

# Malta Country Report



## About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

## Contact details

For contacting ENISA or for general enquiries on the Country Reports:

### Mr. Giorgos Dimitriou

ENISA External Relations Expert

[Giorgos.Dimitriou@enisa.europa.eu](mailto:Giorgos.Dimitriou@enisa.europa.eu)

Internet: <http://www.enisa.europa.eu>



## Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Vincent Bouckaert, Dan Cimpean, Johan Meire and Nicolas Roosens.**

## Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA) 2011

## Table of Contents

<b>MALTA.....</b>	<b>4</b>
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS .....	4
<b>NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES .....</b>	<b>5</b>
OVERVIEW OF THE NIS NATIONAL STRATEGY .....	5
THE REGULATORY FRAMEWORK .....	8
<b>NIS GOVERNANCE .....</b>	<b>12</b>
OVERVIEW OF THE KEY STAKEHOLDERS.....	12
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS.....	13
FOSTERING A PROACTIVE NIS COMMUNITY .....	14
<b>COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....</b>	<b>15</b>
SECURITY INCIDENT MANAGEMENT .....	15
EMERGING NIS RISKS .....	16
RESILIENCE ASPECTS .....	16
PRIVACY AND TRUST.....	17
NIS AWARENESS AT THE COUNTRY LEVEL .....	18
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY.....	19
<b>RELEVANT STATISTICS FOR THE COUNTRY .....</b>	<b>21</b>
INTERNET ACCESS OF POPULATION AND ENTERPRISES .....	21
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS.....	22
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS .....	23
OTHER STATISTICS.....	23
<b>APPENDIX.....</b>	<b>24</b>
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES .....	24
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs) .....	25
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	26
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES .....	26
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	27
REFERENCES .....	28

## Malta

### The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader on the following Network and Information Security (NIS) related topics:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
  - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
  - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
  - *Security incident management*
  - *Emerging NIS risks*
  - *Resilience aspects*
  - *Privacy and trust*
  - *NIS awareness at the country level*
  - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

## NIS national strategy, regulatory framework and key policy measures

### Overview of the NIS national strategy

Malta has an agency responsible for the implementation of the National Strategy for Information Technology: the Malta Information Technology Agency (MITA).

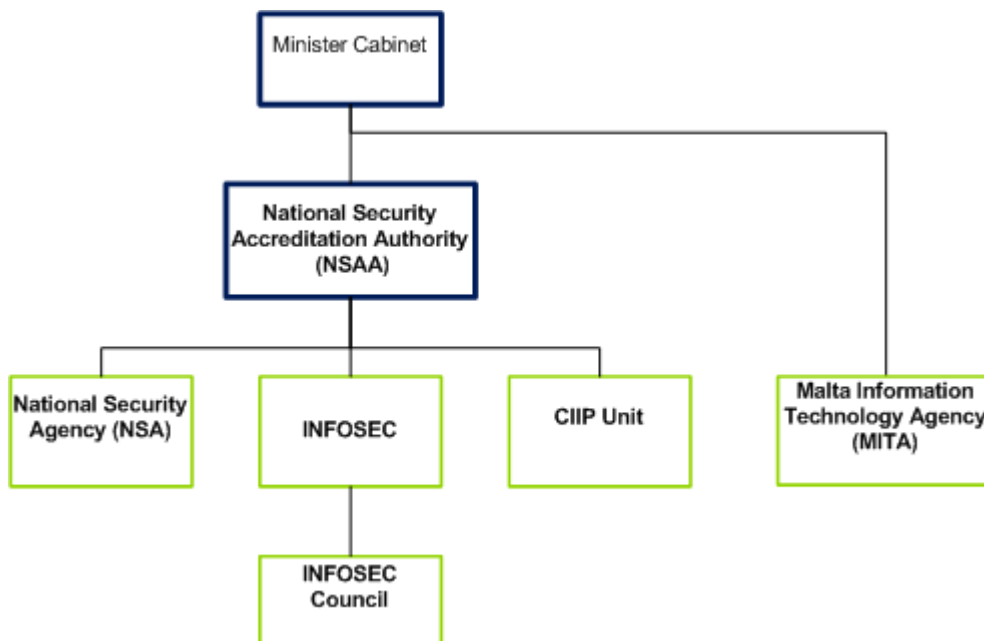
In 2010, this agency had some of its roles transferred to two new agencies:

- INFOSEC, which is responsible for information security for the government, and has the task of defining the national direction for security;
- The Critical Information Infrastructure Protection (CIIP) Unit, which will be responsible for critical infrastructure protection as well as coordinate all the stakeholders involved in critical information infrastructure issues. The aim of the CIIP Unit is to create a protection plan on a national level. It also has the task of encouraging actors from the private sector (ISPs, banks, etc.) to form their own CERT teams. From that point on, the CIIP Unit will start a forum involving those private sector CERT teams.

A new information security organisation was also created, the National Security Accreditation Authority (NSAA). This entity is now the overall security authority, under supervision of the prime minister's cabinet.

Also, the National Security Agency (NSA) was created and is now responsible for security in general, physical security issues and EU information matters.

Additionally, the INFOSEC Council was created in order to bring all the government entities together for discussing INFOSEC and CIIP issues. See below for an organisational chart of these different entities:



Also, the Malta Communication Authority (MCA) assumes responsibility for the implementation of the projects and initiatives to improve the external infrastructure of ICT, to end the digital divide and to promote eCommerce.

### **National Strategy for Information Technology 2008-2010**

As stated in the previous issue of this report, Malta launched a National Strategy for Information Technology in 2007. This ICT strategy was to proactively address several major challenges, including:

- The need to be proactive in identifying and addressing the new digital divides which will emerge in the coming years;
- The successful application of various technologies in the enhancement of the quality of life;
- The constantly moving target of becoming (and remaining) a leading ICT industry in the region.

Within the context of these five parameters, the Smart Island strategy is a complex web of intertwined initiatives constructed through a simple traditional 'hub-and-spoke' model, with the vision serving as the hub and seven inter-related strategic streams as spokes. The seven strategic streams are the following:

- Stream 1: Robust ICT Environment and next generation infrastructure
- Stream 2: A connected society – bridging the last and the new miles
- Stream 3: Develop human potential into a smart workforce
- Stream 4: "e for everything" – enhancing our citizens' quality of life through ICTs
- Stream 5: Re-inventing Government – transformation and open Government
- Stream 6 :Taking Care of eBusiness
- Stream 7: Developing a world-leading ICT industry

The Smart Island strategy is a cornerstone of Government's 2015 vision of transforming Malta into a regional ICT services hub alongside healthcare, education, financial services, logistics and maritime services.

