# MALTA CYBER SECURITY STRATEGY 2016

MINISTRY FOR COMPETITIVENESS AND DIGITAL, MARITIME AND SERVICES ECONOMY

# Contents

# Minister's Foreword

In today's globalised world, the extensive and efficient use of Information and Communications Technologies (ICTs) is increasingly critical for the effective functioning and growth of our economy. It is an increasingly essential means for the private sector to compete and prosper, through its ability to connect to the local markets as well as to those beyond our shores, efficiently and cost effectively. Competitiveness in a digital economy however calls for resilience to the security challenges posed within the realm of cyber-space - ICT and its constituent elements and its dependents.

This Strategy aims to establish the foundations to ensure effective cyber security within Government, the private sector and civil society. It does not simply entail technology security controls but involves measures related to regulation, legislation, awareness, education, expertise and foreign affairs.

Striving for cyber security is a continuous journey. Cyber security can never be fully attained, considering that the technology itself, the day to day realities in technology adoption as well as the modes of cyber attack are in a continuous state of evolution. Hence the Strategy is not seen as cast in stone, but it shall need to evolve, in line with a national commitment and collective effort to adopt a cyber security culture.

Embracing security as a normal way of everyone's cyber lives is in the common interest. Ultimately, cyber security needs to be seen as a key cornerstone to Malta's competitiveness within the digital world by positioning it as a secure online jurisdiction and potentially presenting opportunities for the development of centres of excellence in a number of local business sectors interacting within the realm of cyberspace.

**Hon Dr. Emmanuel Mallia**
**Minister for Competitiveness and Digital, Maritime and Services Economy**

# Executive Summary

Cyber-space is far from perfect. It is at risk of vulnerabilities, some of which involve genuine human error, whilst others are exposed to malicious intent. Furthermore, global innovations within its realm are even faster than the ability to secure it. Hence the need for cyber security, that is, ensuring the safety, confidentiality, integrity and availability of cyber-space.

Launching cyber security on a national scale, essentially calls for a planned, collective and systemic approach, thus leading to the need of a National Cyber Security Strategy. *Digital Malta* – the National Digital Strategy for Malta for the period 2014-2020 - recognises and proposes the fulfilment of such need, in the light of Malta's increased dependence upon cyber-space in its day to day interactivity, within and beyond its shores. Indeed, in 2015, the European Commission's *e-Government Benchmark Report* re-confirmed Malta as the leader in the delivery and performance of e-Government services amongst thirty-three countries.

Malta is addressing such a need. A Green Paper for a National Cyber Security Strategy was launched in October 2015, as a basis for consultation. The Green Paper presented a high level, strategic approach for cyber security on a national scale. It intended to inculcate an awareness of cyber security, its extent and its implications of which Malta, as an integral part of cyber-space, needs to consider. The National Cyber Security Strategy being launched is a consolidation of the proposals presented by the Green Paper following online feedback and a number of consultation sessions held.

The National Cyber Security Strategy recognises that tackling cyber security entails the need to:

- Safeguard **the rule of law** in line with Malta's Constitution and Malta's role as a European Union Member State
- Adopt a **multi-disciplinary approach**
- Ensure that all stakeholders of cyber-space; government, private sector, and civil society understand their **shared responsibility** and thus commitment to collaboration and cooperation, to ensure a safe, stable and secure environment
- Adopt a **risk based approach**, based upon the premise that it is impossible to guarantee immunity from any cyber attack.

All of the above constitute the fundamental principles upon which the overall vision is based. In essence, the Vision covers the need and expectations of three key national stakeholders – the **public sector**, the **private sector** and **civil society** to ensure cyber security. Five dimensions enable articulation of the vision into the strategy. They are Policy, Legislation, Risk Management, Awareness and Education upon which the subsequent proposed strategy is based.

Prior to proposing the strategy however, research and assessments have been made so as to enable a high level pragmatic approach towards cyber security within the local context. The ensuing strategic direction within the Green Paper is proposed to be attained by six goals, each of which carries a number of proposed measures, as follows:

1. **Goal: Establish a Governance Framework** that is based upon the premise that a cyber security strategy needs to be established, and more importantly, be effectively implemented and maintained on a continuous basis. Hence the need to ensure the key coordination structures, processes, roles and practice with particular focus on cyber risk management within the public and private sector.
2. **Goal: Combat Cybercrime** which aims to ensure and consolidate capabilities to tackle cybercrime.
3. **Goal: Strengthen National Cyber Defence** which aims to foster sharing of cyber security knowledge and intelligence, review current legislation and regulations in line with cyber-space developments and ensure digital resilience on a national and organisation wide

scale of particular consideration are recent legal developments at EU level, notably legislation pertaining to data protection and that related to Network and Information Security.

4. **Goal: Secure cyber-space**
   which aims to foster self regulation and voluntary self commitment, bearing in mind that legislation is not a panacea to cyber security commitments. It also aims to stimulate use of standards and best practices that guarantee security whilst allowing for interoperability. Special focus is also given to promote security and trust of online public services and to consolidate support to the private sector.

5. **Goal: Cyber security Awareness and Education**
   which aims to target academia, the public and private sector and citizens as a means to sensitize awareness, knowledge as well as capabilities and expertise in cyber security. A national strategic approach towards an ongoing educational and awareness campaign is especially recommended.

6. **Goal: National and International Cooperation**
   which aims to ensure effective consultation, cooperation and collaboration on a national level, on a European and on a global basis, enabled by EU and international institutions and activities, based on the understanding that cyber security has no bounds.

All six goals aim to cover two key strategic outcomes expected of the Strategy, namely those of:

- Defending and protecting the national information infrastructure from cyber threats.
- Ensuring the security, safety and protection of users of cyber-space.

The proposed strategic approach is by no means the end in itself. It is understood that the launch of the Strategy is only the start of a continuous process that calls for its implementation, evaluation and maintenance so as to ensure its currency and effectiveness in line with:

*“ Launching cyber security on a national scale, essentially calls for a planned, collective and systemic approach, thus leading to the need of a National Cyber Security Strategy. ”*

- Increased recognition on a nation-wide scale of the importance to adopt cyber security measures in day to day corporate and individual activities
- Evolving maturity of overall cyber security capability
- Technological developments and applicability, along with related cyber security challenges
- Evolution in cybercrime behaviour
- Developments on a national scale, in line with European Union direction on cyber security to its Member States of which Malta forms part.

Hence, the Strategy would be expected to be periodically reviewed and updated. Ultimately, the Strategy is understood as a means for national cyber security investment that indicates Malta as a :

- Secure online jurisdiction
- Centre of excellence in various business sectors interacting within cyber-space.

Part One

# Introduction

# 1. BACKGROUND

Up to a few decades ago, a country's security interests focussed on protecting its borders, its waters and its airspace. Today, cyber-space forms an integral part of a country's day to day reality.

Information and Communications Technology (ICT) leads the way in interaction within and outside of a country's territory and its disruption may potentially affect life. Hence, cyber-space cannot be left out of a country's span of protection.

Malta is no island within the realm of cyber-space! Cyber-space knows no boundaries. It transcends national borders, promoting online opportunities of dialogue, mutual cooperation and understanding beyond our shores. However, the cyber world makes no distinction between its users of good intent or not.

Therefore, as opportunities are limitless, so are cyber threats. Such malicious attempts in cyber-space may be launched anywhere, in any vulnerable area of a digital network, instantaneously leaving no time for an appropriate response and with very minimal traceability or detection of its perpetrator.

Ultimately, cyber-space is man-made and like anything else of its sort, it is never perfect. The rapid advances of technology itself and the opportunities that arise from it do not allow it either. Indeed the innovations in technology and its adoption are even faster than the ability to secure it.

Malta's security of cyber-space ultimately calls for a planned, collective and systemic approach that respects fundamental rights and freedoms whilst ensuring confidentiality, integrity and availability of cyberspace on a day-to-day basis. Such is the intention of **Digital Malta** – the National Digital Strategy for the period 2014 till 2020 – which identifies a National Cyber Security Strategy as one of its required actions.

