CYBERSECURITY CAPACITY REVIEW

Republic of Lithuania

August 2017

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: *Dr Maria Bada, Carolin Weisser*

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

Approved by: *Professor Michael Goldsmith*

LIST OF ABBREVIATIONS

BKA	Baltic computer academy
CCU	Cyber Crime Unit
CDEP	Committee for Digital Economy Policy
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CERT-LT	National Lithuanian Computer Emergency Response Team
CISN	Cybersecurity Stakeholder Information Sharing Network
CITE	Centre of Information Technology of Education
CMM	Cybersecurity Capacity Maturity Model for Nations
CNI	Critical National Infrastructure
DNS	Domain Name Server
ECTEG	European Cybercrime Training and Education Group
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
HRMI	Human Rights Monitoring Institute
HS	Hosting Services
ICT	Information and Communication Technology
ICS	Industrial Control Systems
ISAE	International Standard on Assurance Engagements
ISPs	Internet Service Providers
ITI	Public institution Information Technologies Institute
LCHR	Lithuanian Centre for Human Rights
LEA	Law Enforcement Agencies
L3CE	Lithuanian Cyber Crime Competence Centre
LLPPD	Law on Legal Protection of Personal Data of the Republic of Lithuania
MoI	Ministry of Interior
MoND	Ministry of National Defence

MRU	Mykolas Romeris University
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NIS Directive	**(EU)** Directive on Security and Information Systems
RRT	Ryšių Reguliavimo Tarnyba (Communication Regulation Authority)
SMEs	Small and Medium Enterprises
SPB	State Patent Bureau of the Republic of Lithuania
SPDE	Security and Privacy in the Digital Economy
VCP	Vilnius County Police Headquarters

EXECUTIVE SUMMARY

The Global Cyber Security Capacity Centre (GCSCC, or 'the Capacity Centre') has facilitated a review of the maturity of cybersecurity capacity of the Republic of Lithuania, hosted by Vilnius University and NRD Cyber Security. The objective of this review is to enable the government of Lithuania to reassess its cybersecurity capacity in order to prioritise strategic investment in national cybersecurity.

From 24-26 April 2017, stakeholders from the following sectors participated in a series of consultations with GCSCC research and analysis staff: government departments and ministries, legislators and policy owners, criminal justice, defence, academia, as well as the private and financial sectors.

The consultations were premised on the Centre's Cybersecurity Capacity Maturity Model for Nations (CMM), which defines five areas of cybersecurity capacity:

- Policy and strategy
- Culture and society
- Education, training and skills
- Legal and regulatory frameworks
- Standards, business models and technologies

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators, which describe steps and actions that once observed define which state of maturity this specific element of aspect is. There are five stages of maturity, ranging from the start-up stage to the dynamic stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. For more details on the definitions of these please consult the CMM document (p.5)[1]

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

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

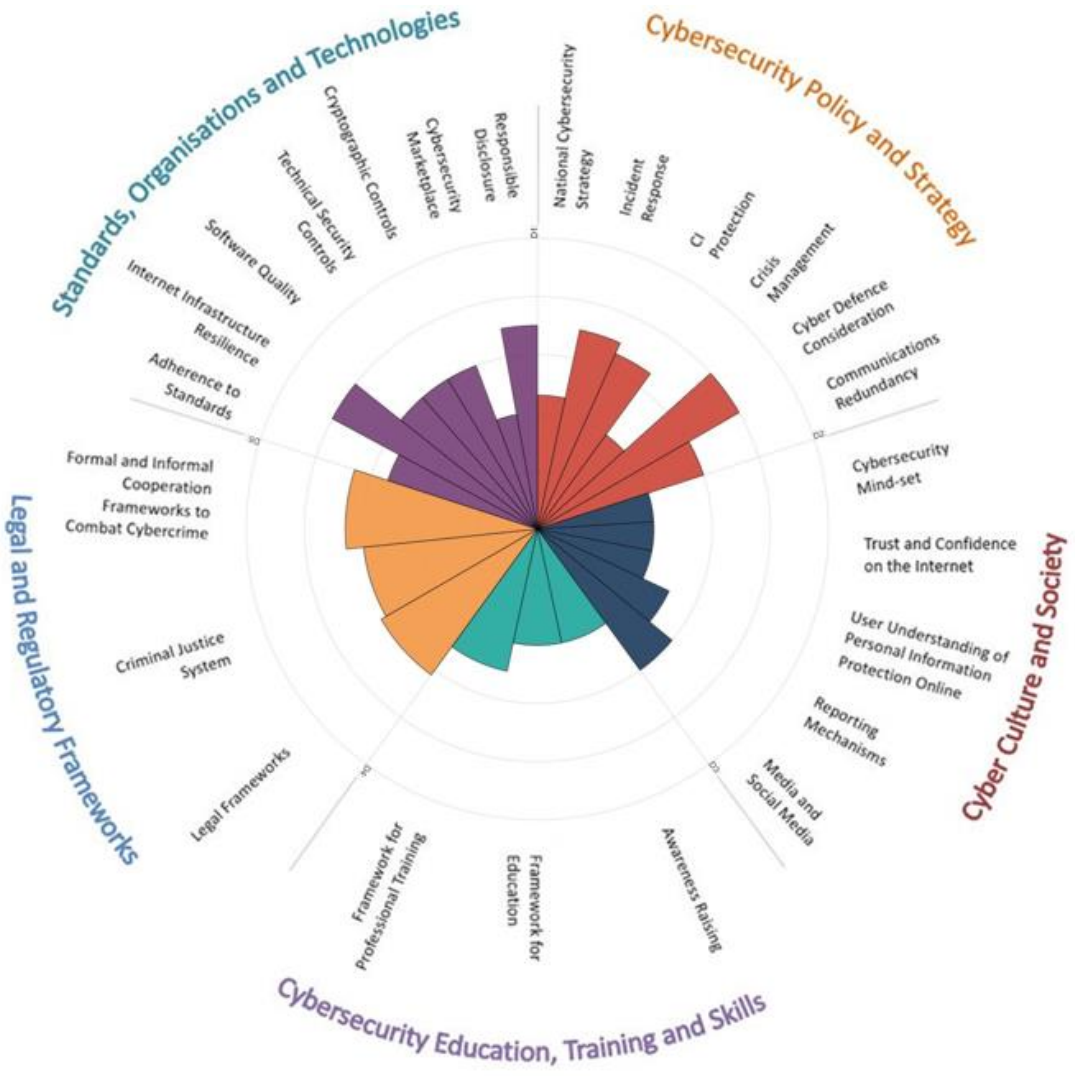

Figure 1: Overall representation of the cybersecurity capacity in the Republic of Lithuania

Policy and Strategy

The *policy and strategy* dimension of cybersecurity capacity for Lithuania was gauged to range from *formative to established stages* of maturity. For specific factors, some indicators could be acknowledged reaching a strategic stage of maturity.

Lithuania is currently in the process of developing a national cybersecurity strategy under the lead of the Prime Minister's Office and the Ministry of National Defence (MoND). Until now, Lithuania has undertaken several steps to enhance national strategic capacity to manage cybersecurity, such as the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019.

Lithuania's incident response capacity is at an *established* stage of maturity and is on the verge of reaching the *strategic* stage. The government developed the National Lithuanian Computer Emergency Response Team (CERT-LT) in 2008. CERT-LT coordinates and collaborates with sub-national/sectorial/international incident-response organisations and reports to the relevant

responsible authorities. The National Cybersecurity Centre (NCSC), developed recently under the auspices of the MoND, undertakes cyber incident management, acts as an information sharing platform and publishes vulnerabilities and related legal measures.

The protection of critical infrastructure (CI) from cyber-threats is a priority for Lithuanian authorities. An officially approved list of critical assets and equipment has been prepared in conjunction with the Law on Enterprises and Equipment of Strategic Importance to National Security (2002) and is disseminated to all relevant stakeholders. A detailed audit of CI assets is performed at least every two years in response to changes in the threat environment.

Simulations and training exercises have been conducted by the MoND as well as CI owners, at national, regional and international levels, in order to better prepare for a cybersecurity crisis of some sort. Additionally, CI owners organise sector-specific exercises.

Lithuania's Cyber Defence considerations are at a *strategic stage* of maturity. The Military Strategy of the Republic of Lithuania (Chapter 3) recognises cyber-attacks among the main national risks, dangers and threats. In 2009, the MoND approved the first National Defence System Cyber Security Strategy and Implementation Plan, which was updated in 2013. The strategy emphasises ensuring the secure transfer of electronic information, ensuring cybersecurity of institutions of the national defence system and protecting the cybersecurity of the state's CII. There is no Command and Control Centre established in Lithuania however, the National Cyber Security Centre has that responsibility.

In the event of a major national or sectoral communications disruption, mechanisms are in place to maintain operational functionality of the national emergency communication network. MoND has identified and mapped redundancy measures, in the form both of substitute digital networks and non-digital means for communication.

Culture and Society

During consultations, the national capacity regarding *cybersecurity culture and society* ranges from *formative* to *established* stages. A cybersecurity mind-set in Lithuania is consistently being adopted and certain leading government agencies are beginning to incorporate cybersecurity into their daily practice. Within the private sector most companies are aware of the financial risks of cyber(in)security and able to identify high-risk practices in their business processes. However, there are differences depending on the sector and the scale of the organisations. Among society-at-large there is a shift towards a more proactive approach to cybersecurity, however there are differences between different age groups.

Overall, the participating stakeholders accepted that most Internet users in Lithuania trust in the security of the Internet but this is often "blind" trust. E-government services have been fully established whereas e-commerce services are gradually expanding. To ensure security, there is special monitoring of these services for the event of an incident which are published and discussed in the public sphere.

Users and stakeholders within the public and private sectors have general knowledge about how personal information is handled online, but (proactive) cybersecurity practices are either

not used due to convenience or people weigh up the protection of their personal information. Lithuania has established the Law on Legal Protection of Personal Data and is now in the process of implementing the EU General Data Protection Regulation (GDPR).

In Lithuania, several reporting mechanisms have been established and are regularly used, such as an online platform of the e-police. Moreover, cybersecurity is a common subject across print, online and social media. Journalists also explain the importance of cybersecurity measures and behaviour and write about the reports published by the government, which describes quite a strategic approach by the media.

Education, Training and Skills

The observations during the consultations show that the *cybersecurity education, training and skills* capacity in Lithuania is at a *formative stage of maturity*. Awareness-raising programmes, courses, seminars and online resources are available for target demographics from public, private, academia, and/or civil society sources. However, a national programme for cybersecurity awareness-raising, led by a designated organisation is not currently established. The National Cybersecurity Strategy which is currently under development will include awareness-raising as one of its priorities. Executives are aware of cybersecurity risks in general and how their organisation deals with cybersecurity issues. However, there are no requirements for CEOs to receive certain trainings.

In higher education, some courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered in Lithuania. Cybersecurity is often a module within the curriculum of those courses. However, the existing courses do not provide a specialised degree in cybersecurity. Research and development is an important consideration in cybersecurity education. The Council of Science has recognised the necessity for research and organises a cybersecurity Forum to identify needs and allocate resources for research in cybersecurity.

The need for training professionals in cybersecurity has been documented in Lithuania, at the national level. Training programmes in cybersecurity are offered for the public and private sector employees as well as for the general public. Training courses are delivered by local industry bodies for experts and CEOs, providing certification. However, it was identified that overall there is not enough expertise among educators to provide training in cybersecurity.

Legal and Regulatory Frameworks

The *legal and regulatory* frameworks in Lithuania range between *established and strategic* stages of maturity. The Law on Cyber Security, passed in December 2014, defines the organisational structure of cybersecurity in Lithuania. The Resolution on the Cyber Security Council and its regulation (2015, No. 422) appoints the Council as the body, analysing the state of cybersecurity in the Republic of Lithuania. The rights and obligations of public communications networks and service providers are governed by the Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks

and Public Electronic Communications Services. Additionally, the Law on Electronic Communications of the Republic of Lithuania sets an obligation on providers of to implement appropriate technical and organisational measures to safeguard the security and integrity of their services.

Substantive cybercrime legal provisions are contained in the general criminal law. The country has ratified regional or international instruments on cybercrime and is consistently seeking to implement these measures into domestic law. The Criminal Code of Lithuania has provisions for crimes committed with electronic devices, however, it does not provide any sanctions for identity theft in the electronic and non-electronic space. The Criminal Procedure Code is harmonised with European Union legislation and includes provisions on the investigation of crime and evidentiary requirements.

Lithuania has ratified or acceded to international agreements on human rights and has acknowledged their protection in all new codes. Domestic law specifies safeguards to protect the individual's right to privacy during the collection, use and disclosure of personal information, while comprehensive data protection legislation has been adopted and enforced through the Law on Legal Protection of Personal Data of the Republic of Lithuania (LLPPD) and the Personal Data Protection Act.

Comprehensive legislation on protection of children has been adopted and enforced, and ensures data protection and privacy rules for legal minors. Lithuania is party to the UN Convention on the Rights of the Child and other relevant international conventions. Currently, legislation on intellectual property online is under development through consultation with key stakeholders.

Advanced investigative capabilities allow the investigation of complex cybercrime cases. Law enforcement have sufficient capacity to prevent and combat cybercrime and receive specialised training on cybercrime investigations. Moreover, there are specialised prosecutors and judges both at the central and local level. However, there is no mechanism to enable the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.

Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime. Lithuania has established agreements with Interpol and Europol as well as bilateral agreements with neighbouring countries on cross-border information sharing. Moreover, informal relationships between government and criminal justice as well as between ISPs and law enforcement exist with clear communication channels resulting in the regular exchange of information on cybercrime cases.

Standards, Business Models and Technologies

Lithuania's capacity in *cybersecurity standards, business models and technologies* was identified to range from *formative and established* up to *strategic* stages. 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 the

private sector. Adoption and compliance is measured and reported, with adoption oversight from government. The use of standards to mitigate CNI supply systems' risk is also considered.

The country has established reliable Internet services and infrastructure. Regular assessments of processes according to international standards and guidelines are conducted together with assessment of national information infrastructure security and critical services that drive investment in new technologies. Monitoring processes are also in place.

Reliable software applications that adhere to international standards and good practices are being used widely in the public and private sectors. A catalogue for secure software platforms and applications exists. Policies and processes for software updates are established and regulated in the public sector. The Government has established certain requirements such as risk assessments and audits for state registrars and there is guidance to meet these requirements.

Technical security controls including patching and backups, are deployed across sectors. The technical cybersecurity control set is based on established cybersecurity frameworks, such as the SANS top 20 cybersecurity controls. Also, the cryptographic controls deployed meet international standards and guidelines accordingly for each sector and are kept up-to-date. However, it was noted that the general public is not aware or does not have the appropriate knowledge to deploy such controls.

The domestic market in Lithuania may provide specialised cybersecurity products, but these are not market-driven. Although domestic suppliers exist, these cannot cover the country's needs, therefore Lithuania relies on software mostly to international producers. Additionally, a market for cyber insurance is established and encourages information sharing among the market. The companies offering these products are not local but international.

A vulnerability disclosure framework is in place, which includes a disclosure deadline, scheduled resolution, and an acknowledgement report. The Programme for the Development of Electronic Information Security (Cybersecurity) for 2011-2019 also recommends implementing a stronger legal requirement for incident reporting, as part of a wider strengthening of the legal framework supporting electronic information security. Currently, organisations have established their own processes and mechanisms to receive, disseminate and share information on vulnerabilities.

Additional Reflections

This was the 17th 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 Lithuania to gain insights into the breadth and depth of the country's cybersecurity capacity. Lithuania has commenced the process of developing different aspects of cybersecurity capacity across all dimensions, including through revising the National Cybersecurity Strategy and revisiting legal frameworks and regulation. The review suggests a number of specific steps by which Lithuania's cybersecurity capacity might achieve greater levels of maturity.

INTRODUCTION

The Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') has facilitated a review of the maturity of cybersecurity capacity of the Republic of Lithuania, hosted by Vilnius University and NRD Cyber Security. The objective of this review is to enable the government of Lithuania to reassess its cybersecurity capacity in order to prioritise strategic investment in national cybersecurity.

From 24-26 April, 2017, stakeholders from the following sectors participated in a three-day consultation with GCSCC research and analysis staff to review Lithuania's cybersecurity capacity:

- Public Sector Entities:
  - Government Chancellery
  - Information Society Development Committee under the Ministry of Transport and Communications
  - Information Technology and Communications Department under the Ministry of Interior
  - Ministry of Agriculture
  - Ministry of Communications
  - Ministry of Education
  - Ministry of Energy
  - Ministry of Environment
  - Ministry of Finance
  - Ministry of Health
  - Ministry of Interior
  - Ministry of Justice
  - Ministry of National Defence
  - National Court Administration
  - National Cybersecurity and Telecommunications Service under the Ministry of National Defence
  - National Data Protection Inspectorate
  - Parliament's National Security and Defence Committee
  - State Security Department
- Legislators/Policy owners
- Criminal Justice and Criminal Police Bureau
- Finance sector
- Academia
- Private Sector

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model[2] for Nations (CMM) 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 therein. Table I below shows the five dimensions with their comprising factors:

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

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

STAGES OF CYBERSECURITY CAPACITY MATURITY

In each factor there are indicators which identify five stages of maturity. The maturity scale ranges from the *start-up* stage, implying an elementary and ad-hoc approach to capacity, to the *dynamic* stage where a strategic approach has been articulated and where the relevant agencies and organisations have developed the ability to respond and adapt as environmental considerations demand. The five stages are 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 an absence of 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. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision making has been made concerning the "relative" investment in the various elements of the aspect. But the aspect is functional and defined.
- **Strategic:** Choices have been made about which parts of the aspect are important, and which are less important for the particular organisation or nation. The strategic stage reflects the fact that these choices have been made, conditional upon the nation or organization'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 feature of this stage.

CYBERSECURITY CONTEXT IN LITHUANIA

Since 2001 there has been a substantial increase in the number of internet users in Lithuania due to efforts by the government to extend internet infrastructure to rural areas (such as the Rural Area Information Technology Broadband Network - RAIN I, RAIN II and PRIP - projects). The proportion of the Lithuanian population using the Internet regularly has stabilized around 72 percent for the last three years. According to the European Commission[3], as of 2016, almost a quarter (22 percent) of the population has never used the Internet and only 63 percent of households in Lithuania have a fixed broadband connection[4] with even less access to mobile internet (37 percent). With these values, Lithuania is below the European Union (EU) average regarding broadband and mobile Internet connection, despite being top performer regarding connectivity. Under RAIN III, which is part of the country's Next Generation Internet Access Development Plan running until 2020, the government seeks to close these gaps and aims to stimulate both supply and demand. A different picture is provided for enterprises: 95 percent have a broadband connection and 18 percent of Lithuanian companies sold services and products online in 2016, which is more than companies to in other European countries.

During the GCSCC review, participants often referred to regulations, laws, activities, processes etc. which are either mandatory or recommended as a consequence of Lithuania's membership of the European Union, NATO and other organisations such as Interpol. As an EU member state, Lithuania is also part of the Digital Single Market strategy, the goal of which is both to develop European Data Economy and to promote online platforms, protecting Europe's assets by tackling cybersecurity challenges.[5] This initiative includes the planned review of the EU Cybersecurity Strategy in September 2017 as well as additional measures addressing cyber security standards, certification and labelling to make connected users more cyber secure. These developments may have an impact on the Lithuanian national cybersecurity strategy.

In 2015, Lithuania also started the process towards OECD membership. This will most likely have impact on the cybersecurity landscape in the country. Lithuanian officials are engaged with OECD Committees including the Committee for Digital Economy Policy (CDEP) which is supported by the OECD Working Party for Security and Privacy in the Digital Economy (SPDE)[6]. During the review, participants expressed concerns regarding specific cybersecurity threats arising from the current geopolitical situation in Europe and Lithuania's geographical situation. In technological terms, the use of the Internet for phishing and spear phishing, ransomware attacks and website defacement were of particular concern.

3 https://ec.europa.eu/digital-single-market/digital-scoreboard
4http://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={%22indicator-group%22:%22broadband%22,%22ref-area%22:%22LT%22,%22time-period%22:%222016%22}
5 http://europa.eu/rapid/press-release_IP-17-1232_en.htm
6http://www.oecd.org/internet/ieconomy/workingpartyonsecurityandprivacyinthedigitaleconomyspde.htm

REVIEW REPORT

OVERVIEW

This section provides an overall representation of cybersecurity capacity in Lithuania. The graphic (Graphic I) shows the maturity estimates made in each dimension. The circular gridlines radiation from the centre of the graphic correspond to the five-stage maturity scale, with 'start-up closest to the centre and 'dynamic' at the furthest. The stages of maturity for each factor extend out from the middle as an individual bar, and each colour-coded dimension covers one fifth of the graphic.

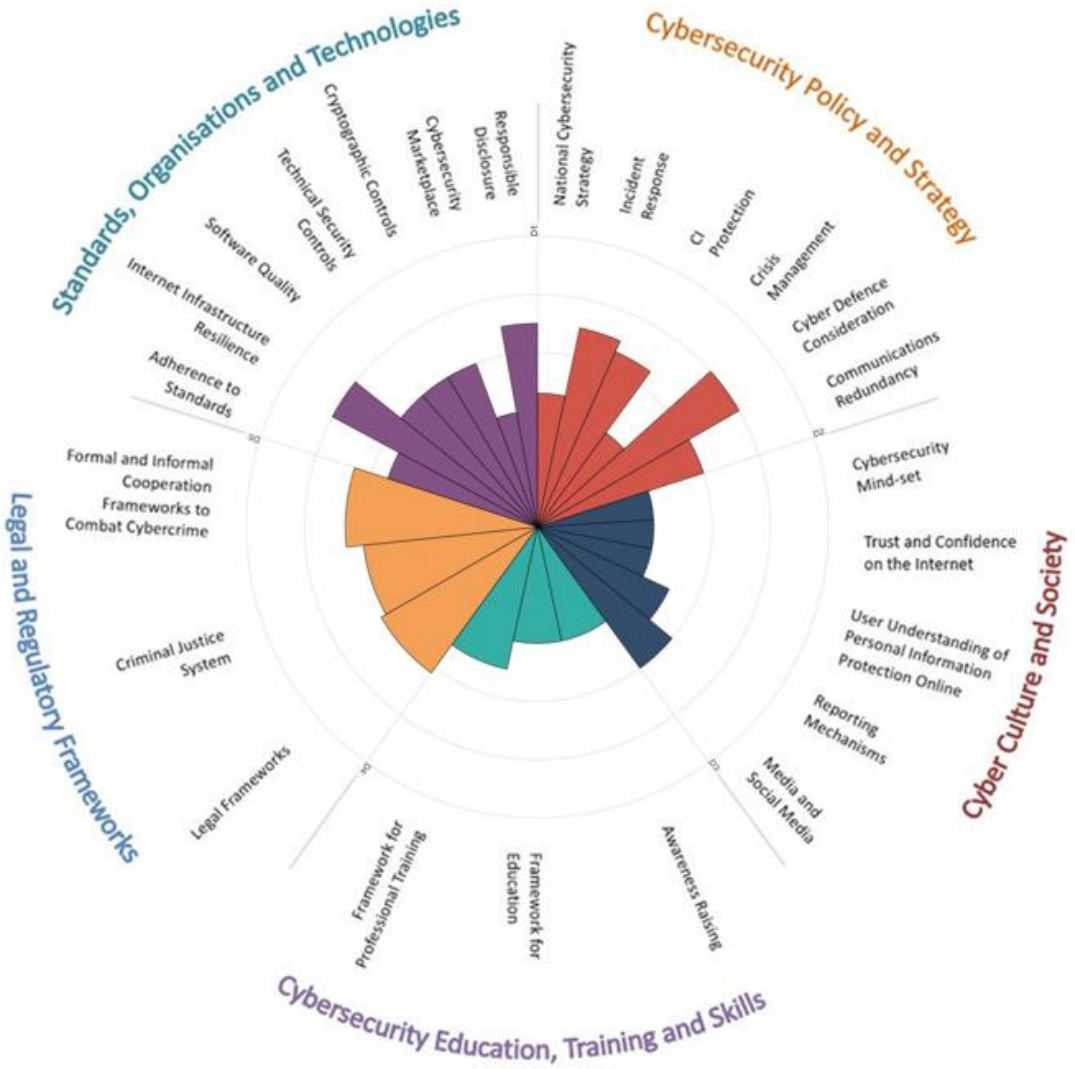

Figure 1: Overall representation of the cybersecurity capacity in the Republic of Lithuania

DIMENSION 1
CYBERSECURITY POLICY AND STRATEGY

Dimension 1 gauges Lithuanian 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. The Cybersecurity Policy and Strategy dimension also includes consideration of early warning, deterrence, defence and recovery. This dimension assesses the effectiveness of policy in advancing national cyber defence and resilience capacity, while facilitating the access to cyberspace increasingly vital for government, international business and society in general.

D1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to the coordination and direction of the government's cybersecurity agenda. A cybersecurity strategy makes it possible to prioritise cybersecurity as a critically important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs necessary and appropriate allocation of resources to emerging and existing cybersecurity issues and priorities.

Maturity Stage: **Formative to Established**

The Republic of Lithuania is currently developing a National Cybersecurity Strategy under the lead of the Prime Minister's Office and the Ministry of National Defence (MoND).

Although Lithuania's cybersecurity strategy is under development, there have been several important initiatives to enhance national strategic capacity to manage cybersecurity. The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019[7] was adopted by the Lithuanian government in 2011. It complies with the action steps presented in the Communication of the European Commission of 30 March 2009 "Protecting Europe from large scale cyberattacks and disruptions: enhancing preparedness, security and resilience" – COM (2009)149. It is a comprehensive plan that includes an assessment of

[7] http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

Lithuania's cybersecurity capacity and a set of clearly stated objectives, which are mapped to an implementation schedule.

The Programme also informed the establishment of the National Cyber Security Centre (NCSC)[8] of Lithuania in 2015 under the auspices of the MoND. The Law on Cyber Security designates authorities responsible for the development and implementation of cybersecurity policies and sets out their competences, functions, rights and obligations. The law stipulates that the MoND is to formulate, coordinate and implement the organisation of the national cybersecurity policy. The NCSC analyses the cybersecurity environment in Lithuania, prepares for the protection of national databases, manages the Internet operations of national organisations, prepares cybersecurity plans and investigates Internet attacks.