### **Strategic NIS-related measures under the Stream 1: Robust ICT Environment and next generation infrastructure**

As stated in last year's ENISA country report, a set of 19 strategic measures and targets<sup>1</sup>, defined by the MITC and containing very relevant NI elements, were to be met in 2010. See below:

<p><b>Strategic Measure 1:</b> <b>Review the current eLegislation and transform it into a next generation e-legislative framework.</b></p>	<ul style="list-style-type: none"> <li>• Create an information society law bringing together all aspects of mobile and e-authentication, e-identification, e-commerce, biometrics, e-accessibility, electronic signing and electronic voting.</li> <li>• Expand the focus on cyber-crime in the Criminal Code making sure that it is appropriate for the fight against cyber-criminals.</li> <li>• Strengthen our data protection legislation to enhance the safeguards of data subjects and facilitate the use of data across information systems.</li> </ul>
<p><b>Strategic Measure 7:</b> <b>Establish a Regional Information Security Centre in Malta.</b></p>	<ul style="list-style-type: none"> <li>• Develop a physical hub for information security facilities aimed to house not only the local public and private sensitive infrastructure but also to serve as an international reputable hub for information security services.</li> </ul>
<p><b>Strategic Measure 9:</b> <b>Establish a National Information Security</b></p>	<ul style="list-style-type: none"> <li>• A principal measure of the Strategy and responsibility of the Agency shall be the development of a Framework of inter-related programs and initiatives (together with the respective benchmarking standards) aimed at establishing national information security baselines, the protection of</li> </ul>

<sup>1</sup> See the details available at: <https://mitc.gov.mt/page.aspx?pageid=262>

<b>Framework.</b>	critical components, the assurance of business continuity of public and private critical systems and national disaster recovery services.
<b>Strategic Measure 10: Keeping kids safe.</b>	<ul style="list-style-type: none"> <li>• In full partnership with the Commissioner of Children sustain the alliance with all the public and non-governmental stakeholders involved, to develop an innovative awareness, educational and prevention program to protect children from physical, psychological or moral abuse over the Internet or any other electronic channel.</li> </ul>
<b>Strategic Measure 11: Introducing School Safety Packages.</b>	<ul style="list-style-type: none"> <li>• Government and its public-private partners shall develop a series of School Safety Packages aimed at educating and equipping children, teachers and parents with the technologies they need to protect their online environment.</li> </ul>
<b>Strategic Measure 12: Strengthening fight against cyber-crime.</b>	<ul style="list-style-type: none"> <li>• Building on the capabilities of the cyber-crime unit of the Malta Police Force to mobilise a strong response to the threats posed by the activities of cyber-criminals by:           <ul style="list-style-type: none"> <li>◦ Strengthening the same cyber-crime unit with the objective of establishing it as a competence centre.</li> <li>◦ Ensuring that the cyber-crime legislation is adequate and enables law enforcers to apprehend and prosecute perpetrators effectively.</li> <li>◦ Establishing more innovative measures through which citizens can alert authorities on cyber-criminal activity, they come across.</li> </ul> </li> </ul>

### eGovernment elements of the national strategy

As stated in last year's Malta country report published by ENISA, several elements of the Malta **eGovernment** national strategy<sup>2</sup> (under the Stream 5: Re-inventing Government – transformation and open Government) also include a series of interesting NIS elements.

The Malta Information Technology Agency is responsible for the implementation of the strategic stream "Reinventing Government" and has developed the agency's related 2009-2012 strategy on the following objectives:

- Design, develop and operate a state-of-the-art next-generation eGovernment platform
- Retrofit all current eGovernment services into the new eGovernment platform to enhance the consolidation effect of having a single point of contact for citizens' access to online public services.
- Develop a secure, scalable and open technological layer to enable trusted third parties to integrate their electronic services with the facilities offered by the next generation eGovernment platform.
- Establish a Government-to-Business (G2B) variant of the eGovernment platform
- Develop and deploy an eProcurement system
- Develop a policy framework and implement a mechanism to enrol and enable trusted third party individuals and organisations to serve as 'Agents' for the delivery of over-the-counter public services through the use of the agent-enabling capability eGovernment platform.

Most of these objectives were met in 2010, with Malta being reported as the best performing country in terms of eGovernment, by achieving 100% in five of six core indicators. This effectively established Malta as the European leader in eGovernment<sup>3</sup>.

<sup>2</sup> Source: <http://www.epractice.eu/files/eGovernment%20in%20MT%20September%202009.pdf>

<sup>3</sup> Source: <https://www.mita.gov.mt/news.aspx?nid=173&catid=8>

## SmartCity Malta

SmartCity Malta heralds the transformation of the country's economy to one powered first and foremost by knowledge. It forges a premier ICT and media park, showcasing Malta to the world as the region's new destination for high-tech industries. In doing so, it is expected to generate a minimum of 5,600 jobs in these fields and to spur development across many sectors of the nation's economy<sup>4</sup>.

## The regulatory framework

The following Maltese national regulations have relevance and applicability in the domain of network and information security:

### Data Protection/Privacy Legislation

#### *Data Protection Act*<sup>5</sup>

The Malta Data Protection Act was passed on 14 December 2001 and came into force in July 2003. It was introduced in order to render Maltese law compatible with EU Data Protection Directive (95/46/EC), even though Malta had not yet been an EU Member State at that time.

It outlines nine principles of 'good information handling' to guarantee the protection of personal information. Data collectors, such as educational institutions, employers and banks, are obliged to inform individuals of the reasons for collecting information about them. Furthermore, individuals are to be assured that the data collected will not be used for any other reason than that specified by the data collector. The act also contains accuracy requirements and specifies that 'explicit' consent from individuals is necessary in order to process 'sensitive personal data'.

The Office of the Commissioner for Data Protection (i.e. the "Office") is responsible for supervising the enforcement of the Data Protection Act, thus ensuring the respect of the individuals' right to privacy with regard to personal information. Data subjects, who hold that their personal data are being abused, may refer the case to the Office of the Commissioner for Data Protection. See also the Privacy & Trust section of this country report.

### Cybercrime

#### *Computer Crimes Involving Electronic Data covered by the Electronic Commerce Act III of 2001 (the eCommerce Act)*

The eCommerce Act<sup>6</sup> also typifies as criminal some acts that violate data security or computer misuse. For instance, those who without authorization use a computer or any other device to access data, software, or documentation held in a computer or in any other computer; or uses, copies, or modifies such data, software, or documents is guilty of an offense. Also, impair of the operation of a system or software also constitutes a computer crime under Malta's law.

Additionally, any person who outputs or copies any data, software, or supporting documentation from a computer in which it is held or stored, is guilty of a computer crime. Moreover, altering, taking, installing, moving, erasing, destroying, or adding to any data, software, or supporting document, without authorization, constitutes a computer crime. Disclosing or using another

<sup>4</sup> Source: <http://www.tvworldwide.com/events/malta/smartcity/videos.cfm>

<sup>5</sup> Source: <http://www.epractice.eu/en/document/288316>

<sup>6</sup> Source: [http://www.ibls.com/internet\\_law\\_news\\_portal\\_view.aspx?s=latestnews&id=2233](http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2233)

person's password or discovering a code or other access information without authorization constitutes computer misuse crime. The following are computer crimes when committed without proper authorization:

- Modifying computer equipment or supplies used or intended to be used in computer, computer system, or computer network;
- Taking possession of, damaging or destroying computer, computer system, computer network, or computer supplies used or intended to be used in computer, computer systems, or computer networks.