# 2. PURPOSE AND SCOPE

This Strategy intends to set an overall high level direction in cyber security across all strata of the Maltese economy and society. As a first issue, it also intends to consolidate a recognition of the need for a planned and concerted effort by the various stakeholders involved so as to protect Malta and its interests.

*" Everyone is affected by cyber issues and everyone needs mutual assistance. It is therefore in everyone's interest and responsibility to ensure a secure and safe cyber-space for all. "*

This Strategy should translate into timely, specific and actionable measures that set the foundations for a national cyber security framework that shall need to be implemented, maintained and updated so as to ensure currency and relevance in a highly challenging, dynamic and complex environment as that posed by cyber-space.

Through its various goals and corresponding measures, the National Cyber Security Strategy aims to:

- Position cyber security as a national investment, that gives an indication beyond Malta's shores of the country's commitment to a secure cyber-space for online transaction and interaction
- Convey the key message that cyber security cannot be achieved in isolation. It does not

simply fall within the domain of Information and Communications Technology experts and practitioners. Everyone is affected by cyber issues and everyone needs mutual assistance. It is therefore in everyone's interest and responsibility to ensure a secure and safe cyber-space for all.

The National Cyber Security Strategy, above all, aims to align itself within the scope of:

- Specific **EU legal requirements**[1]. Reference to such legal requirements, however, does not preclude the need to refer to the specific legal requirements for further direction.
- Digital Malta and other local strategy documents such as **e-Commerce Malta** - the National e-commerce Strategy (2014-2020) - published by the Malta Communications Authority[2].

## 3. THE PRE-LAUNCH OF THE STRATEGY

On 30th October 2015, the Minister for the Economy, Investment and Small Business launched a Green Paper for a National Cyber Security Strategy. The Green Paper followed extensive research based upon various published sources to assess cyber security from:

(i) A global and from a European Union perspective, based on the understanding that the interconnectedness in cyberspace renders any challenge in cyber security as potentially impacting any country applying Information and Communications Technology, including Malta.

(ii) A domestic perspective, particularly with respect to:

- Experiences and concerns expressed by Maltese participants in annual Euro Barometer surveys specialising in cyber security
- Malta's current official position in particular aspects of cyber security

(iii) A multi-stakeholder perspective, based on the understanding that apart from technology, cyber security impacts upon all of country's political, legal, economic and social well being.

The Green Paper set the basis for consultation through:

1. Online feedback using http://mita.gov.mt/ncss and http://www.konsultazzjoni.gov.mt that lasted till 14 February 2016
2. A series of consultation events, which were held between March and June 2016 and which targeted a number of social and economic sectors, namely:
   - Economy and Finance
   - Education and National Awareness
   - Justice and Legislation
   - Infrastructure and Health
   - National Security
   - The Public

The consultative process led to relevant updates to the proposals made within the Green Paper; leading to the issue of this first version of the National Cyber Security Strategy.

Part Two

# Overall Direction

# 4. PRELUDE

This Section sets the scene for the National Cyber Security Strategy, through a definition of what is meant by cyber-space and its security and an outline of the key principles leading to the vision expected to be attained through the strategy.

A Cyber Security Model presented encapsulates the key dimensions that are to be addressed by means of goals and corresponding measures, proposed in Part 3, for the implementation of the Strategy.

# 5. WHAT IS MEANT BY CYBER SECURITY

Definitions for cyber security abound; however they all essentially point to the **security** of the **cyber-space**; namely all:

- Interconnected ICT hardware and software infrastructure
- Data in transit and at rest on the networks
- Connected users
- Logical connections established among them

In view of the above[3], the following definition of cyber security is being adopted:

*It is the safeguards and actions that can be used to protect cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure. It strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.*

Essentially, cyber security is based upon the foundations of information security, namely confidentiality, integrity and availability. However, whilst information security is business driven and results in prudent investment in safeguards and countermeasures, cyber security is threat driven where all cyber-space is at risk. The inherent interconnectedness of cyber-space exposes all of its constituents to a failure of their most vulnerable elements[4] .

Additionally effective cyber security cannot be reached by technological measures alone as modern cyber attacks could bypass all defence layers by exploiting the human factors through techniques such as social engineering[5].

Hence, *safeguards* and *actions* hereby refer to ongoing and planned measures which may potentially be of technical, operational, legislative, educational, behavioural or disseminative nature.

Above all, cyber security cannot be seen from a technological aspect only, but needs to cover the needs and expectations of the state, the economy and society, all of which are increasingly active participants in an interactive digital world.

# 6. GUIDING PRINCIPLES

Within this context, the Strategy, in its lifecycle, shall be guided by a number of principles as follows:

## Rule of Law

The approach on cyber security shall respect and promote fundamental rights and freedoms as chartered within European Union and national legislation. All measures shall comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and redress.

## Multi-stakeholder, cooperative and collaborative approach

The pervasive nature of cyber-space, essentially calls for a multi-stakeholder approach towards its security – both at a national level as well as beyond Malta's shores. Hence, on a national level, cooperation and collaboration of various stakeholders, including the

*“ Whilst leading in its commitment towards cyber security on a national scale, Government cannot assume sole responsibility for protecting all of cyberspace. All users of ICT are responsible to take reasonable steps to protect systems and data on an individual and on a collective basis. ”*

public sector, the private sector, academia and civil society is necessary. A cooperative and collaborative approach at an EU and international level is also required.

### Shared goal and responsibility

Effective cyber security essentially calls for the sharing of one common goal that transcends boundaries. Whilst leading in its commitment towards cyber security on a national scale, Government cannot assume sole responsibility for protecting all of cyberspace. All users of ICT are responsible to take reasonable steps to protect systems and data on an individual and on a collective basis.

### Risk Management

The widely diffused use of cyberspace coupled with its rapid and continuous evolvement, renders it impossible to guarantee immunity from any form of cyber attack. Hence a risk-based approach to assess, prioritise and take measures to ensure cyber security, along with any technology investment is necessary.

## 7. OVERALL VISION

Within the context of the articulated principles, an overall vision for the National Cyber Security Strategy is:

*To ensure a secure, resilient and trusted digital interactive environment that supports Malta’s safety and security whilst maximising on the benefits of a digital economy.*

In specific terms, the vision entails that:

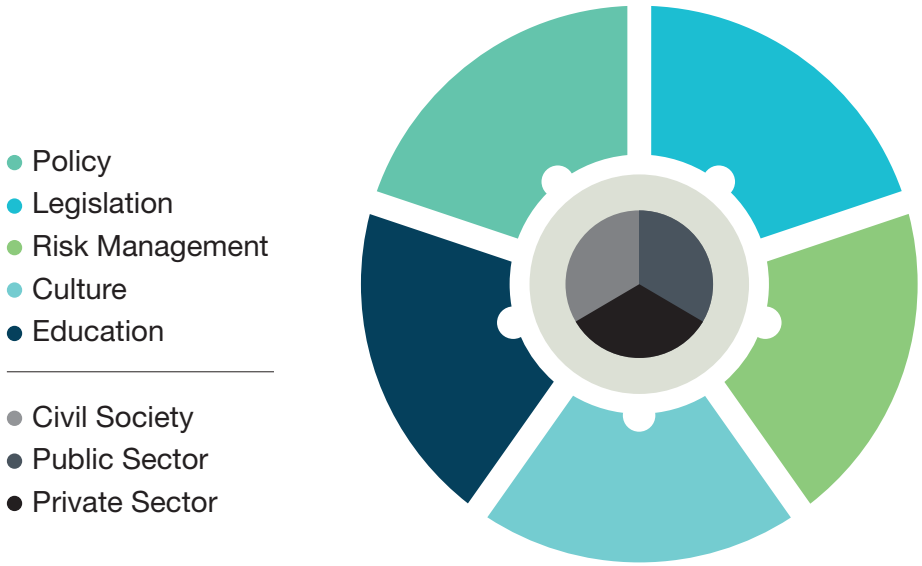
- Civil society is aware of cyber risks and undertakes necessary precautions to protect its privacy, confidentiality, personal integrity, identity and well-being
- The Private Sector, whilst tapping the opportunities resulting from the technology developments, actively ensures that it operates in a secure and resilient digital economy, whilst ensuring effective delivery of their services and/or goods and protection of their customer’s privacy and integrity
- The Public Sector leads the way in ensuring a secure and resilient digital environment for its interaction with and/or service delivery to civil society, private enterprise and with regional and international partners, as well as in placing Malta as a secure online location for business interaction.