The Programme for the Development of Electronic Information Security is also linked to Lithuania's overarching National Security Strategy (NSS)[9]. The NSS includes the following as *vital* interests of the country: a) security of the infrastructure of the economic sectors of strategic importance to national security; b) information security; and c) cyber security. Accordingly, Lithuania aims to determine the objectives and tasks for the development of electronic information in order to ensure safeguarding of electronic communication networks, information systems and critical information infrastructure against incidents and cyber-attacks as well as the protection of personal data and privacy.

Having initiated the process for the development of the National Cybersecurity Strategy the MoND has consulted key stakeholder groups including those in both the public and private sectors such as ministries (e.g. Interior and Foreign Affairs), financial institutions, universities and international partners. A first draft of the strategy is being developed and further discussions with stakeholders are planned. The final draft of Lithuania's National Cybersecurity Strategy (NCS) is due to be released in September 2017. The country plans to publish the strategy, which will be approved by the Government Resolution, until 2018.

Currently budgets reside in disparate public departments without a discrete cybersecurity budget line. It is important for a central cybersecurity budget to be allocated and departments to have a discrete cybersecurity line item to allocate resources according to needs.

In its present draft form, the NCS is linked directly to various different objectives: national risks, priorities and objectives on the one hand; and business development opportunities and priorities on the other. The NCS seeks to raise public awareness, mitigate cybercrime, establish incident response capability and protect critical infrastructure from external and internal threats. The methodology used in the preparation of the NCS included a) a review of other European national cybersecurity strategies; b) reference to guidance from the (EU) Directive on Security and Information Systems (NIS directive); c) reference to guidance provided by the Lithuanian NCSC; d) reference to the annual report on risk and threat analysis conducted by Lithuania's intelligence services; and e) reference to an annual report provided by the MoND's internal CERT.

[8]http://www.nksc.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/rysiu_ir_informaciniu_sistemu_tarnyba_prie_kam_2482/nacionalinis_kibernetinio_saugumo_centras.html

[9] https://www.bbn.gov.pl/ftp/dok/07/LTU_National_Security_Strategy_2012.pdf

D1.2 INCIDENT RESPONSE

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

Maturity Stage: Established to Strategic

The government's capacity to organise, coordinate, and operationalise incident response is advanced. The government developed the National Lithuanian Computer Emergency Response Team (CERT-LT) under the Communication Regulation Authority - Ryšių Reguliavimo Tarnyba (RRT) in 2008. The purpose of CERT-LT is to promote security by preventing, observing, and solving cybersecurity incidents and disseminating information on threats to information security. Its concrete tasks include the provision of capability to deal with network and information security incidents in Lithuanian public electronic networks and it is further responsible for coordinating security and incident response measures across all Lithuanian networks. CERT-LT is additionally tasked with managing the reporting of cybersecurity incidents. With that task in mind, the agency is collects information of national-level cybersecurity incidents which are then classified according to their urgency and their scope. Regular and systematic updates are made to the national-level incident registry. CERT-LT provides an online reporting platform to log cybersecurity incidents (see also D2.4).

CERT-LT coordinates and collaborates with sub-national/sectoral incident-response organisations and reports to other authorities as required: regarding national level issues CERT-LT would report to the Government; on security issues related to the Critical National Infrastructure (CNI) CERT-LT's reporting line is to the MoND; on personal data protection issues to the State Data Protection Inspectorate; and on suspected criminal activity to Lithuanian Cyber-Police.[10] Internet Service Providers and hosting companies are obliged to disclose incidents to CERT-LT. Users main report incidents directly to the Cyber-Police.

The NCSC has several key functions concerning Incident Response: the agency undertakes cyber incident management; it acts as an information sharing platform, including notification of vulnerabilities; and it publishes legal and regulatory decisions and amendments as necessary.

The members of CERT-LT and the NCSC are being trained in specialised subjects and accredited by internationally recognised bodies such as Trusted Introducer. CERT-LT is a member of FIRST[11] thus enabling the team to respond more effectively to security incidents, both reactive as well as proactive. Team members are able to carry out sophisticated incident analysis investigation while key processes (detection, resolution, prevention, etc.) are being monitored, reviewed and tested with different case scenarios on a regular basis. CERT-LT also coordinates activities with other National Incident Response Teams and cooperates with counterparts in other EU states and neighbouring countries.

[10] https://www.epolicija.lt/en/home
[11] http://www.first.org

D1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

Maturity Stage: Established to Strategic

This factor studies the government's capacity to identify Critical Infrastructure (CI) and Critical Information Infrastructure (CII) assets and the risks associated with them, to engage in response planning and critical assets protection, to facilitate quality interaction with CI asset owners, and to enable comprehensive general risk management practice including response planning.

The protection of critical infrastructure from cyber-threats is a priority for Lithuanian authorities. To that end, the Law on Cyber Security[12] gives significant attention to the inclusion of cybersecurity of Hosting Services (HS), Critical Information Infrastructure (CII) and Industrial Control Systems (ICS). Within the Law CII is defined as an electronic communications network or part of it, an information system or part of it, a group of information systems or industrial control system or part of it, regardless of whether the administrative owner is from the public or private sector, where a cyber-incident can cause harm to national security, economy, state or public interest. In Lithuania, rural areas have also been included in addition to extending Internet infrastructure to major cities and towns[13].

The Ministry of the Interior (MoI) is responsible for the preparation of the CI identification methodology and for presenting the list of CI to the Government for approval. The list of critical information infrastructure has been approved in 2016. Moreover, an officially approved list of critical objects and equipment is included in the Law on Enterprises and Equipment of Strategic Importance to National Security[14] which was originally passed in 2002. A detailed audit of CI assets is performed at least every two years with the possibility to update the list in response to any actual or expected changes in the threat environment. The last assessment and identification of CI assets took place in July 2016, including vulnerability/asset management plans and processes. CI asset audit lists are disseminated to relevant stakeholders.

Monitoring and assessment provisions are included in the Law on the Management of State Information Resources 2011[15] that require an audit of government information technologies be carried out at least once every three years. Furthermore, a provision in Article 3 of the State and Official Secrets Act 1999[16] allows the State Security Department to monitor compliance with state secrecy classification, use, and storing procedures. However, this

[12] Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (Cyber security law of the Republic of Lithuania 11 December 2014 Nr. XII-1428, I-2.
https://www.etar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.
[13] www.InternetLiveStats.com
[14] Strateginę reikšmę nacionaliniam saugumui turinčių įmonių ir įrenginių bei kitų nacionaliniam saugumui užtikrinti svarbių įmonių įstatymas (Law on enterprises and equipment of strategic importance to national security) 2002 October 10 Nr. IX- 1132.
15 https://e-seimas.lrs.lt/portal/legalAct/en/TAD/TAIS.432270
16 www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=91654

provision does not identify a specific auditing process, nor does it require this process to be carried out within a specific timeframe.

The NCSC is responsible for collecting all incident disclosures and notifications when it comes to CI assets. CI owners are also required to report incidents to CSC and this mechanism is mandatory. A mechanism is also established for regular vulnerability disclosure with defined scope for reporting incidents between CI asset owners and the government. Formal internal and external CI communication strategies have been defined and are consistent across sectors, with clear points of contact within government departments and agencies. Participating stakeholders indicated that in 2017 the country will establish reporting as mandatory for all sectors, a requirement that is expected to make risk management and response processes faster, more efficient and more effective.

The importance of cybersecurity in risk management and response planning in CI is recognized in all sectors. Best practices in security measures, guidelines and standards for CI cybersecurity have been identified and adopted in Lithuania. Cybersecurity risk management processes have been established, supported by appropriate technical security solutions, communication links, and harm mitigation measures. CI risk management procedures form the basis of a national response plan in which all vital entities participate. It has to be mentioned that review participants informed us that training on the technical and policy level is provided to these institutions, also those from private sector.

D1.4 CRISIS MANAGEMENT

This factor addresses crisis management planning, the conduct of 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 as well as inform budgetary allocations.

Maturity Stage: Established

Simulations and training exercises have been conducted at national, regional and international levels in order to better prepare for a cyber-crisis situation. Specifically, in 2016 the MoND initiated national cybersecurity exercises which are henceforth to be conducted annually. Together with other CI owners, the MoND also participates at NATO and ENISA organised exercises such as NATO's multi-national cybersecurity exercise Cyber Coalition 2013.

Other, sector-specific exercises are also conducted. The Bank of Lithuania, for example, delivers table top and technical exercises for their constituency, in order to measure the resilience of the banking sector in case of an incident. Regional and bilateral exercises are also conducted by the Bank of Lithuania on an annual basis for the banking sector.

Lithuania does not currently have an overarching crisis management law that recognises a crisis caused by a cyber incident or cyber attack. The crisis management system in Lithuania currently works through relevant ministries and institutions according to their competencies. However, some elements of centralized crisis management can be observed; the recently approved Law on Cyber Security makes clear that in the case of a cyber incident or cyber-attack with consequences for national security the leading ministry would be the Ministry of National Defence.

D1.5 CYBER DEFENCE CONSIDERATION

This factor reviews the government's capacity to design a cyber defence strategy and 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.

Maturity Stage: Strategic

Lithuania's Defence Policy is an integral part of the National Security Policy[17] aimed at the development (formation) of the international security environment and at the same time contributing to international stability and peace. It also is intended to drive the creation and maintenance of a national defence capability able to ensure both deterrence from an armed attack, and reliable defence in case of armed aggression.

The Military Strategy of the Republic of Lithuania 2016 (Chapter 3)[18] recognises cyber-attacks among the main national risks, dangers and threats Lithuania faces. Lithuania is increasingly dependent on modern information and communications technologies and is aware that certain states and non-state actors will seek to employ cyber-attacks more frequently, posing a significant threat to national security. Lithuania acknowledges the widely held view that cyber capabilities would likely be used extensively during any type of conventional or unconventional conflict in the region.

In 2009, the MoND approved the first National Defence System Cyber Security Strategy and Implementation Plan, which was updated in 2013. The strategy emphasises the need to ensure the secure transfer of electronic information, to ensure the cybersecurity of the institutions and agencies of the national defence system and to protect the cybersecurity of the state's CII. Capacity exists to support the coordination of resource allocation for national cyber defence based on the national strategic objectives. The understanding of strengths and weaknesses within the coordination mechanism, then feeds into the re-evaluation of the national security posture of the nation.

[17] http://kam.lt/en/defence_policy_1053/important_documents/strategical_documents.html
[18] http://kam.lt/en/defence_policy_1053/important_documents/strategical_documents.html

There is no Command and Control Centre established in Lithuania. However, the NCSC (mentioned in D1.1) has that responsibility and was established due to increasing Internet attacks against Lithuanian government organisations. In response to malicious attacks on strategic information systems and critical infrastructure, communication and coordination between relevant public and private sector actors is achieved through the Cybersecurity Information Network. Cybersecurity Information Network is established by the Law on the Cybersecurity of the Republic of Lithuania (2014, par.17)[19].

D1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify redundancy within digital and non-digital data management and communications systems. Digital redundancy implies a cybersecurity framework in which duplication and failure of any component is safeguarded by frequent and effective backup. Most of these backups will use digital networks that are readily available but are also isolated (from mainline systems. Redundancy in communications systems can be achieved by supporting a digital communications network with a radio communications network.

Maturity Stage: Established

In the event of a communications disruption, mechanisms are in place to maintain the operational functionality of the national emergency communications network. MoND has identified and mapped redundancy measures, both readily available digital networks and non-digital means for communication. This includes the Cybersecurity Information Network mentioned above.

Responsibility for communication security is distributed across different geographical areas to emergency agencies, public and private responders and command authorities. Crisis response simulations are conducted regularly and emergency drills are tested frequently.

[19] https://www.etar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4

RECOMMENDATIONS

The Global Cyber Security Capacity Centre offers the following recommendations for consideration by the Government of the Republic of Lithuania. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the GCSCC Cybersecurity Capacity Maturity Model. Recommendations (R1.1 etc.) are grouped according to the respective factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 Modify the content of the strategy in response to the cybersecurity environment and incorporate it in the strategic plan.

R1.2 Ensure that the National Cybersecurity Strategy content includes, at a minimum: explicit links to national risks, priorities, objectives, and business development, raising public awareness, mitigating cybercrime, and protecting critical infrastructure from external and internal threats.

R1.3 Encourage the promotion and implementation of the National cybersecurity strategy by multiple stakeholders across government and other sectors.

R1.4 Administer a discrete cybersecurity budget line in order to allocate resources.

INCIDENT RESPONSE

R1.5 Improve incident identification and analysis in response to environmental changes and conduct regular, systematic updates to the national-level incident registry.

R1.6 Ensure that the human and financial resources allocated to incident response are adequate to the cybersecurity threat environment by conducting regular scenario exercises designed to test the human and financial capacity.

R1.7 Incorporate an early warning capacity into the mission of the emergency response organisation.

R1.8 Develop a culture of risk assessment and management predictive methods to assess risk, its propagation and its aggregation for the National and CI lens.

R1.9 Establish mechanisms for regional cooperation to resolve incidents as they occur.

R1.10 Promote a platform for the reporting and sharing of incidents across sectors.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.11 Prioritise listing of CNI assets and regularly re-appraise to capture changes in the threat environment.