Any of these crimes are sanctioned under Malta law even if committed outside Malta, when they affect computers, computer software, data, or supporting documentation located in Malta or connected to a computer located in Malta.

#### *Criminal Code*

Several articles of the Malta Penal Code are of relevance in the NIS context, as they directly address the computer misuse and the unlawful access to, or use of, information.

#### **Secondary legislation on eCommunications**

MCA published the following secondary legislation on eCommunications relevant<sup>7</sup> to NIS in Malta (see below). Only the titles are included, as long as they are self-explanatory:

- Chapter 49.02: Wireless Installation on Ships Rules
- Chapter 49.04: Wireless Telegraphy (Certificates of Operators) Regulations
- Chapter 399.06: Electronic Communications Appeals Board (Jurisdiction) Regulations
- Chapter 399.07: Electronic Communications Appeals Board (Rules of Procedure) Regulations
- Chapter 399.09: Internet and other Data Networks (Service Providers) Regulations
- Chapter 399.10: Electronic Communications Services (General) Regulations
- Chapter 399.13: Electronic Communications Services (Modification of Maltacom p.l.c and Vodafone Malta Limited Licences) Regulations
- Chapter 399.15: Electronic Communications Service (Modification and Provision in respect of a Joint Venture and Shareholders Agreement) Regulation
- Chapter 399.19: Electronic Communications Service (Modification of Radio Tracking System and Services Licence) Regulations
- Chapter 399.20: Electronic Communications Service (Modification of Radio Paging System Agreements and Licence) Regulations
- Chapter 399.21: Electronic Communications Service (Modification of Cable System Agreement and Licences) Regulations
- Chapter 399.25: Electronic Communications (Personal Data and Protection of Privacy) Regulations
- Chapter 399.26: Electronic Communications (Unbundled Access to the Local Loop) Regulations
- Chapter 399.27: Electronic Communications (Leased Lines) Regulations
- Chapter 399.28: Electronic Communications Networks and Services (General) Regulations.

---

<sup>7</sup> See: <http://www.mca.org.mt/corporateprofile/openarticle.asp?id=21>

## Self-regulations

### *Self-regulation by telecom providers*

In June 2008 the two major mobile operators in Malta – GO and Vodafone – have signed a “Code of Conduct for Electronic Content Provision by Electronic Communications Undertakings in Malta” by which they agree to use common measures to combat illegal use of their networks in order to protect users, and particularly minors, from unsuitable content and unsolicited communication.

The code reflects the recognition that undertakings believe that users and, in particular persons under 18 years of age (hereafter 'minors'), should use the services reasonably and responsibly and that undertakings shall facilitate this process. In fact, this code will empower parents, legal guardians and other persons who are responsible for the care of minors with information and tools to educate themselves and their children and to exert oversight<sup>8</sup>. The terms used in this code have the same meaning as under the Electronic Communications (Regulation) Act (Cap. 399 of the Laws of Malta).

### *Self-regulatory Code of Conduct for Electronic Content Provision by Electronic Communications Undertakings in Malta*

The Maltese mobile telecom operators have adopted a code of conduct<sup>9</sup> that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Maltese mobile electronic telecommunications market and complies with applicable European and national legislation.

## eIdentity

### *General overview*

Malta plans to use an eID card for all its citizens over the age of 14. The Maltese government uses a PKI based system with soft non-qualified signature certificates. Non-PKI systems are also used in local council offices. These are based on a multifactor authentication scheme (password/username/PIN-code). Additionally, single factor (username/password) systems are also used in the public sector.

Some tax related and public procurement services use eID Level 2 certificates (conform to x509 v3 standard) as a method of authentication (services like: Online VAT return, Corporate eTAX services, ROC Online System and Public Procurement).

The Government CA Certificates are intended solely for client authentication to electronic services offered through the portal of the Government of Malta. While these certificates are technically capable of use for other Advanced Electronic Signature (or “digital” signature) purposes, such use is entirely at the subscriber’s risk. The Government CA publishes CRLs at regular intervals.

### *eIdentity legislation - Electronic Signatures and Certification Services covered by the Electronic Commerce Act III of 2001 (the eCommerce Act)*

The part V of the eCommerce Act addresses signature certification services. The general rule is the provision of signature certification services or services related to electronic signatures do not require prior authorization. However, Minister's regulations may establish and maintain an

---

<sup>8</sup> See: <http://downloads.vodafone.com.mt/downloads/pdfs/codeofconduct.pdf>

<sup>9</sup> Source: [http://www.qsmeurope.org/safer\\_mobile/national.shtml](http://www.qsmeurope.org/safer_mobile/national.shtml)

accreditation scheme that enhances the levels of signature certification services, and designate accreditation authorities.

The Minister may supervise signature certification services that provide qualified certificates. Also, the eCommerce Act states that those who provide qualified certificates are liable for damages caused to any person who reasonably relies on such certificates. Providers of qualified certificates may limit the use of such certificates provided that those limitations are clear and readily identified as limitations. In this case, the provider shall not be liable for damages caused for uses that did not acknowledge the limitations.

## NIS Governance

### Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

<b>National Authorities</b>	<ul style="list-style-type: none"> <li>• Ministry for Infrastructure, Transport and Communications / Ministru għall-Infrastruttura, Trasport u Komunikazzjoni (MITC)</li> <li>• Malta Communications Authority (MCA)</li> <li>• Malta Police Force - Cyber Crime Unit</li> <li>• Office of the Data Protection Commissioner</li> <li>• Malta Standards Authority / Awtorita' Maltija Dwar L-Istandards ( )</li> <li>• Malta Council for Science and Technology</li> <li>• National Security Accreditation Authority (NSAA)</li> <li>• National Security Agency (NSA)</li> <li>• The CIIP Unit</li> <li>• INFOSEC</li> </ul>
<b>CERTs</b>	<ul style="list-style-type: none"> <li>• mtCERT</li> </ul>
<b>Industry Organisations</b>	<ul style="list-style-type: none"> <li>• Malta Information Technology Agency (MITA)</li> <li>• Chamber of Engineers (CoE)</li> </ul>
<b>Academic Organisations</b>	<ul style="list-style-type: none"> <li>• Malta College of Arts, Science &amp; Technology- Institute of Information and Communication Technology</li> </ul>
<b>Others</b>	<ul style="list-style-type: none"> <li>• Information Systems Audit and Control Association – Malta Chapter (ISACA)</li> <li>• APPOGG</li> </ul>

For contact details of the above-indicated stakeholders we refer to the ENISA “Who is Who”<sup>10</sup> – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory<sup>11</sup>.