The National Cyber Security Strategy aims to address the needs and expectations of each of the above stakeholders, in the light of the proposed vision.

Proposed goals and related measures underscore in more specific terms how the strategy is expected to be implemented.

# 8. A CYBER SECURITY STRATEGY MODEL

As outlined in **Figure 1**, the strategy addresses five dimensions which are identified within the **Cyber Security Capability Maturity Model** of the Global Cyber Security Capacity Centre, University of Oxford[6].




| Policy | Legislation | Risk Management | Culture | Education |
|---|---|---|---|---|
| Devising cyber security policy and strategy that sets the direction on a national level. | Creating effective legal and regulatory frameworks to support all aspects of the strategy. | Controlling risks through organisation, standards and technology. | Fostering awareness to encourage a responsible cyber culture throughout society. | Building cyber skills into the workforce and leadership through effective education. |

**Figure 1 – A Cyber Security Strategy Model for Malta**

Part Three

# The Strategy

# 9. THE GOALS AND ACCOMPANYING MEASURES

## 9.1 The Goals

**Digital Malta**, and in particular, **Action 53**, proposes four high level goals for a National Cyber Security Strategy, which are:

- **Combat Cybercrime**
  Law enforcement agencies are to identify gaps and strengthen their capability to investigate and combat cybercrime.
- **Strengthen National Cyber Defence**
  Public and private entities are to be guided and assisted in strengthening their cyber defence capabilities.
- **Secure Cyber-space**
  Higher levels of trust are to be instilled through awareness programmes and the delivery of trustworthy, ICT-enabled services that assure confidentiality, integrity, availability and privacy.
- **Build Capacity (Cyber security Awareness and Education)**
  The skills and educational frameworks required are to be identified and developed.

However, sound and stable governance essential for the effective ongoing implementation of a National Cyber Security Strategy, calls for two other goals, namely:

- **Establish a Governance Framework to attain a National Cyber Security Strategy**
  Given that at this stage, only the technical and operational structures are in formation. The strategic level that focuses on the long term trends, analysis and coordination in cyber security is also necessary.
- **National and International Cooperation**
  given that the borderless nature of cyber-related activity, essentially calls for particular regard to the global and regional aspect, apart from the national focus of related security. In all, the six goals aim to cover two key strategic outcomes expected from the Strategy, namely:
  - **Defending and protecting the national information infrastructure from cyber threats**
  - **Ensuring the security, safety and protection of users of cyber-space.**

## 9.2 The Proposed Measures

A set of measures to each corresponding goal are proposed below, based upon:

- Analysis, as well as consultations undertaken within the local context,
- Best practices noted in cyber security strategies within the European Union and worldwide,
- EU legal requirements and direction. The measures outlined do not exclude action that may need to be taken with respect to specific EU legal requirements[7].
- Relevant action items within **Digital Malta** and other local strategies such as **e-Commerce Malta**.[8]

## 1. Goal: *Establish a governance framework*

The governance framework covers the necessary key functions and corresponding roles and responsibilities, as well as policies and processes necessary[9] to constitute a robust foundation for an effective national cyber security strategy.

### *i. Establish the necessary key coordination structures*

It is envisaged that the following functions (involving multiple stakeholders) shall be required to ensure sustainability of the National Cyber Security Strategy:

a. At the strategic level:

i. A function for the articulation and periodic review of the National Cyber Security Strategy. The creation of this function is required in the short term. This body would need to work in close cooperation with the strategy implementation function(s) referred to below

ii. A strategy implementation function to oversee implementation of the strategy and monitor cyber security operations. Such function needs to have the necessary funding, resources and mandate to:

- take a leading, active role in the implementation of the National Cyber security strategy, keeping in view of policy and planning developments within the realm of Malta's digital economy and society as well as further cyber security related developments on a national, EU and international perspective
- ensure security preparedness of the public and private sector of their ICT, in line with established security requirements. This implies driving for effective engagement and ongoing high level coordination across Malta's public and private sector.

b. At the operational level, function(s) for the national coordination of cyber detection and response. Computer Security Incident Response Teams (CSIRTs) tend to be of such technical and operational nature. This entails ensuring consolidation of a top level National CSIRT[10]. It also implies close communication and coordination of the CSIRT with the proposed strategy implementation function, given that it would need to be involved on:

- Real-time information sharing and response to calls
- Longer term planning[11]. Communication and coordination, as the need arises, with other CSIRTS existing in Malta would also be necessary.

The structure[12] and responsibilities of these functions is subject to further reference and alignment to the relevant European Union legal requirements[13] as well as to further consultation.

### *ii. Foster the coordination to protect national critical information infrastructure*

Measures of preparedness, response and recovery, including cooperation and ongoing coordination mechanisms are particularly necessary to protect national critical information infrastructure. It is thus necessary to ensure that such national coordination between all stakeholders concerned[14] is fostered.

### *iii. Ensure clear delineation and communication of roles and responsibilities*

Cyber related roles and responsibilities - such as those identified above and potentially those arising from the proposed measures, as well as those resulting from relevant EU legal requirements[15], need to be clearly delineated and agreed upon accordingly. Communication of their establishment further ensures the effective coordination that may be necessary between the effected stakeholders themselves.

### *iv. Ensure the conduct of a national cyber risk assessment exercise*

A National Cyber Risk Assessment exercise shall need to identify the major national cyber threats and risks, assess respective impacts and

suggest risk mitigation and management strategies accordingly. The exercise entails participation and coordination between all stakeholders involved[16] and it needs to be updated on a regular basis, so as to ensure its currency with:

- The cyber threat landscape
- Evolution in the adoption of existing and emerging ICT.

One key deliverable of the National Cyber Risk Assessment is a strategic plan that includes cooperation and communication processes needed to ensure prevention, detection, response, repair and recovery (including communication), that are modulated according to the alert level are to be ensured.

Such processes also refer to national incident cyber handling procedures and business continuity plans to ensure resilience. Furthermore, it is understood that such processes need to be subject to a schedule of regular testing and validation exercises[17], with the resulting outcome (including lessons learnt) used as a basis for any related updates.

***v. Ensure necessary measures in line with individual cyber risks assessments by key Public and Private sector organisations falling within the scope of related EU legal requirements***

The conduct of a National Cyber Risk Assessment does not exclude the conduct of individual cyber risk assessments particularly by the public and private sector organisations falling within the scope of related EU legal requirements on network and information security[18].

Data Protection Regulation (EU) 2016/679 and other Directives coming into force by June 2018 across the EU, also call for all organisations to ensure regular risk assessments by organisations to understand the degree of threat imposed on them when processing personal data. The legislation demands a risk-based approach with the development of appropriate controls.

***vi. Encourage cyber risk assessments by other organisations not falling within the scope of Measure 1 (v)***

The emphasis on individual risk assessment made to specific organisations with respect to network and information security, in **Measure 1 (v)** should not however construe that other organisations need not adopt similar activities. Indeed, data protection legislation, also referred to in **Measure 1 (v)** is applicable to all organisations processing personal data.

An assessment of financial risks related to cyber-related incidents could possibly also indicate a market in cyber insurance, which may in turn contribute to information sharing among its participants, apart from availability of financial coverage to mitigate consequential losses.

Ultimately, however, it needs to be borne in mind that cyber insurance coverage alone is not a panacea to cyber security threats. It needs to be carried out with in conjunction with consideration and applicability of cyber security measures in line with the risks assessed.

***vii. Consolidate the Information Security Framework within the Public Sector***

The Government of Malta Information Security Policy is expected to come into force in the near future. It is based upon ISO 27001 Information Security international standard and applies to all of the Public Sector.