R1.12 Implement regular audit practices to assess network and system dependencies to inform continuous reassessment of risk portfolio. Identify and establish specific auditing processes.

R1.13 Develop a strategy for strengthening formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector.

R1.14 Establish a mechanism for regular vulnerability disclosure with defined scope for reporting incidents between CI asset owners and the government.

R1.15 Optimize the legal framework concerning CNI by amending existing legislation or enacting new legal regulations as needed to encompass incident prevention, detection and response.

R1.16 Continue to invest in capability of Board Members and Senior Leaders of CI organisations to understand cyber-risk intelligence, in both private and public sector, so that they can lead in the face of crisis and take their part in risk management more generally.

R1.17 Allocate resources in proportion to the assessed impact of an incident to ensure rapid and effective incident response.

CRISIS MANAGEMENT

R1.18 Prioritise crisis management exercises, especially at a local level, and communicate the value of these exercises to all sectors.

R1.19 Conduct compromised communications scenarios and exercises to test emergency response asset interoperability and effective functionality and incorporate the results of the exercises to inform strategic investment in future emergency response assets.

R1.20 Share evaluation of the crisis management exercises with the international community, so that lessons learnt can contribute toward an improved global understanding of crisis management.

CYBER DEFENCE CONSIDERATION

R1.21 Review compliance of the National Security Strategy with international law and its consistency with national and international rules of engagement in cyberspace.

R1.22 Enhance funding efforts for research and development, possibly by establishing a cyber defence research centre, focused on automated cyber defence response systems.

COMMUNICATIONS REDUNDANCY

R1.23 Undertake outreach to, and education of key stakeholders in the need for digital and communications redundancy.

R1.24 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.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including Internet users. All actors and 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 in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for the challenge of 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, and the risks and threats have influenced the processes and structures across government institutions but in particular leading agencies. This results from regulations that the government has implemented since 2008, which include e.g. mandatory training programs

and secure procedures. The government also publishes an annual report on the country's state of cybersecurity.

In several ministries, cybersecurity has become a priority, in particular those which focus mostly on cybersecurity, such as the MoND which is responsible for cybersecurity across the country (see D1.1). A few other agencies have incorporated cybersecurity into their daily practice. However, there are variations across departments and levels of the government. Overall, participants from the private and public sector agreed that cybersecurity does not always receive the attention it deserves and actions are often taken only after an incident has happened. As a result, the cybersecurity mind-set in government remains at a formative stage, but the efforts by the government provide evidence that the criteria of a more mature stage can be reached in the near future.

The private sector was considered to be of a similar mind-set regarding cybersecurity practice. According to the participants, most companies are aware of the financial risks of cyber(in)security and able to identify high-risk practices in their business processes. In particular, security teams in organisations are perceived to have a cybersecurity mind-set. However, there are differences across sectors and the scale of the organisations. In particular, for smaller companies, a cybersecurity mind-set has not been fully adopted. International and online banks are more often aware of cybersecurity risks and therefore more likely to prioritise cybersecurity in their risk management approach. Banks are also leading in the efforts to build a cybersecurity mind-set among consumers, as the majority of the population owns accounts that they can access online. Stakeholders during the consultation agreed that there is a need to foster this mind-set, which also includes cross-sectoral cooperation and information sharing. Infobalt[20], the representation body of the Lithuanian ICT industry regularly organises events, also in cooperation with government and the police, to foster attention for cybersecurity practices within their members but also attract participants from government institutions (see also D3.1).

Individuals across society-at-large inconsistently adopt a cybersecurity mind-set, but according to stakeholders, there is a shift towards a more proactive approach to cybersecurity. The differences occur between different age groups, but also between e.g. IT personnel and cybersecurity experts on one side and general users on the other. The reason for this gap is often a lack of communication or differences in language, according to the review participants. It was also agreed that even if awareness exists, for instance among younger people, the appropriate actions are not necessarily understood or taken. Programmes and materials are available to train and improve cybersecurity practices from the private sector and government agencies to raise awareness in schools, universities and among clients. However, it often stays on an institutional level and is not coordinated nationally.

[20] http://www.infobalt.lt

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, the participating stakeholders accepted that most Internet users in Lithuania trust in the security of the Internet but this is 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. For instance, only 66% of users are aware of cookies, which is below the EU average[21] and do not know how to assess a website's legitimacy. ISPs do not promote security as elements of their services. While there are not many efforts established that seek to promote trust in the use of Internet services, the increased media coverage of incidents and the following debates in the public sphere influence users who are beginning to adopt a healthier level of scepticism of security when being online.

E-government services have been established in Lithuania. Via the *e-Government Gateway / Elektroniniai valdžios vartai*[22] which is managed by the Information Society Development Committee under the Ministry of Transport and Communications, citizens and businesses are offered a broad range of services e.g. social security, healthcare, education and employment, and also provides an inventory of documents by public authorities. Lithuania also has a comprehensive, centralised e-health system, which allows patients to subscribe to doctor services online instead of physically visiting an office, and an e-police system allows individuals to report any incidents (not only cyber) online. There is good uptake of these services by citizens, in particular for the e-health services. Participants considered this fact as a sign that people have trust in the institutions and the services they offer online. To ensure security, there is special monitoring of these services to detect the event of a breach or other security problems. If incidents occur, they are published and discussed in the public sphere. However, while this is an effort to build and maintain trust in these services, there is no coordinated programme to promote it across platforms and to follow specific international web standards.

E-commerce services are expanding also in Lithuania, particularly online-banking and other commercial services from local suppliers, but the number of people buying services and goods online is still below EU average. Digital signatures are allowed under the *Law on Electronic Signatures* (see in D4.1), and in particular, banks recognise the need for secure and reliable systems to protect their own business and customer data. However, there are no feedback mechanisms in place to provide evidence on trust in e-commerce services by other e-commerce companies. Nevertheless, the e-Commerce Division under the Ministry of Economy has the authority to ensure the security of e-commerce services in the country. It has

[21] http://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={%22indicator-group%22:%22security-privacy%22,%22ref-area%22:%22LT%22,%22time-period%22:%222016%22}

[22] https://www.epaslaugos.lt

established a methodology to create a Customer Satisfaction Index to evaluate the service level of e-commerce services. In addition, the taxation authority is currently evaluating the satisfaction levels of their 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

Lithuania has approved the Law on Legal Protection of Personal Data (see D4.1) and is in the process of implementing the EU General Data Protection Regulation (GDPR). An independent inspector of the State Data Protection Inspectorate is responsible for prosecuting breaches.

Users and stakeholders within the public and private sectors have general knowledge about how personal information is handled online but (proactive) cybersecurity practices are either not used, due to perceived inconvenience, or due to the way people weigh up the trade-offs in service and protection of their personal information. Review participants also agreed that skills do often not exist and services to protect themselves are neither offered nor known. Discussions regarding the protection of personal information and about the balance between security and privacy are discussed in the media, but this has not resulted in concrete actions or policies that reach beyond the EU regulation.

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 to Established

In Lithuania, several reporting mechanisms have been established and are regularly used. Any incident, also not cyber-related, can be reported via an online platform of the e-police[23] or traditionally via the emergency number 112. This includes online fraud, cyber-bullying, child abuse online, identity, theft, privacy and security, breaches, and other incidents. CERT-LT

[23] https://www.epolicija.lt

provides end users the opportunity to report incidents via their website. CERT-LT has also the role to measure the effectiveness of these mechanisms and the RTT publishes an annual report with incidents and threats faced (see also D1.1). Customers of banks and ISPs can also report directly to their supplier. Within Universities, according to the Academic Ethics Code, students can report incidents to the University that has the authority to take actions and to monitor the amount of students facing harassment or bullying online.

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: Established

Cybersecurity is a common subject across print, online and social media. Incidents and cybercrime cases receive attention of the audience and are widely discussed in the public. Journalists also explain the importance of cybersecurity measures and behaviour and write about the reports published by the government. This practice indicates quite a strategic approach by the media.

Academics are regularly asked to provide expert knowledge for media and social media. However, the participants of the review also admitted that users do not necessarily associate the issues discussed on the media with themselves, also because the media tend to exaggerate and only present threats rather than providing directions for users. Research has shown that the invocation of fear can be indeed a counterproductive tactic unless accompanied by useful instructions on what users can do[24].

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 Lithuania. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

[24] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/csss2015_bada_et_al.pdf

CYBERSECURITY MIND-SET

R2.1 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.

R2.2 Routinize cross-sectorial cooperation and information sharing among private and public sector organisations on cybersecurity risks and good practice.

R2.3 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

R2.4 Establish ISP programmes to promote trust in their services based on measures of effectiveness of these programmes.

R2.5 Promote privacy-by-default as a tool for transparency in the provision of e-governance services (including e-health and e-police). Implement feedback mechanisms for use to ensure that the e-services are continuously improved and trust is strengthened among users.

R2.6 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.7 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

R2.8 Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online.

R2.9 Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

R2.10 Promote privacy by default as a tool for transparency.

REPORTING MECHANISMS

R2.11 Encourage different stakeholders to coordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms.

R2.12 Establish awareness programmes to promote the regular use of reporting mechanisms by public and private sectors, and their use as an investment in loss prevention and risk control.

R2.13 Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.

MEDIA AND SOCIAL MEDIA

R2.14 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.

R2.15 Encourage a frequent discussion about cybersecurity on social media.

R2.16 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

Awareness-raising programmes, courses, seminars and online resources are available for target demographics from public, private, academia, and/or civil society sources. However, a national programme for cybersecurity awareness-raising, led by a designated organisation is currently not established. Awareness-raising programmes may be informed by international initiatives but are not linked to the national strategy. The National Cybersecurity Strategy draft will include awareness-raising as one of its main objectives.

One of the objectives of the Programme for the Development of Electronic Information Security (Cyber Security) 2011-2019[25] is to enhance the culture of protection of electronic information security and increase the number of organised events to increase awareness on the importance of electronic information security.

[25] http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

Lithuania participates in the ''European Cyber Security Month (ECSM): get in the driving seat of your own online security''[26] which provides the public advice on staying safe online. NRD CS[27] also participates at the ECSM and invites stakeholders from CI, public, private sector and academia to take part in various activities.

Also, Lithuania celebrates a Safer Internet Day and Safer Internet Week organised by the Safer Internet Centre (SIC) [28], a multi-stakeholder consortium whose main activities are: 1) awareness-raising; 2) hotline; 3) helpline activities and 4) promotion of youth's initiatives as well. Since 2005, the European Commission sponsors a programme by SIC for raising awareness among school children. It brought together the private sector, the Ministry of Education and Science (currently leading) and the Communications Regulatory Authority.

The Centre of Information Technology of Education (CITE, Švietimo informacinių technologijų centras)[29] is a member of the consortium of SIC and technical coordinator for the awareness-raising activities. It initiates and coordinates the work of various national and private organisations in computerising the educational administration agencies, develops ICT applications in the process of education and promotes international cooperation of educators and students on a web-based learning platform. At the same time, it develops, accumulates and disseminates digital learning tools, administrates the information systems of education and develops and supervises the computer networks in education. The School programme Busiu[30] joins schools with companies in order to raise cybersecurity awareness and is funded by Swedbank. Several other awareness campaigns on topics such as phishing are also organised in cooperation with the Association of Lithuanian Banks. Academia also participates in different efforts regarding raising cybersecurity awareness as mentioned above. Usually the Ministry of Education or other stakeholders might lead also such efforts.

Lithuanian Communications Regulatory Authority has developed a website in order to raise awareness "Be safe in cyberspace!''[31] in partnership with private companies, the Police and the MoI. This website is to provide more knowledge on how to behave safely in cyberspace. It provides information about malware, unwanted e-mail (spam), fraud and other ways of online consumer safety threats. It also contains recommendations under which users will be able to prevent incidents, or tips on what to do case of security being compromised.

CERT-LT offers technical information specifically for enterprises. Moreover, review participants mentioned that, Infobalt organises events in cooperation with the Police and MoD in order to raise awareness and present solutions for small-scale events for SMEs (see D2.1).

Overall, the level of awareness and knowledge about the protection of personal information online among users and business in Lithuania is not sufficient. A study conducted from the Human Rights Monitoring Institute (HRMI) on the Lithuanian Public's Perceptions of Data Protection revealed the existence of the so-called "privacy paradox", which means that the

[26]https://ec.europa.eu/digital-single-market/en/news/european-cyber-security-month-get-driving-seat-your-own-online-security
[27] https://www.nrdcs.lt/
[28] http://www.draugiskasinternetas.lt/en/main/about/info
[29] http://www.draugiskasinternetas.lt/en/main/awareness_centre
[30] http://busiu.eu/
[31] www.esaugumas.lt

majority of Lithuanian residents perceive the right to data protection to be just as important as the freedom of expression. A possible explanation for this paradox is the lack of awareness of the right to data protection among the public. Accordingly, another study from HRMI revealed similar findings regarding awareness of businesses in the country about the current Data Protection Regulation.

Executives are aware of general cybersecurity issues, but not how these issues and threats might affect their organisation necessarily. Executives of particular sectors, such as finance, telecommunications, Internet providers and cloud operators are aware of cybersecurity risks and how the organisation deals with cybersecurity issues, but not of the strategic implications. However, there are no requirements for CEOs to receive certain trainings.

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: Formative

Some educational courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered in Lithuania. It was noted during the consultations that the demand for cybersecurity education is evidenced through course enrolment and feedback within Universities.