**NOTE:** only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, eID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

<sup>10</sup> The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

<sup>11</sup> <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

## Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

### Co-operation and information exchange mechanisms facilitated by MITA

MITA is responsible for the governance of the Government of Malta ICT Policies, Directives and Standards (collectively referred to as GMICT Policy). The function of compilation and publication of GMICT Policy lies in the Enterprise Architecture Unit within the Government's Office of the CIO, with each GMICT Policy document being assigned to the appropriate Enterprise Architecture Domain/s<sup>12</sup>.

Malta has a good practice example of transparency with respect to the Government of Malta ICT Policies, Directives and Standards – a compilation of policies and standards is published on the web site of the government<sup>13</sup> and relevant business and technical players were involved in compiling them including:

- Enterprise Architect - ICT Governance
- Chief Enterprise Architect and/or other Enterprise Architect/s
- The respective Domain Owner/s
- Compliance Manager
- An INFOSEC Authority representative
- Legal Counsel
- Government representative/s
- Third parties, where appropriate

GMICT Policy documents are also reviewed by Chief Information Officers from Public Sector entities before being forwarded to the Chairman, CIO Council for authorisation to publish. The Compliance Manager within the Business Excellence and Compliance Department of MITA carries out compliance audits to determine the degree of adherence to GMICT Policy.

Amongst other things, this activity identifies those areas where improvements in the implementation of policies are required. The Compliance Manager is also responsible for the approval or otherwise of requests for exemption from specific policies, which are assessed through consultation with the appropriate experts.

### Co-operation via Malta Communications Authority (MCA)

As stated in last year's report, MCA organises on a regular basis public discussions and consultations on NIS domain. In 2010, on the MCA web site there were published<sup>14</sup> several Public consultations a draft amendments to different acts.

Currently, a number of Maltese providers exchange information (on a confidential basis), on a voluntary basis, with the Malta Communications Authority (MCA) regarding the resilience of their networks. However, such information is only provided when requested by the MCA. Besides, not all the providers are willing to forward such information.

Consequently, the kind and the amount of detail exchanged vary from one provider to another. Hence, the MCA's efforts to issue the appropriate legislation. This would permit the MCA to request predefined resilience-related information and have providers update this information on a periodic

---

<sup>12</sup> [http://mitts.gov.mt/PortalPublic/ICT-HTML/GMICT\\_Policy\\_Main.html](http://mitts.gov.mt/PortalPublic/ICT-HTML/GMICT_Policy_Main.html)

<sup>13</sup> See the compilation of Government of Malta ICT Policies, Directives and Standards available at <http://ictpolicies.gov.mt>

<sup>14</sup> See: <http://www.mca.org.mt/>

basis. The information collected is reviewed and assessed by the MCA. The aim is for the MCA to better understand, and have a clear picture, of Malta's standing vis-à-vis resiliency.

MCA is currently in the process of reviewing the contingency plans for international connectivity submitted by the various Maltese providers. Having evaluated the information provided, the MCA may then revert to the respective operator to discuss any pitfalls which it foresees in its networks, and possibly even mandate measures to address these pitfalls.

Additionally, this information will come in handy to the MCA when it commences to draft guidelines/recommendations which will accompany the regulations in the near future.

### **Co-operation on Safer Internet Use and prevention of child pornography on the Internet**

The institutional framework for the hotline's operation exists and national responsibilities with regard to safer Internet have been defined. The Malta hotline is managed by the APPOGG who also supports the European network by cooperating with and assisting the network coordinator, exchanging reports with other members of the network, participating in network meetings and working groups established by the network, and in other collaborative activities, such as drafting of best practice papers and documentation or training schemes to exchange expertise between hotlines. APPOGG is full member of the International Association of Internet Hotlines (INHOPE).

### **Fostering a proactive NIS community**

Malta Information Technology Agency (MITA) and Malta Government Technology Investments Limited (MGTIL) have recently hosted a Cypriot delegation having chosen Malta as a best practice country in the implementation of e-Government. During this two-day visit, MITA showcased a number of e-Government services together with its vision for the future.

During the various information sessions, the delegation from Cyprus Paralimni Municipality and Larnaca District Development Agency were presented with information on the local ICT policies and standards in Malta and an overview of the e-Government shared services and platforms. They also visited MITA's Data Centre and Network Operations Centre.

The visit was initiated through MGTIL which is currently participating in an EU funded Interreg IVc project - Digital Cities (DC). This three year project brings together municipalities of different maturity in ICT adoption to exchange information, know-how, experience and good practices.

## Country-specific NIS facts, trends, good practices and inspiring cases

### Security incident management

As specified in the 2010 report, mtCERT is Maltese responsible to proactively monitor for security threats and to try to prevent any security incidents, to respond to any reported security incidents on the MAGNET (Maltese Government Network) and to educate all government employees who use computers on the prevention of such threats.

The security incident management services are provided by mtCERT on a 24x7 basis, except during the maintenance periods. mtCERT provides to its constituents:

- Reactive services: Triage, Incident Resolution, Incident Co-ordination
- Proactive Services: Training, Contacts, Information propagation methods.

### Incidents affecting networks

Network operators are the prime responders in the case of problems in their networks. In the case of a major incidents, representatives from every incident respondent and a representative from the Malta Communications Authority (MCA) - representing the providers - team up to coordinate the event.

Depending on the seriousness of the incident, a number of Ministers (together with the heads of the incident respondents) may also group in the Government Contingency Centre to manage matters. Incident identification and analysis is often carried out by the operators themselves (in the case of communications). Many of the communication companies in Malta have foreign mother companies. Therefore, it is possible that they exchange information with their counterpart colleagues abroad. Both MITA and the providers carry out post-mortem investigations following an accident.

Additionally, providers are not obliged to report security incidents affecting the resilience of their networks. Very often, the authorities learn about such incidents in the media. Information (often confidential information) is subsequently forwarded to the authorities on request. Since the providers are currently not obliged to forward such information to the authorities, the detail of the information disclosed with the regulator is up to the discretion of the respective operator.

The international connectivity regulation which the MCA is currently working on will mandate providers to inform the MCA and their subscribers when an incident or fault occurs in their network. Rightly so, providers may wish to provide more detailed information regarding the accident to the MCA than to its subscribers.

### Other incident reporting via MITA

In 2010, no specific information was published on the web site of Information Security and Risk Management Department of the Malta IT Agency (MITA) concerning the cyber-attacks on Maltese infrastructure of the public authorities. For consistency, we remind that in March 2009, MITA published information on identified unauthorised software on a server used for the storage of user credentials of personnel in Embassies of Malta abroad<sup>15</sup>.

---

<sup>15</sup> Source: MITA press release of 05.03.2009, available at <http://www.mita.gov.mt>

Overall, in Malta there are no central, formal and statistical sources of information about the issues of online security, spam, spyware and related matters. Available information is scattered amongst different organisations, websites and individuals.

