employees as well as for the general public.

The National Cybersecurity Strategy provides in Action 13 for the development of suitable human resources that will have the necessary technical know-how and certifications to implement the provisions of this Strategy to a high level.

ICT professional certification with some security modules or components is available. Private companies and local chapters of international training and certification organisations such as (ISC)^2, ISACA, CISCO, Deloitte, PwC, KPMG and ICIS offer courses on ethical hacking and other topics as well as professional certification. Participants from these organisations noted that

updating the syllabus is very complex due to the specifications of the Institution for accreditation of higher education.

Review participants noted that in the last few years there has been an increase in the demand for training courses. Moreover, more cybersecurity practitioners are being trained to receive certifications. However, still the limited numbers of applicants for example for the CISSP certification lead to the course being offered once or twice every year, if a sufficient number of candidates is available.

It was noted that the government has to realize the value of these certifications and expertise and highlight that through their project management. There is a gap currently between graduates and their professional opportunities. A well-defined career path, is necessary as well as the levels of expertise that they need to develop after graduation. Participants mentioned an existing model for accounting and law which is very successful and academia is supporting qualification in other sectors.

Demand is driven by the regulatory obligations in the country and not by capacity. There are many old laws and the public sector has restrictions in procurement processes. There is a gap in the salary levels and promotions. Security professionals are not promoted based on their certifications. Cyprus is a small country and the best way to solve this problem is outsourcing and collaborating with the private sector. Currently, if an expert is certified then it is expected to pass the knowledge further or develop something internally.

Metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings exist, but are limited in scope.

Review participants stated that there is a big need for qualified employees especially in the private sector. Moreover, the private sector can create career paths for their employees. However, at a national level there is no strategy for professional qualifications, certificates and accreditation currently. Participants suggested that a constructive collaboration between Universities and the public sector in updating the curriculum and communicating clear requirements for graduates to progress professionally would enhance the numbers of employees certified and trained in cybersecurity issues.

The personnel of the DEFL and the OCC follow special training courses each year in the investigation of cybercrime. The majority of these training courses are organised by CEPOL, FBI, OLAF and ECTEG. As for the field officers, there is a specialised training session organised by the Cyprus Police Academy on cybercrime investigation (collection of e-evidence, investigative procedures) and legislation. Police training in international cooperation and cybercrime is provided to all recruits at basic level at the Police Academy. Furthermore, police officers benefit from further training in international police cooperation from the EU and international organisations such as Europol and CEPOL, according to their duties.

Moreover, the Ministry of Commerce, Industry and Tourism together with the Ministry of Education and Culture and the Ministry of Communication, Transport and Works decided in 2016 to introduce and finance the certification of European Computer Driving License (ECDL)

certification for all students in secondary education in order to create a digital culture in Cyprus. It is worth mentioning that this is the first time that public schools provided vocational ICT certification. This is considered to be a breakthrough for the Cypriot education system. The implementation of the programme started in January 2017 and will run for 3 years, with a budget of nearly €1 million. They also decided to provide training and ECDL certification to a number of soldiers and unemployed people as well as the provision of training programmes to people with disabilities.

Executive training courses for CEOs or chief account executives are offered on an ad-hoc manner, including topics such as good governance practices related to cybersecurity and risk management.

During the consultations it was identified that overall an established cadre of cybersecurity-certified employees does not exist in Cyprus. Currently, many experts are self-educated or gain their expertise on the job, and knowledge transfer from employees trained in cybersecurity to untrained employees is also ad hoc.

RECOMMENDATIONS

Following the information presented on the review of the maturity of C*ybersecurity Education, Training and Skills*, the following set of recommendations are provided to the Republic of 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.

AWARENESS RAISING

R 3.1 Continue working on the development and the implementation of the National Work Plan for cybersecurity awareness-raising programme, with specified target groups, focusing on the most vulnerable users.

R 3.2 Appoint a designated organisation (from any sector) to lead the cybersecurity awareness-raising programme.

R 3.3 Engage relevant stakeholders from public and private sectors in the development and delivery of the awareness-raising programme as well as for the creation and utilisation of programmes and materials.

AWARENESS RAISING

R 3.4 Enhance the existing efforts on raising awareness for school children at all ages, especially on grooming.

R 3.5 Special attention should also be placed on the awareness of parents about online activities of their children.

R 3.6 Create a single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform.

R3.7 Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns taking into account gaps or failures.

R 3.8 Promote awareness of risks and threats at all levels of the government.

R 3.9 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors, particularly those in the financial and telecommunications sectors.

R 3.10 Promote awareness regarding the protection of personal information online.

R 3.11 Promote awareness raising efforts of cybersecurity crisis management at the executive level.

R 3.12 Develop operational cyber security self-education websites.

FRAMEWORK FOR EDUCATION

R 3.13 Create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff is available to teach newly formed cybersecurity courses.

R 3.14 Create accredited cybersecurity-specific degree courses at undergraduate and post-graduate level, in addition to the other existing cybersecurity-related courses in the various Universities in Cyprus.

R 3.15 Promote efforts by Universities and other bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists.

R 3.16 Allocate additional resources to cybersecurity education for public universities, dedicated to national cybersecurity research and laboratories at universities.

R 3.17 Inform cybersecurity education priorities through broad consultation across government, private sector, academia and civil society, linked to the National Cybersecurity Strategy.

R3.18 Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, in order to enhance their expertise by combining education and practical training.

R 3.19 Promote cooperation between academia and industry in order to bring together cybersecurity educational offerings weighted based on an understanding of current skills requirements.

R 3.20 Promote competitions and initiatives for students by government and/or industry in order to increase the attractiveness of cybersecurity careers.

R 3.21 Ensure the sustainability of research programs.

R 3.22 Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment.

R 3.23 Gather statistics on the supply and demand of cybersecurity graduates.

FRAMEWORK FOR PROFESSIONAL TRAINING

R 3.24 Establish more structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity-specific professionals.

R 3.25 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, and models and operation of these tools.

R 3.26 Train general IT staff on cybersecurity issues so that they can react to incidents as they occur.

R 3.27 Ensure that affordable security professional certification is offered across sectors within the country.

R 3.28 Develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts.

R 3.29 Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms.

R 3.30 Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals.

R 3.31 Work on establishing a collaboration between Universities and the public sector in updating the curriculum and communicating clear requirements for graduates regarding certification in cybersecurity according to the demand of the market.

R 3.32 Simplify the process of updating the cybersecurity syllabi.

FRAMEWORK FOR PROFESSIONAL TRAINING

R 3.33 Develop a skills framework in cybersecurity or use an existing skills framework in the country in order to define clear career paths for cybersecurity experts.

R 3.34 Update the regulatory environment in terms of cybersecurity skills procurement.

R 3.35 Create a system of metrics to determine and monitor supply and demand of professional training in cybersecurity.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly or indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law-enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Established

Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been implemented and legislation protecting the rights of individuals and organisations in the digital environment has been adopted in Cyprus.

Specific legislation and regulation related to cybersecurity has been enacted in Cyprus through the following laws: Electronic Commerce Law (156(I)/2004)[60,61]; the Law for the Protection of Confidentiality of Private Communications (92(I)/1996)[62]; the Law Regulating Electronic Communications and Postal Services 112(I)/2004, last amended by Law No.

[60] http://www.cylaw.org/nomoi/enop/ind/2004_1_156/section-scdcb51201-8591-c875-d84b-3e20c399891a.html
[61] http://www.ac.ac.cy/images/media/assetfile/law_ammendment.pdf
[62] http://www.cylaw.org/nomoi/arith/1996_1_092.pdf

76(I)/2017[63]; the Legal Framework for Electronic Signatures and for Relevant Matters Law 188(I)/2004 [64] and the Processing of Personal Data Law L.138(I)/2001[65].

The Electronic Commerce Law (156(I)/2004) Law entered into force in 2004 for the purpose of the implementation of Directive 2000/31/EC66 of the European Parliament and the Council of the European Union of the 8th of June 2000 on certain legal aspects of information society services, in particular electronic commerce in Internal Market. The Law 156(I)/2004 aims at ensuring the free movement of information society services between the Republic of Cyprus and the EU/EEA Member States regarding the establishment of service providers, commercial communications, the conclusion of electronic contracts, the liability of intermediaries, out-of-court dispute settlements, codes of conduct, means of legal protection and the cooperation between Member States. Additionally, the law regulates the following online activities: online information services; online advertising and marketing; online selling of products and services; and online entertainment services.

Furthermore, Cyprus Law for the Protection of Confidentiality of Private Communications (Interception of Conversations) of 1996 prohibits the unauthorized interception of any private communication, subject to certain exceptions.

The Legal Framework for Electronic Signatures and for relevant matters Law (N. 188(I)/2004) implements the European Directive 1999/93/EC regarding the EU Framework for Electronic Signatures. The Law effectively establishes the legal framework governing electronic signatures and certain certification services for the purpose of facilitating the use of electronic signatures and their legal recognition. It does not, however, cover aspects related to the conclusion and validity of contracts or other legal obligations which are governed by requirements, as regards their form. Furthermore, it does not affect rules and limitations in relation to the use of documents provided by other applicable legislation in force. Based on the provisions of this Law, Regulations may be issued so as to define additional requirements, amongst others, for the use of electronic signatures in the public sector.

Law 112(I) 2004 on the Regulation of Electronic Communications and Postal Services provides protection against matters such as messages being sent by means of a public communications network that are grossly offensive. This Law prohibits any person, other than users communicating between themselves from time to time, to listen into, tap, store, intercept and/or undertake any other form of surveillance of communications without the consent of the users concerned, except where this is provided for by Law and where there is an authorisation by the Court.