Several Universities offer programmes in Computer Science and computer engineering at an undergraduate and postgraduate level while cybersecurity is often a module within the curriculum of these. However, there are no specialised degrees in cybersecurity.

The Faculty of Mathematics and Informatics[32] at Vilnius University awards Bachelor and Master's Degrees in Information Technologies, Informatics, Software Engineering and Computer modelling. Those programmes offer modules in subjects such as information systems security[33]. Within the Department of Software engineering of Vilnius University[34] research focuses on topics such as Information System Engineering and Software Service Engineering.

[32] http://mif.vu.lt/lt3/studijos/studiju-programos/ba-studiju-programos/informacines-technologijos
[33]http://www.ef.vu.lt/dokumentai/sandai/VIS/Informacini%C5%B3_sistem%C5%B3_saugumas_2016.pdf
[34]http://www.vu.lt/en/scientific-report-2013/faculties-and-institutes/institute-of-mathematics-and-informatics-of-vilnius-university#Department-of-Software-Engineering

Moreover, Mykolas Romeris University (MRU)[35] awards Bachelor Degrees in Informatics and Digital Contents as well as in Informatics and Business Informatics. Kaunas University of Technology[36] also offers minor study programmes in Informatics, Applied Mathematics, Industrial Technology Management, and Industrial Design as part of Engineering Design.

Additionally, Kaunas University of Technology awards a Master's degree in Information and Information Technology Security[37], designed to prepare experts with cybersecurity theoretical framework, methods and technology, information security management and cyber regulatory knowledge, able to independently and competently work in the cybersecurity field.

Qualification programmes for cybersecurity educators are being explored, with a small cadre of existing professional educators. As mentioned by review participants, because expert educators are limited, some Universities have introduced a scheme of "industry professors", inviting experts from industry to teach specific topics.

Schools, government, and industry collaborate in an ad-hoc manner to supply the resources necessary for providing cybersecurity education but a national budget focused on cybersecurity education is not yet established. The MoI is responsible for the approval of educational programmes while the Department of State is responsible for licensing and accreditation. The Ministry of Education and Ministry of Economy through INFOBALT is now working on creating a competence map for the ICT field to identify the specialisation and the competence required. Review participants noted that this map may result in the creation of new courses and influence the field and the professionalization of the cybersecurity workforce in the country.

The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 (see D1.1) includes a comprehensive educational plan and an implementation schedule, for example, the establishment of a cybersecurity self-help website and the development of at least two programmes for the training and professional development of specialists in electronic information security (cybersecurity) by 2019.

Research and development is an important consideration in cybersecurity education. The Council of Science[38] has recognised the necessity for research and organises a cybersecurity forum to identify needs and allocate resources for research in cybersecurity. The Council is also facilitating the collection of knowledge and its integration into government and academia. However, there is no systematic approach at the moment to ensure the sustainability of research programmes.

[35] https://www.mruni.eu/en/current_students/degree_programmes_in_lithuanian/
[36] http://ktu.edu/en/studies
[37] https://stojantiesiems.ktu.edu/programme/m-informacijos-ir-informaciniu-technologiju-sauga/
[38] http://www.lmt.lt/en/about.html

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.

Review participants mentioned that overall there is not enough expertise among educators to provide training in cybersecurity. Training for general IT staff is provided on cybersecurity issues so that they can react to incidents as they occur, but no training for dedicated security professionals exists. According to the participants there is an existing gap in the demand and supply for trainings as well as the incentives for participation (skills development increases job offerings in particular in the private sector). However, at university level supply is limited because of lack of teachers and researchers.

The universities in partnership with companies such as CISCO/Huawei provide training in different topics as well as certification. Review participants noted that it is often challenging to identify lecturers to teach specialised topics in cybersecurity. As mentioned above, this is why experts from the private sector often teach at Universities.

The MoI and other government organisations, such as the State Enterprise Infostruktūra[39] provide training for their employees. The ministries provide a list of possible, evaluated training courses, for public servants (e.g. ECDL, and more specialised courses on cybersecurity). According to review participants, the servants who are qualified often move on to the private sector. To ensure that they remain in the organisation and transfer the knowledge within government, there are agreements for them to remain at their post for at least 2 years after the training.

The Public institution Information Technologies Institute (ITI)[40] also provides the official ECDL Foundation Sub-licensee for Lithuania. Professors and lecturers from different Kaunas and Vilnius Universities were involved in temporary work groups as a part-time staff at the Institute. Moreover, ITI conducts scientific research activities in customizable design of computer literacy tests.

The local industry, for instance the Baltic Computer Academy (BKA)[41] organise and delivers IT training courses and certification. ISACA-LT[42] is listed as training and certification provider in

[39] http://www.is.lt/en/home.html
[40] http://www.ecdl.lt/english/
[41] http://www.bka.lt/en/
[42] http://www.isaca.org/chapters1/Lithuania/Pages/default.aspx

Lithuania, endorsed by local companies. It has also established partnerships with universities, funds projects and later on hires graduate students. Within different projects in academia (e.g. infrastructure, or customs, data mining) there is funding for training as well. Since 2016, demand is identified for the provision of cybersecurity training from the public and private sector on cybersecurity fundamentals, including risk, vulnerabilities and controls. The Police, ISACA-LT and universities offer training in Digital Forensics Trainers usually come from abroad.

Large international companies usually require certification. Often they will cover training expenses for employees; however, for smaller companies it depends on the individual interest of employees if they receive training and acquire certification. According to participants, the private sector is able to provide higher salaries and therefore to have more specialised staff. An interesting finding from the consultations is that university graduates usually start working for the Government initially before moving on to the private sector.

Review participants mentioned that there have been large national awareness building efforts since 2004 with the result that more experts are being trained mostly within the public and private sector. However, there is still a gap between IT experts and users. Courses on Internet use and Internet services, including security for users, are offered but the take-up is limited.

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 Lithuania. However, a list of experts within the public sector exists. 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 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 Lithuania. 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

R3.1 Develop a national cybersecurity awareness-raising programme with specified target groups, focusing on the most vulnerable users.

R3.2 Appoint a designated organisation (from any sector) to lead the cybersecurity awareness-raising programme.

R3.3 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.

R3.4 Create a single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform.

R3.5 Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns taking into account gaps or failures.

R3.6 Promote awareness of risks and threats at lower levels of the government.

R3.7 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors.

R3.8 Promote awareness regarding the protection of personal information online.

R3.9 Develop operational cyber security self-education websites.

FRAMEWORK FOR EDUCATION

R3.10 Create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff is available to teach newly formed cybersecurity courses.

R3.11 Create accredited cybersecurity-specific degree courses at the university level, in addition to the other existing cybersecurity-related courses in the various Lithuanian universities.

R3.12 Promote efforts by Universities and other bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists.

R3.13 Allocate additional resources to cybersecurity education for public universities, dedicated to national cybersecurity research and laboratories at universities.

R3.14 Inform cybersecurity education priorities through broad consultation across government, private sector, academia and civil society, linked to the National Cybersecurity Strategy.

R3.15 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.

R3.16 Ensure the sustainability of research programs.

R3.17 Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.18 Establish more structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity-specific professionals.

R3.19 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, and models and operation of these tools.

R3.20 Train general IT staff on cybersecurity issues so that they can react to incidents as they occur.

R3.21 Ensure that affordable security professional certification is offered across sectors within the country.

R3.22 Develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts.

R3.23 Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms.

R3.24 Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals.

R3.25 Create incentives for employees within the public sector to maintain their posts after receiving training.

R3.26 Begin to implement metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly and 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.

D4.1 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.

Maturity Stage: Established to Strategic

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 Lithuania. Overall, European Union laws apply in Lithuania while the government is planning to revise all legal acts during 2017.

The Law on Cyber Security, passed in December 2014, defines the cybersecurity organisational structure of Lithuania. The significant points include the transfer of the national cybersecurity policy coordination function to the MoND, the establishment of a new operational National Cyber Security Centre (NCSC)[43] under the MoND, the creation of an Advisory Council on Cyber Security chaired by the MoND, and the establishment of a cybersecurity stakeholder information sharing network (CISN) managed by NCSC. This Law is not effective yet but it will ensure to develop an information network of cybersecurity and a safe platform for

[43] Nacionalinis kibernetinio saugumo centras (National Cyber Security Centre) web page. http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/rysiu_ir_informaciniu_sistemu_tarnyba_prie_kam_ 2482/nacionalinis_kibernetinio_saugumo_centras.html.

information exchange. The Law also defines competences and responsibilities of different institutions. For example, the MoND is responsible for incidents of CNI and ISPs, the Communications Authority has responsibility for supervision of requirements for the market, the police is responsible for cybercrime and the National Data Protection Agency is responsible for data protection.

The MoI and its cybercrime unit (CCU), the Personal Data Inspectorate, and the Communication Regulatory Authority (National CERT) which existed before the law were included in the new national cybersecurity organisational structure and assigned responsibilities as defined in the law. Also significant is the inclusion to the cybersecurity of Hosting Services (HS), Critical Information Infrastructure (CII) and Industrial Control Systems (ICS) in the text of the law[44].

The Resolution on the Cyber Security Council and its regulation (2015, No. 422)[45] describes that the Council is a permanent collegial body, analysing the state of cybersecurity in the Republic of Lithuania shaping and implementing cybersecurity policy as well as managing and (or) handling state information resources.

The State Information Resources Management Council is responsible for the formation of policy, guidelines, and priorities with regard to state information. This includes document protection procedures and classification of documents according to importance of the data they contain. The duties of the Council are set out in the Law on the Management of State Information Resources (2011).

The Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services (Order No 1V-1013 of RRT Director of 21 October 2011)[46] ''*governs the rights and obligations of public communications networks and/or public electronic communications service providers in ensuring the security and integrity of public communications networks and/or public electronic communications services provided by them, the rights and obligations of electronic information hosting service providers ensuring security and integrity of electronic information hosting services provided by them, the terms and conditions for provision of information on cyber- or security incidents (hereinafter - the Incidents) and/or breaches of integrity, the applied incident management measures and technical information for the assessment of the cybersecurity condition of public communications networks, public electronic communications services and/or electronic information hosting services to the Communications Regulatory Authority of the Republic of Lithuania as well as the procedure for investigation of incidents and breaches of integrity*''. This Order also requires that providers of public communications network report certain types of security incidents.

[44] Lietuvos Respublikos kibernetinio saugumo įstatymas 2014 m. gruodžio 11 d. Nr. XII-1428 (Cyber security law of the Republic of Lithuania 11 December 2014 Nr. XII-1428, I-2. https://www.etar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4.

[45] LRV 2015 m. balandžio 23 d. Nutarimas Nr. 422 Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo (Government decree on approval of the cyber security council and regulation) https://www.e-tar.lt/portal/lt/legalAct/4e3539f0ee4611e4927fda1d051299fb

[46] www.cert.lt/doc/CERT_LT_rules[EN].pdf
https://www.cert.lt/doc/Rules_on_the_Ensurance_of_the_Security_and_Integrity.pdf

The Law on Electronic Communications of the Republic of Lithuania[47] specifies that the use of electronic communications services, including electronic mail, for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. This law also obliges providers of public communication networks and/or public electronic communication services to implement appropriate technical and organisational measures to safeguard the security and integrity of their services.

Substantive cybercrime legal provisions are contained in the general criminal law. The country has ratified regional or international instruments on cybercrime and consistently seeks to implement these measures into domestic law. The Criminal Code of the Republic of Lithuania[48] (Chapter XXX, Crimes against security of electronic data and information systems, Chapters – 196- 198) includes in its provisions the a) unlawful Influence on Electronic Data; b) unlawful Influence on an Information System; c) unlawful Interception and Use of Electronic Data; d) unlawful Connection to an Information System and e) unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data. The Criminal Code goes into force upon co-ordination with the country's Code of Criminal Procedure and the Penal Code. The Code has a special chapter devoted to crimes committed with electronic devices. The Criminal Code, which was updated in 2014, does not provide for any sanctions for identity theft in the electronic and non-electronic space. This Code has not been criminalised in Lithuania in general. Usually, identity theft is a constituent element of other acts.

The Criminal Procedure Code[49] is harmonised with European Union legislation and includes provisions on the investigation of crime and evidentiary requirements. Lithuania has established agreements with Interpol and Europol as well as bilateral agreements with non-EU neighbouring countries, on cross-border information sharing. However, the existing legislation does not include specific provisions on the investigation of cybercrime.

The protection of human rights is acknowledged the purpose of practically all new codes in Lithuania[50]. The country has ratified or acceded to international agreements and instruments in this regard, e.g. the European Convention for the Protection of Human Rights and Fundamental Freedoms, ratified in 1995, and the Universal Declaration of Human Rights of the United Nations General Assembly and the International Charter of Human Rights. Lithuania will also commit to new, tougher standards of corporate behaviour in the updated OECD Guidelines for Multinational Enterprises[51]. Domestic law recognises fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association. It also specifies safeguards to protect the individual's right to privacy during the collection, use and disclosure of personal information. All relevant actors from private sector and civil society are involved in shaping laws and regulations on privacy, freedom of speech, and other human rights online.