### Emerging NIS risks

As stated in last year's report, no information is available on the participation of authorities, academic bodies or industry organisations from Malta on pan-European initiatives to promote the collaboration and partnership initiatives focused on emerging NIS risks, like for instance the FORWARD<sup>16</sup> initiative.

The FORWARD initiative aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of cyber-threats defences, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures.

No relevant information was identified on the participation of Maltese CERT, ISPs, etc in other European-wide projects aiming at identifying emerging NIS risks, like for example in the Worldwide Observatory of Malicious Behaviours and Attack Threats (WOMBAT)<sup>17</sup>.

### Resilience aspects

As defined in the previous issue of this report, international connectivity is crucial to Malta. Consequently, the MCA deemed it appropriate to commence evaluating Malta's resiliency status by first looking at the resiliency of its international connections. In 2009, MCA issued a regulation on international connectivity<sup>18</sup> - this gives the MCA the required powers to ensure that international gateway providers are caring for redundancy in their links.

The regulation also demands that international gateway providers forward their contingency plans to the MCA who can require any international gateway operator and any undertaking providing international electronic communications services to submit, and where appropriate to publish, information regarding the plans and measures that it has put in place in order to meet the continuity obligations in regulation.

To date, providers are not audited on issues related to the resilience of their networks, but MCA may, in accordance with the provisions of Part VII of the Malta Communications Authority Act, impose sanctions as it may consider appropriate in accordance with the upon any person who acts in breach of any provision of the regulations. To date, in Malta there is no public information available on a national repository of good practices on the resilience of public and/or other essential eCommunications networks.

In Malta, reliability of the eCommunications is one of the key element considered by the end-users, as highlighted in the "Consumer Perceptions Survey 2009 - Internet Services" published by Malta Communications Authority (MCA). See below.<sup>19</sup>

---

<sup>16</sup> See: <http://www.ict-forward.eu/home>

<sup>17</sup> See: <http://www.wombat-project.eu/>

<sup>18</sup> See: *Electronic Communications (Regulation) Act (CAP. 399) - International Connectivity (Continuity of Operation) Regulations, 2009*

<sup>19</sup> Source: <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies>

## Privacy and trust

### Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Data Protection Act 2001 (the "DPA"), Chapter 440 of the Laws of Malta. The competent national regulatory authority on this matter is the Office of the Data Protection Commissioner (the "Office").

### Personal Data and Sensitive Personal Data

The definition of personal data in the DPA is closely based on the standard definition of personal data. In particular, it only applies to individuals as opposed to legal entities. However, subsidiary legislation implementing the Privacy and Electronic Communications Directive establishes a broad definition of "personal data". Insofar as direct marketing rules are concerned, the definition also includes data relating to legal entities unless otherwise specified by the subsidiary legislation. The Office has not issued guidance on the definition of personal data to date. In all likelihood, it will follow the Article 29 Working Party's Opinion on Personal Data.

Under the DPA, sensitive personal data means the standard types of sensitive personal data. Data relating to offences, criminal convictions or security measures may only be processed under the control of a public authority and a complete register of criminal convictions may only be kept under the control of a public authority. Legal Notice 142 of 2004 contains a set of more detailed regulations on the processing of personal data by the police.

Sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. Insofar as the explicit consent condition is concerned, while the law does not lay down any requirement for such consent to be given in writing, this is normal practice, and the Office usually requires some written evidence of such consent if this condition is invoked by the data controller.

### Information Security aspects in the local implementation of the Data Protection Directive

In line with Malta legislation, data controllers are obliged to comply with the general data security obligations. Regard should also be had to the cost of implementing the security measures.

### Data protection breaches and Enforcement

The DPA does not contain any obligation to inform the Office or data subjects of a security breach. However, the DPA does provide that the Commissioner is entitled to obtain, on request, information and any documentation in relation to data security.

The Maltese Office of the Data Protection Commissioner has the power to perform enforcement actions, in cases where the DPA has been or is about to be violated:

- (i) institute civil legal proceedings;
- (ii) order the rectification, blocking, erasure or destruction of data;
- (iii) impose a temporary or definitive ban on processing; or
- (iv) warn or admonish the data controller.

In certain circumstances, such as where the data controller does not implement the security measures required of him by the DPA, the Office may impose an administrative fine. The Office also has the power to refer to the competent public authority any criminal offence encountered in

the course of, or by reason of his functions, such authority then being responsible for imposing any criminal penalty contemplated by the DPA (be that a criminal fine, imprisonment or both).

An aggrieved data subject may, by writ of summons filed in the competent civil court, exercise an action for damages against a data controller who processes data in contravention of the DPA. Such action must be commenced within 12 months from the date when the said data subject becomes aware or could have become aware of such a contravention, whichever is the earlier.

## NIS awareness at the country level

### Awareness actions targeting the public authorities and security experts

Basic legislation is in place covering NIS awareness aspects but investments are limited by the government (financial and human resources) to raise awareness, prevent or investigate incidents. MITA plays a key role in Information Security awareness in Malta, by providing (especially to public authorities) a set of services related to:

- Information Security Policy Development;
- Anti-Virus services;
- Information Security Audit services;
- Investigations and Digital Forensic services;
- INFOSEC Authority services;
- Computer Emergency Response services;
- Information Security Technology review services;
- EU Council Networks support services;
- Data Protection Consultancy.

MITA published on its web site<sup>20</sup> a series of information security policies aimed at improving the overall security of the Maltese public organisations. These security policies define/cover/address:

- Password Policy
- Information Security Policy
- Minimum Information Security Directive
- Information Security Organisation Policy
- Information Security Organisation Directive.

### Awareness actions targeting the consumers/citizens

The major ISPs in Malta provide extensive information on their websites to help consumers/citizens to fight spam and other security issues. This includes detailed help pages, FAQs, recommendations on installing antivirus software, examples of 'phishing' emails and online channels for reporting incidents and queries directly to their customer care representatives. They also follow best practices and use industry standard infrastructure and software to reduce the impact of spam upon their users including automated spam filtering and blacklisting.

Both **myWeb** and **myWebplus** courses are offered by the MITC free of charge. Each course is 20 hours long, taught once weekly for 2 hours spread over a period of 10 weeks. These courses are delivered at the Community Technology Learning Centres. They are aimed on increasing awareness on use of computers, Internet and email, and cover also aspects related to: how to search safely on the Internet; how to protect the computer from viruses and spam, how to use

---

<sup>20</sup> See the published security policies available at: <https://www.mita.gov.mt/page.aspx?pageid=223>

eGovernment services, etc. No specific information is published on the results of **myWeb** and **myWebplus** initiatives<sup>21</sup>.