The Republic of Cyprus is a party to the Council of Europe Convention on Cybercrime (Budapest Convention). The relevant ratification law is L.22(III)/2004. The incorporation of the Budapest Convention into the Republic's domestic law is stated in Law 22(III)/2004. The law deals with, inter alia, illegal access, illegal interception, data interference, system

[63]http://www.ocecpr.org.cy/el/content-menu/9-nomothesia/1-nomos-112-i-2004
[64] http://journals.sas.ac.uk/deeslr/article/viewFile/1756/1693
[65]http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/138(I)-2001_en.pdf
[66] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

interference, the misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringement of copyright and related rights and sanctions and measures. The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, is L.26(III)/2004. This legislation covers racism and xenophobia via computer systems and the Internet. Additionally, Law 147(i)/2015[67] is implementing the Directive 2013/40/EU on attacks against information systems. This Law has provisions on the illegal interference to systems and data.

Domestic law recognises fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. Domestic law specifies safeguards to protect the individual's right to privacy during the collection, use and disclosure of personal information in investigations involving electronic evidence. The Constitution of the Republic of Cyprus, Article 5[68] states that the Republic of Cyprus shall secure to 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. The country has 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. Additionally, Section 19 of the Cyprus Constitution protects the right to freedom of speech and expression. More specifically, paragraph 2 of the aforementioned Section explicitly provides that the above right includes: the freedom to hold opinions and receive and impart information.

The Processing of Personal Data (Protection of Individuals) Law (N. 138(I)/2001)[69] entered into force in November 2001 in order to address privacy issues related to collection, storage, processing, dissemination and use of personal data, and was amended by Law N. 37(I)/2003[70]. It is compliant to the acquis communitaire, and especially, the European Directive 95/46/EC on Data Protection[71]. The Office of the Commissioner for Personal Data Protection (OCPDP) was established in Nicosia on 1st May 2002. The OCPDP is an independent administrative authority which deals with the protection of personal information relating to an individual, against its unauthorised and illegal collection, recording, and further use.

Issues concerning Internet safety and protection of personal data are addressed in Part 14 of The Regulation of Electronic Communications and Postal Services Law 112(I)/2004[72]. Part 14 of this Law (Security, Secrecy and Data Protection) is essentially the incorporation of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

[67] http://www.cylaw.org/nomoi/arith/2015_1_147.pdf
[68] http://www.kypros.org/Constitution/English/appendix_a.html
[69] http://www.cylaw.org/nomoi/arith/2001_1_138.pdf
[70] http://www.cylaw.org/nomoi/arith/2003_1_037.pdf
[71] http://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:31995L0046
[72] http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/112(I)-2004_section106_en.pdf

concerning the processing of personal data and the protection of privacy in the electronic communications sector into the Republic's municipal law.

Moreover, the Law on the Retention of Telecommunication data for the investigation of serious offences, L.183(I)/2007[73] reordered the Directive 2006/24/EC[74]. The law regulates the terms under which the retention of personal data for the purpose of crime investigation, detection and prosecution is legal. This Law forces the ISPs to store telecommunication and traffic data (IP addresses, calling numbers and emails) for the purpose of investigation for the period of six months. The police are able to access this data (under court warrant) during the investigation of serious crimes that are punishable by the given legislation with imprisonment more than five years.

Comprehensive legislation on protection of children has been adopted and enforced, through the Law for Combating Trafficking, Exploitation of Human Beings and for the Protection of Victims[75]. This Law ensures data protection and privacy rules for legal minors. The legal and institutional framework for the protection of children's rights is largely in line with the international human rights obligations in this field. In particular, the Fighting of Marketing of Persons and Sexual Exploitation of Minors Law 2000 2(I)/2000 and the Budapest Convention of the Rights of the Child (Ratifying) Law 1990 (No. 243 199) are laws aimed at the protection of children, particularly online.

Law L.91(I)/2014 revises the legal framework on the prevention and combating sexual abuse and sexual exploitation of children and child pornography. This legislation ratifies the EU Directive 2011/93/EE and covers child pornography and grooming. During the adaptation of the Law different stakeholders were involved in discussions such as the Police, NGOs and the Cybercrime Unit. Review participants noted that although there is a general increase in child pornography, most of the cases are prosecuted. There are processes in place to trigger changes in legislation. For example, the Ministry of Justice organises regular meetings in order to reassess which articles need changes and should be improved. Additionally, gaps identified during the prosecution and every day practice lead to recommendations for changes in the law.

Comprehensive legislation protecting consumers from business malpractice online has been adopted and is enforced. E-commerce in Cyprus is regulated by the Electronic Commerce Law 156/2004[76]. The Law entered into force on the 30th of April 2004 for the purpose of the implementation of Directive 2000/31/EC of the European Parliament and the Council of the European Union of the 8th of June 2000 on certain legal aspects of information society services, in particular electronic commerce in Internal Market. The Law 156(I)/2004 aims at ensuring the free movement of information society services between the Republic of Cyprus and the EU/EEA Member States regarding the establishment of service providers, commercial communications, the conclusion of electronic contracts, the liability of intermediaries, out-of-court dispute settlements, codes of conduct, means of legal

[73] http://www.cylaw.org/nomoi/arith/2007_1_183.pdf
[74] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14012
[75] http://www.infobuscy.eu/resources/legislation/Legislation-05_EN.pdf
[76] http://www.cylaw.org/nomoi/enop/non-ind/2004_1_156/full.html

protection and the cooperation between Member States. Additionally, the law regulates the following online activities: online information services; online advertising and marketing; online selling of products and services; online entertainment services;

A lead agency responsible for the protection of consumers online has been designated. The Competition and Consumer Protection Service[77] constitutes one of the divisions of the Ministry of Energy, Commerce, Industry and Tourism. The main objective of the Service is the protection of the consumers' health, safety and economic interests, by creating a competitive environment throughout the domestic market. This is achieved through effective enforcement, improving monitoring of consumer markets and better informing and educating consumers. The Competition and Consumer Protection Service is responsible for the enforcement of Law. Participants informed us that Cyprus is now in the process of adapting and implementing a new law on e-commerce, which has provisions on cybercrime incidents such as online fraud, spams, phishing sites etc. Overall, the country follows international and EU good practises and is taking part in many EU meetings on the changes required in legislation.

Comprehensive legislation addressing intellectual property of online products and services has been adopted and is enforced. Cyprus statutory legislation, regarding Intellectual Property, is 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 intellectual-property related Law is harmonised with EU law. Cyprus has always made a consistent effort to remain in line with international developments in intellectual-property law. Cyprus is signatory to the following international conventions relevant to IP such as: the European Community Trademarks; Convention Establishing the World Intellectual Property Organisation (WIPO); WIPO; The Madrid Agreement Concerning the International Registration of Marks (the "Madrid Agreement") and Protocol to the Madrid Agreement; The Patent Cooperation Treaty; Berne Convention for the Protection of Literary and Artistic Works; Paris Convention for the Protection of Industrial Property.

Substantive cybercrime legal provisions are contained in the general criminal law. The Criminal Code[78] (Ch. 154) comprises a codified version of all main offenses and criminal responsibilities. Matters of criminal proceedings are governed by the Criminal Procedure Code (Cap 155). The Criminal Procedure Code is structured to provide support to all significant provisions of the Constitution of the Republic of Cyprus, the European Convention of Human Rights and international treaties. This provides for the application of the law in such a way, so as to safeguard the rights of citizens, while not hindering the protection of individuals from criminal wrongs and the suitable conferment of justice.

[77] http://www.mcit.gov.cy/mcit/cyco/cyconsumer.nsf/index_en/index_en?OpenDocument
[78] http://www.sbaadministration.org/home/legislation/01_02_09_01_COLONIAL_CAPS_1959/01_02_01_04_Caps-125-175A/19600101_CAP154_u.pdf

The Code includes provisions on the investigation of crime and evidentiary requirements. Cyprus has established agreements with Interpol and Europol as well as bilateral agreements with non-EU neighbouring countries, on cross-border information sharing. For example data is preserved via 24/7 channel and then members have to apply for formal authorisation to receive more data from services. Europol is responsible to collect and lead investigations with the member states. Review participants noted that the new GDPR will cover this gap for most cases.

However, the existing legislation does not include specific provisions for incident reporting. ISPs are not obliged to report to the police but they are obliged to report to OCECPR. The police may request access to the information provided to OCECPR. However often ISPs report voluntarily to the police in serious incidents. There are provisions that facilitate the investigation of cybercrime. The country is now in the progress of developing a framework for incident-reporting within the public sector. Cyprus is also at the final step towards introducing the right for courts and police to block sites and remove unlawful content. A platform exists for communication between ISPs and other law-enforcement agencies for the removal of copyright-infringing content. Participants noted that there is very good cooperation established with the ISPs and, although it is not legislated, they regularly comply with the recommendations of the cybercrime unit.

Participants identified a gap regarding online reporting of complaints. Moreover, it was mentioned that a common platform for e-evidence solutions would facilitate existing processes and minimise the timeframe currently needed.

Participants mentioned that the existing frameworks need to be extended to other sectors. There is also a need to evaluate the existing legal frameworks and make proposals for amendments. Participants noted that the implementation of the NIS Directive will make things much easier in this regard.

D 4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Formative to Established

A comprehensive institutional capacity with necessary human, procedural and technological resources to investigate cybercrime cases has been established in Cyprus. Digital chain of custody and evidence integrity is established including formal processes, roles and responsibilities. The Office for Combating Cyber Crime (OCC) was established in 2007 based

on the Police Order 3/45 and it comprises investigators as well as forensic analysts. The Digital Evidence Forensic Laboratory (DEFL) is under the same administration and was established in 2009. DEFL is staffed with specialist personnel in the collection of evidence and digital forensic analysis of electronic devices. It is the only Government Computer Forensic Lab in Cyprus. The types of cases handled include: child pornography (content-related crimes); attacks on information systems (hacking); computer-related forgery (phishing sites); malware; gambling and requests from other countries (Mutual Legal Assistance Treaty, MLAT).