[47] http://www.rrt.lt/en/legal-acts_250.html

[48] https://www.unodc.org/res/cld/document/ltu/criminal_code_of_lithuania_html/Lithuania_Criminal_Code_2000_as_amd_2010.pdf

[49] http://www.wipo.int/wipolex/en/details.jsp?id=8195

[50] http://www3.lrs.lt/docs2/CSFIAIZY.PDF

[51] http://www.oecd.org/newsroom/newoecdguidelinestoprotecthumanrightsandsocialdevelopment.htm

The Law on the Provision of Information to the Public of the Republic of Lithuania (1997)[52] guarantees freedom of information and opinion and prohibits censorship and monopolisation. Additionally, the Lithuanian Draft Law on The Right to Receive Information[53], article 19, provides a safeguard to the public's right to know effectively and to free flow of information.

The Human Rights Monitoring Institute (HRMI) released its 8th overview ''Human Rights in Lithuania: 2013-2014"[54]. The periodic assessment of the human rights state in Lithuania conducted by more than 20 independent experts. It covers the rights of the child, women's rights, freedom of speech, assembly and religion, prohibition of torture and other fundamental rights.

The Lithuanian Centre for Human Rights (LCHR)[55] is a non-governmental organisation which has been working in the field of human rights education, advocacy and research, implementing numerous projects and activities in the field.

Comprehensive data protection legislation has been adopted and enforced, which includes conditions for the collection of personal data and protection from misuse. The Law on Legal Protection of Personal Data of the Republic of Lithuania[56] (LLPPD), according to its Article 1(1), safeguards the inviolability of an individual's private life in the course of processing personal data. It should be noted that processing of personal data is considered lawful only when it is in compliance with the requirements of Articles 3 and 5 of the LLPPD and, in relation to personal ID numbers, also with the requirements of Article 7 of LLPPD(i.e. personal data are provided for specified and legitimate purposes only to the extent necessary to achieve this purpose and only when there is at least one of the lawful processing criteria provided for in paragraphs 1 and/or 2 of Article 5 of the LLPPD). Persons in breach of the LLPPD are liable under the procedure prescribed by laws (administrative liability).

The Inspectorate of Data Protection[57] is responsible for the supervision and control of enforcement of the Law on Legal Protection of Personal Data and aspires that personal data protection is compatible with the requirements of the European Union and is properly ensured in information society environment. Additionally the Personal Data Protection Act[58] (from 1996) speaks on the protection of an individual's right to private life while processing personal data and includes conditions for the collection of personal data, their protection from misuse and forms of disclosure of personal Data.

Comprehensive legislation on protection of children has been adopted and enforced, and 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. Lithuania is party to the UN Convention on the Rights of the Child and other relevant international conventions. The Law on the Protection of Minors

[52]http://merlin.obs.coe.int/iris/1997/3/article20.en.html
[53] https://www.article19.org/data/files/pdfs/analysis/lithuania-foi.pdf
[54] https://hrmi.lt/en/human-rights-in-lithuania-2011-2012-overview/
[55] http://manoteises.lt/lchr/information-in-english/
[56] https://www.ada.lt/images/cms/file/pers.data.prot.law.pdf
[57] https://www.ada.lt/go.php/eng/More
[58] http://www.wipo.int/wipolex/en/text.jsp?file_id=202094

Against Detrimental Effect of Public Information (2002)[59] provides provisions on protection of personal information for minors and its dissemination and includes the procedures for supervision of the implementation of the provisions of this Law. However, the review participants informed us that this law is not speaking specifically on protection of children online nor directly to the criminal procedures. The Criminal Code, chapter XXIII, has provisions on crimes and misdemeanours against a child and a family.

The Law of the Republic of Lithuania on Electronic Signature[60] (July 11, 2000. No. VIII – 1822) regulates the creation, verification, and validity of electronic signature, signature users' rights and obligations, establishes the certification services and requirements of their providers and the rights and functions of the institution of electronic signature supervision.

The Law on Consumer Protection[61] defines consumer rights and spheres of their protection, lays down an institutional system of their protection and the competence of the authorities to protect those rights. It also regulates the education of consumers, relations of consumers and sellers, suppliers of services, the protection of consumer rights out of court and the liability for violations of the legal acts regulating the protection of consumer rights. The State Consumer Rights Protection Authority[62] coordinates state institutions' activities on protection of consumers and is responsible for drafting proposals to the Ministry of Justice relating to changes in the law. The Bank of Lithuania[63] investigates impartially and free of charge disputes between consumers and financial market participants.

Legislation on intellectual property online is under development, through consultation with key stakeholders. The State Patent Bureau of the Republic of Lithuania (SPB)[64] publishes data on industrial property rights protected in Lithuania. Moreover, the Law on Fees for the Registration of Industrial Property Objects[65] establishes the payment of fees for the registration of industrial property objects and issue of documents related thereto. The Law on Copyrights and Related Rights[66] establishes remedies for intellectual property right infringements, of copyrights and/or related rights. However, all these laws do not include provisions for intellectual property online.

[59] http://www.rrt.lt/en/legal-acts_250.html
[60] http://www.rrt.lt/download/21996/tais_110909%20(2)_signature.doc
http://www.rrt.lt/en/legal-acts_250.html
[61] https://eseimas.lrs.lt/portal/legalAct/lt/TAD/e86e8310231911e6acbed8d454428fb7?jfwid=181l7lifma
[62] http://www.vvtat.lt/index.php?2917529633
[63] http://www.lb.lt/en/sfi-disputes-between-consumers-and-financial-market-participants
[64] http://www.vpb.lt/index.php?n=296&l=en
[65] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.151225
[66] http://www.wipo.int/wipolex/en/details.jsp?id=2852

D4.2 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.

Maturity Stage: Established

Advanced investigative capabilities allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators. The Police and the Cyber Crime Unit within the Police is trained at police academy and also in cooperation with various Universities. The Police is also in collaboration with Universities on various research projects. The participants also informed us that the Institute of Law conducts investigations in collaboration with some European institutions.

The Lithuanian Cyber Crime Competence Centre (L3CE)[67] was established in 2013 by consolidating academia and business resources for Training, Research and Education. It is a member of the international network of Centres of Excellence for Cybercrime and Cybersecurity (2Centre). The Network brings together national Cybercrime Centres of Excellence in many EU countries and provides the countries' Law Enforcement Agencies (LEA) access to Network resources (including officers' training and certification programmes as well as to forensics tools, developed by researchers and scientists). The network and the research is supported by EU institutions such as EUROPOL, Joint Research Centre of the Commission, the European Cybercrime Training and Education Group (ECTEG) and others. In cooperation with Lithuanian LEA, the Vilnius County Police Headquarters (VCP) developed two new curricula for Lithuanian LEA on "Identity theft in cyberspace. Legal aspects" and "Forensics investigation in a virtual environment and hidden crime information detection". Review participants mentioned that although experts are available in the field, they are concentrated in the capital and not at the local level in the country.

Resources dedicated to operational cybercrime units have been allocated based on strategic decision-making. Moreover, resources are allocated to maintain the integrity of data and by this to meet international evidential standards in cross-border investigation. Statistics and trends on cybercrime investigations are also collected and analysed.

A comprehensive institutional capacity, including sufficient human, training and technological resources, to prosecute cybercrime cases and cases involving electronic evidence is established in Lithuania. The review participants mentioned specialised prosecutors both at the central and local level in the country. At the moment there is approximately one cybercrime case prosecuted per day, thus the participants expressed their view that the number of specialised prosecutors is expected to rise as the cases increase each year. A mechanism that ensures that all state servants receive training, including prosecutors, exists

[67] http://www.l3ce.eu

providing the Courses for Competence improvement offered by the Public Service Department[68].

Sufficient human and technological resources are available to ensure effective and efficient legal proceedings regarding cybercrime cases, and cases involving electronic evidence. Judges receive specialised training on cybercrime and electronic evidence. Review participants informed us that initial training is mandatory, while later judges can choose from trainings offered from the National Court Administration[69] which organises the training of judges. Moreover, the E-Service Portal of Lithuanian Courts[70] provides a platform for judges to perform a detailed search of the court resolutions and civil cases. It was mentioned that the Portal can also function as a toll for judges to advice on by reading the proceedings of previous cases. However, participants claimed that there is no existing mechanism to enable the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.

D4.3 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.

Maturity Stage: **Established to Strategic**

Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution with established communication channels. Lithuania has established 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.

Legislative requirements for the exchange of information between domestic public and private sectors have been established. Law Enforcement agencies also have formal agreements in place on information sharing.

The Law on Cyber Security requires cooperation between different sectors domestically. The Government has prioritised the establishment of efficient cooperation with the private sector, ISPs, telecommunication companies and banks. Moreover, the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 recognises the need to encourage public-private cooperation. While there is no industry-led

[68] http://www.vtd.lt/
[69] http://www.teismai.lt/en/
[70] https://e.teismas.lt/en/public/home/

cybersecurity platform in Lithuania, Infobalt[71], engages with various cybersecurity actors in the course of its operations.

Moreover, effective informal relationships between government and criminal justice actors and between ISPs and law enforcement have been established, resulting in the regular exchange of information on cybercrime issues with clear communication channels. All institutions have Intranet where they share cases and statistics as well as good practices informally.

Domestic law enforcement agencies are informally integrated with regional and international counterparts and networks, such as Interpol or 24/7 networks. Law enforcement agencies work jointly with foreign counterparts, potentially through joint task forces, resulting in successful cross-border cybercrime investigations and prosecutions. As mentioned above, Lithuania is a member of Interpol and Europol, therefore several international contact points exist and channels for collaboration are very well established.

RECOMMENDATIONS

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

LEGAL FRAMEWORKS

R4.1 Set mechanisms in place for continuously harmonising ICT legal frameworks with national cybersecurity-related ICT policies, international law, standards and good practices.

R4.2 Inform the existing legislation on protecting consumers from business malpractice online based on regional and international consumer protection standards.

R4.3 Develop a comprehensive legislation on intellectual property online through consultation with key stakeholders.

R4.4 Adopt the legislation currently under development to address the protection of intellectual property of online products and services.

[71] www.infobalt.lt

CRIMINAL JUSTICE SYSTEM

R4.5 Strengthen national investigation capacity for computer-related crimes, with increased cooperation between the National Crime Agency and local police forces.

R4.6 Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators.

R4.7 Enhance investigative capacity and skills locally.

R4.8 Allocate resources dedicated to fully operational cybercrime units based on strategic decision making.

R4.9 Expand and allocate funding on work in training law enforcement in understanding computer related crime, in order to support investigations, especially at local level.

R4.10 Enhance training and education of prosecutors and judges on computer related crimes, and allocate additional resources for this purpose.

R4.11 Establish a mechanism to enable the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.

R4.12 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

R4.13 Expand and enhance formal cooperation mechanisms on cybercrime as needed.

R4.14 Allocate resources to support the exchange of information between public and private sectors domestically and enhance legislative framework and communication mechanisms.

R4.15 Enhance established informal cooperation mechanisms between Internet Service Providers and law enforcement with clear communication channels.

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.

D5.1 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.

Maturity Stage: Formative to Established

Nationally agreed baselines of cybersecurity-related standards and minimal acceptable practices have been identified and adopted widely across the public sector and Critical National Infrastructure (CNI) organisations. International standards and good practices such as ISO 27:001 are being adhered to by the public sector and all information system owners. However, compliance to these standards and good practices is not mandatory for the private sector in general.

Adoption and compliance is measured and reported, with oversight of adoption from government – while the use of standards to mitigate risk in CNI supply systems is also considered. A provision in Article 3 of the State and Official Secrets Act 1999[72] allows the State Security Department to monitor compliance with state secrecy classification, use, and storing

[72] www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=91654

procedures. However, this provision does not identify a specific auditing process, nor does it impose a requirement to carry out this process within a specific timeframe.

Participants from the banking sector noted that due to the specific nature of the risks that they are exposed to, there are no strict requirements for adherence to standards. Some banks adhere to ISO standards, SANS standards and PCI standards. However, it was mentioned that some banks, after conducting their own risk assessments, may judge that ISO 27:001 is too costly and might not meet their needs. They might decide to follow other standards and good practices such as the International Standard on Assurance Engagements (ISAE) 3420. The Central Bank monitors the implementation of standards for the financial sector. The Association of Lithuanian Banks is in contact with the Central Bank and the European Central Bank in order to monitor compliance, through the compliance and crime-prevention committee.

Cybersecurity standards and good practices guiding procurement processes have been identified for use. Critical aspects of procurement such as prices and costs, quality, timescales and other value-added activities are continuously improved in the context of wider resource-planning across enterprises.

The extent of the implementation of standards in procurement depends on the sector and whether it adopts a reactive or a proactive approach. Large organisations follow their own procure processes but these are ad hoc. There is also a requirement from the Central Bank for conducting risk assessments and adopting procurement standards. However, there is no evidence for the adoption of and compliance to standards in procurement practices within the public and private sectors through measurement and assessments of process effectiveness.

Professional communities in Lithuania discuss core activities and methodologies for software-development processes focused on integrity and resilience. The Government promotes relevant standards in software development, but there is no widespread use of these standards yet. There are sector-specific requirements, but no policy or regulation for secure software development exists yet.

D5.2 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.

Maturity Stage: Strategic

Reliable Internet services and infrastructure have been established in Lithuania. Technology and processes deployed for Internet infrastructure meet international IT guidelines,

standards, and good practices. Internet is used for e-commerce and electronic business transactions. National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy.