APPOGG publishes on its web site a set of guidelines<sup>22</sup> for parents, kids and young people on safer use of Internet, and on actions to be taken if inappropriate Internet content is noted. Additionally, the Malta Communications Authority is currently setting up the National Information Security Agency and one of the primary objectives of the agency would be to "To inform companies and the general public about information security threats and the related means of protection through an active communication policy."<sup>23</sup>

### **Other awareness-raising events**

NexTech<sup>24</sup> (last organised event: October 11-16, 2009) is a yearly action that groups several events such as Conference on Advanced Engineering Computing and Applications in Sciences, Conference on Advances in Circuits, Electronics and Micro-electronics, Conference on Advances in P2P Systems, Conference on Emerging Network Intelligence, etc.

The Malta Communication Authority (MCA) organises a yearly event on subjects related to communication; however this year's topic was not related to NIS awareness, this was the case last year (eCommerce). See the MCA Annual Conference.

### **Country-specific activities for identifying and promoting economically efficient approaches to information security**

In general, no public available information was posted in 2010 on the web sites of MITA or MCA on the economic impact assessment at national level for the various laws, regulations with relevance on NIS domain in Malta.

### **Openness and freedom of choice in technology**

In October 2010, the Maltese government announced its position with respect to Open Standards and Open Source Software (OSS). MITA published policies and directives aimed at guiding ministries and other entities specifically on the adoption of Open Standards and the facilitation of non-intrusive adoption of OSS within Government. As a result of past monitoring of the OSS landscape by MITA, a quarter of Government ICT solutions are based on Open Source software.

### **TrolleyMania eMall portal – Public-Private Partnership**

In October 2010, Malta launched a new online shopping mall, TrolleyMania. This eCommerce portal is aimed at all local businesses which want to venture in the world of Internet commerce and start selling their products online. TrolleyMania is an eCommerce platform – an eMall - to be used by Maltese businesses and other organisations that have a useful product/service to sell to the public. The main aim of the eMall is to kick-start the use of eCommerce in the Maltese islands by reducing barriers to entry to the bare minimum.

---

<sup>21</sup> Source: <http://www.epractice.eu/en/cases/icttrainingelderly>

<sup>22</sup> See [http://www.appogg.gov.mt/hotline\\_aboutappogg.asp](http://www.appogg.gov.mt/hotline_aboutappogg.asp)

<sup>23</sup> Source:

[http://ec.europa.eu/information\\_society/policy/ecommerce/doc/library/ext\\_studies/privacy\\_trust\\_policies/spam\\_spaware\\_legal\\_study2009final.pdf](http://ec.europa.eu/information_society/policy/ecommerce/doc/library/ext_studies/privacy_trust_policies/spam_spaware_legal_study2009final.pdf)

<sup>24</sup> See: <http://www.iaria.org/conferences2009/NexTech09.html>

The project is a public-private partnership between Alert Communications and the Government of Malta. Alert Communications is in charge of the creation and operation of the eMall, while the Ministry for Infrastructure, Transport and Communications is responsible for the funding of a promotional campaign to create recognition of the TrolleyMania brand and generate traffic to the site.

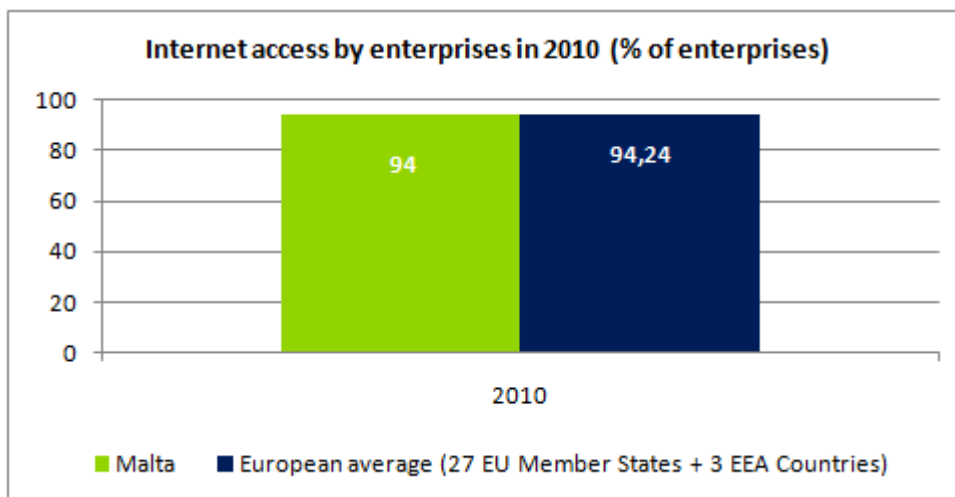
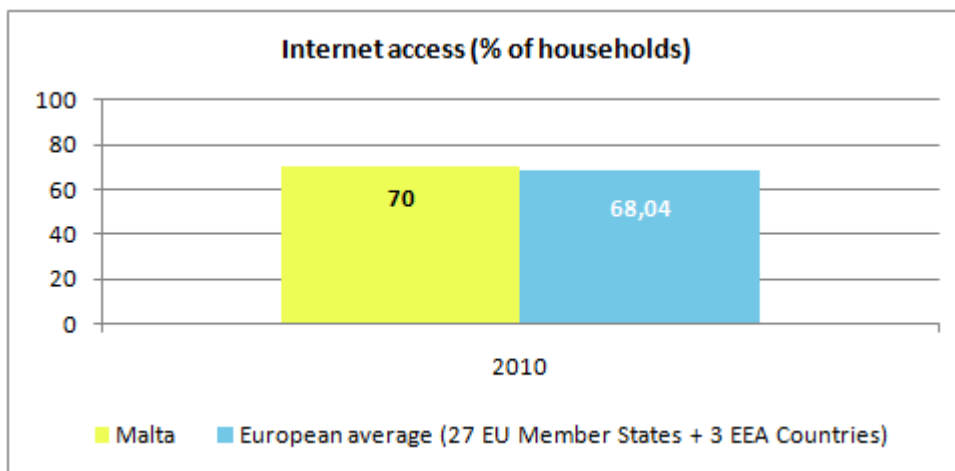
What is interesting in this project is that it offers a very low cost secure eCommerce framework, with extremely reduced prices (€250 for a one-time setup fee, €232 for a per annum fee and a transaction charge of 0.25% on purchases, all excluding VAT).

## Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Malta, a series of relevant statistics are included in this section. These statistics show that Malta is somehow on the European average regarding information technology matters.

### Internet access of population and enterprises

The following graphs provide an overview of the situation<sup>25</sup> of Internet access in Malta for enterprises and respectively households, relative to the European average.