The OCC participates in Europol lEC3, Cyborg and the Terminal 24/7 service. It also participates in EMPACTS on Child Sexual Exploitation (CSE) and cyber attacks. Moreover, cooperation agreements have been established with the Europol Malware Analysis System (EMAS); with OCECPR on the development of the National Cybersecurity strategy; ENISA; the European Police College (CEPOL); CERTEU; the European Commission; the Council of Europe and the Violent Crimes Against Children International Task Force (VCACITF). Furthermore, it is an active member of Europol INTERPOL, the European Union Cybercrime Taskforce (EUCTF), the European Union's Judicial Cooperation Unit (EUROJUST) and an active collaborator of the FBI as well as the European Cybercrime Training and Education Group (ECTEG).

Within the framework of Prevention of and Fight against Crime Programme of the European Union, Cyprus was granted funding for the establishment of the Cyprus Cybercrime Centre of Excellence (3CE). 3CE provided short-term, highly focused and specialized training seminars on cybercrime-related issues for public and private sector participants. Modules were developed especially for judges, prosecutors and law-enforcement officers. However, this was a project of limited duration. The Ministry of Justice is now evaluating a proposal by OCECPR to develop a structure and take over actions similar to those of 3CE under a new national framework.

Cypriot authorities indicated that international cooperation and contribution from specialist organisations such as Europol are considered very important for the successful investigation of many cases. Currently, the responsibility for the investigation of fraud and other economic crimes committed via the Internet lies with the Criminal Investigation Department of each District. Financial offences committed via the Internet are also investigated by the Financial Crime Unit at Cyprus Police Headquarters. Within the context of the Convention for Cybercrime, the 24/7 point of contact is the Head of the OCC, who is also responsible for the execution of MLAT requests. The second point of contact is the National Central Bureau (NCB Interpol) Nicosia, which is responsible for forwarding requested information to the Head Officer of the Cybercrime Department outside working hours. The Cyprus Police is also the contact point provided for in Law 147(I)/2015 transposing Directive 2013/40/EU.

There is specific training within the police academy on topics such as forensics and there are lectures related to cybercrime issues in general. There is also dedicated training provided within the 3CE, such as the crime investigation officer course and the advanced crime course. These are related to preliminary investigation and forensics. Participants noted that overall there is sufficient training and expertise in these fields. Law enforcement are also

evaluators for other countries' law enforcement agencies. What are missing are specific cases concerning cyber-incidents and attacks on information systems. Participants noted that there is a gap in cyber investigations and plans are being made to purchase a tool that has the ability to collect and analyse information related to dark markets.

A limited number of specialist cybercrime prosecutors have the capacity to build a case based on electronic evidence, but this capacity is largely ad-hoc and is not institutionalised. If prosecutors receive training on cybercrime and digital evidence, it is ad-hoc and not specialised. Participants noted that there is a gap here, since not many prosecutors have basic knowledge and can prosecute such cases.

Most judges have the capacity to preside over a cybercrime case, and receive training on cybercrime and digital evidence. The European Commission is offering training for judges. Also, 3CE provides a highly focused and specialised training seminar for Law Enforcement Agents and Judicial Authorities. Experts from abroad, from Interpol and similar organisations, present at these events.

Another aspect mentioned by participants is the fact that it is important for Cyprus to know what it is really happening, what the new threats are, who are the targets and what are the gaps. Currently, there is no capacity to measure incidents. Participants suggested that the National CSIRT should have the leading role for collection and analysis of cyber incidents and this would benefit prosecutors as well. The government is already considering allocating budget for building a semi-automated information-sharing platform.

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Stage: Established

Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime by facilitating its detection, investigation, and prosecution, with established communication channels. Cyprus cooperates with EU and third countries on the basis of bilateral and multilateral agreements in this field and other channels for exchange of information. Law 102(I)/2011 regulates all formal procedures for cooperation with Europol. Law 112(I)/2004, as amended, does not contain any specific procedures in relation to cybercrime cases. However, it contains general provisions for the representation of Cyprus

in international organisations such as ENISA through OCECPR, ITU and ICANN. The cooperation with third countries regarding the investigation of police cases is based on bilateral and multilateral agreements. As mentioned above, the OCC cooperates closely with the Europol lEC3, Cyborg and the Terminal 24/7 service as well as Europol Malware Analysis System (EMAS). Furthermore, it is an active member of Europol, INTERPOL, the European Union Cybercrime Taskforce (EUCTF), the European Union's Judicial Cooperation Unit (EUROJUST) and an active collaborator with the FBI as well as the European Cybercrime Training and Education Group (ECTEG).

Mutual legal assistance and extradition agreements and mechanisms have been established and are applied to cybercrime cases, both within the EU and with a number of other countries. Legislative requirements for the exchange of information between domestic public and private sectors have been determined. Law 23(I)/2001[79] on International Cooperation in Criminal Matters is the national law applicable to Mutual Legal Assistance (MLA) requests. In addition, MLA is carried out on the basis of bilateral agreements and conventions such as the European Convention on Mutual Assistance in Criminal Matters, Law 2(III)/2000 and the Convention on Cybercrime Law 22(III)/2004.

The National Cybersecurity Strategy provides scope for using a Public-Private-Partnership (PPP) in the prevention of and fight against cybercrime. It is currently under examination by Cyprus authorities. However, a model of cooperation specifically in the field of prevention and raising awareness has been developed with involvement of actors such as OCECPR, GOV CSIRT, Ministries, ISPs, etc.

The police cooperate with private companies reporting a cyber-attack to help them resolve this problem and investigate the offence. Critical infrastructure operators in the field of electronic communications have specific legal and regulatory obligations as regards network and information security which cover availability, cyber-attacks, prevention and mitigation measures. Operators also have reporting obligations relating to incidents affecting availability of networks and services and to data breaches. Review participants suggested that multifaceted cooperation between public authorities and the financial sector could work to benefit both of them and significantly increase the level of cybersecurity in Cyprus. At the moment, the public authorities do not cooperate directly with banks and other financial institutions, but a cooperation framework is under consideration.

RECOMMENDATIONS

Based on the review of the cybersecurity capacity maturity of legal and regulatory frameworks, the Centre has developed the following set of recommendations to be considered by the Cypriot government for the enhancement of existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

[79] http://www.cylaw.org/nomoi/arith/2001_1_023.pdf

LEGAL FRAMEWORKS

R 4.1 Ensure that the GDPR is implemented and that legal mechanisms are in place which enable strategic decision-making and determines the timeframe after which personal data is no longer required as evidence for investigation and must be deleted. Identify International and regional trends and good practices to inform the assessment and amendment of data-protection laws and associated resource planning.

R 4.2 Enact commencement orders for existing legislation and assign bodies to monitor the enforcement of cybersecurity and data protection-laws such as the GDPR.

R 4.3 Ensure that international and regional trends and good practices inform the assessment and amendment of domestic legal frameworks protecting human rights online and any associated resource planning.

R 4.4 Develop and adopt legal provisions on procedural powers for investigations of cybercrime and crimes involving electronic evidence.

R 4.5 Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted in order to successfully investigate cybercrime.

R 4.6 Adapt and implement legal provisions on e-commerce, regarding cybercrime incidents such as online fraud, spam, and phishing sites.

R 4.7 Consider developing a platform for sharing electronic evidence between regional cybercrime forces.

R 4.8 Enhance the existing cooperation between ISPs and law-enforcement agencies for removal of copyright-infringing content from websites.

R 4.9 Consider joining regional cybercrime forces to enhance international cooperation to combat cybercrime.

LEGAL FRAMEWORKS

R 4.10 Foster research on human rights on the Internet and ensure that measures are in place to exceed minimal baselines specified in international agreements.

CRIMINAL JUSTICE SYSTEM

R 4.11 Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators.

R 4.12 Allocate resources dedicated to fully operational cybercrime units based on strategic decision-making in order to support investigations, especially at a local level.

R 4.13 Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence through 3CE or other organisations.

R 4.14 Build a cadre of specialist prosecutors and judges to handle cybercrime cases and cases involving electronic evidence.

R 4.15 Establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges, in order to ensure efficient and effective prosecution of cybercrime cases.

R 4.16 Work on building on the cooperation between the National CSIRT and other sectors on collecting and analysing cyber-incidents through an information-sharing platform.

R 4.17 Collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

R 4.18 Allocate resources to support the exchange of information between public and private sectors domestically and to enhance the legislative framework and communication mechanisms.

R 4.19 Enhance cooperation between the public sector and banks and other financial institutions regarding the sharing of incidents, in order to increase the level of cybersecurity awareness in Cyprus.

R 4.20 Strengthen informal cooperation mechanisms within the police and criminal-justice system, and between police and third parties, both domestically and across borders. Consider know-hows from other areas, such as anti-corruption cooperation.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses 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.

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-up – Formative

The Republic of Cyprus has established the Cyprus Organisation of Standardisation (*Κυπριακός Οργανισμός Τυποποίησης*)[80] under the Ministry of Finance (*Υπουργείο Οικονομικών*). There is a specific branch for information and technology sector standardisations[81] where organisations, both private and public, can refer to for accreditation to ICT standards.