Regular assessments of processes according to international standards and guidelines are conducted together with assessment of national information infrastructure security and critical services that drive investment in new technologies. Monitoring processes are also in place.

Within the financial sector, payment institutions are mostly regulated by the Central Bank and the European Central Bank. There are authentication processes followed and there is new identification ID system established.

Within Academia, good practices are being followed and different collaboration mechanisms have been established with the Bank of Lithuania and commercial Banks on research and exchange methodologies in order to contribute to the national security.

D5.3 SOFTWARE QUALITY

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

Maturity Stage: Established

Software quality and functional requirements in public and private sectors are recognised and established. Reliable software applications that adhere to international standards and good practices are being used widely in the public and private sectors. Policies and processes for software updates are established and regulated.

The Government has established certain requirements such as risk assessments and audits for state registrars and there is guidance to meet these requirements. A catalogue for secure software platforms and applications exists but is not widely known according to the review participants. This catalogue is part of the resolutions compliance of organisations. Some participants expressed the opinion that it would improve the country's resilience if the government provided such a catalogue to all stakeholders in public and private sector.

In the banking sector various requirements for different banks exist. As participants informed us, the Central Bank will usually issue authentication systems, but not provide specific requirements or standards for others to follow.

D5.4 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.

Maturity Stage: Established

Up-to-date technical security controls, including patching and backups, are deployed in all sectors in Lithuania. Physical security controls are employed to prevent unauthorised personnel from entering computing facilities and that is mandatory for state information sources and CNI. ISPs establish policies for technical security control deployment as part of their services. The technical cybersecurity control set is based on established cybersecurity frameworks, such as the SANS Top-20 cybersecurity controls.

Overall, EU regulations apply in Lithuania and there are provisions within the domestic law on the technical and organisational measures to safeguard the security and integrity of services, such as within the Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services and within the Law on Electronic Communications of the Republic of Lithuania.

Review participants mentioned that the members of the MoND are trained domestically as well as internationally (e.g. by the EU, NATO, the Marshall Centre, UNODC, Barclays Training Centre and the Western Union Training Centre) on the deployment of technical security controls. Moreover, reports about risks and the threat landscape are published by the National Cybersecurity Centre (NCSC).

In the banking sector technical security controls are being deployed and each bank has a developed a separate department looking at security issues. Review participants noted that consumers face incidents of ransomware, and that this is why banks are developing programmes to regularly raise awareness among their customers. Also, some commercial banks have their own programmes for school children and universities. However, there is no legally binding requirement for the private sector at large to deploy technical security controls.

Users have an understanding of the importance of anti-malware software and network firewalls but not all users deploy such controls. Consumers' skills are very diverse, in particular depending on region and gender. The participants noted that usually the digital divide separates off females and the rural regions in the country.

The government has seen the need for more awareness, and there are various efforts to increase ICT skills. However, participants suggested that ISPs should take more responsibility, in particular at the technical level, and not rely on consumer skills.

D5.5 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.

Maturity Stage: Established

Cryptographic techniques are available for all sectors and users for protection of data at rest or in transit. There is a broad understanding of secure communication services, such as encrypted/signed email.

The cryptographic controls deployed meet international standards and guidelines for each sector and are kept up-to-date. State-of-the-art tools, such as SSL or TLS, are deployed routinely by web service providers to secure all communications between servers and web browsers, and all EU standards are followed on data protection and e-signatures. Moreover, domestic legislation asks for secure information transmission in all sectors. However, review participants expressed that they have doubts that the general public is aware and deploys cryptographic techniques.

D5.6 CYBERSECURITY MARKETPLACE

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

Maturity Stage: Formative

The domestic market in Lithuania may provide specialised cybersecurity products, but these are not market-driven. Although domestic suppliers exist, these cannot cover the country's needs. Penetration testing and auditing is provided by local companies. Also, there are vendors not only selling technology but also services.

Mostly Lithuania relies on international producers for software. Banks usually buy technology from the international market. Review participants mentioned that the MoND has developed an informal scheme to assess products from international producers.

A market for cyber insurance is established and encourages information sharing among participants of the market. The companies offering these products are not local but international. Cyber insurance is usually offered only to the banking sector, and covers cyber components only for catastrophic events.

D5.7 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.

Maturity Stage: Established to Strategic

A vulnerability disclosure framework is in place, which includes a disclosure deadline, scheduled resolution, and an acknowledgement report. Organisations have established processes to receive and disseminate vulnerability information.

The Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services[73] requires that providers of public communications networks report certain types of security incidents.

The Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019[74] also recommends implementing a stronger legal requirement for incident reporting, as part of a wider strengthening of the legal framework supporting electronic information security. Different CSIRTs in the country such as CERT-LT and LITNET CERT as well as the NCSC have mechanisms in place to share information including specific timeframes. Software and service providers commit to refrain from legal action against a party disclosing information responsibly.

RECOMMENDATIONS

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

ADHERENCE TO STANDARDS

R5.1 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.

[73] www.cert.lt/doc/CERT_LT_rules[EN].pdf
[74] www.ird.lt/viewpage.php?page_id=83&lang=en

R5.2 Establish a body within government to assess the level of adoption of standards across public and private sectors. Apply metrics to monitor compliance.

R5.3 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.

INTERNET INFRASTRUCTURE RESILIENCE

R5.4 Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors.

R5.5 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.

R5.6 Identify and map points of critical failure across the Internet infrastructure.

SOFTWARE QUALITY

R5.7 Develop a catalogue for secure software platforms and applications within the public and private sectors and share with all stakeholders.

R5.8 Establish software quality and functional requirements in public and private sectors, including policies on software updates.

R5.9 Promote the use of reliable software applications that adhere to international standards and good practices in the public and private sectors.

R5.10 Monitor and assess the quality of software used in public and private sectors.

TECHNICAL SECURITY CONTROLS

R5.11 Promote user understanding of the importance of anti-malware software and network firewalls.

R5.12 Establish policies for technical security control deployment in critical infrastructure and ISPs.

R5.13 Within the public and private sectors, keep technical security controls up-to-date, monitor for effectiveness and review on a regular basis.

CRYTOGRAPHIC CONTROLS

R5.14 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.

R5.15 Raise public awareness of secure communication services, such as encrypted/signed emails.

R5.16 Promote deployment of state-of-the-art tools, such as SSL or TLS, by web service providers, to secure all communications between servers and web browsers.

R5.17 Develop encryption and cryptographic control policies within the public and private sectors based on previous assessments, and regularly review the policies for effectiveness.

CYBERSECURITY MARKETPLACE

R5.18 Promote the production of cybersecurity products by domestic providers in accordance with market needs.

R5.19 Ensure that cybersecurity technology development abides by secure coding guidelines, good practices and adheres to internationally accepted standards.

R5.20 Promote the establishment of a market for cyber-insurance and encourage information-sharing among participants of the market.

RESPONSIBLE DISCLOSURE

R5.21 Develop a responsible vulnerability-disclosure framework or policy within all stakeholders involved (product vendors, customers, security vendors and public) and facilitate its adoption in the private sector, including a disclosure deadline, a schedule for resolution and an acknowledgment report.

R5.22 Encourage software and service providers to address bug and vulnerability reports, by applying configuration and patch management processes

R5.23 Encourage sharing of technical details of vulnerabilities among critical infrastructure organisations and ISPs.

R5.24 Publish the analysis of the technical details of vulnerabilities and disseminate advisory information according to different individual roles and responsibilities.

ADDITIONAL REFLECTIONS

Overall, the representation and composition of stakeholder groups was balanced and comprehensive. Vilnius University and NRD CS extended invitations to stakeholders in advance of the review, and while it is difficult to ascertain whether all relevant experts were present, the input gathered over the three days was key in arriving at our results.

This was the seventeenth country review that we have supported directly. Lithuania has commenced the process of developing different aspects of cybersecurity capacity across all dimensions, including through revising the National Cybersecurity Strategy and revisiting legal frameworks and regulation.

These efforts will establish the foundations for more advanced capacity in the future. We hope that this review will offer useful insights to Lithuania and that our recommendations 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**	Programme for the Development of Electronic Information Security (Cyber-Security) for 2011-2019 http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf National Security Strategy https://www.bbn.gov.pl/ftp/dok/07/LTU_National_Security_Strategy_2012.pdf	**R1.1** Modify the content of the strategy in response to the cybersecurity environment and incorporate it in the strategic plan. **R1.2** Ensure that the National Cybersecurity Strategy content includes, at a minimum: explicit links to national risks, priorities, objectives, and business development, raising public awareness, mitigating cybercrime, and protecting critical infrastructure from external and internal threats. **R1.3** Encourage the promotion and implementation of the National cybersecurity strategy by multiple stakeholders across government and other sectors. **R1.4** Administer a discrete cybersecurity budget line in order to allocate resources.
D1.2 Incident Response	**Established to Strategic**	CERT-LT25 https://www.cert.lt/en/index.html Lithuanian Cyber-Police https://www.epolicija.lt/en/home Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services https://www.cert.lt/doc/Rules_on_the_Ensurance_of_the_Security_and_Integrity.pdf	**R1.5** Improve incident identification and analysis in response to environmental changes and conduct regular, systematic updates to the national-level incident registry. **R1.6** Ensure that the human and financial resources allocated to incident response are adequate to the cybersecurity threat environment by conducting regular scenario exercises designed to test the human and financial capacity. **R1.7** Incorporate an early warning capacity into the mission of the emergency response organisation. **R1.8** Develop a culture of risk assessment and management predictive methods to assess risk, its propagation and its aggregation for the National and CI lens.

		FIRST http://www.first.org	**R1.9** Establish mechanisms for regional cooperation to resolve incidents as they occur. **R1.10** Promote a platform for the reporting and sharing of incidents across sectors.
D1.3 Critical Infrastructure (CI) Protection	**Established to Strategic**	Law on Cybersecurity of the Republic of Lithuania 11 December 2014 https://www.etar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4 http://www.internetlivestats.com/ Law on enterprises and equipment of strategic importance to national security, 2002 Law on the Management of State Information Resources 2011 https://e-seimas.lrs.lt/portal/legalAct/en/TAD/TAIS.432270 State and Official Secrets Act 1999 https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.9165	**R1.11** Prioritise listing of CNI assets and regularly re-appraise to capture changes in the threat environment. **R1.12** Implement regular audit practices to assess network and system dependencies to inform continuous reassessment of risk portfolio. Identify and establish specific auditing processes. **R1.13** Develop a strategy for strengthening formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector. **R1.14** Establish a mechanism for regular vulnerability disclosure with defined scope for reporting incidents between CI asset owners and the government. **R1.15** Optimize the legal framework concerning CNI by amending existing legislation or enacting new legal regulations as needed to encompass incident prevention, detection and response. **R1.16** Continue to invest in capability of Board Members and Senior Leaders of CI organisations to understand cyber-risk intelligence, in both private and public sector, so that they can lead in the face of crisis and take their part in risk management more generally. **R1.17** Allocate resources in proportion to the assessed impact of an incident to ensure rapid and effective incident response.
D1.4 Crisis Management	**Established**		**R1.18** Prioritise crisis management exercises, especially at a local level, and communicate the value of these exercises to all sectors. **R1.19** Conduct compromised communications scenarios and exercises to test emergency response asset interoperability and effective functionality and incorporate the results of the exercises

			to inform strategic investment in future emergency response assets. **R1.20** Share evaluation of the crisis management exercises with the international community, so that lessons learnt can contribute toward an improved global understanding of crisis management.
D1.5 Cyber Defence Consideration	**Strategic**	Lithuania's Defence Policy http://kam.lt/en/defence_policy_1053/important_documents/strategical_documents.html The Military Strategy of the Republic of Lithuania (Chapter 3) http://kam.lt/en/defence_policy_1053/important_documents/strategical_documents.html National Cyber Security Centre of Lithuania http://www.nksc.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/rysiu_ir_informaciniu_sistemu_tarnyba_prie_kam_2482/nacionalinis_kibernetinio_saugumo_centras.html	**R1.21** Review compliance of the National Security Strategy with international law and its consistency with national and international rules of engagement in cyberspace. **R1.22** Enhance funding efforts for research and development, possibly by establishing a cyber defence research centre, focused on automated cyber defence response systems.
D1.6 Communications Redundancy	**Established**		**R1.23** Undertake outreach to, and education of key stakeholders in the need for digital and communications redundancy. **R1.24** 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.

DIMENSION 2 CYBER CULTURE AND SOCIETY

D2.1 Cybersecurity Mind-set	**Formative**		**R2.1** Enhance efforts at all levels of government, especially officials, and the private sector to employ cybersecurity good (proactive) practices, but also to design systems that enable users across society to more easily embed secure practices into their everyday use of the Internet and online services. **R2.2** Routinize ross-sectoral cooperation and information sharing among private and public sector organisations on cybersecurity risks and good practice and promote that a cybersecurity mind-set informs strategic planning. **R2.3** 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**	European Commission Digital Single Market Country Profiles http://digital-agenda-data.eu/charts/country-profiles-the-relative-position-against-all-other-european-countries#chart={%22indicator-group%22:%22security-privacy%22,%22ref-area%22:%22LT%22,%22time-period%22:%222016%22} e-Government Gateway / Elektroniniai valdžios vartai https://www.epaslaugos.lt	**R2.4** Establish ISP programmes to promote trust in their services based on measures of effectiveness of these programmes. **R2.5** Promote privacy-by-default within government as a tool for transparency in e-services provision (including e-health and e-police) and implement feedback mechanisms for use to ensure that the e-services are continuously improved and the trust in strengthened among users. **R2.6** Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content. **R2.7** 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**		**R2.8** Promote the understanding of protection of personal information online among users and promote the development of their skills to manage their privacy online. **R2.9** Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making. **R2.10** Promote privacy by default as a tool for transparency.