***viii. Ensure classification of data within the Public Sector and encourage it within the private sector***

The classification of electronic data within the Public Sector and the application of security controls commensurate to the security marking assigned is one area, among others, referred to

within the Information Security Policy, referred to in **Measure 1 (vii)**. This aspect is a critical initial step in ensuring effective cyber security, also keeping in view of the inherent sensitivity of data dealt within the sector. Nonetheless, the classification of data as one of the primary tasks to be undertaken by any organisation (public sector or otherwise) is one of the key awareness targets that needs to be taken into account.

*"Internal security is crucial. Yet, it also needs to be borne in mind that threats to EU citizens are increasingly cross border and varied in nature. EU Member states, including Malta, can thus no longer succeed on their own."*

## 2. Goal: *Combat Cybercrime*

***i. Establish Forum for Internet Safety and Protection of Minors***

This measure is referred to in **Digital Malta**, and it proposes a number of relevant public sector stakeholders and industry representatives as the Forum's members. The Forum aims to:

- Share knowledge
- Monitor developments
- Put forward policy ideas
- Represent Malta on European bodies working in this field

This Forum could potentially help out in reviewing the Cyber security strategy itself with respect to combating cybercrime activity.

***ii. Identify gaps and strengthen capability to investigate and combat cybercrime***

A regular assessment of present state cybercrime capability in Malta among all relevant law enforcement, investigative and judicial roles and any related action necessary is indeed a prerequisite in the light of the continuously evolving threat vector landscape.
Internal security is crucial. Yet, it also needs to be borne in mind that threats to EU citizens are increasingly cross border and varied in nature. EU Member states, including Malta, can thus no longer succeed on their own. The **European Agenda on Security** – the EU's strategy to tackle security threats in the EU for period 2015-2020[19] is intended to contribute in this respect. Cybercrime is one of the Agenda's priorities for the years 2015-2020.

The Agenda aims to strengthen and make more effective the exchange of information and operational cooperation between Member states, EU Agencies and the critical information infrastructure sector; by aiming to:

- Reinforce the capacity of law enforcement authorities in Member states, in particular through the Europol's European Cybercrime Centre

- Address obstacles to criminal investigations on cybercrime, notably with respect to access to evidence
- Prioritise the implementation of existing legislation on attacks against information systems and on combating child abuse.

***iii. Assess and consolidate on-line reporting of cybercrime***

The on-line mechanism is needed to report illicit online activity for the required action to be taken as well as to determine the extent of cybercrime. It entails:

- The ability to track cybercrime at a national level
- Ensuring further nation-wide related awareness, especially among citizens and small businesses.

It is also recommended to ensure that a strategic approach on the applicability of online services related to cybercrime handling is taken, so as to enhance effectiveness, whilst maximising the use of resources.
Additionally, the ability to handle cases related to cyber bullying (or any other form of cyber abuse) also needs to be ensured among online support personnel handling services pertaining to abuse.

## 3. Goal: *Strenghten National cyber defence*

***i. Establish a collective approach for sharing cyber security knowledge and intelligence***

A collective approach, involving both the public and private sector, potentially facilitated through the use of ICT is needed to:

- Allow participants from across sectors and organisations to exchange information on cyber threats and to mutually strengthen response to cyber threats, vulnerabilities and incidents securely, efficiently and effectively[20], whilst operating within a framework that protects the confidentiality of the shared information.[21] It may also allow for intra-business sect oral communication, particularly in areas where particular information may be deemed as of a highly sensitive nature to be shared with all participants
- Analyse new trends and identify opportunities and emerging threats
- Work to strengthen cyber security
- Provide framework for sharing best practice[22]
- Potentially improve professionalism in information assurance and cyber defence across the private and public sector through schemes for certifying related competence and specialist training.

***ii. Review existing legislation and provide measures through legislation and regulation to ensure relevance and effectiveness to the cyber world***

This measure builds upon two objectives of Digital Malta, as follows:

- Objective 43 – review existing legislation to ensure relevance and effectiveness in the cyber world'
- Objective 44 – provide measures to maintain privacy, safety and security while surfing, transacting and operating on-line. Legislation will address several matters such as safeguarding intellectual property rights, patents, sensitive and personal information, cloud computing and

data ownership, contentious content, net neutrality, vendor lock-in and exit management strategies; online contracts and license agreements.

The measure is also highly relevant taking into consideration:

- The requirements arising from the European Agenda on Security, referred to in Measure 2.2.
- Action 38 – Digital Single Market – of Digital Malta, which states Government's intention to maximise the benefits and opportunities deriving from legislation adopted within the EU such as those related to data protection, electronic identification and trust, etc
- Relevant EU Directive and regulation , notably among others, recent EU data protection legislation and legal requirements pertaining to Network and Information Security

Within this light, the notion of having one national legislation for cyber security, merits active consideration. It is understood that its effectiveness would need to be backed by:

- Prior multi-displinary wide national consultation
- Consideration and alignment to existing national and EU legal requirements covering aspects of cyber security[24]
- A balance between incentives and sanctions
- Promotion of related awareness and cooperation with the various stakeholders involved in working towards cyber resilience.

The legislation may be positioned in a way so as to allow sectors (regulated or otherwise) to adopt any further measures as necessary.

***iii. Ensure the country's digital resilience to cyber attack as well as the capability to protect its interests***

As an independent sovereign state and as a member of the United Nations (UN), Malta has the right to defend its own territory and its infrastructure from acts of aggression from other states[25]. Cyber-space is no exception and Malta has the right and obligation to defend its cyber-space territory to ensure that the security of the nation is maintained.Such measure entails ensuring that the following are addressed:

- Cyber-space defences
- Structures to counter terrorist attacks
- Ability and capacity to detect threats in cyber-space
- Capability to disrupt attacks on the country from cyber-space
- Active consideration of direction being taken at EU level on areas such as cyber diplomacy[26] and on ways to counter hybrid threats[27].

*"Malta has the right and obligation to defend its cyber-space territory to ensure that the security of the nation is maintained."*

***iv. Conduct national cyber simulation exercises***

Cyber simulation exercises are to be scheduled and conducted from time to time, at a national level. Such measure contributes to the need to review the ability to anticipate, prepare for, identify and attribute, combat hostile cyberspace acts. Apart from technical considerations, cyber simulation exercises should also assess non-technical areas both at an operational, tactical as well as at a strategic level such as testing national and international coordination and any relevant Standard Operational Practices.

The participation of key public and private sector stakeholders[28] in such exercises is crucial. The participation of other organisations is also encouraged.

## 4. Goal: *Secure Cyberspace*

***i. Establish regulation and voluntary self-commitment for guaranteeing cyber security***

The current scenario analysis of cyber security in Malta indicates areas of regulation and policy particularly within the local regulated industry sectors. Focus appears to be mainly on policy frameworks covering the licensing approaches which seek to mitigate risk.

*"Interoperability is one means of broadening and strenghtening collaboration, establishing intelligence and improving situational awareness, all of which are essential for effective cyber security."*

Whilst legislation may help, Maltese regulatory authorities may also need to address further emerging technology such as cloud computing applicability, through regulation within their respective sectors.

The formulation of regulation pertaining to cyber security would need to take into consideration, among others, the latest EU data protection legislation[29] as well as of legal requirements pertaining to network and information security, where applicable.

Regulation within sectors may also include conformance to internationally recognised security standards or industry led cyber security related standards or practices, with the aim of bolstering cyber security as well as establishing centres of excellence within the sectors themselves.

Such alignment may also call for particular consideration, in terms of support, to organisations having limited or constrained resources (including human and financial).
On the other hand, it is understood that legislation and regulation cannot necessarily cover all aspects of cyber security; particularly considering potential financial and human resource constraints for robust cyber security.