Focusing on the public sector, participants noted that there are criteria and minimal security requirements across all departments. These are recommended and advertised by DITS,

[80] http://www.cys.org.cy/el/
[81] http://www.cys.org.cy/en/who-we-are/organization-charts

however, they are not mandatory. As it was mentioned, these security suggestions are based on a general controls-review that was conducted a few years ago across all government departments. These minimal controls follow to a certain extent ISO 27001 but are tailored to the gaps identified in the governmental systems. Unfortunately, as participants suggested, the lack of an authority to ensure that standards are adhered to resulted in a low adoption rate of the security requirements.

Although a uniform application of good practices is promoted, participants deemed that the public sector is segmented and each department decides on which policies should be followed by departments. The main reason is the absence of a mechanism to enforce a uniform application of policies. A new cybersecurity framework for the public sector as a whole is under development and final decisions are expected by the end of 2017. As participants acknowledged the new policies and the administrative, organisational and technical measures will apply for all government services.

The lack of accountability to employees in cases of policy misuse, financial constraints as well as limited human resources are the main reasons for the poor cybersecurity posture of the public sector. It was mentioned that IT personnel might have to undertake multiple roles with limited training. These multiple roles potentially reduce the number of related job opportunities in the public sector. It is noted that the Republic of Cyprus is the last country in the EU in terms of employment in the ICT sector[82]. Additionally, cybersecurity initiatives are often not supported, due to the fact that government officials perceive these more as additional, potentially unnecessary, expenses rather than investments. Furthermore, current employment legislation is out of date and disciplinary actions relating to policy violations cannot be enforced.

Participants theorised that the lack of (known) major incidents in the Republic of Cyprus results in lack in motivation to spend more money on security. They believe that only with mandatory requirements for the adherence to standards, with the appointment of security officers who will be held responsible for the implementation of these standards and with periodic audits will the public sector's cybersecurity posture improve. Participants concurred that the NIS Directive will provide valid grounds for promoting all the aforementioned recommendations.

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, with finance and electronic communication companies being pioneers in this area. Certain sectors, such as electronic communications and finance have mandatory security requirements; however, in the majority of the cases the driving force for adherence to standards is market demand and business needs. ISO 27001 is the most frequently adopted framework, although rarely does the whole organisation adhere to this. Rather, critical parts are certified, and the remaining systems follow it vaguely.

More specifically, some electronic communication companies have adopted ISO 27001 ten years ago and, as participants suggested, a comprehensive information security

[82] http://digital-agenda-data.eu/

management system should be mandatory for the entire organisation. Other standards regarding business continuity are followed as well. External auditing processes are conducted only for critical systems and there is no internal auditing for the remaining parts of the organisation.

Participants agreed that the banking sector is heavily regulated, despite the fact that there is no specific standard promoted by Central Bank. There are regulations and processes for high-level security and audit processes are conducted by Central Bank, which holds the role of the regulator. The frequency of these audits depends on the criticality of the system. Participants described a security procedure which details four lines of defence based on how critical the function is determined to be. When gaps in security practices are identified, reforms must be made, otherwise the regulator has the mandate to fine banks. There are a combination of international standards, such as PCI DSS[83] for data security and others imposed by MasterCard[84] and Visa[85], which companies usually set out to follow strictly.

Focusing on the standards related to procurement of hardware, similar conclusions regarding the maturity of the public and private sectors can be drawn. There is an attempt to provide a unified process to guide the identification of standards for procurement of hardware in the public sector, but it is not standardised in every department. Instead, a more general framework based on procurement laws is provided and different ministries have different procedures and policies in place. Considering the private sector, there are internal policies and procedures in place that participants characterised as thorough. These are often evaluated and updated. In some cases, business-continuity requirements are included in tenders. It is worth noting that there is no mandatory procurement standard for any sector except the telecommunication sector. There, procurement requirements are covered within specific legislation, however there are discussions about the revision of this legislation between the regulator and the companies.

Focusing on standards in software development, there are guidelines in place in both public and private sectors, but the extent to which these guidelines are related to cybersecurity is not clear. Participants suggested that there are requirements in the public sector in terms of library usage in coding. The finance sector has principles for considering software purchase while the private sector relies on testing and audits such as source-code reviews and security assessment of software.

Participants acknowledged the need for a security-related authority to set standards across all sectors and promote adherence to these standards. The importance of streamlining the process of software and hardware procurement was highlighted as well. It was further suggested that discussions with all relevant stakeholders and regulators must commence before the adoption of the NIS Directive and the GDPR, to agree on criteria for the creation of frameworks that will cover the requirements of these EU legislative efforts.

[83] https://www.pcisecuritystandards.org
[84] http://www.mastercard.com/sea/consumer/standard-mastercard.html
[85] https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf

D 5.2 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 aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Established

There are specific provisions described in order 253/2011 for the security of network and information systems, which ensure the resilience of the Internet infrastructure. These provisions are mandatory within the infrastructure of ISPs and other electronic communication organisations. Risk assessment and business continuity planning documents are produced and reviewed by OCECPR annually, complemented by on-site audits.

According to the EU Digital Agenda Scoreboard key Indicators (DISA[86]), the Republic of Cyprus is one of the few countries within the European Union that provides 100% coverage and availability of standard fixed broadband services[87]. However, these services are the least affordable in terms of standalone fixed Internet access amongst all the European Union member states[87]. This probably explains why the percentage of households that do not have Internet access is one of the highest in Europe[87]. Another possible explanation is the fact that the percentage of users with basic or above basic digital skills is one of the lowest amongst EU countries[87].

These statistics provide the foundations to understand the maturity of Internet infrastructure resilience and the security standards in the e-services offered by public and private organisations. Participants suggested that a wide range of e-government services are offered via a system named Ariadne. There was recently an effort to enforce the submission of tax forms through online systems (TAXISNET), but according to DISA the percentage of citizens who interact online with the public sector is one of the lowest in EU[87]. There are plans in place to provide citizens with certificates for authentication and digital signing that may come to fruition within the next year. There are also suggestions to create pilot programmes within the public sector to boost the uptake of the new initiatives.

Regarding the private sector, there are an abundance of e-services offered and participants deemed that their uptake is increasing. The telecommunication sector has programmes in place to boost customer confidence and trust in electronic services. Efforts to urge users to use stronger passwords were in vain due to the users' inability to use password management applications. ISPs have succeeded in obtaining users' consent stipulating that they, as users, are responsible for possible cyber-incidents due to their negligence. ISPs provisionally monitor some services for cyber-attacks and in the case of certain incidents

[86] http://digital-agenda-data.eu/

provide guidance on how to resolve the problem. They also offer to certain customers protection from Distributed Denial of Services (DDoS), however, this service is rather expensive.

In the finance sector, online services are heavily regulated and it is to the benefit of the banks to promote these services and mandatory to raise security awareness amongst their customers. Individual banks decide the means through which this will be achieved. Most common practices in raising security awareness include email notifications promoting best practices for online security, the adoption of minimum password policies and camera stickers for mobile and laptop devices. Recently there has been an effort by the banks to incentivise people to use online services by offering their customers online services free of charge and cheaper transaction fees than within bank branches. However, the percentage of people who are using online banking is one of the lowest in the EU, according to DISA[87]. Participants' opinions were split as to the origins of this issue. Some suggested that despite recent efforts there is still a lack of promotion of these services from the banks. Others mentioned that the crisis in 2013 has affected the public's trust in banks, hence people are hesitant to accept online offers. They deemed, however, that the situation is gradually improving.

D 5.3 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 criticality of services.

Stage: Formative

The processes of developing an inventory of software in the public and private sector and a catalogue of secure software are in a primitive stage. The public sector manually maintains an inventory of the software used in their internal network, while remaining oblivious to the software users install in other systems. In a similar vein, private organisations maintain up-to-date inventories mainly of critical assets and on certain parts of the network they restrict users' ability to install software. The majority of the participants noted that their organisations depend heavily on software purchased from multinational companies. In cases where software is developed in-house, it is used only internally as opposed to customer-facing applications.

Participants mentioned that in the public sector system administrators are responsible for maintaining a test environment, but budget restrictions render this task difficult. Antivirus

[87] http://digital-agenda-data.eu/

updates are performed in an automatic fashion, while updates to operating systems may be executed manually, depending on the department and the criticality of the system. Some participants noted that in certain departments, software updates might take up to a month, due to human-resource limitations. As it was mentioned, updates are required to take place outside normal working hours and in several cases there is a single employee responsible for upgrading software for a whole department. They also acknowledged that bandwidth problems impede the updating process and on certain occasions these updates are not available from the central system which provides all the necessary executable files. Participants also noted that for personal laptops, which are widely used by employees in the public sector, IT personnel are responsible neither for the updating of software nor for software installation. Therefore it is up to users to keep their personal laptops secure. However, there are plans in progress to acquire specialised services (Zeus System Corporation[88] was mentioned) to allow automatic updates for core software and applications, such as MS Office, Java and email clients.

Participants considered that software quality development in the private sector is more mature. There are more human resources available and, depending on the criticality of the system, either system administrators are responsible for updates or these happen automatically. In the latter scenario, updates are installed within a day depending on availability requirements. The extent to which the timing of these updates (when these updates will take place) is determined based on risk-assessment processes that consider cyber-incidents is unclear. There were cases where the updates of systems, especially for SCADA systems, would be performed by vendor experts and only on the organisations' premises.

To conclude, quality assessments and, in particular, monitoring of performance of deployed software are issues of concern. These practices are conducted in an ad-hoc manner and usually focus on critical aspects of systems.

D 5.4 TECHNICAL SECURITY CONTROLS

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

Stage: Formative

The adoption of technical security controls in the Republic of Cyprus varies across sectors and organisations. Participants suggested that the adoption and implementation of controls in government bodies is elementary and inconsistently promoted, due to financial

[88] http://www.zeussystems.com

restrictions, limitations in human resources and lack of appropriate organisational structure. It was further emphasised that, as of spring 2017, a new centralised framework of critical controls is being implemented across all ministries and services in the public sector. The plan is scheduled to be completed within 18 months, with its progress being monitored by DITS and the auditing services of the government.