D2.4 Reporting Mechanisms	**Formative**	E-Police https://www.epolicija.lt CERT-LT https://www.cert.lt	**R2.11** Encourage different stakeholders to coordinate the reporting mechanisms and their roles and responsibilities, and to collaborate and share good practices to improve the mechanisms. **R2.12** Establish awareness programmes to promote the regular use of reporting mechanisms by public and private sectors and promote their use as an investment in loss prevention and risk control. **R2.13** Employ effectiveness metrics for all existing mechanisms and ensure that they contribute to their improvement.
D2.5 Media and Social Media	**Established**	https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/csss2015_bada_et_al.pdf	**R2.14** 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 social impacts. **R2.15** Encourage a frequent discussion about cybersecurity on social media. **R2.16** Ensure that the debate in social and mainstream media and the attitudes expressed inform policy making.

DIMENSION 3 CYBERSECURITY EDUCATION, TRAINING AND SKILLS

D3.1 Awareness-raising	**Formative**	Programme for the Development of Electronic Information Security (CyberSecurity) 2011-2019 http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf European Cyber Security Month https://ec.europa.eu/digital-single-market/en/news/european-cyber-security-month-get-driving-seat-your-own-online-security NRDCS https://www.nrdcs.lt/ Safer Internet http://www.draugiskasinternetas.lt/en/main/about/info Centre of Information Technology of Education (CITE) http://www.draugiskasinternetas.lt/en/main/awareness_centre School programme Busiu http://busiu.eu/ Be safe in cyberspace http://www.esaugumas.lt	**R3.1** Develop a national cybersecurity awareness-raising programme with specified target groups, focusing on the most vulnerable users. **R3.2** Appoint a designated organisation (from any sector) to lead the cybersecurity awareness-raising programme. **R3.3** 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. **R3.4** Create a single online portal linking to appropriate cybersecurity information and disseminate the cybersecurity awareness programme via this platform. **R3.5** Enact evaluation measurements to study effectiveness of the awareness programmes at a level where they inform future campaigns taking into account gaps or failures. **R3.6** Promote awareness of risks and threats at lower levels of the government. **R3.7** Develop a dedicated awareness-raising programme for executive managers within the public and private sectors. **R3.8** Promote awareness regarding the protection of personal information online. **R3.9** Develop a dedicated awareness-raising programme for executive managers within the public and private sectors.
D3.2 Framework for Education	**Formative**	Faculty of Mathematics and Informatics, Vilnius University http://mif.vu.lt/lt3/studijos/studiju-programos/ba-studiju-programos/informacines-technologijos http://www.ef.vu.lt/dokumentai/sandai/VIS/Informacini%C5%B3_sistem%C5%B3_saugumas_2016.pdf http://www.vu.lt/en/scientific-report-2013/faculties-and-institutes/institute-of-mathematics-and-informatics-of-vilnius-	**R3.10** Create cybersecurity education programmes for instructors of cybersecurity to ensure that skilled staff is available to teach newly formed cybersecurity courses. **R3.11** Create accredited cybersecurity-specific degree courses at the university level, in addition to the other existing cybersecurity-related courses in the various Lithuanian universities. **R3.12** Promote efforts by Universities and other bodies to hold seminars/lectures on cybersecurity issues aimed at non-specialists. **R3.13** Allocate additional resources to cybersecurity education for public universities, dedicated to national

		university#Department-of-Software-Engineering Mykolas Romeris University https://www.mruni.eu/en/current_students/degree_programmes_in_lithuanian/ Kaunas University of Technology http://ktu.edu/en/studies https://stojantiesiems.ktu.edu/programme/m-informacijos-ir-informaciniu-technologiju-sauga/ Council of Science http://www.lmt.lt/en/about.html	cybersecurity research and laboratories at universities. **R3.14** Inform cybersecurity education priorities through broad consultation across government, private sector, academia and civil society, linked to the National Cybersecurity Strategy. **R3.15** 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. **R3.16** Ensure the sustainability of research programs. **R3.17** Develop effective metrics to ensure that educational and skill enhancement investments meet the needs of the cybersecurity environment.
D3.3 Framework for Professional Training	**Formative**	State Enterprise Infostruktūra http://www.is.lt/en/home.html Public institution Information Technologies Institute (ITI) http://www.ecdl.lt/english/ Baltic computer academy (BKA) http://www.bka.lt/en/ ISACA-LT http://www.isaca.org/chapters1/Lithuania/Pages/default.aspx	**R3.18** Establish more structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity-specific professionals. **R3.19** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, and models and operation of these tools. **R3.20** Train general IT staff on cybersecurity issues so that they can react to incidents as they occur. **R3.21** Ensure that affordable security professional certification is offered across sectors within the country. **R3.22** Develop a central platform for sharing training information for experts and create a national-level register of cybersecurity experts. **R3.23** Establish requirements for joint cybersecurity training for the public and private sector, and develop collaborative training platforms. **R3.24** Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals. **R3.25** Create incentives for employees within the public sector to maintain their posts after receiving training**.** **R3.26** Begin to implement metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings.

DIMENSION 4 LEGAL AND REGULATORY FRAMEWORKS

D4.1 **Legal Frameworks**	**Established to** **Strategic**	National Cyber Security Centre http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/rysiu_ir_informaciniu_sistemu_tarnyba_prie_kam_2482/nacionalinis_kibernetinio_saugumo_centras.html Law on Cyber Security of the Republic of Lithuania 11 December 2014 https://www.etar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4. Government decree on approval of the cyber security council and regulation) https://www.e-tar.lt/portal/lt/legalAct/4e3539f0ee4611e4927fda1d051299fb Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services www.cert.lt/doc/CERT_LT_rules[EN].pdf https://www.cert.lt/doc/Rules_on_the_Ensurance_of_the_Security_and_Integrity.pdf Law on Electronic Communications http://www.rrt.lt/en/legal-acts_250.html The Criminal Code https://www.unodc.org/res/cld/document/ltu/criminal_code_of_lithuania_html/Lithuania_Criminal_Code_2000_as_amd_2010.pdf Criminal Procedure Code http://www.wipo.int/wipolex/en/details.jsp?id=8195 Protection of human rights http://www3.lrs.lt/docs2/CSFIAIZY.PDF OECD Guidelines for Multinational Enterprises	**R4.1** Set mechanisms in place for continuously harmonising ICT legal frameworks with national cybersecurity-related ICT policies, international law, standards and good practices. **R4.2** Inform the existing legislation on protecting consumers from business malpractice online based on regional and international consumer protection standards. **R4.3** Develop a comprehensive legislation on intellectual property online through consultation with key stakeholders. **R4.4** Adopt the legislation currently under development to address the protection of intellectual property of online products and services.

http://www.oecd.org/newsroom/newoecdguidelinestoprotecthumanrightsandsocialdevelopment.htm

'Human Rights in Lithuania: 2013-2014
https://hrmi.lt/en/human-rights-in-lithuania-2011-2012-overview/

Law on the Provision of Information to the Public
http://merlin.obs.coe.int/iris/1997/3/article20.en.html

Draft Law on The Right to Receive Information
https://www.article19.org/data/files/pdfs/analysis/lithuania-foi.pdf

The Lithuanian Centre for Human Rights (LCHR)
http://manoteises.lt/lchr/information-in-english/

Law on Legal Protection of Personal Data
https://www.ada.lt/images/cms/file/pers.data.prot.law.pdf

The Inspectorate of Data Protection
https://www.ada.lt/go.php/eng/More

Personal Data Protection Act
http://www.wipo.int/wipolex/en/text.jsp?file_id=202094

Law on the Protection of Minors Against Detrimental Effect of Public Information (2002)
http://www.rrt.lt/en/legal-acts_250.html

Law of the Republic of Lithuania on electronic signature
http://www.rrt.lt/download/21996/tais_110909%20(2)_signature.doc

http://www.rrt.lt/en/legal-acts_250.html

Law on Consumer Protection
https://eseimas.lrs.lt/portal/legalAct/lt/TAD/e86e8310231911e6acbed8d454428fb7?jfwid=181l7lifma

State Consumer Rights Protection Authority

		http://www.vvtat.lt/index.php?2917529633 Bank of Lithuania http://www.lb.lt/en/sfi-disputes-between-consumers-and-financial-market-participants State Patent Bureau of the Republic of Lithuania http://www.vpb.lt/index.php?n=296&l=en Registration of Industrial Property Objects https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.151225 Law on Copyrights and Related Rights http://www.wipo.int/wipolex/en/details.jsp?id=2852	
D4.2 Criminal Justice System	**Established**	The Lithuanian Cyber Crime Competence Centre (L3CE) http://www.l3ce.eu Public Service Department http://www.vtd.lt/ National Court Administration http://www.teismai.lt/en/ E-Service Portal of Lithuanian Courts https://e.teismas.lt/en/public/home/	**R4.5** Strengthen national investigation capacity for computer-related crimes, with increased cooperation between the National Crime Agency and local police forces. **R4.6** Invest in advanced investigative capabilities in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators. **R4.7** Enhance investigative capacity and skills locally. **R4.8** Allocate resources dedicated to fully operational cybercrime units based on strategic decision making. **R4.9** Expand and allocate funding on work in training law enforcement in understanding computer related crime, in order to support investigations, especially at local level. **R4.10** Enhance training and education of prosecutors and judges on computer related crimes, and allocate additional resources for this purpose. **R4.11** Establish a mechanism to enable the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases. **R4.12** 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 to Strategic**	Infobalt www.infobalt.lt	**R4.13** Expand and enhance formal cooperation mechanisms on cybercrime as needed. **R4.14** Allocate resources to support the exchange of information between public and private sectors domestically and enhance legislative framework and communication mechanisms. **R4.15** Enhance established informal cooperation mechanisms between Internet Service Providers and law enforcement with clear communication channels.

DIMENSION 5 STANDARDS, ORGANISATIONS AND TECHNOLOGIES

D5.1 Adherence to Standards	**Formative - Established**	State and Official Secrets Act 1999 www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=91654	**R5.1** 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. **R5.2** Establish a body within government to assess the level of adoption of standards across public and private sectors. Apply metrics to monitor compliance. **R5.3** 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.
D5.2 Internet Infrastructure Resilience	**Strategic**		**R5.4** Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors. **R5.5** 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. **R5.6** Identify and map points of critical failure across the Internet infrastructure.

D5.3 **Software Quality**	**Established**		**R5.7** Develop a catalogue for secure software platforms and applications within the public and private sectors and share with all stakeholders. **R5.8** Establish software quality and functional requirements in public and private sectors, including policies on software updates. **R5.9** Promote the use of reliable software applications that adhere to international standards and good practices in the public and private sectors. **R5.10** Monitor and assess the quality of software used in public and private sectors.
D5.4 **Technical Security Controls**	**Established**		**R5.11** Promote user understanding of the importance of anti-malware software and network firewalls. **R5.12** Establish policies for technical security control deployment in critical infrastructure and ISPs. **R5.13** Within the public and private sectors, keep technical security controls up-to-date, monitor for effectiveness and review on a regular basis.
D5.5 **Cryptographic Controls**	**Established**		**R5.14** 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. **R5.15** Raise public awareness of secure communication services, such as encrypted/signed emails. **R5.16** Promote deployment of state-of-the-art tools, such as SSL or TLS, by web service providers, to secure all communications between servers and web browsers. **R5.17** Develop encryption and cryptographic control policies within the public and private sectors based on previous assessments, and regularly review the policies for effectiveness.
D5.6 **Cybersecurity Marketplace**	**Formative**		**R5.18** Promote the production of cybersecurity products by domestic providers in accordance with market needs. **R5.19** Ensure that cybersecurity technology development abides by secure coding guidelines, good practices and adheres to internationally accepted standards. **R5.20** Promote the establishment of a market for cyber-insurance and encourage

			information-sharing among participants of the market.
D5.7 Responsible Disclosure	**Established to Strategic**	Order on the Approval of the Rules on the Ensurance of Security and Integrity of Public Communications Networks and Public Electronic Communications Services https://www.cert.lt/doc/CERT_LT_rules%5bEN%5d.pdf Programme for the Development of Electronic Information Security (Cybersecurity) for 2011-2019 http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf	**R5.21** Develop a responsible vulnerability-disclosure framework or policy within all stakeholders involved (product vendors, customers, security vendors and public) and facilitate its adoption in the private sector, including a disclosure deadline, a schedule for resolution and an acknowledgment report. **R5.22** Encourage software and service providers to address bug and vulnerability reports, by applying configuration and patch management processes. **R5.23** Encourage sharing of technical details of vulnerabilities among critical infrastructure organisations and ISPs. **R5.24** Publish the analysis of the technical details of vulnerabilities and disseminate advisory information according to different individual roles and responsibilities.

The review was conducted in cooperation with Vilnius University and NRD CS

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