Voluntary self commitment is, thus, also key to cyber security. The notion of the applicability of a European security trust mark, applied also in a number of EU states [31]may encourage voluntary self commitment and may therefore be one item to explore the possibility of its use locally. Local national strategy may already serve as a potential opportunity for further consideration in fostering self commitment, such as:

- **e-Commerce Malta** which highlights three pillars as its basis:
  i. Engendering trust in ecommerce
  ii. Transforming micro-enterprises
  iii. Taking Small to Medium sized Enterprises and industry to the next level; which specifically also refers to an audit-kit – through a Specialist advisory service *(Measure 2)* and the European trust-mark *(Measure 9)*
- **Digital Malta** which refers to the *Forum for the transformation of industries through ICT* that aims to raise awareness about how ICT can help industries transform themselves and to discuss items such as self-regulation.

Other potential opportunities which may be explored include financial incentives, such as in the form of grant schemes, as a means to entice the applicability of necessary cyber security related measures.

***ii. Stimulate use of interoperable and secure standards on the basis of good practice***

Digital Malta, through Action 42 – Standards and Good Practice, states Government's intention to collaborate with stakeholders to support and promote

National and EU cross-border interoperability, ICT standards based on industry best practices and Green ICT.

Interoperability is one means of broadening and strenghtening collaboration, establishing intelligence and improving situational awareness[32], all of which are essential for effective cyber security[33]. With respect to the notion of nationally and EU recognised interoperability, which also effectively promotes the use of safe secure standards, **Digital Malta** states as one of its objectives, Government's commitment to revise and revamp the current National Interoperability Framework including related policies[34].

The implementation of internationally recognised information security standard[35] controls within the public sector[36] and potentially within the private sector should contribute to cyber security on the local scenario. The applicability of such controls may serve as a good initial basis.

However consideration of industry led standards and guidance that put in place a series of measures specifically aimed to address cyber threats[37] are also to be encouraged for use. This could form an integral part of what is proposed in **Measure 4 (i)**.

In particular, special consideration needs to be given by operators and users of emerging technologies. In such areas, related standards and security controls, may still be in the very early stages of maturity and may thus pose cyber security vulnerability challenges for interoperability which need to be carefully assessed.

***iii. Promote robust levels of cyber security in online public services***

Such measure may alleviate concerns expressed within Euro barometer findings with respect to Maltese accessing online services[38]. The applicability of interoperable and secure standards, as referred to in **Measure 4 (ii)**, may potentially contribute for the attainment of such measure.It also calls for an emphasis to ensure security and privacy in the design of ICT products and services for Government as well as in other areas of application.

*"A chain is only as strong as its weakest link. Unfortunately, within the realm of cyber security, weakest link could, more often than not, be traced to the human factor. The behavioural and educational aspect of cyber security cannot thus be discounted."*

Additionally, the use of cloud computing services within the public sector needs to be seen to in the light of EU legal requirements pertaining to security of network and information systems[39] as well as those pertaining to the **Data Protection Regulation (EU) 2016/679** and other Directives.

***iv. Consolidate support to the private sector on cyber security***

**Measure 4 (i)** outlines how cyber security can be facilitated in the private sector. Apart from potential public sector driven incentives, private sector participation in awareness and advice programmes as well as cyber related exercises to specific sectors may additionally help.

For example, ways may potentially be sought with business service providers (e.g. lawyers, insurers) of how they can potentially develop services to incentivise and help businesses manage and reduce risks[40].

## 5. Goal: *Cyber security Awareness and Education*

***i. Encourage cyber security education and training***

A chain is only as strong as its weakest link. Unfortunately, within the realm of cyber security, weakest link could, more often than not, be traced to the human factor. The behavioural and educational aspect of cyber security cannot thus be discounted. It is therefore of tantamount importance to ensure a rigorous and ongoing educational and training exercise that targets both the current workforce as well as the younger student generation

This measure thus primarily entials:

- Further recognition of the need for cyber security skills and competencies
- Academic and training programmes designed to consolidate cyber security expertise
- The review of existing curricula that focusses on cyber security along with ICT and media competencies.

**Action 60 - Building national capacity in specialist skill sets** - of **Digital Malta** states Government's commitment, through educational institutions and industry to support the creation of specialist educational pathways, addressing labour market requirements and to develop the curriculum and provide technical materials. Cyber security expertise also needs to be seen within the context of such initiative. Specialist cyber-security related education and training is to be actively considered in areas such as those related to cybercrime[41].

Cyber security related training and certification programmes are to be further encouraged, as an opportunity to effectively increase security level[42] of organisations and maintaining such increased level of security in the long term. Prior and post assessment of such programmes may serve as one way of ensuring their effectiveness.

However, consideration should also be taken that such programmes may not necessarily focus only on traditional modes of education but also on experimentation of innovative ways of their conduct[43].

From a younger generation perspective, **Action 2 - Empowering the young through a safer Internet** - of **Digital Malta** states that "Digital Citizenship will become part of the National Education Curriculum, to equip children and youths with the abilities to interact and use the Internet safely and intelligently. Parents and carers will be involved together with educators and youth workers. This action will stimulate the production of creative online content, empower the younger generation and help create a safer environment. With the support of competent authorities this measure will help combat cyber child abuse and exploitation".

Within the current cyber security scenario, there appear to be related awareness campaigns, as well as curricular–related plans and developments in schools.

The imparting of cyber security awareness in schools in particular calls for its sustainability in the long term, also keeping in view of related European Union direction to Member States with respect to teaching online safety in schools[44]. It also calls for consideration of a holistic perspective in the process, such as through:

- A focus on basic cyber hygiene[45] and protection of personal data
- A sound understanding by students of the concepts behind Information and Communication technologies being used and their potential vulnerabilities and risks, apart from the opportunities that they offer[46]. This includes the proper handling and use of the technologies being applied for interaction
- Ensuring cyber related training for all teachers
- Ensuring effective engagement, participation and support of all school management on cyber security education and awareness
- Seeking further ways to enage parents/ guardians of students in learning on cyber security related matters

*"It is highly recommended that a concerted, ongoing strategic approach is undertaken, potentially through a nationwide Communications strategy for cyber security; aimed at addressing the various strata of society, business and public sector along with their corresponding needs, expectations, and potential ICTs and concepts applied"*

- Ensuring the necessary legal safeguards to protect both the student as well as the teaching profession on cyber related challenges such as cyber bullying.

Curricular developments and academic programmes aimed at establishing a cyber security focus[47] is to be further encouraged, seeking further creative ways of instilling such education[48] in the process.

***ii. Explore possibility of establishing a Cyber Centre of Excellence***

The establishment of a cyber centre of excellence may serve as:

- A form of implementation of Action 60 – Building national capacity in specialist skill sets of Digital Malta , refered to in the previous measure
- A training base for cyber security expertise.
- Having a maintained comprehensive list of professionals certified under internationally recognised certification programs in cyber security[49]
- A source of promotion of related best practice
- A means of proposing legislative or regulatory updates, based on relevant research or lessons learnt
- A potential agent for future economic growth in Malta within the cyber security domain
- A complementary mechanism to a collective approach for sharing cyber security knowledge and intelligence, proposed as **Measure 3 (i)**.

The establishment could potentially be enabled through:

- Agreement of overseas cooperation on related matters
- Related EU supporting initiatives
- Inclusion of existing internationally certified local expertise in cyber security.

***iii. Ensure relevant education and training to public sector staff and other stakeholders[50]***

Training and education on cyber security is one key priority within the public sector, especially given the sector's wider extensive use of ICT and sensitive data, compared to other sectors. In any office environment it needs to be kept in view, that technology controls are not sufficient to protect data from related cyber security threats. The controls need to go hand in hand with human resource, awareness and employee guidance programs[51].

The development of cyber security expertise within the public sector is another key area that merits particular attention. In the process, it also needs to be ensured that a comprehensive list of public sector professionals certified under internationally recognised certification programs in cyber security is established and maintained[52]. Furthermore, it needs to be ensured that ICT personnel are trained so as to enable them to recognise cyber incidents, to detect anomalies in their ICT systems and to respond and to report them accordingly.