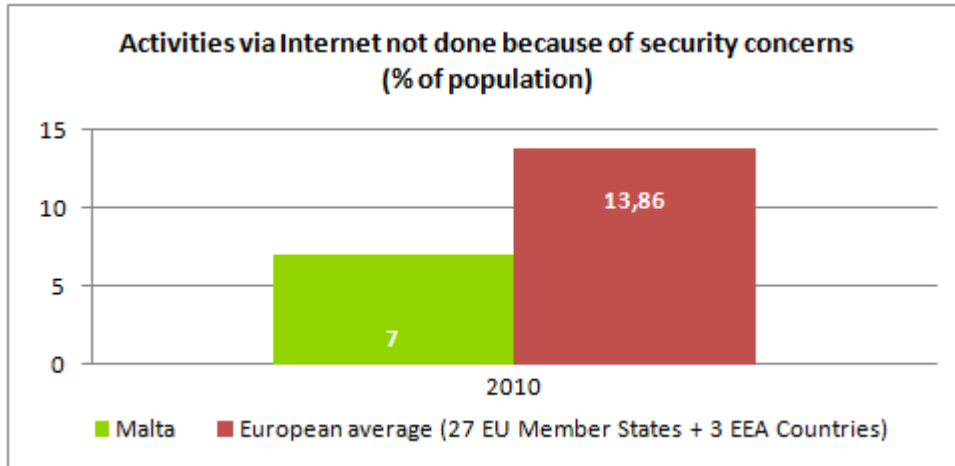


In 2010, the statistics indicate that both the enterprises and the households in Malta have a level of Internet access that is on the European average.

<sup>25</sup> Source: Eurostat

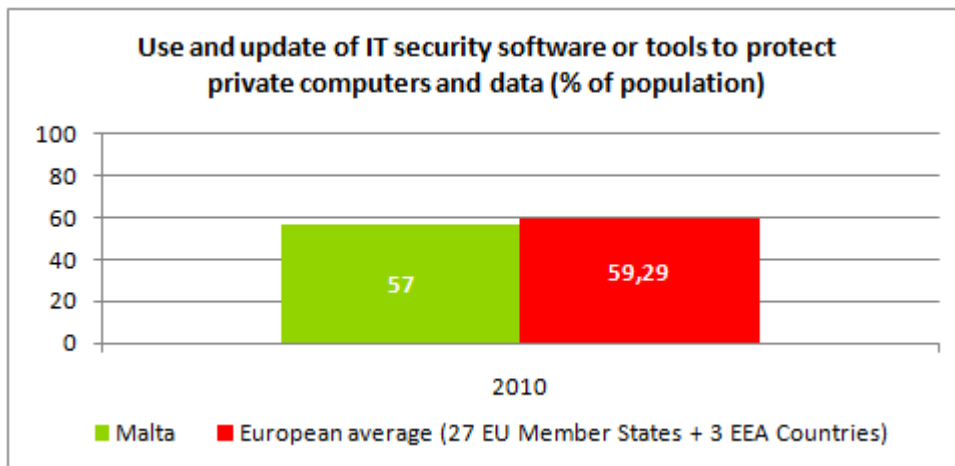
### Statistics on use of Internet by individuals and related security aspects

The percentage of population in Malta that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is about half the European average:



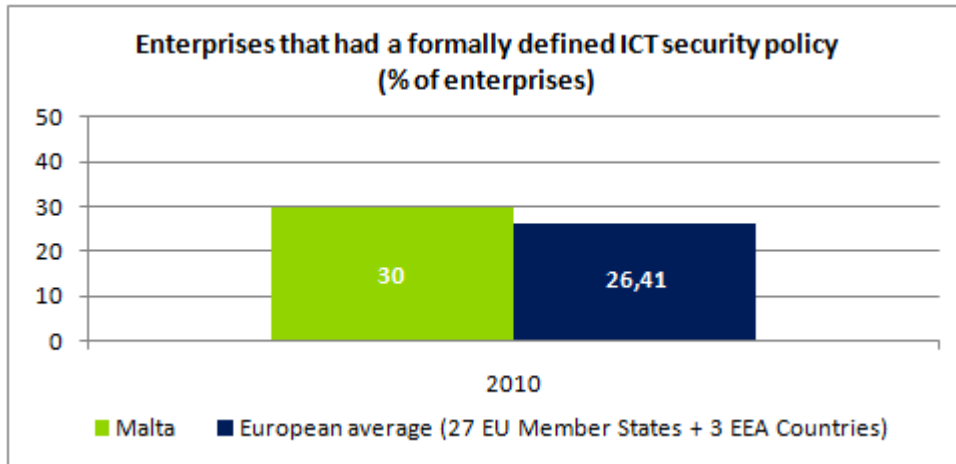
This can be an indication of either much confidence regarding web-based transactions or of a general lack of awareness regarding IT security threats.

Meanwhile, it appears that the use of security tools to protect private computers and data is about the same as the European average.



### Statistics on use of Internet by enterprises and related security aspects

More enterprises in Malta have a formally defined ICT security policy, compared with their European peers. See below:



### Other Statistics

It is interesting to also mention that during the 1<sup>st</sup> half of 2010, and respectively for the 1<sup>st</sup> half of 2009, Malta was mentioned in the global report<sup>26</sup> published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



<sup>26</sup> See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: [http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey\\_1H2010.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf)

## APPENDIX

### National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry for Infrastructure, Transport and Communications / Ministru għall-Infrastruttura, Trasport u Komunikazzjoni (MITC)	The Ministry has been assigned responsibility for the Malta Communications Authority, The Information and Communications Technology Strategy and National Identity Management. The Ministry is also responsible to ensure the national interest in the policy setting, regulation and operations of entities owned or partly owned by the Government.	<a href="http://www.mitc.gov.mt">www.mitc.gov.mt</a>
2. Malta Communications Authority (MCA)	The mission of the MCA is to regulate the electronic communications, eCommerce and postal sectors with a view to achieving sustainable competition, enabling customer choice and value for money. Also, to facilitate the development of an environment that is conducive to investment, and continued social and economic growth.	<a href="http://www.mca.org.mt">http://www.mca.org.mt</a>
3. Malta Police Force - Cyber Crime Unit	The Cyber Crime Unit within the Malta Police Force assists in the investigation of all crimes in which computer and computer systems are used as a target of an attack, and/or used as the medium to launch any attack on any entity. Collects and preserves evidence and present same evidence before judicial authorities; along with providing a 24 hour 7 days-a-week level of support to international law enforcement agencies. The Cyber Crime Unit within the Police Force <sup>20</sup> is an active member of the COSPOL group (Protection against Child Pornography)	<a href="http://www.police.gov.mt/">www.police.gov.mt/</a>
4. Office of the Data Protection Commissioner	Responsible for protecting the individual's right to privacy by ensuring the correct processing of personal data and enforcing the Data Protection Act of 2001	<a href="http://www.dataprotection.gov.mt/index.aspx">http://www.dataprotection.gov.mt/index.aspx</a>
5. Malta Standards Authority / Awtorita' Maltija Dwar L-Istandards	The Authority's mandate is being the National Standards Body entrusted to adopt, publish and disseminate voluntary standards. Maltese Technical Committees of the Standards are responsible to develop purely national standards (MSA) or technical specifications (MSA TS) on request by the Maltese industry. For instance, Maltese Data and Information Requirements on Information and Communication Technology.	
6. Malta Council for Science and Technology	The Malta Council for Science and Technology (MCST) is the national advisory body to Government on science and technology policy. The MCST is also the national agency responsible for the management of the local RTDI programme, as well as the national contact organisation for the Seventh Framework Programme (FP7).	<a href="http://www.mcst.gov.mt">www.mcst.gov.mt</a>
7. National Security Accreditation Authority (NSAA)	The NSAA is the overall security authority, under supervision of the prime minister's cabinet. It supervises the NSA and the CIIP Unit.	No website available.
8. National Security Agency (NSA)	The NSA is responsible for security in general, physical security issues and EU information matters.	No website available.