The main technical controls which are implemented in almost every single government department are the use of back-ups and antivirus services. Files stored in Active Directory are automatically backed-up. There are additional servers which departments are responsible for maintaining and on these back-ups may be conducted manually. Guidelines are available to users detailing how to back-up data stored on their personal devices. Participants noted that the majority of employees lack the knowledge to utilise these back-ups in emergency situations. There have been instances where automatic back-up services have failed, but it is not feasible for the time being to monitor which devices failed to successfully back-up data.

Antivirus services are automatically updated in all departments and on all personal devices. Additional technical controls are implemented for the Active Directory, where hardware and software inventories are manually maintained for all workstations that are connected through it. Participants admitted, however, that servers exist which are not visible to the main system and IT personnel from specific departments are responsible for their security.

Further concerns were raised over the lack of financial resources and organisational structure. As participants explained, often departments maintain their own servers, but due to limited resources back-ups are not implemented, there is no monitoring of sensitive files and security responsibilities are delegated to simple users. In addition, unauthorised machines may obtain access to these servers, since there are no controls to maintain an inventory of or authenticate access to these servers by laptops or Internet of Things (IoT) devices. Furthermore, the understaffed IT departments report to the general secretaries of their respective ministries rather than DITS, which handle central IT such as email services and Internet.

Participants voiced concerns over the shortage of personnel and the lack of training for existing IT employees. They mentioned that for the past ten years requests for IT specialists have been systematically ignored by government officials. They also identified a lack of clear policies regarding implementation of controls and guidance on best practice. Communication problems between departments were highlighted, which render the implementation of critical controls such as patching and software updates for critical systems in danger.

Finally, of particular concern is the complete absence of evaluation metrics for determining the effectiveness of the existing technical controls. This is due to the fact that monitoring practices, which may allow such evaluations as well as the detection and prevention of incidents, are scarce. A characteristic example is the fact that for 200 critical systems, including water and electricity, participants suggested that there are only 2 people performing IT audits.

To move forward, the replacement of PCs with thin clients was suggested because it may provide a centralised structure and remove the burden of implementing technical controls from the users. Additionally, participants concurred that a single authority should be responsible for strategic decisions on technical controls, should supervise all networks end-to-end and promote the adoption of a unified framework for security controls.

In the private sector there is an understanding that organisations adopt adequate technical controls tailored to their networks. Network-segmentation controls and monitoring tools are evident in this sector, as well as the use of Intrusion Detection Systems (IDS) and other Security Information and Event Management tools (SIEM). Some organisations have recently upgraded their security controls and the majority obtain high-level information from reporting mechanisms. Finally, there are organisations that have decided to outsource security to third parties, especially for SCADA systems.

Some participants, however, questioned the level of security that many banks may have. As an example, a case of online fraud exceeding the amount of €1,000,000 was mentioned. This incident originated from a phishing email. It involved an international transaction and it was only stopped and reported as a cyber-incident because the company that was supposed to have requested the transfer questioned the legitimacy of the transaction. Both the Cypriot and the receiving bank had authorised the transaction.

Generally, the level of understanding and deployment of security controls in the private sector is thought by the participants to be adequate. However, no mechanisms are in place to assess the effectiveness of these controls, nor processes to recommend further improvements.

D 5.5 CRYPTOGRAPHIC CONTROLS

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.

Stage: Formative

The use of cryptographic controls varies across sectors and organisations. In the public sector cryptographic controls are applied to data at rest and in a small number of cases to data in transit. Participants mentioned that critical data is encrypted, as well as all communications between different departments as long as they use government equipment. No encryption is provided for personal devices, however, and the same remark applies for back-up systems. Exceptions may occur only for high-ranking officials. Their devices are encrypted, but not their email exchanges.

Participants were concerned that all email exchange within the government is conducted unencrypted through personal devices, whereas they highlighted that users may send sensitive information (the example of a police report was mentioned) from their personal devices using non-governmental email clients, such as Yahoo or cloud services such as Dropbox.

Regarding the private sector, similar observations can be made. Encryption is considered mainly for critical systems both for data in transit and data at rest. Certain sectors have their back-up systems encrypted as well. Some participants mentioned that their organisations are in the process of encrypting all personal devices.

A major difficulty in applying cryptographic controls is the archaic legislation that governs how sensitive information is handled. Top-secret files should be protected to the extreme, within Faraday cages (according to participants this legislation has been in place since 1960). Handling of sensitive information which does not classify as top-secret is defined according to recent European directives with mandatory processes and requirements for all levels of classification. However, participants suggested that there is a lack of understanding in how encryption works and the level of security it may offer.

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-up to Formative

The domestic market for cybersecurity technologies revolves around services. There are a limited number of software products on offer as well as SIEM systems (*Clear Skies*[89]). Participants suggested that the demand for these services in the public sector is low and focuses mainly on cleaning bad traffic from governmental networks. On the contrary, consultancy firms ("the Big Four"[90]) regularly offer their services to the private sector, whereas some companies also acquire software and utilise SIEM systems designed "locally", either in Cyprus or in Greece.

The cyber-insurance market in Cyprus is in its infancy. There are a small range of products on offer and usually these detail situations under which the insurance is valid and, on a positive note, specify policies that organisations must adhere to in order to be insurable. A small number of participants noted that their organisations are covered for specific cyber-incidents. These insurance products define what an incident is, the level of exposure and

[89] http://www.odysseycs.com/home/
[90] The big four are Deloitte, KPMG, Ernst & Young and Mackenzie

coverage offered, forensic investigation and support. They are rather vague on the types of controls that organisations must adhere to, since they merely stipulate that they should follow best practice in security.

Participants concurred that it is beneficial for all organisations to obtain cyber–insurance, since, as they suggested, even the cost of one incident justifies the expense. Additionally, they highlighted that the support offered during incidents and specifically the forensic analysis is invaluable. As insurance companies are re-evaluating their options in Cyprus, they could potentially offer tailored products for this type of assistance only. Finally, in order to boost the market in cyber-insurance, participants suggested that the OCECPR could require all companies that want to be licensed to operate critical information infrastructure to be cyber insured.

D 5.7 RESPONSIBLE DISCLOSURE

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

Stage: Start-up

No responsible disclosure policy or framework has been established in the public sector. Participants acknowledged that there are channels in place to report incidents, but the majority were not aware how to do so. Despite the fact that there is a hotline desk and a mobile application dedicated to incident reporting, these are not advertised and promoted effectively. Participants suggested that police do not currently have the resources to deal with all types of incidents and mainly focus on illegal online content. Additionally, there is no specific framework to dictate what information should be shared, and incident notification is not mandatory.

Focusing on the financial sector, although vulnerabilities are an increasing concern, incidents are perceived as confidential commercially valuable information. As a consequence, and due to the fact that banks are not obliged to report incidents, they tend to conceal any issues that they detect. Information is shared formally by banks with the Cypriot Central Bank only in the case of major incidents. Depending on the severity of the attack, the Central Bank will decide whether or not to inform other Cypriot financial institutions. Information on incidents is shared through formal channels and there are thresholds set by the European Central Bank as well as the Cypriot Central Bank for recording incidents.

In the electronic communications sector there is a platform for threat-intelligence sharing. Notification of incidents to OCECPR is mandatory once a certain threshold is exceeded.

There is no sharing of intelligence, however, either between electronic Comuunications stakeholders or across other sectors. Participants noted that the EU will define thresholds and notification requirements for all sectors as part of the NIS directive. These requirements will not only consider availability of services, but also the integrity and confidentiality of data. Furthermore, clear instructions will be provided on how to share information uniformly within the EU in a formal and structured manner.

RECOMMENDATIONS

Based on the review of the maturity of standards, organisations, and technologies, the following recommendations are provided for consideration by the government of the Republic of Cyprus. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R 5.1 Adopt a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors, including standards in procurement and software development.

R 5.2 Establish or assign an institution responsible for the implementation, auditing and measurement of the success of standards across public and private sectors. Apply metrics to monitor compliance and establish periodic audits.

R 5.3 Promote discussions on how standards and good practices can be used to address risk within critical infrastructure supply chains by both government and infrastructure organisations. Identify and mandate standards to which CIIs should adhere to.

R 5.4 Identify a minimum set of controls for all governmental departments based on annual assessments and establish a controls-review to assess the effectiveness of the current controls and practices.

R 5.5 Establish frequent training for IT employees.

R 5.6 Establish mandatory requirements for the adherence to standards by appointing security officers who will be held responsible for their implementation.

ADHERENCE TO STANDARDS

R 5.7 Enact legislation to allow the enforcement of disciplinary action for policy violations.

R 5.8 Streamline clear guidance for the procurement of hardware and software.

R 5.9 Commence discussions with all relevant stakeholders and regulators before the adoption of the NIS and GDPR Directives, to agree on criteria for the creation of frameworks that will cover the requirements of these EU legislative efforts.

R 5.10 Promote the awareness and implementation of standards among SMEs.

R 5.11 Establish a framework to assess the effectiveness of standards for procurement and software development.

INTERNET INFRASTRUCTURE RESILIENCE

R 5.12 Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors.

R 5.13 Conduct regular assessments of processes according to international standards and guidelines together with assessment of national information infrastructure security and critical services that drive investment in new technologies.

R 5.14 Identify and map potential points of critical failure within the Internet infrastructure.

R 5.15 Establish a system to formally manage the national infrastructure, with documented processes, roles and responsibilities, and adequate redundancy.