***iv. Foster application of research and development on cyber security***

Such measure aims to ensure cyber security as among key research priorities. It effectively calls for encouragement and support for research in any

national and EU research projects and initiatives on cyber security. Essentially, it entails participation not only from Government but also from the private sector and the academia.

***v. A Strategic, target-oriented national awareness and advice campaign***

It is highly recommended that a concerted, ongoing strategic approach is undertaken, potentially through a nationwide Communications strategy for cyber security[53]; aimed at addressing the various strata of society, business and public sector along with their corresponding needs, expectations, and potential ICTs and concepts applied[54].

Such an approach may ensure:

- Avoiding piecemeal, potentially one-off approaches to awareness campaigns
- No duplication of effort
- Maximisation of cyber security related financial and human resources
- Identification and engagement of all potential sources of dissemination of the awareness campaigns
- Imparting effective awareness and knowledge on cyber security patterns and measures that is commensurate to the specific target audience and to the medium used[55]
- A measure of the extent of national awareness and understanding of cyber security over time
- That cyber security is not simply a concern of ICT professionals.

Ultimately, the key factors that need to be borne in mind in the establishment of such campaign is:

- Finding the right way to raise awareness, keeping in view of the target audience
- Ensuring motivation to learn and pay particular attention to various signals of fake communications on a day to day basis (particularly to counter social engineering threats)
- Ingraining a culture of cyber security awareness on the potential misuse, vulnerabilities and risks potentially arising from the ICTs and concepts applied (particularly those emerging); whilst embracing the opportunities arising from their use
- Imparting the key message that it is ultimately in everyone's interest and responsibility to take the necessary relevant cyber security safeguards; keeping in view of the inherent inter-connectedness of individuals and organisations alike in cyber-space.

Most measures highlighted within **Goals 4** and **5** of this strategy as well as any established national way of sharing related knowledge, experience and insight as referred to in **Measure 3 (i)**[56] may potentially serve as key sources for the establishment and maintenance of such a concerted strategic campaign.

***vi. Encourage 'cyber hygiene' and personal responsibility***

Ultimately, citizens are expected to apply at least some form of basic 'cyber hygiene' in using ICT, such as through careful disposition and use of personal information on-line, installing software updates and anti-virus software, using basic security controls such as strong passwords and, as much as possible, seeking to be more wary of any suspicious activity related to their personal on-line accounts. The national awareness campaign, as highlighted in **Measure 5 (v)**, should help in reaching this objective.

Furthermore, the possibility of a national *responsible disclosure policy* framework that enables well-intentioned system users to safely inform Government, businesses or institutions about detected vulnerabilities in their ICT systems or services may also be explored. The framework would need to establish the right parameters and conditions so as to ensure its effectiveness[57].

## 6. Goal: *National and International Cooperation*

***i. Effective cooperation and collaboration on cyber security on a national, European and global basis***

On a national level, most of the measures highlighted earlier essentially call for national cooperation and coordination.

Malta is no island in cyberspace. Hence, cooperation and collaboration on cyber security needs to be sustained both locally as well as on a European and on a global level. A co-ordinated approach, among all local key stakeholders in cyber security interacting locally and overseas needs to be ensured so as to ensure synergy of national and international effort, knowledge and expertise within the domain.

Thus, active consideration needs to be given to:

- Cyber related activities, such as those conducted by the European Network and Information Security Agency (ENISA), which may potentially involve both local public as well as private sector organisations
- EU legal requirements such as those pertaining to network and information security[58] which, among others, calls for a body responsible for coordinating NIS issues and for acting as a single point of contact for cross-border cooperation and communication at EU level, within each Member State
- Activities such as those undertaken by the Council of the European Union on cyber-diplomacy[59] which aim to foster increased global cyber capacity building, as well as international cooperation and judicial capacity on cybercrime
- Confidence Building Measures (CBMS) proposed by the Permanent Council of the Organisation for Security and Cooperation in Europe (OSCE) which propose, among others, measures of mutual communication, dialogue and collaboration on the security and use of Information and Communication Technologies within and across OSCE participating states of the related Permanent Council Decision[60]
- Any other cyber security related initiatives on a European Union and/or on a wider international context.

*“ Ultimately, it needs to be borne in mind that mutual cooperation, openness and understanding is the success to effective cyber security ”*

Ultimately, it needs to be borne in mind that mutual cooperation, openness and understanding is the success to effective cyber security[61].

# 10. CONCLUSION

### 10.1 The Cyber Security Strategy Model Revisited

As indicated in Figure 2, the National Cyber Security Strategy, through its goals and subsequent measures, shall be covering areas of governance, legislation, regulation and voluntary commitment, risk management and education and awareness – all of which position cyber security on a sustainable, long term path.

| | | Policy | Legislation | Risk Management | Culture | Education |
|---|---|---|---|---|---|---|
| | | Devising national cyber security policy and strategy that addresses the needs of the various stakeholders. | Creating effective legal and regulatory frameworks to support all aspects of the strategy. | Controlling risks through organisation, standards and technology. | Fostering awareness to encourage a responsible cyber culture throughout society. | Building cyber skills into the workforce and leadership through effective education. |
| GOAL | MEASURE | | | | | |
| Establish a governance framework | 1(i) Establish the necessary key coordinating structures | | | | | |
| | 1(ii) Foster the coordination to protect national critical information infrastructure | | | | | |
| | 1(iii) Ensure clear delineation and communication of roles and responsibilities | | | | | |
| | 1(iv) Ensure the conduct of a national cyber risk assessment exercise | | | | | |

| | | Policy | Legislation | Risk Management | Culture | Education |
|---|---|---|---|---|---|---|
| | | Devising national cyber security policy and strategy that addresses the needs of the various stakeholders. | Creating effective legal and regulatory frameworks to support all aspects of the strategy. | Controlling risks through organisation, standards and technology. | Fostering awareness to encourage a responsible cyber culture throughout society. | Building cyber skills into the workforce and leadership through effective education. |
| GOAL | MEASURE | | | | | |
| Establish a governance framework | 1(v) Ensure necessary measures in line with individual cyber risk assessments by key Public and Private sector orgnaisations falling within the scope of related EU legal requirements | | | | | |
| | 1(vi) Encourage cyber risk assessments by other organisations not falling within the scope of Measure 1.5 | | | | | |
| | 1(vii) Consolidate the IS Framework within the public sector | | | | | |
| | 1(viii) Ensure classification of data within the Public Sector and encourage it within the private sector | | | | | |
| Combat cybercrime | 2(i) Establish Forum for Internet safety and protection of minors | | | | | |
| | 2(ii) Identify gaps and strengthen capability to investigate and combat cybercrime | | | | | |
| | 2(iii) Assess and consolidate on-line mechanism to report cybercrime | | | | | |

| | | Policy | Legislation | Risk Management | Culture | Education |
|---|---|---|---|---|---|---|
| | | Devising national cyber security policy and strategy that addresses the needs of the various stakeholders. | Creating effective legal and regulatory frameworks to support all aspects of the strategy. | Controlling risks through organisation, standards and technology. | Fostering awareness to encourage a responsible cyber culture throughout society. | Building cyber skills into the workforce and leadership through effective education. |
| GOAL | MEASURE | | | | | |
| Strengthen national cyber defence | 3(i) Establish a collective approach for sharing cyber security knowledge and intelligence | ■ | | | ■ | |
| | 3(ii) Review existing legislation and provide measures through legislation and regulation to ensure relevance and effectiveness to the cyber world | | ■ | | | |
| | 3(iii) Ensure the country's digital resilience to cyber attack as well as the capability to protect its interests | ■ | | | | |
| | 3(iv) Conduct cyber defence exercises | ■ | | | | |
| Secure cyber-space | 4(i) Establish regulation and voluntary self commitment for guaranteeing cyber security | | | ■ | ■ | ■ |
| | 4(ii) Stimulate use of interoperable and secure standards on the basis of good practice | | | ■ | ■ | ■ |
| | 4(iii) Promote robust levels of cyber security in online public services | | | ■ | ■ | |
| | 4(iv) Consolidate support to the private sector on cyber security | | | ■ | ■ | |
| Cyber Security Awareness and Education | 5(i) Encourage cyber security education and training | | | | ■ | ■ |

| | | Policy | Legislation | Risk Management | Culture | Education |
|---|---|---|---|---|---|---|
| | | Devising national cyber security policy and strategy that addresses the needs of the various stakeholders. | Creating effective legal and regulatory frameworks to support all aspects of the strategy. | Controlling risks through organisation, standards and technology. | Fostering awareness to encourage a responsible cyber culture throughout society. | Building cyber skills into the workforce and leadership through effective education. |
| GOAL | MEASURE | | | | | |
| Cyber Security Awareness and Education | 5(ii) Explore possibility of a Cyber Centre of Excellence | | | | | |
| | 5(iii) Ensure relevant education and training to public sector staff and other stakeholders | | | | | |
| | 5(iv) Foster application of research and development on cyber security | | | | | |
| | 5(v) A strategic, target-oriented national awareness and advice campaign | | | | | |
| | 5(vi) Encourage 'cyber hygiene' and personal responsibility | | | | | |
| National and International cooperation | 6(i) Effective cooperation and collaboration on cyber security on a national, European and global basis | | | | | |