National authorities	Role and responsibilities	Website
9. The Critical Information Infrastructure Protection Unit (CIIP Unit)	The CIIP Unit is responsible for critical infrastructure protection as well as for the coordination of all the stakeholders involved in critical information infrastructure issues. The aim of the CIIP Unit is to create a protection plan on a national level. It also has the task of encouraging actors from the private sector (ISPs, banks, etc.) to form their own CERT teams. From that point on, the CIIP Unit will start a forum involving those private sector CERT teams.	No website available.
10. The Critical Information Infrastructure Protection Council (CIIP Council)	The CIIP Council was created in order to bring all the government entities together to discuss on Information Security and CIIP issues.	No website available.
11. INFOSEC	INFOSEC is responsible for information security for the government, and has the task of defining the national direction for security.	No website available.

### Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
12. mtCERT	<p>mtCERT is the Computer Emergency Response Team of the previous Malta Information Technology and Training Services Ltd (MITTS), Malta. MITA is taking over the strategic and operational functions of the formerly known MITTS. Mission:</p> <ul style="list-style-type: none"> <li>• Provide a central point of contact once an incident occurs.</li> <li>• Provide technical assistance and help to correct the damage caused by an incident.</li> <li>• Educate on known threats and risks when using the Internet and how to protect from these threats.</li> <li>• Advise and alert, in the least possible time, on new risks and threats as well as the measures to be taken to prevent these new threats.</li> <li>• Team up with International CERT teams to keep the CERT updated with the latest threats and methods for their prevention.</li> </ul> <p>mtCERT is:</p> <ul style="list-style-type: none"> <li>• Not FIRST member;</li> <li>• TI listed.</li> </ul>	<a href="http://www.mtcert.gov.mt">www.mtcert.gov.mt</a>

<sup>27</sup> <http://www.first.org/members/teams/>

<sup>28</sup> <http://www.trusted-introducer.nl/>

### Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
13. Malta Information Technology Agency (MITA)	<p>The MITA has been appointed by the Government of Malta as the prime Agency for propagating Information and Communication Technology (ICT) policy in the country and the executor of The Smart Island Strategy – 2010. MITA has taken over the functions of several entities, namely: the former Information Society Secretariat; the ICT in Government Unit; the Core ICT Advisory Committee; and the Malta Information Technology and Training Services Ltd (MITTS Ltd, a Government owned company which was supplying IT systems and services to Government departments).</p> <p>The main functions of MITA are to:</p> <ul style="list-style-type: none"> <li>• Be the main motor in the development of policies, programmes and initiatives in the sector of information and communication technology;</li> <li>• Carry out all the programmes related to the implementation of the systems connected with information technology within the public sector with the main aim of consolidating the services offered to the public;</li> <li>• Provide an efficient and effective infrastructure for services to Government in ICT as requested by the Minister concerned;</li> <li>• Work to increase the application of information and communication technology in society and on an economic level;</li> <li>• Promote and carry out programmes with the intention of expanding ICT education and so that ICT application serves as a tuition tool.</li> </ul>	<a href="http://www.mita.gov.mt">www.mita.gov.mt</a>
14. Chamber of Engineers (CoE)	<p>The Chamber of Engineers (CoE) is the local organisation catering for the interests of Maltese professional engineers. The Chamber organises courses for the Engineering Community on Technical and Information Technology subject having an awareness raising role.</p>	<a href="http://www.coe.org.mt">www.coe.org.mt</a>

### Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
15. Malta College of Arts, Science & Technology- Institute of Information and Communication Technology	<p>The Institute of Information and Telecommunications Technology offers numerous diploma options in all areas of IT, and has a key role in the NIS-related education in Malta.</p>	<a href="http://www.mcast.edu.mt">www.mcast.edu.mt</a>

## Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
16. Information Systems Audit and Control Association – Malta Chapter (ISACA)	<p>The primary purpose of the Malta chapter of ISACE is to promote the education of professionals for the improvement and development of their capabilities relating to IT Governance, auditing, control, assurance and security. The objectives of the Chapter are:</p> <ul style="list-style-type: none"> <li>• To promote the education of, and help expand the knowledge and skills of its members in the interrelated fields of IT Governance, IS auditing, assurance, security, and control;</li> <li>• To encourage an open exchange of IT Governance, IS audit and control, assurance, and security techniques, approaches and problem solving by its members;</li> <li>• To promote adequate communication to keep members abreast of current events in IT Governance, IS audit and control, assurance, and security fields that can be of benefit to them and their employers,</li> <li>• To communicate to management, auditors, universities and to IT governance professionals the importance of establishing controls necessary to ensure the effective organisation and utilisation of information technology resources, and</li> <li>• To promote the Association’s professional certifications and IT Governance principles and standards.</li> </ul>	<a href="http://www.isaca-malta.org/">www.isaca-malta.org/</a>
17. APPOGG	APPOGG is the national social welfare agency for children and families in need – and also full INHOPE <sup>29</sup> member on behalf of Malta.	<a href="http://www.appogg.gov.mt">www.appogg.gov.mt</a>
18. CA Malta	CA Malta is the Consumer’s Association of Malta. It aims at protecting and educating consumers.	<a href="http://www.camalta.org">www.camalta.org</a>

<sup>29</sup> INHOPE is the International Association of Internet Hotlines.

---

## References

- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- European Commission, Europe's Digital Competitiveness Report, Volume 2: i2010 — ICT Country Profiles available at [http://ec.europa.eu/information\\_society/eeurope/i2010/key\\_documents/index\\_en.htm#EDCR](http://ec.europa.eu/information_society/eeurope/i2010/key_documents/index_en.htm#EDCR)
- Code of Conduct for Electronic Content Provision by Electronic Communications Undertakings in Malta, available at <http://www.mca.org.mt/infocentre/openarticle.asp?id=1199&pref=2>
- Malta Electronic Communications (Regulation) Act (CAP. 399) - International Connectivity (Continuity of Operation) Regulations, 2009 - Published by the Department of Information (doi.gov.mt)
- MITA press release of 05.03.2009, available at <http://www.mita.gov.mt>
- Compilation of Government of Malta ICT Policies, Directives and Standards, available at <http://ictpolicies.gov.mt>
- Malta- ENISA CERT Directory: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/malta>



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280  
[www.enisa.europa.eu](http://www.enisa.europa.eu)