SOFTWARE QUALITY

R 5.16 Develop a catalogue of secure software platforms and applications within the public and private sectors.

R 5.17 Develop an inventory of software and applications used in public sector and Critical Infrastructure.

R 5.18 Develop policies and processes on software updates and maintenance.

R 5.19 Gather and assess evidence of software quality deficiencies regarding their impact on usability and performance.

R 5.20 Establish or assign an institution to elicit in a strategic manner common requirements for software quality and functionality across all public and private sectors.

R 5.21 Monitor and assess the quality of software used in public and private sectors.

Technical Security Controls

R 5.22 Encourage ISPs and banks to offer anti-malware and anti-virus services.

R 5.23 Establish metrics for measuring the effectiveness of technical controls across the public domain.

R 5.24 Develop processes for reasoning about the adoption of more technical controls based on risk assessment methodologies across the public domain.

R 5.25 Provide citizens with certificates for authentication and digital signing and create pilot programmes within the public sector to boost the uptake of the new initiatives.

R 5.26 Promote best practices in cybersecurity for users.

R 5.27 Consider a centralised structure by replacing PCs with thin clients to alleviate the burden of implementing technical controls from users.

R 5.28 Designate an authority to be responsible for strategic decisions on technical controls that will supervise all networks end-to-end and promote the adoption of a unified framework for security controls.

R 5.29 Keep technical security controls up-to-date within the public and private sector, monitor their effectiveness and review on a regular basis.

R 5.30 Conduct penetration testing for protection of both private and public sectors.

R 5.31 Develop encryption and cryptographic control policies within the public and private sectors and regularly review the policies for effectiveness.

CRYPTOGRAPHIC CONTROLS

R 5.32 Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines.

R 5.33 Raise public awareness of secure communication services, such as encrypted/signed emails.

R 5.34 Use SSL/TLS connections to secure communications between schools and the registry office for the collection of students' data.

R 5.35 Ensure that data are stored in an encrypted format in the schools' equipment.

R 5.36 Establish or assign an institution responsible for designing a policy, aiming to assess the deployment of cryptographic controls according to their objectives and priorities within the public and private sector.

CYBERSECURITY MARKETPLACE

R 5.37 Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development.

R 5.38 Promote sharing of information and best practices among organisations, to explore potential insurance coverage.

RESPONSIBLE DISCLOSURE

R 5.39 Develop a responsible vulnerability-disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledgment report.

R 5.40 Establish or assign an institution responsible for supervising the process of responsible disclosure and ensure that organisations do not conceal vulnerability information.

R 5.41 Develop a system to facilitate threat-intelligence sharing among the critical infrastructure partners. Promote sharing of threat-intelligence in the financial sector and incentivize companies to actively participate.

R 5.42 Promote the hotline and mobile application for incident reporting in the public sector.

R 5.43 Define thresholds and notification requirements for all sectors. These requirements should not only consider availability of services but the integrity and confidentiality of data.

R 5.44 Agree on clear instructions on how to share information uniformly within EU in a formal and structured manner.

ADDITIONAL REFLECTIONS

This was the 19th country review that we have supported directly, and the second review in the Mediterranean region. The Republic of Cyprus has commenced the process of developing different aspects of cybersecurity capacity across all dimensions, including through developing educational programmes and cybersecurity training offerings. If efforts in different organisations and sectors can be linked and coordinated, alongside the establishment of a comprehensive legal, strategic and operational framework for national cybersecurity, it will set the foundations for more advanced capacity in the future.

We hope that this review will offer useful insights to Cyprus and that our recommendations on how to increase cybersecurity capacity will contribute to the on-going work on enhancing cybersecurity capacity across all five dimensions of the CMM.

APPENDIX

SUMMARY OF REVIEW RESULTS

CAPACITY FACTORS	STAGE OF MATURITY	REFERENCES	RECOMMENDATIONS
Dimension 1 Cybersecurity Policy and Strategy			
D1.1 National Cybersecurity Strategy	**Formative to Established**	National Cybersecurity Strategy (NCS) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-cyprus/view OCECPR http://www.ocecpr.org.cy/ NIS Directive http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN	**R 1.1** Develop general KPIs to monitor progress of the implementation of the strategy. **R 1.2** Allocate budget based on cybersecurity strategic plans to drive capacity building investments in security. Strategic plans must consider the implementation of the NIS and GDPR Directives. **R 1.3** Design a methodology to analyse the results of the national cyber risk-assessment and incorporate lessons learnt from this exercise in the revision of the strategy. **R 1.4** Expand the key stakeholder group (steering committee), which is involved in the revision of the national cybersecurity strategy, to include the financial sector, the private sector (including SMEs) that might be considered part of CNI in the near future and international partners. **R 1.5** Enhance collaboration with ENISA regarding the revised strategy and seek advice on the effective implementation of the NIS Directive. **R 1.6** Design and disseminate coordinated cybersecurity programmes. Strengthen and promote inter-departmental cooperation in cybersecurity to ensure full implementation of the cybersecurity programmes. **R 1.7** Design and conduct regular scenario and real-time cyber exercises that provide a contemporary picture of

			national cyber resilience.
D1.2 Incident Response	**Formative**	Ministry of Transport and Communications and Works http://www.mcw.gov.cy/mcw/mcw.nsf/index_gr/index_gr?OpenDocument Ministry of Defence http://www.mod.gov.cy/mod/mod.nsf/index_en/index_en?OpenDocument Ministry of Foreign Affairs http://www.mfa.gov.cy/mfa/mfa2016.nsf/index_en/index_en?OpenDocument Ministry of Justice and Public Order http://www.mjpo.gov.cy/mjpo/mjpo.nsf/index_en/index_en?OpenDocument	**R 1.8** Develop an operational central registry of national-level cybersecurity incidents and designate an entity to be responsible for maintain the list (it is recommended that the national CSIRT must have this role). **R 1.9** Establish a national CSIRT with clear processes, defined roles and responsibilities. Draft legislation that will allocate mandates to the national CSIRT. CSIRT should according to NIS Directive: • ensure high level of availability and business continuity, • monitor incident at a national level, • provide early warnings, alerts, announcements and disseminate threat intelligence to relevant stakeholders, • respond to incidents, • provide risk and incident analysis, • establish relationships with the private sector and other countries. **R 1.10** Establish metrics to monitor and evaluate progress on implementing the CSIRT **R 1.11** Establish metrics to monitor and evaluate CSIRT's effectiveness. Enhancing collaboration with ITU Malaysia and ENISA will be beneficial for this recommendation. **R 1.12** Establish regular training for the CSIRT's employees and design metrics to assess the results of this training. **R 1.13** Create a mandate for a national cyber incident response detailing when and how organisations should report incidents. Reach consensus among stakeholders on architecture, interfaces and standards for information exchange. Common standards promoted by EU are STIX and TAXII. **R 1.14** Identify and document key incident response processes highlighting when and how different Ministries should be involved. **R 1.15** Enhance collaboration with other EU CERTs by establishing formal channels of communication and

			agreeing on specific standards for threat intelligence sharing. **R1.16** Develop coordination and information/cybersecurity threat sharing mechanisms between the private and public sectors, as well as within the cybersecurity community at national, regional and international levels. Ensure the involvement of the financial sector. **R 1.17** Enhance the operational ability of the governmental CERT either by increasing the number of employees involved in incident response or by outsourcing certain parts of the incident handling to other organisations and re-instate the academic CERT.
D1.3 Critical Infrastructure (CI) Protection	**Start-up to Formative**	ISO 27032 https://www.iso.org/standard/44375.html ENISA https://www.enisa.europa.eu TAXISNET https://taxisnet.mof.gov.cy/displayWelcome.do	**R 1.18** Perform detailed audits of CNI assets as it relates to cybersecurity on a regular basis and disseminate CNI asset audit lists to relevant stakeholders. Inform the CNI stakeholders of their responsibilities. **R 1.19** Mandate the design and implementation of appropriate regular cyber risk assessments for all CII stakeholders, in line with recommendations from the NIS Authority and identify the required information to be shared. Design cyber risk assessments for all CNI CII stakeholders based on the national risk assessment approach. **R1.20** Establish a mechanism for regular vulnerability disclosure and information sharing between CNI asset owners and the government. Establish regular dialogue between tactical and strategic/executive levels regarding cyber risk practices and encourage communication among CNI operators. Ensure that the financial sector is involved in the discussions. **R 1.21** Ensure GDPR guidelines are adhered to in the sharing of threat-intelligence information. **R 1.22** Identify internal and external CI communication strategies with clear points of contact. **R 1.23** Establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an

			incident response plan for cyber incidents. **R 1.24** Establish common processes to measure and assess the capability of CI asset owners to detect, identify, respond to and recover from cyber threats.
D1.4 **Crisis Management**	**Formative**	ZENON http://www.mod.gov.cy/mod/CJRCC.nsf/cjrcc45_en/cjrcc45_en?OpenDocument	**R 1.25** Design a cybersecurity needs assessment of measures and techniques for crisis management. The involvement of key stakeholders and other experts, such as think tanks, academics and civil society leaders should be sought. **R 1.26** Participate more actively with more personnel in all exercises organised by ENISA. **R 1.27** Develop a national business continuity plan. **R 1.28** Organise national cyber security exercises, identify metrics to evaluate the success of this exercise and ensure that lessons will inform the decision-making process for future exercises. Plan the exercises by engaging relevant participants, outlining their role in the exercise, and articulating benefits and incentives for participation.
D1.5 **Cyber Defence**	**Formative**		**R 1.29** Develop an official cyber defence document based on the national strategy developed by OCECPR. This document should consider the threats to national security that might emerge from cyberspace. **R 1.30** Develop a cyber risk assessment methodology based on the national risk assessment designed by OCECPR. **R 1.31** Create a CERT for the Ministry of defence. **R1.32** Establish formal communication channels with the forthcoming national CSIRT and OCECPR. **R 1.33** Establish training programs for employees and develop awareness campaigns. **R 1.34** Develop a communication and coordination framework for cyber defence in response to malicious cyber-attacks on military information systems and critical infrastructure.