**Figure 2 – Detailed proposed strategy through the Cyber Security Strategy Model**

### 10.2 The Way Forward

The launch of the National Cyber Security Strategy is not an end in itself. It is the beginning of a continuum, starting with implementation that is in line with:

- Increased awareness and recognition on a national scale of the importance to tackle cyber security in a comprehensive and systemic manner
- Related ICT, legislative, regulatory, social and economic updates on a national scenario
- Rapid developments within the cyber threat landcape.

The implementation of the Strategy is expected to involve multiple stakeholders within the public and the private sector as well as cooperation and coordination with civil society. It is expected to be evaluated on a periodic basis, based upon the progress registered from such implementation, along with related directional developments on a national and European Union front. The evaluation is expected to lead to maintenance and updates of the Strategy, leading to a subsequent new version, reflecting the maturity undertaken in cyber security on a national scale since its initial launch.

# REFERENCES


BSA| The Software Alliance (www.bsa.org), *European Union Cybersecurity Maturity Dashboard (2015) A Path to a Secure European Cyberspace*

Council of the European Union (7 October 2015), *EU Cyber Security Strategy: Roadmap Development, Brussels*

Council of the European Union (11 February 2015), *Council Conclusions on Cyber Diplomacy*, Outcome of Proceedings, Brussels, 6122/15

Council of the European Union (12 March 2015), *Global Conference on Cyberspace 2015*, The Hague Natherlands, 6181/3/5/15 REV 3

Council of the European Union (28 May 2015), *Non-Paper on Fostering Cyber Security and Cyber Defence in Europe by means of Responsible Disclosure Polices*, Meeting Document, Brussels, DS 1340/15

Council of the European Union (18 December 2015), *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, Examination of the final compromise text in view to agreement, Brussels 15229/2/15 REV 2

Council of the European Union (May, 2016), *Improving cyber security across the EU*, http//www.consilium.europa.eu/en/policies/cyber-security [Accessed on 23/5/2016]

Cyber Security Raad (CSR) Nederland (2016) *Cyber Security Council (CSR) Magazine 2016*, Year 2, No. 2, January 2016, Special EU Edition

Digital Malta, *National Digital Strategy 2014-2020 – Programme of Initiatives 2014*, www.digitalmalta.gov.mt

Dutton, J.(June 2015), *Ten essential cyber security questions to ask your CISO*, http://www.itgovernance.co.uk/blog/ten-essential-cyber-security-questions-to-ask-your-ciso/?utm_source=Email&utm_medium=Macro&utm_campaign=S01&utm_content=2015-06-22

European Commission (May 2012), *European Strategy for a Better Internet for Children*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels 2.2.2013, COM (2012) 196 final.

European Commission, *Implementation of the Digital Agenda for Europe*, http://daeimplementation.eu/member_states.php?id_pillar=45&id_country=18.

European Commission (July 2012), Special Eurobarometer 390 – Cybersecurity http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pd

European Commission (November 2013), *Special Eurobarometer 404 – Cybersecurity* http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

European Commission (November 2013), *Special Eurobarometer 423 – Cybersecurity*, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

European Commission (2013), *Cyber security Strategy of the European Union, An Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013 JOIN(2013) 1 final, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

European Commission (28 January 2015) *Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market*, Press Release, http://europa.eu/rapid/press_release_MEMO-15-3802_en.htm

European Commission (April 2015), *Connecting Europe Facility,Digital Service Infrastructures (DSI)* Maturity Study, Deloitte for the European Commission, DG Communications Networks, Content and Technology

European Commission (28 April 2015), *European Agenda on Security: Questions and Answers, Strasbourg, Fact Sheet*, http://europa.eu/rapid/press-release_MEMO-15-4867_en.htm

European Commission (6 May 2015), *A Digital Single Market Strategy for Europe, Communication* from the Commission to the European Parliament, The Council, The European Economic and Social Committee of the Regions, SWD(2015) 100 final, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

European Commission (28 July 2015), *eGovernment Benchmark Report 2015* – Malta, https://ec.europa.eu/digital-single-market/en/news/egovernment-benchmark-report-2015-malta

European Network and Information Security Agency (ENISA) (2015), *ENISA Threat Landscape 2014*, https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

European Network and Information Security Agency (ENISA) (2012), *National Cyber Security Strategies, Practical Guide on Development and Execution*, Heraklion, Greece, https://www.enisa.europa.eu

European Network and Information Security Agency (ENISA) (2012), *National Cyber Security Strategies*, https://www.enisa.europa.eu

# REFERENCES


Federal Chancellary of the Republic of Austria (2013), *Austrian Cyber Security Strategy*, Vienna, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AT_NCSS.pdf .

Global Cyber Security Capacity Centre, (2014), *Cyber Security Capability Maturity Model (CMM) - Pilot*, Oxford Martin School, University of Oxford, http://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/Cyber-Security-Capacity-Maturity-Model.pdf

International Telecommunications Union (ITU), *Cyber Wellness Profile Malta* http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Malta.pdf

Malta Communications Authority (MCA), *National eCommerce Strategy (2014 - 2020)*, https://www.mca.org.mt/general/national-ecommerce-strategy-2014-2020

Malta Information Technology Agency (MITA), *MITA Strategy 2015-2017, Version 1.0*, https://www.mita.gov.mt

National Coordinator for Security and Counterterrorism - The Netherlands (2013), *National Cyber Security 2 – From Awareness to Capability*, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

Parliamentary Secretariat for Competitiveness and Economic Growth, Malta Communications Authority (MCA), eCommerce Malta, National Strategy 2014-2020, www.mca.org.mt

Parliamentary Secretariat for Competitiveness and Economic Growth, Malta Information Technology Agency (MITA), Malta Communications Authority (MCA), *Digital Malta, National Digital Strategy 2014-2020*, www.digitalmalta.gov.mt

Puricelli, R.(2015), *The Underestimated Social Engineering Threat in IT Security Governance and Management*, ISACA Journal, 3,24-28

Ross, S.J. (2015), *Frameworks of the World Unite*, ISACA Journal, 3,4-6

White and Case (2015) *EU-wide cybersecurity rules nearing final agreement*, Client Alert, London, UK

van't Hof, C (2016), *Helpful Hackers: How the Dutch do Responsible Disclosure*, Tek Tok Uitgeverij