			R 1.35 Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.
D1.6 Communications Redundancy	**Established**		**R 1.36** Test the interoperability and function of emergency response assets under compromised communications scenarios to inform strategic investment in future emergency response assets based on the results of these scenarios. **R 1.37** Allocate resources to hardware integration, technology stress testing, personnel training and crisis simulations drills. **R 1.38** Establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response asset communications and authority responsibilities. **R 1.39** Connect all emergency response assets into a national emergency communications network with isolated but accessible in emergency situations backup systems. **R 1.40** Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of protocols for communications redundancy tailored to the roles and responsibilities of each organisation in the emergency response plan.

DIMENSION 2 CYBER CULTURE AND SOCIETY

D2.1 Cybersecurity Mind-set	**Formative**		**R 2.1** Enhance efforts at all levels of government, especially officials, and the private sector to employ

			practices. Design systems that enable users across society to embed secure practices more easily into their everyday use of the Internet and online services. **R 2.2** Develop coordinated training programmes for employees in the public sector. **R 2.3** Routinize cross-sectorial cooperation and information sharing among private and public sector organisations on cybersecurity risks and good practice. **R 2.4** Identify vulnerable groups and high-risk behaviour across the public, in particular young people, to inform targeted, coordinated awareness campaigns, as recommended in R3.1.
D2.2 Trust and Confidence on the Internet	**Formative**	DESI (2017) https://ec.europa.eu/digital-single-market/en/scoreboard/cyprus	**R 2.5** Establish ISP programmes to promote trust in their services based on measures of effectiveness of these programmes. **R 2.6** Promote use of e-government services and trust in these services through a coordinated programme, including the compliance to web standards that protect the anonymity of users. **R 2.7** Implement feedback mechanisms for use to ensure that e-services are continuously improved and trust is strengthened among users. **R 2.8** Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content. **R 2.9** Ensure that the private sector applies security measures to establish trust in e-commerce services, including informing users of the utility of deployed security solutions.
D2.3 User Understanding of Personal Information Protection Online	**Formative**		**R 2.10** Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online.

			regarding the protection of personal information and about the balance between security and privacy to inform policy-making. **R 2.12** Promote the compliance to web standards that protect the anonymity of users. **R 2.13** Promote privacy by default as a tool for transparency. **R 2.14** Develop user-consent policies designed to notify practices on the collection, use or disclosure of sensitive personal information.
D2.4 Reporting Mechanisms	**Formative**	Cybercrime Reporting Platform https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm Cyprus Police Mobile Application http://mobile.cypruspolicenews.com/landing/Desktop#.WYI-Fojys2x CyberSafety http://www.cybersafety.cy/	**R 2.15** Develop programmes to promote the use of the existing reporting mechanisms by public and private sectors for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents. **R 2.16** Encourage different stakeholders (public-private sector, Police, CERT) to coordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms. **R 2.17** Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.
D2.5 Media and Social Media	**Formative**	Cyprus News Report https://www.cyprusnewsreport.com/2017/02/cyprus-has-highest-percentage-of-facebook-users-in-eu-cyprus-is-infographic/ Cyprus Mail http://cyprus-mail.com/2017/06/28/major-cyber-attack-disrupts-businesses-around-world/ Cyprus News Agency	**R 2.18** Encourage media and social media providers to further extend the coverage beyond threat reporting and focus on informing the public about proactive and actionable cybersecurity measures, as well economic and social impacts. **R 2.19** Encourage a frequent discussion about cybersecurity on social media. **R 2.20** Ensure that the debate in social and mainstream media and the attitudes expressed inform policymaking.

		http://www.cna.org.cy/webnews-en.aspx?a=da94a22f8d9b4a539c07c6e286ae5d74 Reuters http://www.reuters.com/article/us-cyprus-cyber-cenbank-idUSKCN0XX1NQ

Dimension 3 Cybersecurity Education, Training and Skills

D3.1 Awareness-raising	**Formative to Established**	CyberEthics http://www.cyberethics.info/ CYberSafety http://www.cybersafety.cy/ Helpline http://cybersafety.cy/helpline Hotline http://cybersafety.cy/hotline eSafe Schools http://esafeschools.pi.ac.cy/ Young Coaches for the Internet programme http://youngcoaches.pi.ac.cy/ Annual Short Videos by Students competition http://internetsafety.pi.ac.cy/competitions CYberSafety Youth Panel	**R 3.1** Continue working on the development and the implementation of the National Work Plan for cybersecurity awareness-raising programme, with specified target groups, focusing on the most vulnerable users. **R 3.2** Appoint a designated organisation (from any sector) to lead the cybersecurity awareness-raising programme. **R 3.3** Engage relevant stakeholders from public and private sectors in the development and delivery of the awareness-raising programme as well as for the creation and utilisation of programmes and materials. **R 3.4** Enhance the existing efforts on raising awareness for school children at all ages, especially on grooming. **R 3.5** Special attention should also be placed on the awareness of parents about online activities of their children. **R 3.6** Create a single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform. **R 3.7** Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns taking into account gaps or failures. **R 3.8** Promote awareness of risks and

		http://cybersafety.cy/youth-panel Hope For Children UNCRC Policy Center http://uncrcpc.org.cy/gr/ EU Kids Online survey http://uncrcpc.org.cy/index.php?id=47 Cyprus Research and Academic Network (CyNet) www.cynet.ac.cy/stayalert/ Safer Internet Day http://internetsafety.pi.ac.cy/saferinternetday	threats at all levels of the government. **R 3.9** Develop a dedicated awareness-raising programme for executive managers within the public and private sectors, particularly those in the financial and telecommunications sectors. **R 3.10** Promote awareness regarding the protection of personal information online. **R 3.11** Promote awareness raising efforts of cybersecurity crisis management at the executive level. **R 3.12** Develop operational cyber security self-education websites.
D3.2 Framework for Education	**Established**	University of Nicosia https://www.unic.ac.cy/el University of Central Lancashire Cyprus (UCLan) http://www.uclancyprus.ac.cy/en/ Cyprus Open University http://www.ouc.ac.cy/ European University Cyprus http://www.euc.ac.cy/en/home	**R 3.13** Create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff is available to teach newly formed cybersecurity courses. **R 3.14** Create accredited cybersecurity-specific degree courses at undergraduate and post-graduate level, in addition to the other existing cybersecurity-related courses in the various Universities in Cyprus. **R 3.15** Promote efforts by Universities and other bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists. **R 3.16** Allocate additional resources to cybersecurity education for public universities, dedicated to national cybersecurity research and laboratories at universities. **R 3.17** Inform cybersecurity education priorities through broad consultation across government, private sector, academia and civil society, linked to the National Cybersecurity Strategy. **R 3.18** Provide more opportunities for individuals (such as students and experts) to gain experience, through internships and apprenticeships, in order to enhance their expertise by

			combining education and practical training. **R 3.19** Promote cooperation between academia and industry in order to bring together cybersecurity educational offerings weighted based on an understanding of current skills requirements. **R 3.20** Promote competitions and initiatives for students by government and/or industry in order to increase the attractiveness of cybersecurity careers. **R 3.21** Ensure the sustainability of research programs. **R 3.22** Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment. **R 3.23** Gather statistics on the supply and demand of cybersecurity graduates.
D3.3 Framework for Professional Training	**Formative**		**R 3.24** Establish more structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity-specific professionals. **R 3.25** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, and models and operation of these tools. **R 3.26** Train general IT staff on cybersecurity issues so that they can react to incidents as they occur. **R 3.27** Ensure that affordable security professional certification is offered across sectors within the country. **R 3.28** Develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts. **R 3.29** Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms. **R 3.30** Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals. **R 3.31** Work on establishing a collaboration between Universities and the public sector in updating the

			curriculum and communicating clear requirements for graduates regarding certification in cybersecurity according to the demand of the market. **R 3.32** Simplify the process of updating the cybersecurity syllabi. **R 3.33** Develop a skills framework in cybersecurity or use an existing skills framework in the country in order to define clear career paths for cybersecurity experts. **R 3.34** Update the regulatory environment in terms of cybersecurity skills procurement. **R 3.35** Create a system of metrics to determine and monitor supply and demand of professional training in cybersecurity.

Dimension 4 Legal and Regulatory Frameworks

D4.1 **Legal Frameworks**	**Established**	Electronic Commerce Law (156(I)/2004) http://www.cylaw.org/nomoi/enop/ind/2004_1_156/section-scdcb51201-8591-c875-d84b-3e20c399891a.html http://www.ac.ac.cy/images/media/assetfile/law_ammendment.pdf Law for the Protection of Confidentiality of Private Communications (92(I)/1996) http://www.cylaw.org/nomoi/arith/1996_1_092.pdf Law No. 46(I)/2008 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/112(I)-2004_section106_en.pdf	**R 4.1** Ensure that the GDPR is implemented and that legal mechanisms are in place which enable strategic decision-making and determines the timeframe after which personal data is no longer required as evidence for investigation and must be deleted. Identify International and regional trends and good practices to inform the assessment and amendment of data-protection laws and associated resource planning. **R 4.2** Enact commencement orders for existing legislation and assign bodies to monitor the enforcement of cybersecurity and data protection-laws such as the GDPR. **R 4.3** Ensure that international and regional trends and good practices inform the assessment and amendment of domestic legal frameworks protecting human rights online and any associated resource planning. **R 4.4** Develop and adopt legal provisions on procedural powers for investigations of cybercrime and crimes involving electronic evidence.