# ENDNOTES

1. Particular reference is made to the:
   - **Directive 95/46/EC and the Data Protection Act (Chapter 440) of the Laws of Malta**, – Both Directives shall be repealed by the Data Protection Regulation (EU) 2016/679, which shall come into force by June 2018.
   - **Network and Information Security - NIS Directive (i.e. The Directive of the European Parliament and of he Council concerning measures for a high common level of security of network and information systems across the Union)** which is expected to enter into force in August 2016 for transposition into local legislation within 21 months.
2. https://www.mca.org.mt/general/national-ecommerce-strategy-2014-2020
3. Adapted from the definition cited by the *Cyber security Strategy of the European Union*.
4. Ross(2015)
5. Puricelli (2015)
6. Global Cyber Security Capacity Centre, (2014), Cyber Security Capability Maturity Model (CMM)- Pilot, Oxford Martin School, University of Oxford, http://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/Cyber-Security-Capacity-Maturity-Model.pdf
7. Refer to Note 1.
8. Ibid.
9. Taking into particular consideration of the Network and Information Security (NIS) Directive. Reference is made to Note 1.
10. A top level national CSIRT that acts as the key technical/operational function. Among the responsibilities of such CSIRT are:
    - Monitoring incidents at a national level
    - Providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents
    - Providing dynamic risk and incident analysis and situational awareness
    - Establish cooperative relationships with the private sector
    - Facilitate cooperation through use of common or standardised practices for incident and risk handling procedures
11. European Commission (2015), DSI Maturity Study, p.29
12. Which could take the form of (i) a centralised approach – whereby a national authority has in-house responsibilities with all authorities reporting to it; OR (ii) a decentralised approach whereby roles and responsibilities are spread across a variety of actors who coordinate together to share information and exchange on a voluntary basis OR (iii) a semi-centralised (hybrid) approach whereby a central ministry coordinates implementation of the strategy with designated authorities having the necessary roles and responsibilities over operators and other stakeholders and who report to the central ministry on a periodic basis.
13. Reference is made to Note 1.
14. Refers to Critical Information Infrastructure (CII) operators
15. One of which specifically includes the Network and Information Security – NIS – Directive, referred to in Note 1.
16. Refers to CII operators, Critical Infrastructure (CI) operators, Digital service providers and other potential stakeholders
17. Potentially enabled by National cyber simulation exercises as referred to in Measure 3.1
18. Reference is particularly made to the NIS Directive, referred to in Note 1.
19. European Agenda on Security: Questions and Answers, Strasbourg, 28 April 2015 - European Commission-Fact Sheet.
20. European Commission, Countering hybrid threats: EU Response – Cybersecurity, Presentation, Brussels, 19th February 2016
21. One example of such an arrangement is the Cyber-security Information sharing Partnership, part of CERT-UK; www.cert.gov.uk cisp/
22. Organisation for Security and Cooperation in Euroope (OSCE), Decision No. 102, OSCE Confidence Building Measures to reduce the risks of conflict stemming from the use of ICTs, PCOEW6464, 10 March 2016, Confidence Buidling Measure No. 14. This CBM refers to best practices of responses to common security challenges stemming from the use of ICTs.
23. Areas that could potentially be looked into may include risk assessment and apportioning security practices to risk levels, information security planning, processes, roles and assesments of preparedness.
24. Reference is made in particular to Note 1.
25. Article 2(4) of the UN states that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nation". This Article prohibits any state from attacking another state however in Article 51 of the same charter states that "Nothing in the present Charter shall impair the inherent right of individual or collective self defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."
26. Reference is made to 'Developing a Joint EU diplomatic response against coercive cyber operations', Council of the European

# ENDNOTES

Union, Brussels , 24 February 2016 (Doc 5797/2/16)

27. Reference is made to 'Report of the Expert-level consultation meeting with member states on countering hybrid threats held on 19 February 2016' Permanent Representation of Malta to the European Union.
28. Refers to CII operators, CI operators, Digital Service providers and other potential stakeholders
29. The preparation for the GDPR calls for a review and assessment of number of organisational, procedural, communication steps that need to be undertaken to ensure conformance.
30. The latter aim may serve as good business opportunity, especially for export-oriented sectors, to strenghten their market share overseas.
31. For example Austria and the UK
32. One of the action items of the EU Cyber Security Strategy specifically calls for work on further development of globally interoperable standards and their promotion for their wider use by industry. Reference is made to EU Cyber Security Strategy: Roadmap Development – Council of the EU, Brussels, 7/10/2015.
33. This may imply, amongst others, the improvement of interoperability of national and international systems. Reference is made to measure 5 as part of law enforcement legislation and policy related implementation of the Information Management Strategy (Working Party on Information Exchange and Data Protection – Council of the EU)
34. Public consultation preliminary results on information and communication technologies published by the European Commission in early 2016, reveals cyber security as being one of the areas requiring common standards if completion of a single digital market is to be achieved.
35. Such as ISO 27001
36. Reference is made to Measure 1.7
37. Such as the UK's Cyber Essentials Scheme, http://www.itgovernance.co.uk/cyber-essentials-scheme.aspx#.VaYNvLlBut8
38. The overall confidence to use the Internet for online services (e.g. banking, public services) has decreased from 74% in 2012 to 73% to 2013 across the EU. A proportional increase is noted in 2014 in the level of concern expressed by EU respondents in having access to online services, through the Internet, as a result of cyber attacks. In Malta's case, the findings indicate an increase from 44% in 2013 to 61% in 2014. This could be potentially attributed to an increase in the proportion of the Maltese respondents, from 7% in 2013 to 10% in 2014 who complain of related incidents.
39. Reference is particularly made to the NIS Directive, referred to in Note 1.
40. Potential areas that can be seen to also relate to cyber insurance, due diligence to third party with which businesses may seek strategic relationships,etc
41. Including in roles such as those pertaing to law enforcement, prosecution services, the judiciary.
42. Including educating staff to understand what is harmful to an organisation and what can be done to prevent mistakes which may lead to data breaches.
43. For example apart from use of visual methods, rewards, social engagement and direct feedback during everyday working life; gamification may present one promising method. (Purcelli, op. cit, p.27). Other possiblities include cybercrime simulation workshops as another complementary means to induce awareness on the various forms of cybercrime, who is the likely target, what needs to be done to avoid falling a victim, and what action needs to be taken and to whom to refer to, in case of fallling a victim.
44. Reference is made to the European Strategy for a Better Internet for Children - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels 2.2.2013, COM (2012) 196 final.
45. Such as effective password management
46. The increased focus on environmental concerns and measures within schools in recent years may serve as a potential model for a heightened awareness on cyber security and safety concerns and measures amongst the younger generation, which may in turn expand further within their home environments.
47. With special reference to secondary and tertiary level education
48. Such as through special events, apart from teaching through games, particularly to the younger generation. Estonia for example organises 'Cyber olympics' and specialised summer schools
49. A measure that is particularly required within the public sector as a domain having a wider extensive use of ICT and sensitive data, relative to other sectors
50. In particular, CII operators, CI operators, Digital Service providers and other potential stakeholders
51. Puricelli, op.cit. This may be complemented by related policies, best practices and processes (including those on proper data handling) applied within the context itself.
52. So as to augment and enhance needed cyber security knowledge and expertise within the sector
53. A similar approach has been taken by the Netherlands and Austria

# ENDNOTES

54. For example, it may be appropriate to focus, among others, on cyber security related concerns and measures that may be taken in the applicability of cloud computing or mobile computing within office environments.
55. For example social media, TV, radio, etc
56. Apart from regular Euro barometer surveys dealing with cyber security which provide a significant insight on cyber security experiences and concerns on a domestic level.
57. Such policy is currently mainly applied by a number of organisations – European and worldwide, and also by some EU member states such as the Netherlands. Such framework could be enabled through self-regulation, promotion and encouragement by government as well as the proper framework to ensure responsible vulnerability disclosure.
58. Reference is made to the Network and Information Security - NIS - Directive
59. Reference is made to the Council Conclusions on Cyber Diplomacy (2015) and to the Global Conference on Cyberspace (2015)
60. Permanent Council Decision No. 1039 (26 April 2012) , whereby OSCE participating States, "decided to step up individual and collective efforts to address security of and in the use of ICTs in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and cooperation with relevant international organisations...". This led to the adoption of a number of Confidence Building Measures (CBMs) through Permanent Council Decision 1106 on December 3, 2013, followed by additional, complementary CBMs adopted through Permanent Council Decision No. 1202 on March 10, 2016.
61. It needs to be seen within a 'win-win' perspective including in those areas where business related competition plays a key role.

mita.gov.mt/ncss