Legal Framework for Electronic Signatures and for Relevant Matters Law 188(I)/2004

http://journals.sas.ac.uk/deeslr/article/viewFile/1756/1693

Processing of Personal Data Law L.138(I)/2001

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/138(I)-2001_en.pdf

Directive 2000/31/EC

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML

Law 147(i)/2015

http://www.cylaw.org/nomoi/arith/2015_1_147.pdf

Constitution of the Republic of Cyprus, Article 5

http://www.kypros.org/Constitution/English/appendix_a.html

Processing of Personal Data (Protection of Individuals) Law (N. 138(I)/2001)

http://www.cylaw.org/nomoi/arith/2001_1_138.pdf

Law N. 37(I)/2003

http://www.cylaw.org/nomoi/arith/2003_1_037.pdf

European Directive 95/46/EC on Data Protection

http://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:319

R 4.5 Ensure that in the case of cross-border investigation, procedural law stipulates what actions need to be conducted in order to successfully investigate cybercrime.

R 4.6 Adapt and implement legal provisions on e-commerce, regarding cybercrime incidents such as online fraud, spam, and phishing sites.

R 4.7 Consider developing a platform for sharing electronic evidence between regional cybercrime forces.

R 4.8 Enhance the existing cooperation between ISPs and law-enforcement agencies for removal of copyright-infringing content from websites.

R 4.9 Consider joining regional cybercrime forces to enhance international cooperation to combat cybercrime.

R 4.10 Foster research on human rights on the Internet and ensure that measures are in place to exceed minimal baselines specified in international agreements.

		95L0046 Regulation of Electronic Communications and Postal Services Law 112(I)/2004 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/112(I)-2004_section106_en.pdf Directive 2006/24/EC http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14012 Law for Combating Trafficking, Exploitation of Human Beings and for the Protection of Victims http://www.infobuscy.eu/resources/legislation/Legislation-05_EN.pdf Electronic Commerce Law 156/2004 http://www.cylaw.org/nomoi/enop/non-ind/2004_1_156/full.html Competition and Consumer Protection Service http://www.mcit.gov.cy/mcit/cyco/cyconsumer.nsf/index_en/index_en?OpenDocument Criminal Code http://www.sbaadministration.org/home/legislation/01_02_09_01_COLONIAL_CAPS_1959/01_02_01_04_Caps-125-175A/19600101_CAP154_u.pdf	
D4.2 Criminal Justice System	**Formative to Established**		**R 4.11** Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and

			training of investigators. **R 4.12** Allocate resources dedicated to fully operational cybercrime units based on strategic decision-making in order to support investigations, especially at a local level. **R 4.13** Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence through 3CE or other organisations. **R 4.14** Build a cadre of specialist prosecutors and judges to handle cybercrime cases and cases involving electronic evidence. **R 4.15** Establish a formal mechanism to enable the exchange of information and good practices between prosecutors and judges, in order to ensure efficient and effective prosecution of cybercrime cases. **R 4.16** Work on building on the cooperation between the National CERT and other sectors on collecting and analysing cyber-incidents through an information-sharing platform. **R 4.17** Collect and analyse statistics and trends regularly on cybercrime investigations, on cybercrime prosecutions and on cybercrime convictions.
D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime	**Established**	Law 23(I)/2001 on International Cooperation in Criminal Matters http://www.cylaw.org/nomoi/arith/2001_1_023.pdf	**R4.18** Allocate resources to support the exchange of information between public and private sectors domestically and to enhance the legislative framework and communication mechanisms. **R 4.19** Enhance cooperation between the public sector and banks and other financial institutions regarding the sharing of incidents, in order to increase the level of cybersecurity awareness in Cyprus. **R4.20** Strengthen informal cooperation mechanisms within the police and criminal-justice system, and between police and third parties, both domestically and across borders. Consider know-hows from other areas, such as anti-corruption cooperation.

Dimension 5 Standards, Organisations and Technologies

D5.1 Adherence to Standards	**Start-up to Formative**	Cyprus Organisation of Standardisation http://www.cys.org.cy/el/ Information and technology sector standardisations http://www.cys.org.cy/en/who-we-are/organization-charts Digital single Market http://digital-agenda-data.eu/ PCI SSC https://www.pcisecuritystandards.org MasterCard http://www.mastercard.com/sea/consumer/standard-mastercard.html VISA https://usa.visa.com/dam/VCOM/download/merchants/visa-global-acquirer-risk-standards.pdf	**R 5.1** Adopt a nationally agreed baseline of cybersecurity related standards and good practices across the public and private sectors, including standards in procurement and software development. **R 5.2** Establish or assign an institution responsible for the implementation, auditing and measurement of the success of standards across public and private sectors. Apply metrics to monitor compliance and establish periodic audits. **R 5.3** Promote discussions on how standards and good practices can be used to address risk within critical infrastructure supply chains by both government and infrastructure organisations. Identify and mandate standards to which CNIs should adhere to. **R 5.4** Identify a minimum set of controls for all governmental departments based on annual assessments and establish a controls-review to assess the effectiveness of the current controls and practices. **R 5.5** Establish frequent training for IT employees. **R 5.6** Establish mandatory requirements for the adherence of standards, by appointing security officers that will be held responsible for their implementation. **R 5.7** Enact legislation to allow the enforcement of disciplinary actions for policy violations. **R 5.8** Streamline clear guidance for the procurement of hardware and software. **R 5.9** Commence discussions with all relevant stakeholders and regulators before the adoption of the NIS and GDPR Directives, to agree on criteria for the creation of frameworks that will cover the requirements of these EU legislative efforts. **R 5.10** Promote the awareness and implementation of standards among

			SMEs. **R 5.11** Establish a framework to assess the effectiveness of standards for procurement and software development.
D5.2 **Internet Infrastructure Resilience**	**Formative to Established**	EU Digital Agenda Scoreboard key Indicators http://digital-agenda-data.eu/	**R 5.12** Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors. **R 5.13** Conduct regular assessments of processes according to international standards and guidelines together with assessment of national information infrastructure security and critical services that drive investment in new technologies. **R 5.14** Identify and map points of critical failure within the Internet infrastructure. **R 5.15** Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.
D5.3 **Software Quality**	**Formative**	Zeus system corporation http://www.zeussystems.com	**R 5.16** Develop a catalogue of secure software platforms and applications within the public and private sectors. **R 5.17** Develop an inventory of software and applications used in public sector and Critical Infrastructure. **R 5.18** Develop policies and processes on software updates and maintenance. **R 5.19** Gather and assess evidence of software quality deficiencies regarding their impact on usability and performance. **R 5.20** Establish or assign an institution to elicit in a strategic manner common requirements for software quality and functionality across all public and private sectors. **R 5.21** Monitor and assess the quality of software used in public and private sectors.
D5.4 **Technical Security Controls**	**Formative**		**R 5.22** Encourage ISPs and banks to offer anti-malware and anti-virus services. **R 5.23** Establish metrics for measuring the effectiveness of technical controls

across the public domain.

R 5.24 Develop processes for reasoning about the adoption of more technical controls based on risk assessment methodologies across the public domain.

R 5.25 Provide citizens with certificates for authentication and digital signing and create pilot programs within the public sector to boost the uptake of the new initiatives.

R 5.26 Promote best practices in cybersecurity for users.

R 5.27 Consider a centralised structure by replacing PCs with thin clients to alleviate users from the burden on implementing technical controls.

R 5.28 Designate an authority to be responsible for strategic decisions on technical controls that will supervise all networks end-to-end and promote the adoption of a unified framework for security controls.

R 5.29 Keep technical security controls up-to-date within the public and private sector, monitor their effectiveness and review on a regular basis.

R 5.30 Conduct penetration testing for protection of both private and public sectors.

R 5.31 Develop encryption and cryptographic control policies within the public and private sectors based on previous assessments, and regularly review the policies for effectiveness.

D5.5 Cryptographic Controls	**Formative**		**R 5.32** Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to international standards and guidelines. **R 5.33** Raise public awareness of secure communication services, such as encrypted/signed emails. **R 5.34** Use SSL/TLS connections to secure communications between schools and the registry office for the collection of students' data. **R 5.35** Ensure that data are stored in an encrypted format in the schools' equipment. **R 5.36** Establish or assign an institution responsible for designing a policy, aiming to assess the deployment of cryptographic controls according to their objectives and priorities within the public and private sector.
D5.6 Cybersecurity Marketplace	**Start-up to Formative**		**R 5.37** Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development. **R 5.38** Promote sharing of information and best practices among organisations, to explore potential insurance coverage.
D5.7 Responsible Disclosure	**Start-up**		**R 5.39** Develop a responsible vulnerability-disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledge report. **R 5.40** Establish or assign an institution responsible for supervising the process of responsible disclosure and ensure that organisations do not conceal this information. **R 5.41** Develop a system to facilitate threat-intelligence sharing within the critical infrastructure partners and ISPs. Promote sharing of threat-intelligence in the financial sector and incentivize companies to actively participate. **R 5.42** Promote the hotline and mobile application for incident reporting in the

public sector.

R 5.43 Define thresholds and notification requirements for all sectors. These requirements should not only consider availability of services but the integrity and confidentiality of data.

R 5.44 Agree on clear instructions on how to share information uniformly within EU in a formal and structured manner.

The review was conducted after the invitation from OCECPR.

Office of the Commissioner of Electronic Communications & Postal Regulation

Global Cyber Security Capacity Centre

Oxford Martin School, University of Oxford

Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,

United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435

Email: cybercapacity@oxfordmartin.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity