eSecurity: A Strategic Direction

Consultation paper issued on behalf of the National eSecurity Working Group

Ministry for Investment Industry and Information Technology, Malta

Malta Communications Authority
Valletta Waterfront, Pinto Wharf,
Valletta VLT 01, Malta, Europe
Telephone: +356 21 336 840
Facsimile: +356 21 336 846
Web: http://www.mca.org.mt

Table of Contents

1.0 Forces for Change

Today, Information and Communications Technologies (ICT) underpin the world's economic growth and the Internet has revolutionised the way society, businesses and governments operate. Governments worldwide are encouraging a high level of investment in ICTs and high levels of online participation by local administrations, businesses, institutions and society in general.

In Europe, production and use of ICTs account for around 40% of the productivity growth and one quarter of the overall economic growth. The eCommunications services sector is the largest segment of the overall ICT sector (44.4%).

The Internet has become a fixture of both business and private life. 89% of European Union (EU) enterprises actively used the Internet in 2004; 65% had a website and 47% of people regularly used the Internet. With 25% of households using broadband, millions are now almost permanently connected.[1]

Malta is no exception to this trend. The high level of mobile telephony penetration rates and the increasing number of broadband Internet connections are a sure sign of the growing dependence on ICTs.

In 2003, 94% of Maltese enterprises having more than 10 employees used the Internet and on average 73.1% had a website.[2] In quarter 1 of 2006, there were a total of 52,000 Internet connections in Malta representing 33% of Maltese households[3]. Latest statistics indicate that 57% of the Maltese population have Internet access.

While the permeation of ICT has brought about increased efficiency and productivity in most parts of the economy, it also poses a number of new challenges, mainly related to the need to engender trust and confidence in the online environment. The eSecurity landscape continues to change at an increasing speed with the emergence of new threats to the online environment. These threats range from social engineering techniques that operate over the Internet - where users are tricked into providing personal details - through to a new wave of sophisticated malicious software such as worms, trojans and spyware that embed themselves within a computer system and either damage that system or harvest sensitive or private information. Spam plays a key role in the distribution of this malicious software. The Internet is also proving to be a vehicle for criminal activities such as fraud, paedophilia and the illegal distribution of pornography and other harmful content.

An extensive harmful attack could seriously impact a nation's critical information infrastructure – i.e. those networked systems supporting public health, government, banking, energy and water supply and others - and could have a debilitating impact on the nation's economy and its governance structures.

---

[1] Eurostat

[2] NSO Survey on ICT usage by enterprises; http://www.nso.gov.mt/statdoc/document_view.aspx?formAction=init&id=935&backUrl=%2fsite%2fsearchresults.aspx

[3] Electronic Communications Market Review: October 2005 - March 2006http://www.mca.org.mt/infocentre/openarticle.asp?id=867&pref=1

The European Commission's e-Business W@tch4 indicates that basic security measures (such as firewalls and secure servers, if required) are already highly deployed by European enterprises. Three quarters of employees working in enterprises of all sizes are already equipped with firewall technology. The second most commonly implemented ICT security control is the drafting of a disaster recovery plan. On the other hand, there is still a lot to be done insofar as other methods for countering risks are concerned. For instance, implementing an IT security policy comes third on the list, but at a surprisingly low level: less than half of European employees (48%) work in enterprises with a security policy in place. This, despite consensus across security professionals that such a policy is an essential first step towards ensuring adequate protection from growing security threats[5]. A still lower percentage of enterprises reports that they train their staff in security awareness (15%), carry out risk assessment (15%), or have put a security management system in place (19%).

Many of these threats exploit vulnerabilities in information systems and lack of awareness or good practice in users, be these businesses or consumers. They impact directly on individuals, businesses and governments and can, and do, cause serious economic and personal harm, sometimes at a global level[6].

As ICT systems and networks continue to grow and become increasingly sophisticated and complex, we can expect more security issues to emerge. Moreover, while traditionally most attacks on computer systems have been motivated by curiosity or a desire to show off technical virtuosity, many current attacks are motivated by profit or criminal intent. Links to organised crime put the phenomenon in a particularly alarming light. New technologies and applications, such as mobile devices, RFID (radio frequency identification), and ubiquitous computing (computing embedded in everyday objects) are likely not only to unveil new opportunities but also present new challenges for security and privacy.

Rapid advances in technology which are, to a significant extent, driven by innovation and commercial rivalry within the IT industry, have not only intensified the emergence of new eSecurity threats and vulnerabilities but have also contributed to the development of mitigation strategies. As such, the IT industry plays a vital role in identifying and managing current and emerging threats and the vulnerabilities they exploit.

Network and Information Security (NIS) is crucial for the development and uptake of new systems, applications and online services and thus, for the Maltese information society in general. An absence of adequate NIS not only places ICT users at risk; it also undermines trust and confidence in electronic communications networks and services. It consequently deters the further uptake of these technologies with the attendant negative impact on economic growth.

---

[4] The European e-Business Market Watch "*ICT security, e-Invoicing and e-Payment Activities in European Enterprises*", Special Report, September 2005. The European Commission's e-Business W@tch monitors the adoption, development and impact of electronic business practices in different sectors of the economy in the enlarged European Union.

[5] *Ibidem*, p. 40.

[6] For example, a virus called 'I love you' struck more than 45 million computers worldwide in May 2000. It is believed to have caused up to US$ 10 Billion worth of damages.

Businesses need information and related systems that are secure in order to maintain their competitive edge[7] and commercial image, to ensure business continuity, prevent fraud and comply with legal requirements (e.g. with privacy and data protection laws). Appropriate levels of network and information security provide such protection by ensuring that information transmitted and accessed over electronic communications networks remains available, reliable, authentic and confidential. As such, they underpin the competitiveness of the national economy.

Confidentiality, integrity and availability of information are the pillars of eSecurity: that is, ensuring that only authorised people or organisations can access particular information, that the information has not been altered by non-authorised entities during transmission and that the systems responsible for delivering the information are accessible as needed, by those who need them. This also entails the ability to respond to and recover from attacks, which it is recognised, cannot always be prevented. As more eGovernment and eBusiness solutions are rolled out, eSecurity policy must evolve to also address authentication and non-repudiation. Authentication and non-repudiation encompass the need to ensure that all parties to a transaction are confident about whom they are dealing with and that they are authorised to perform the transaction in question.

Since the announcement of the National ICT Strategy in 2003, there has been a rapid expansion of the information economy, driven primarily by the accelerating growth in the scale, ubiquity and complexity of the Internet. Government alone cannot ensure effective eSecurity. This requires a concerted and continuous effort by all users of ICTs including home users, governmental and non-governmental agencies, SMEs and businesses operating large information systems. eSecurity also requires a coordinated effort that addresses three inter-related elements, that is, network and information security, effective prevention and enforcement of cyber-crime, online privacy and data protection.

The National eSecurity Strategy is being developed to ensure that Malta's national policy and operational framework continues to be responsive to the changing eSecurity environment now and well into the future. It aims to engage all citizens in a national debate on the subject, with a view to ensuring an ongoing and inclusive national effort to secure our information society.

This consultation paper aims to initiate the local debate on this subject and elicit input from all the relevant stakeholders and members of the general public to the formulation of this strategy.

[7] Lack of trust in ICTs may deter businesses from using these technologies to adopt more efficient business processes.

2.0 eSecurity Vision

Government's vision for the information economy is one where government, businesses and society participate in the information society with confidence, are open to innovation and can collaborate to maximise the economic and social benefits associated with the effective use of ICTs.

To keep pace with the growth and transformation of the information economy, governments, businesses, and society alike must be resilient and able to adapt to change. Network and information security, needs to be seen as a virtue and an opportunity rather than a liability and a cost.

The following vision guides the formulation of the eSecurity Strategy:

A Maltese society that is well-informed on, and can effectively respond to, eSecurity threats and vulnerabilities, such that there is full trust and sustainability in the use of ICTs, contributing to a healthier information society in Malta.

3.0 eSecurity Building Blocks

At an international level the subject of eSecurity has been well debated. A number of important activities have been undertaken where the key pillars of effective eSecurity have been identified. These include the World Summit on the Information Society (WSIS), and the European Strategy for a Secure Information Society. Annexes A, B and C provide an overview of the conclusions of the international initiatives that have addressed, or are addressing eSecurity as well as an outline of a number of initiatives directly relevant to eSecurity.

From a review of these findings, it has been concluded that the high-level conditions that must be present at a national level in order to improve the level of eSecurity have been sufficiently discussed and documented. These findings were further corroborated by the outcomes of the workshops held during the MCA Annual Conference in November 2006. These conditions, which correspond to the vision elaborated above, can be said to form the building blocks of eSecurity, and can be categorised as follows:

- Well informed and security-conscious stakeholders;

- Effective and properly enforced cyber crime legislation;

- Secure eGovernment applications and services, including eID Management and authentication;

- Effective Critical Information Infrastructure Protection;

- Security solutions readily available, affordable and user-friendly;

- An industry that gives due consideration to building and implementing effective security and privacy measures with respect to its products and services;

- Privacy protection;

- Multi-stakeholder collaboration and cooperation at a national and international level.

4.0 Strategic Goals and Objectives

The following national strategic goals and objectives have been developed on the basis of the eSecurity building blocks discussed in the previous section.

Strategic Goal: Creation of a culture of security in Malta

Objective: A sustained program of initiatives aimed at educating and engaging all members of society in a national effort to secure our information society

Strategic Goal: Effective prosecution of cybercrime

Objective: An up-to-date legal framework and adequate capacity to deal with the enforcement and prosecution of cybercrime

Strategic Goal: Secure use of ICTs by eGovernment and businesses

Objective: eGovernment and businesses act as drivers of eSecurity best practice, in a number of areas including eID management and authentication.

Strategic Goal: An effective institutional framework capable of addressing eSecurity on an ongoing basis

Objective: Effective national and international collaboration and cooperation on matters related to eSecurity

5.0 Situational Analysis

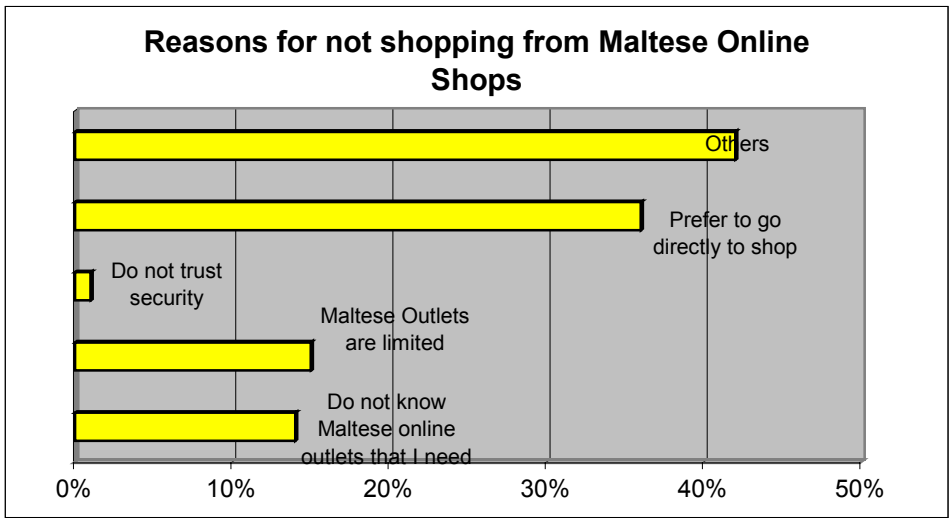
5.1. The General Public and Use of the Internet

Online shopping in Malta

Use of the Internet in Malta is constantly on the increase. More than half (57%) of the population aged over 18 has access to the Internet. This proportion was much higher amongst the younger respondents and was also dependent on the individual's socio-economic background.

Furthermore, 48% of persons having access to the Internet, or 27% of the population, have used it for eCommerce, with the most popular applications being online banking, online shopping and eGovernment services.

Statistics relating to online confidence indicate that eSecurity does discourage the use of eCommerce with about 1% of people with access to the Internet not doing eCommerce from local online shops for security reasons. (3 respondents out of 225).



55% of eCommerce users buy goods or services online with 99% of them carrying out online transfers of money.

One of the most perceived problems related to online shopping is linked to stolen credit card details. However the survey revealed that less than 1% of eCommerce users encountered such problems.

Online buyers tend to deploy some precautionary measures. The majority transact only through:

- sites end-users know are secure (57%), and
- with companies they know (44%).

A high degree of trust is pinned to the Electronic Banking Systems where 75% of Internet users opt to use the eBanking facility.

Children using the Internet

According to a recent survey carried out by the National Statistics Office (NSO)[8], a good portion of children access the Internet on a regular basis. They use it primarily for entertainment and educational purposes. Chatting is also widespread. 8.7% of the children have physically met with someone with whom they first established contact whilst online.

From the survey, it also transpired that 12% of children have accessed websites and chat rooms containing pornography, racism, violence and vulgar language. Other salient results from this survey are summarised in Table 1.

Internet Usage	Aged 8 – 10	68.6%
	Aged 11 – 13	80.0%
	Aged 14 – 16	91.7%
	Total	79.1%
What Children Do		
Schoolwork	67.5%	
Email and Download Music	56.2%	
Chatting	52.3%	
Read Online Magazines	23.1%	
Exposed to:		
Pornography	33%	
Violence	25.6%	
Nude / Semi-Nude pictures or videos	22.9%	
Racism	12%	

Table 1: Abstract of Results from the *Children and the Internet* Survey

One of the most significant findings of this survey was the discrepancy between parents' perception and children's actual activities, as outlined in figure 1.

[8] http://www.miti.gov.mt/docs/Survey%20use%20of%20internet%20Results.pdf

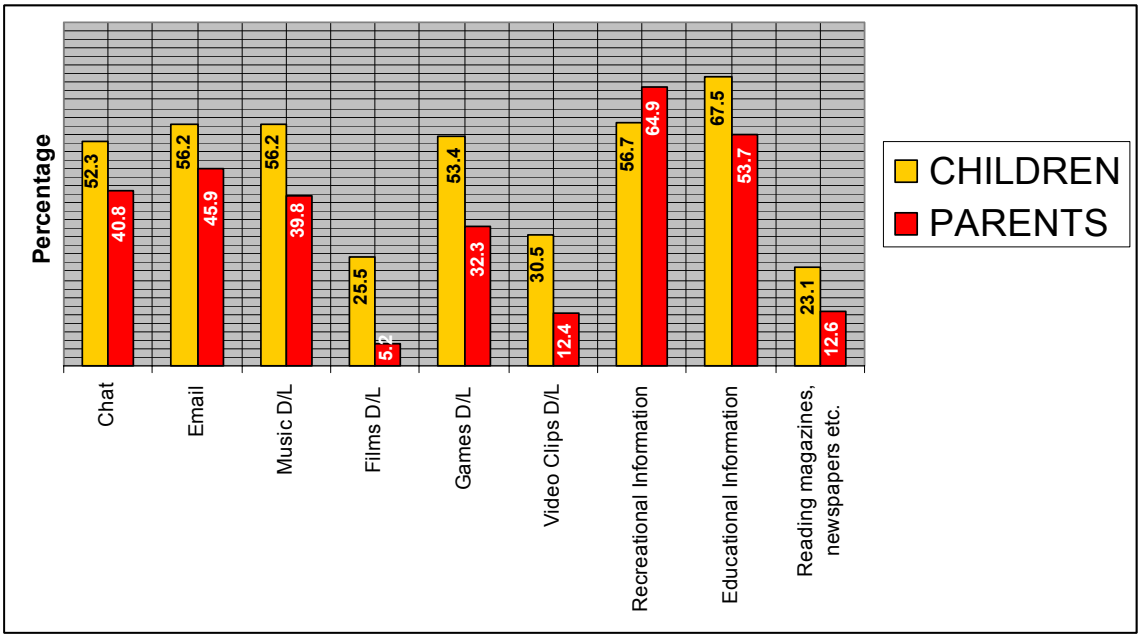


Figure 1: Children's Declaration Vs Parents' Perception

The survey also shed light on the lack of knowledge parents have in the area of eSecurity. Only 1 out of every 3 parents claimed to be aware of content filtering software and only 23% of the interviewed parents had actually installed such software on their home PCs. Moreover some parents were not fully aware of the capabilities of this software.

5.2. The Maltese Enterprise and Internet Usage

An NSO survey[9] carried out in 2003 found that, in general, Maltese enterprises employing more than 10 employees are keen on the uptake of ICTs. Of the surveyed enterprises, over 90% use the Internet, mostly for information searches, market price monitoring, to conduct banking and financial transactions over the Internet, as well as to obtain after-sales services, acquire digital products and for training purposes. On the other hand, teleworking does not seem to be popular, with only 11 per cent of surveyed enterprises responding positively to this practice.

The NSO statistics indicate that small undertakings are making more use of the Internet for procurement than larger businesses, with organisations having between 10 and 49 employees making 21% of all purchases over the Internet, while enterprises employing 250 and over employees make only 4% of their purchases over the Internet.

A good number of these enterprises have a website, with the overwhelming majority – over 90 per cent - using it for marketing the enterprise's products. A relatively small proportion – just over 17% – provide after-sales support over the Internet to their clients.

9 http://www.nso.gov.mt/statdoc/document_view.aspx?id=935&backUrl=publication_catalogue.aspx

20% of the surveyed enterprises stated that they had received orders for their products via the Internet, while 9% had received online payment. The practice of installing electronic customer-complaints facilities is not widespread among enterprises, with over 78 per cent responding that these do not feature on their website.

Antivirus software and firewalls are the online security features most prevalently used by Maltese enterprises. Notwithstanding this, nearly 30% of the surveyed enterprises responded that they had encountered a problem with their online security, with 26% stating that computing virus attacks had cost them loss of information or working time.

It is clear that Malta is not immune to serious attacks with malicious intent. Incidents have occurred where individual companies have been the targets of such attacks.

A particularly serious incident, with nationwide repercussions, occurred a couple of years ago when betting websites were attacked through the Internet with a distributed denial of service attack. A Malta-based company was one of the worst affected. This attack had considerable repercussions on the performance of the local Internet connectivity. As a result of this incident, a number of precautionary measures were put in place.

5.3. Cybercrime in Malta

Reports in relation to computer-related crimes in Malta are on the increase.

Despite being under-reported, cases of computer-related crime have increased by 184% since February 2003, with a total of 145 computer-related incidents reported to the Police in the first 10 months of 2006.

The predominant crime categories are online fraud, child abuse and malicious communications (eg threatening messages, etc). It is to be noted that these three categories are perhaps the most visible computer-related crimes.

To date, 78 persons have been arraigned in court in connection with alleged breaches of computer misuse legislation. The majority of cases were related to child abuse and fraud. As part of its investigations, in 2006 alone, the Cyber Crime Unit analysed over 4,700 computer devices and storage media. Annex D includes further information on the activity of the Unit and the relevant legislation.

The statistics above confirm that the increased use of ICT, especially the use of the Internet, has also increased opportunities for individuals to exploit vulnerabilities with malicious intent. Malta is no exception to the rule. The global reach of the Internet ensures that Malta is exposed to all the risks that prevail throughout this network.

Although official statistics may not appear particularly significant, especially in comparison with the more traditional crimes, it is believed that on examining the dark figures for this category of offences, a different conclusion is reached.

This reasoning is premised on the experience of the Malta Police Cyber Crime Unit over the past few years. Individuals and organisations are failing to report such crimes for a number of reasons. These include:

- Potential embarrassment and bad publicity;

- End-users may not be aware that their computer systems are compromised as the majority of security breaches are not visible to the end-user;

- Lack of awareness of competent authorities' enforcement powers;

- A conviction that cyber criminals cannot be traced and prosecuted;

- Attributing the incident to technical failure rather than possible external unauthorised access or manipulation; and

- Self-blame, which restricts the victim from making an official complaint.

5.4. National Initiatives

The National ICT Strategy

In 2003, Government launched 'The National ICT Strategy - 2003 to 2006', which identified as one of its key objectives the need to make the Internet a secure place and build confidence, trust and security in the use of ICTs. It identified a number of tactical areas to be addressed over this period, as highlighted in Annex E.

As detailed in the coming sections, some of these tasks have been completed while others are currently underway.

Awareness and Education

A number of initiatives focusing on awareness-raising and education on eSecurity have been implemented as part of the strategy.

Promoting safe use of the Internet at schools

The Ministry of Education has promoted the safe use of the Internet as part of its initiative to provide every student in government schools with the facility to have a personal email account and web-page.

This service is backed by internal processes and procedures aimed at ensuring that children do not receive spam or any other form of illegal content.

Furthermore, an Acceptable Use Policy has been drawn up with regard to access to the Internet and email at school. The policy is targeted at both children and parents. It is therefore considered to be an important tool in educating both students and parents about the safe use of the Internet.

Childnet International

In June 2003, the Ministry for Investment, Industry and Information Technology (MIIIT), following a recommendation of the child abuse task

force[10], signed an agreement with Childnet International, a leading organisation in Internet Safety. The agreement enabled:

- the delivery and use of internet safety and awareness materials by the Government of Malta;

- the establishment of a 'train the trainers' programme, following initial training of a pool of ICT and guidance teachers, members of the Police Force and members of Agenzija Appogg.

As a result of this agreement and close co-operation between MIIIT and the Ministry of Education, an awareness campaign on Internet Safety targeted at parents and students, was conducted.

In view of the success of the first agreement, MIIIT is currently in discussion with Childnet International with a view to reaching a similar agreement covering the period 2007-2009.

MyWeb

The MyWeb Programme provides ICT Tuition for members of the general public. Around 5000 individuals were trained in the 1st session.

Following a review of the curriculum of the 1st session, the course was extended to include a module on Internet Safety. This module educates members of the public on how to use the Internet safely and the measures available to protect children and PCs in the online world. 3000 individuals have now been trained in subsequent sessions.

Awareness Campaigns

In February 2006, a month-long awareness-raising initiative was undertaken, aimed at addressing issues evidenced in the results of the survey conducted by the National Statistics Office on Maltese children's use of the Internet.

Child Abuse over the Internet Hotline

A single point of contact for children or adults coming across child abuse over the Internet has been established. This hotline is funded under the Safer Internet programme.[11]

It is intended that further initiatives will be undertaken to increase the awareness of the hotline and encourage its use. The hotline liaises regularly with stakeholders such as Internet Service Providers and the Cyber Crime Unit.

---

[10] http://www.miti.gov.mt/site/page.aspx?pageid=16

[11] **EU response to illegal and harmful content on the Internet**

The Safer Internet *plus* programme provides funding for intiatives promoting safer use of the Internet and new online technologies, particularly for children, as well as fighting illegal content and content unwanted by the end-user, as part of a coherent approach by the European Union.

eSecurity Working Group

On 3rd February 2006 Government established the National eSecurity Working Group. The setting up of this Group followed agreement at NISCO[12] on the need for a focused group to work on eSecurity-related matters and specifically on a national strategy for eSecurity.

The group comprises representatives of key stakeholders in matters of eSecurity. To date, the working group has established three sub-groups with terms of reference addressing critical information infrastructure protection, a review of national cyber crime legislation and the drafting and implementation of the national eSecurity strategy.

eGovernment (MITTS)

MITTS Ltd provides ICT services to the Government of Malta that also include a number of public sector entities and national authorities. The services provided range from Project Management, Software Development, management and operation of Government Network, and the provision of Government's corporate Email, Internet and eGovernment hosting.

The eGovernment hosting infrastructure consists of a multi-tier architecture whereby the service is split between a front-end service and a back-end service.. The protection of the setup employs the defence in-depth concept, employing different layers of security between different zones.

The Information Security and Risk Management (ISRM) Department within MITTS Ltd is responsible to research and compile Information Security Policy for Government and MITTS Ltd as an organization. The ISRM Department has developed a Risk Management Methodology based upon best practices that will be used to determine what security measures can and should be deployed to best protect information.

mtCERT

The Malta Government network (MAGNET) computer emergency response team, mtCERT, was formed in 2000. The purpose of the team was to provide emergency response on security incidents that occur on the MAGNET. The team's constituency is defined as all the Maltese Government employees.

Since its inception, mtCERT has resolved a number of major virus attacks and was also involved in investigations of security breaches to the MAGNET.

In 2002, the team attended the first TF-CSIRT conference. Following that, with the help of JANET-CERT, mtCERT applied to become a Trusted Introducer (TI) accredited team. The application was accepted in January 2004.

The services offered by mtCERT are as follows:

- Constituency advice on well-known threats and security risks when using computer systems and how to protect systems against these risks;

- Alerts on new risks or vulnerabilities;

---

[12] National Information Society Advisory Council
http://www.miti.gov.mt/site/page.aspx?pageid=17

- Advice on what measures have to be taken to prevent identified threats;

- Provision of a central point of contact for assistance once a computer incident occurs;

- Provision of technical assistance and help to correct minor computer incidents; and

- Management of resolution of major computer incidents, co-ordinating both the incident resolution and the incident investigation.

Public/Private Initiatives

eTrust

MIIIT, in conjunction with the Chamber of Commerce, has launched eTrust. This scheme implements the Euro-Label in Malta. Euro-Label is the European electronic shopping Trustmark for consumers and retailers. The Label illustrates that:

- the company selling the product is reliable;

- the selling conditions are clear and available on the website;

- the trader respects laws on data protection and eCommerce; and

- the products will be delivered as specified when the consumer placed the order.

A dispute resolution procedure is in place if anything does go wrong during the transaction.

To be awarded the Euro-Label Trustmark, a trader must implement the European Code of Conduct for retail transactions. The Euro-Label organisation is responsible for ensuring that the trader adheres to this Code of Conduct.

6.0 SWOT/PEST Analysis

Political	**Economic**
Commitment to eSecurity at World Summit on the Information Society (WSIS) EU i2010 programme to enhance the European market through greater use of electronic communications Government drive to turn Malta into a centre of excellence for ICT Early adoption of a legal framework addressing the Information Society Drive for greater inclusion in eServices Strong eGovernment programme Significant effort in driving Electronic Identity Management programmes and related activities	Efficiency-related benefits associated with introduction of technology in our industry Financial loss due to poor risk preparedness Lack of user confidence Increased competitiveness of the Maltese ICT industry Potential for NIS industry to become a strategic sector for Malta Steep increase in demand for secure products and security-related products and services
Social	**Technological**
Importance of uptake of technology at all levels of society to ensure social inclusion Increasing societal dependence on ICTs for everyday activities: - Communications - Leisure activities, e.g. online gaming, video downloads, chats - Shopping Certain strata of society not familiar with internet technologies Increasing trend in negative impact of cybercrime on individuals: - Citizens and consumers may become 'vehicles' of attacks (botnets); - Identity theft, harmful content, fraud etc; - Grooming etc. Need to strike the right balance between NIS policies and civil liberties and fundamental human rights	Pervasiveness of ICT Continuous advances in technology; new opportunities but also new threats Convergence Use of commercial off-the-shelf products on the increase Interdependent devices and applications Move towards IP-based voice communications may facilitate invasion of privacy unless effective security measures are taken

Political

Use of information and communication technologies is an essential element in the drive to boost the global markets, both from a social and economic perspective. This was endorsed by supra-national organisations and individual jurisdictions worldwide, within the context of the global agenda for the Information Society as determined by the World Summit on the Information Society (WSIS) held in Geneva (2002) and Tunis (2005).

WSIS recognised eSecurity as one of the pillars of the Information Society. As a result of this, the Geneva Plan of Action includes an Action Line that is dedicated to eSecurity. The Tunis Commitment and the Tunis Agenda underline the importance of eSecurity and, in particular, the stability and security of the Internet as key contributors to the development of the Information Society at a global level.

The member nations stress that governments, as well as the private sector, civil society, the United Nations and other international organizations, should work together to increase confidence and security in the use of ICTs – this conviction has led to the creation of the Internet Governance Forum, see Annex A. Extracts of the salient points of the Geneva Plan of Action and the Tunis Agenda are included in Annex B. Other supranational organisations such as ICANN and GAC are also actively involved in the area of eSecurity.

From a European perspective, Information and Communications Technologies have, for a number of years, been deemed to play a vital role in Europe's continuing modernisation. ICTs were always seen as essential pillars underlying the European economic growth and wellbeing. The European political agenda set out in the Lisbon strategy – that is, the goal to create a competitive, sustainable and a socially inclusive Europe – largely depends on the take-up of secure and dependable ICTs across all sectors. This view is underlined in the i2010 Strategy for the Information Society and the EU Strategy for a Secure Information Society – "Dialogue, Partnership and Empowerment". The European commitment to eSecurity is further testified through the establishment of European Network and Information Security Agency (ENISA). ENISA is tasked to become a centre of excellence in the field of eSecurity. Annex C provides additional information regarding the European approach to eSecurity.

For a number of years, the Maltese Government has worked towards establishing Malta as a centre of excellence in ICT. One of its first initiatives was to draw up a set of "cyber-laws" covering electronic commerce, data protection and computer misuse. Further initiatives were consolidated in the National ICT Strategy published in 2003.

Another key thrust was the development of a strong eGovernment programme that is being continuously and incrementally enhanced to offer an ever-increasing number of services. The eGovernment programme is a key driver of the Information Society in Malta. It offers services to all strata of society and is therefore also a primary enabler of greater societal inclusion in the national Information Society. Recent surveys testify to the increase in popularity of these services with Maltese Internet users. It is, therefore, within this context and in recognition of the importance of security in eGovernment services, that Government is implementing a national eID project, which is further detailed in Annex G.

Government also established the National Information Society Advisory Council (NISCO), which comprises representatives of all stakeholder groups including the

private sector, NGOs, educational institutions and government agencies. NISCO enables debate and exchange of views on matters related to the information society. The input of stakeholders informs the national agenda for the information society.

Economic

In the EU, the eCommunications services sector continues to represent the largest segment of the overall ICT sector, accounting for 44.4% of the total value, up from 43% last year. The sector was worth €614 billion in 2005, €273 billion of which was derived from eCommunications services. Overall revenue growth remained strong at estimated levels of between 3.8% and 4.7%. The production and use of ICTs account for around 40% of productivity growth and one quarter of overall growth in Europe[13]. It is a highly innovative sector, responsible for more than a quarter of the total European R&D effort and capable of creating growth and jobs.

The emergence of eServices has resulted in greater inclusion through increased accessibility and an enhanced quality of life for all European citizens. Moreover, enterprises have invested in ICT for different reasons: to increase sales and market share, to improve efficiency of internal business processes, or to reduce costs through eProcurement.[14] This investment allowed businesses to reap substantial economic benefits and increased competitiveness.

However, there is a preoccupying tendency of some businesses to keep back from investing in new technologies due to lack of confidence in the security of these technologies.

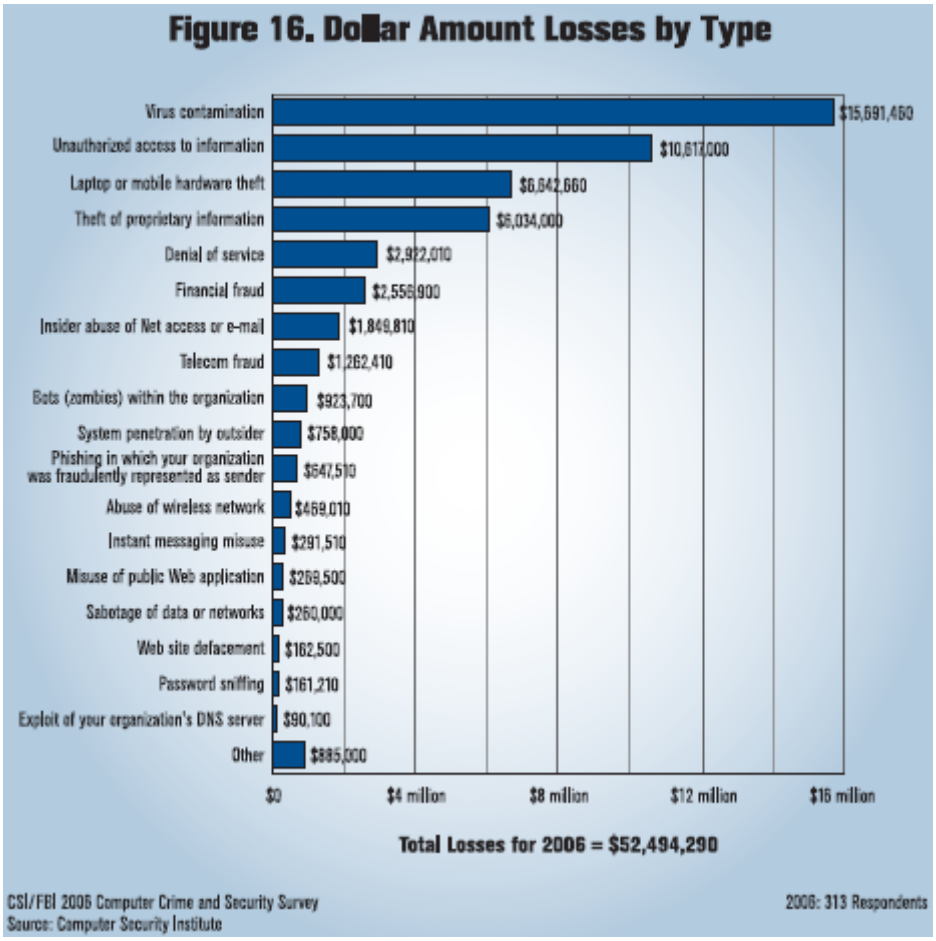
Security breaches could undermine the economic benefits resulting from the use of ICTs. Statistics show that the financial loss resulting from poor risk preparedness has, in some cases, also led to bankruptcy. The CSI/FBI 2006 Computer Crime and Security Survey[15] gives the following estimates of financial losses caused by various types of security incidents:

---

[13] European Electronic Communications Regulation and Markets 2005, 11th Implementation Report - COM(2006) 68.

[14] Source: Information Society Benchmarking Report, 2005, available at: http://europa.eu.int/information_society/eeurope/2005/all_about/benchmarking/index_en.htm

[15] 11th Annual CSI/FBI Computer Crime and Security Survey 2006. This survey is carried out among a number of organizations member of the Computer Security Institute which are therefore considered 'security savvy'



The cost of disruption to business processes is difficult to quantify. The impact may range from nuisance (employee's productivity hindered for a few minutes) to more serious disruptions (e.g. when a corporate network is closed for repair; this is particularly harmful for organisations that rely on permanent availability of the networks 24 hours a day, 7 days a week) to loss of business opportunities[16]. One has to take into account collateral damage as well, in particular the impact of negative media coverage on the corporate image.

Sustained use of eServices is highly dependent on user confidence. A single security breach could undermine the trust a consumer has in eServices in general, with long-term negative economic impacts for the demand side of the eServices equation.

It is anticipated, indeed desired, that public and private sector organisations will become more appreciative of the benefits to be gained through the deployment of secure ICT solutions. This, in turn, is expected to drive the demand for secure ICT products and security-related products and services. As a result, the European Commission anticipates that the network and information security industry is set to become a strategic sector at a European level. The local industry should also gear up to be ready to meet this expected surge in demand.

16 "Security Breaches and the Cost of Downtime", a report by Endforce Inc., 2004.

Social

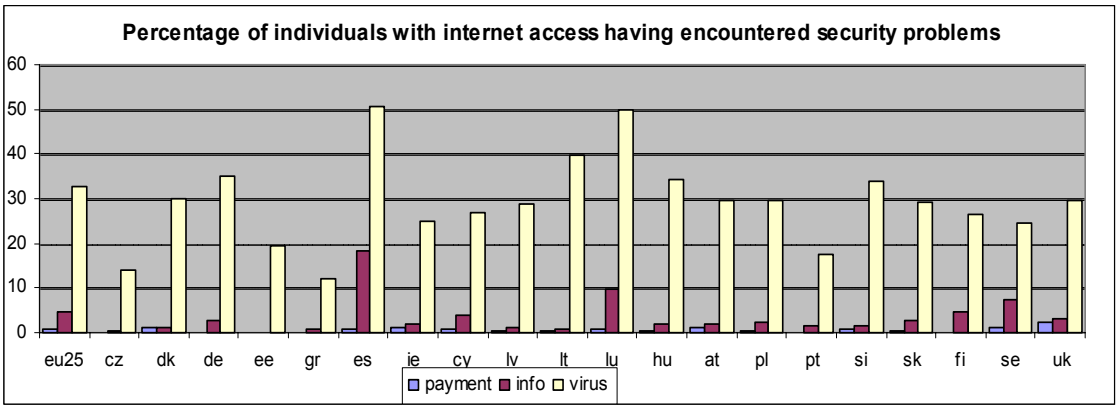
The impact of ICTs on our social lives is undisputed. Governments are increasingly relying on these technologies to combat social divides. ICTs play an essential role in meeting the demand for health and social care and in supporting the state-of-the-art and innovative provisioning of essential public and private services such as education, learning, national security, energy, transport and environment.

For younger generations, and increasingly older generations as well, ICTs represent an essential utility in all their activities being study, work or leisure. In particular, peer-to-peer, instant messaging, online games and mobile phones feature quite highly in their daily lives.

Information, processed and transmitted over electronic networks, including the Internet, has become a strategically important, integral part of everyday social life. ICT and communications networks are now becoming ubiquitous utilities in the same way as electricity or water supply already are, underpinning many social activities, but also introducing unknown interdependencies. The security of electronic communications networks and information systems, in particular their availability, is therefore of increasing concern across the globe.

However, any security plan is as strong as its weakest link, which all the more often happens to be unknowing members of the general public. Studies show that there exists a generational gap in the level of ICT knowledge and competence. This could undermine the general efforts devoted to NIS. Security threats have emerged where an end-user could unwittingly become the 'vehicle' for an attack where his or her PC would be compromised and used to perpetrate an attack on other computer systems, sometimes for criminal ends.

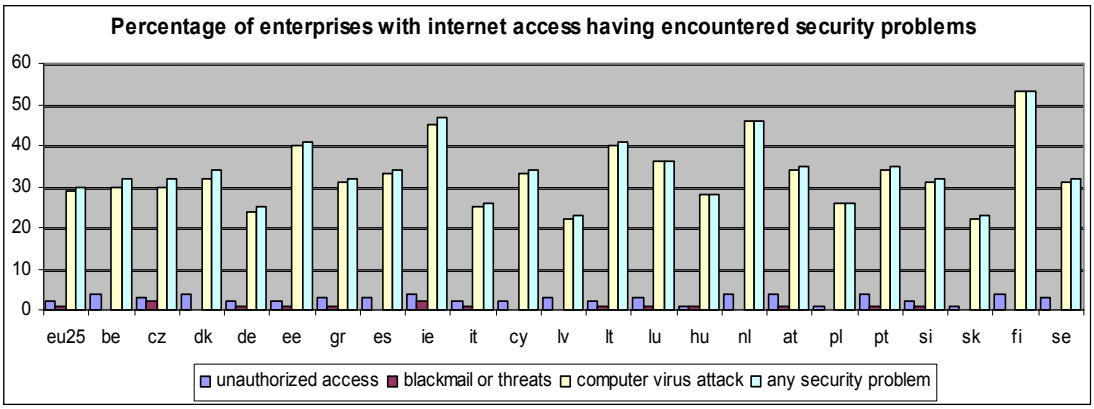
The following data from Eurostat[17] shows the percentage of European citizens and businesses with an Internet connection having encountered security problems during the year 2004. The graph shows that viruses represent the most important security problem which EU citizens are confronted with. More than 30% of EU citizens reported a virus in their computer.



The same situation holds for enterprises: around 30% of EU enterprises with Internet access were attacked by a virus in 2004. 2% reported unauthorized access.

---

17 The data can be accessed at: http://epp.eurostat.cec.eu.int/



Reportedly, a new computer connected to the Internet without a firewall and virus protection will be taken under control by hackers within a few minutes[18].

As highlighted earlier on, security breaches are no longer the domain of computer geeks intent on displaying their technical virtuosity. The exploitation of vulnerabilities is increasingly used by cyber-criminals to perpetrate their criminal affairs, which could range from paedophilia to identity theft to fraud.

With the growing deployment of eCommerce, eBusiness and eGovernment services, more and more personal data is transferred via electronic communications networks. This, in itself, could increase the risk of ID theft if the data is not sufficiently secured. In addition to eavesdropping during transmission or unauthorised access to network storage systems, *phishing* also carries the threat of ID theft.

In most cases however, security policies implemented might restrict users' ability to perform certain tasks: for example, one could have limited download capabilities or else, innocuous emails might be blocked by mail filters. This could be construed as a limitation of one's freedom and therefore creates the need to ensure that any NIS policies in place respect civil liberties and protect the individual's fundamental rights.

Technical

According to the OECD[19] report published in 2004, '*a number of factors are likely to contribute to continuing vulnerability over the next few years, among them:*

- *The introduction of entirely new and potentially more destructive forms of malicious code and cyber attacks;*

- *The proliferation of new web applications, many of which have relatively straightforward remote accessibility that is easy to exploit;*

- *The spread of (often unauthorised) use of instant messaging applications and peer-to-peer applications;*

- *The growth of mobile devices with always-on connectivity and remote access to critical sensitive data.'*

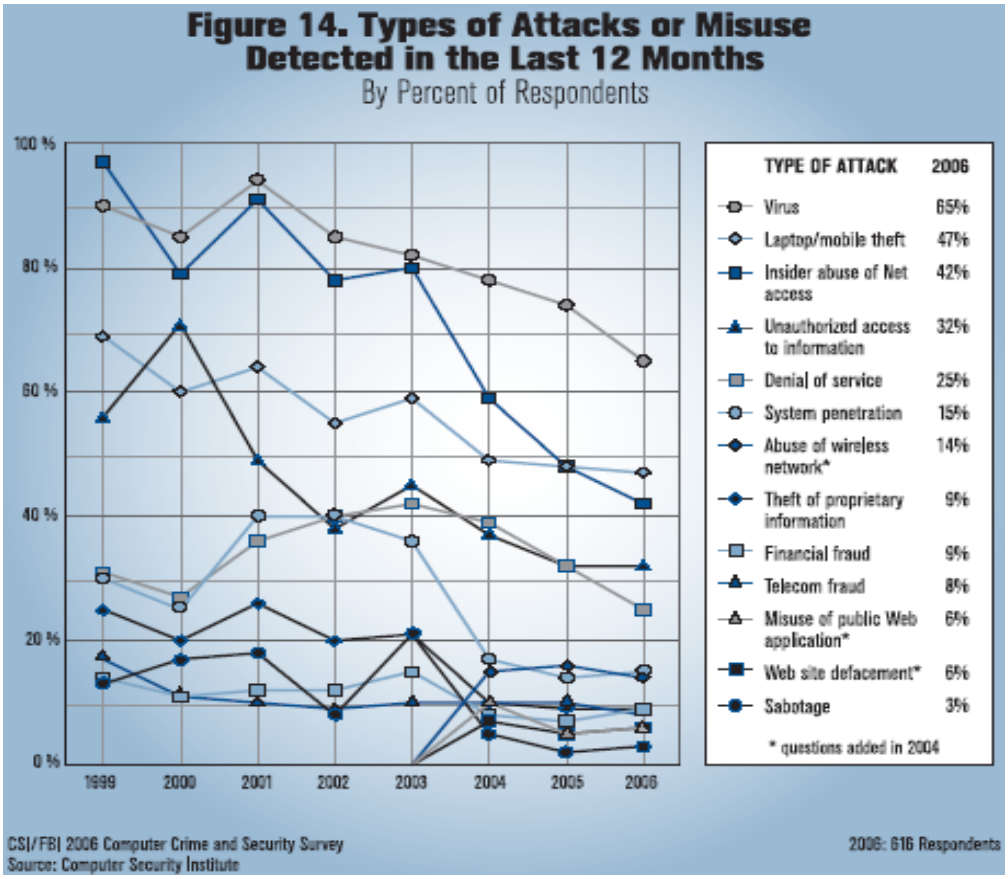
---

[18] See e.g. results of an experiment conducted in the US in 2004 available at: http://www.freerepublic.com/focus/f-news/1291394/posts.

[19] "The Security Economy", OECD, 2004.

Some countries already had to face threats arising out of these trends.

In addition, an interesting change in the "threat landscape" is currently taking place[20]. A couple of years ago, most security problems were reportedly caused by viruses and worms. However, the CSI/FBI 2006 Computer Crime and Security Survey shows that this trend is slowly being reversed as can be seen from the graph below:



Nearly all categories of attacks or misuse are in decline in the interviewed organisations. However, there have been some small increases in attacks involving financial fraud, system penetration, sabotage, website defacement and misuse of public Web applications. Attacks involving unauthorized access to information and theft of proprietary information were reported at virtually the same levels as reported for 2005.

Technological innovations are unrelentingly presenting us with significant opportunities. As a result of prevalent market forces, network operators are moving towards network and service convergence, deployment of emerging wireless technologies, adoption of open standards and increased use of commercial off-the-shelf packages. These developments have led to greater interoperability at all network levels and have given end-users the possibility to access any service, at any time, at any place, using any device. This creates more choice for consumers and increased competition in the market.

---

[20] Symantec Internet Security Threat Report, Volume VIII, trends for January 2005 – June 2005, published in September 2005.

However, these technological advances have also given rise to new threats. Moreover cyber criminals are constantly searching for new breaching methodologies. It is therefore a major technical feat to maintain state-of-the-art networks and ensure adequate protection levels for all users.

Strength	Weaknesses
High usage of communication technology Small community High-level of investment by government Clear political will MAGNET – Public infrastructure resident on one network A modern set of technology-neutral laws covering cybercrime, data protection and eCommerce	Level of awareness generally poor Reluctance to inform competent authorities of security breaches Low levels of expenditure for eSecurity Industry comprises mainly of micro enterprises having less resources to deal with eSecurity issues Insufficient statistical data on eSecurity incidents in Malta A large number of ISPs with small subscriber bases No CERT type services directed at private industry Fragmentation of competencies[21] Government dependence on a single network Lack of trained personnel and absence of certifications for personnel
Opportunities	**Threats**
Increased uptake of online services Strong eGovernment programme eID project Population generally willing to embrace technology Small community – national awareness campaigns should be more effective Industry comprises mainly of micro enterprises where security risks could be addressed without significant effort A large number of ISPs leaving room for differentiation on the basis of quality of service Malta's geographical characteristics render it ideal to be used as a test bed for eSecurity products	Evolving cybercrime activity Difficulties in keeping up-to-date with technological advances and changing patterns in security issues Risk-taking culture

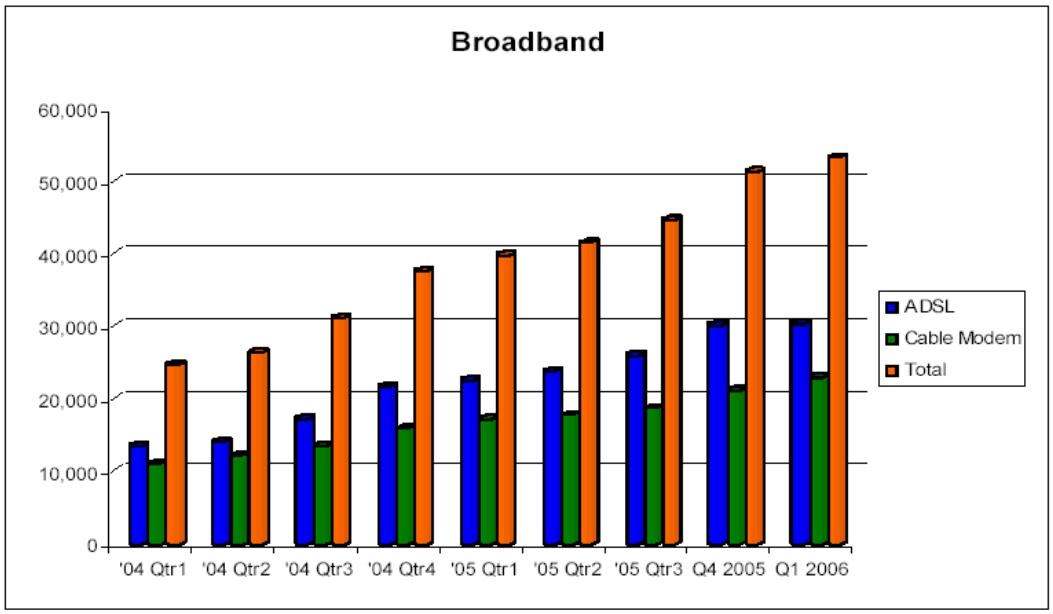
[21] A list of agencies / authorities having competencies in matters related to eSecurity is included in Annex F.

The local scenario presents particular nuances that can be leveraged when addressing eSecurity issues:

Strengths

As testified by the available statistics, the uptake of ICTs and eServices in Malta is considerably high and tends to increase year-on-year.

The small size of the nation facilitates the deployment of new and innovative technologies, which the general public seems generally keen to embrace.



Broadband uptake since 2004

In this regard, Government is leading by example through the significant investment in technology, coupled with a keen attention to security.

MAGNET, the government-owned infrastructure supporting all Government IT systems, is a major strength in relation to eSecurity. Significant effort was dedicated to network design and implementation to ensure optimal security in the network operation. The setting up of mtCERT and the risk management programme ensure that the network is adequately safeguarded. In this regard, Malta faces significantly less complexities in securing the public infrastructure, since this is not fragmented and under the control of different entities, as is the case in other jurisdictions.

Government also paved the way for secure use of information and communications technology by adopting a comprehensive set of technology-neutral laws covering cybercrime, data protection and eCommerce.

Opportunities

MAGNET forms the basis for the eGovernment services which, as indicated earlier, are registering increased usage as time goes by, with the most popular services being online payments and certificate services. These developments were the main driving force behind the electronic identity management (eID) project, which is further detailed in Annex I.

The eID project offers a number of opportunities for Malta. In deploying the eID, Malta can avoid pitfalls encountered by other jurisdictions that adopted PKI technologies some years ago. Malta can also use the initiative to showcase its potential as a test bed facility and to drive the European initiative for interoperable European eID services. This will contribute further to the development of broad-based national competencies on eSecurity, while ensuring secure use of those services that will be accessible using the eID.

The structure of the local economy is also seen as an opportunity with regard to eSecurity. The Maltese economy is mainly composed of micro enterprises that do not operate complex ICT systems and should be able to secure their operations effectively, without having to incur prohibitive costs.

This reality, coupled with the fact that micro-enterprises generally establish a single relationship with a service provider for all their technical needs, should also encourage ICT service providers to consider the provision of security related services as an additional basis for differentiation and competition in the ICT services market.

Malta's size renders it a very attractive proposition to have enterprises wishing to test bed innovative technologies on security services.

It is universally recognised that the main requirement in achieving true security is the creation of a culture of security. The Maltese population is effectively a small community and this characteristic should facilitate the design and implementation of effective national education schemes and awareness-raising campaigns.

Weaknesses

Despite the fact that physical security is today practically on every organisation's agenda, the same cannot be said of measures related to eSecurity, notwithstanding the relatively high level of technology uptake.

Qualitative and quantitative information available so far points to a relatively low level of awareness of cybercrime and network and information security issues. Anecdotal evidence suggests that this is not only true of the general public, but is also true of small enterprises.

There are also indications that where sufficient awareness does exist, micro-enterprises do not feel that they have the resources to tackle eSecurity effectively. This is further compounded by the lack of training programmes available on eSecurity matters.

Statistical data on perceptions and beliefs, precautionary actions taken and eSecurity incidents in Malta is only scantily available. In particular, there is no concrete data on either the costs incurred by companies as a result of security breaches, or the investments made by local enterprises in eSecurity.

This lack of publicly available information on the subject seriously hampers the national debate on eSecurity. It can preclude interested actors from adopting awareness-raising campaigns that effectively address national realities. Lack of information on the impact of security breaches also makes it very difficult for enterprises, in particular SMEs, to justify any investment in security equipment and services.

It is acknowledged that, in most cases, ICT users do not report security incidents and the implications these have on their activities. Enterprises, in particular, are generally wary of the possible negative publicity associated with security breaches. Members of the general public, on the other hand, might not see the benefit of such a report.

As in most jurisdictions, there is significant fragmentation of competencies in the area of eSecurity, given the horizontal nature of the subject. This creates a layer of complexity when addressing eSecurity at a national level.

In particular, the fragmentation of competencies hampers communication. This may lead to duplication of work or, worse still, to lacunas in addressing the relevant issues.

The existence of only one CERT offering services primarily to government entities and employees is considered to be a weakness as it is important that *all* organisations are provided with such services at a local level.

Threats

As we have seen, there is evolving and increasing cybercrime activity worldwide, leading to significant challenges in keeping up with the technological advances and changing patterns in security issues.

To further compound these threats, the Maltese society is generally known to embrace a risk-taking culture.

The ever-changing ICT environment demands regular legislative reviews. Apart from changes to computer misuse and child abuse laws, Malta has yet to ratify the Cybercrime Convention (2001) that is necessary for law enforcement to investigate cybercrime.

Scams, phishing and spam are still a daily feature of life on the Internet. Despite the publicity surrounding these forms of attack, Maltese Internet users are still susceptible to such crimes. Evidence from cases investigated by the Cyber Crime Unit and statistics available point to the following realities:

- Consumers lack basic precautionary skills that are advisable when purchasing over the Internet;

- Home users are still not conversant with basic safety measures such as anti-virus software, firewalls and anti-spyware software, thus exposing their equipment to unnecessary risks. Recent experiences confirm that such users are being targeted for planned 'bot' attacks against international targets.

- Parents and minors are still unaware of the perils related to unmonitored internet use. Minors, quick to adapt to new technologies, are being targeted by individuals who are ready to exploit such situations.

7.0 Strategies and priority areas

The preceding discussion highlights a number of priority areas that the strategy needs to address. In order to effectively deal with these, the following guiding principles are being adopted:

Adopt fully integrated and collaborative approaches

To date, eSecurity-related initiatives have generally been developed in collaboration between a number of, but not all, stakeholders involved. This approach may result in an element of duplication and missed opportunities that can be avoided.

Do not re-invent the wheel

It is important that Malta draws upon, amongst others, the expertise of ENISA which has been established specifically to provide support to Member States in all aspects of eSecurity and which has already produced very valid documents that draw upon the experience of other Member States on the subject.

Base strategic actions on a sound situational analysis

Effective strategies must be based on a detailed understanding of the gaps to be addressed. A prerequisite therefore is sound, up-to-date and relevant statistical information on security issues encountered in Malta, security practices adopted and knowledge levels across the various strata of society.

In this regard, it is proposed that an ongoing programme of data collection related to security is established and that the first phase of the strategic planning programme should include an extensive data collection exercise.

7.1. Creation of a culture of security in Malta

The National Minimum Curriculum

The National Minimum Curriculum already places great emphasis on the need for Maltese students to be well versed in the use of information and communication technologies, with the aim of ensuring that the next generation is well positioned to benefit and contribute to the Information Society. It is recognised that, in order to achieve these objectives the national curriculum needs to adopt a holistic approach to eSecurity and achieve a minimum threshold of knowledge on the secure use of ICTs.

Education at the Tertiary Level

In this context, at an enterprise level, it is imperative that not only security specialists but also entrepreneurs, people in top management, as well as professionals, come to recognise that eSecurity can no longer remain solely the remit of the technical manager. ESecurity needs to come to be seen as an asset to any organisation, rather than a burden. It is also recognised that adequate eSecurity in an organisation can only be achieved if security measures are actively supported by all members of the organisation in question. For this to be possible, employees in all levels of the organisation need to be conversant with

these issues and appreciative of the serious implications of failure to respect security procedures.

The inclusion of security-related subjects in the curriculum of relevant tertiary level courses, complemented by the availability of specialist courses in the field of security is therefore essential.

It is being proposed that this strategy will ensure the provision of ongoing support to the education institutions, with respect to the integration of eSecurity aspects at all levels of education.

Training programmes and Awareness-Raising Campaigns

In achieving the goals of the eSecurity strategy it is clear that all levels of society need to be well informed on security risks which are present in the on-line environment and how to address these.

Investing in the formal education of our children and youths will lay the groundwork that will enable the next generations to address tomorrow's needs. Therefore, the education system can contribute directly to the attainment of the long-term objectives of this strategy. However, a number of targeted initiatives are needed in the short-to-medium term to address the knowledge and cultural gaps that exist today in the Information Society. It is inevitable that the threats that we face tomorrow will be considerably different from those we are dealing with today. ESecurity must therefore necessarily become a matter of lifelong learning.

Lifelong learning requires a supply of training programmes for the workforce, as well as a demand for such programmes. Demand for such programmes will only materialise with sufficient awareness of the risks associated with poor security practices and more so, with an appreciation that effective security management adds value to any organisation. Supply of training programmes will inevitably follow demand. Encouraging and aiding representative institutions and chambers to carry out such programmes will also help ensure that SMEs have proper access to them.

It is proposed that an ongoing awareness-raising campaign targeting three main societal groups (these will, as indicated earlier, be validated and fine-tuned on the basis of statistical data gathered) should be elaborated and implemented:

- ***Private sector – especially Small & Medium Size Enterprises SMEs/Micro enterprises;***
- ***General public – in view of increased online trading;***
- ***Children, youths, teachers and parents.***

The awareness campaign should amongst others seek to secure the availability of resources[22] for users, specifically parents, teachers and internet/mobile providers providing sensible, helpful and reliable advice and information about potential problems, dangers and threats present

[22] A wealth of such resources has already been developed both in Malta and abroad and the strategy should make us of material which is relevant to Malta.

on the Internet and ways in which users can act to minimise or avoid these problems.

7.2. Effective prosecution of cybercrime

The cybercrime sub-group of the eSecurity Working Group has already identified a number of tasks that need to be undertaken with respect to cyber crime legislation. These include.

- The ratification of the Cybercrime Convention (2001), which lays out specific instruments that will help law enforcement during the investigations of cybercrime.

- A review of computer misuse legislation to consider whether this should require the complaint of an injured party before the police take action.

  Existing computer misuse legislation allows the police to investigate and prosecute ex-officio. Although this provides the police with an opportunity to investigate without a request from the injured party, in the long term, this is proving to be an obstacle by discouraging victims to speak out in an attempt to avoid adverse publicity.

- The introduction of legislation that identifies critical infrastructure and provides the minimum security requirements necessary to prevent pre-determined and targeted attacks.

- Legislative amendments to ensure effective prosecution of child abuse. Changes include:

  - The introduction of 'grooming' as a distinct and specific offence.

  - A review of article 208a of Chapter 9 of the Laws of Malta that would separate the act of possession from the act of manufacturing and distributing child pornographic material. The latter should carry a harsher penalty.

  - The introduction of legislation providing against the downloading, procurement and offering of child pornographic material.

  - Introduction of legislation safeguarding against the possession, distribution and manufacture of 'child erotica'.

  - Introduction of legislation that safeguards against the possession, distribution and manufacture of any computer generated image, sketch or drawing, story and cartoon that depicts child pornographic material.

  - Introduction of legislation that prohibits subscription to child pornographic material and erotica-related web pages.

  - To provide law enforcement with necessary legislative tools to allow for covert online operations, real time investigations and active pursuit of internet uses with specific interest in minors.

It is proposed that the strategy will ensure that this legislative review is undertaken at the earliest and that the institutional structures necessary

to ensure that cyber crime legislation is updated as necessary and effectively enforced are in place.

7.3. Secure use of ICTs by eGovernment and businesses

CERTs

Today mtCERT is the only CERT operating in Malta. There are no local CERTs targeting the private sector. It is proposed that this strategy will establish mechanisms for providing CERT type service to key constituencies such as:

- Academia
- Industry
- Small & Medium Size Enterprises (SME)

One consideration to bear in mind is that, given the size of our organisations, having a number of CERTs in place targeting different constituencies is possibly inefficient.

It is proposed that the strategy will evaluate models for improving information dissemination and make the most effective use of the services already available.

Information sharing

The gathering, analysis and sharing, amongst all stakeholders, of information related to eSecurity vulnerabilities, threats, incidents, best security practices and solutions, is critical to the management of online security.

In particular MITTS Ltd, as well as the larger enterprises operating in Malta, could help in disseminating best practice amongst other, possibly less well-resourced enterprises, without incurring any significant additional costs.

Such a framework could be organised as an offshoot of NISCO, where all stakeholders are already represented. The key success factors of such an initiative are expected to be real value added to SMEs at minimal time and resource investment.

It is also recognised that the involvement of representative institutions and chambers, in particular with respect to regulated professions, in this process of information sharing and awareness, would ensure that the desired outcomes are better achieved.

It is being proposed that a framework for networking and information-sharing between members of the various communities be established as a means of raising the level of security at an enterprise level.

eID Management and Authentication

With the advent of eCommerce, eID management and authentication become particularly crucial for the continued development of the sector. Interoperability of these systems is currently at the centre of considerable debate worldwide.

It is being proposed that the Strategy will analyse the possible synergies of private organisations and government in this area.

Best practice guidelines

Another simple but effective means of raising security levels is the development of best practice guidelines, tailored to fit local needs. Ideally, these would be developed by industry, with a particular focus on SME needs. Organisations might for instance seek to adopt internal policies in line with international standards such as ISO 17799 and ISO 27001.

Guidelines regarding proper risk assessments are also considered key to ensuring that industry implements effective measures that are adequate but not over-burdensome, both economically and in their implementation.

It is suggested that the national strategy should ensure the dissemination of best practice guidelines.

Critical Information Infrastructure Protection

The outcomes of the sub group on Critical Information Infrastructure Protection, established under the eSecurity Working Group will be integrated into this strategy.

It is being proposed that a formal framework for Critical Information Infrastructure Protection be established as part of the national strategy for eSecurity.

Incentives

As indicated earlier the Maltese economy is mostly composed of micro enterprises. It is proposed therefore, that the strategy will focus primarily on such undertakings.

The Strategy will consider what incentives, not necessarily financial, can be provided to SMEs who implement security measures associated with their use of ICTs.

7.4. Effective institutional arrangement to address eSecurity

It is evident that most of the initiatives emerging from the strategy will be ongoing and will need to be monitored, reviewed and updated on a regular basis.

Currently, the eSecurity working group is entrusted with this role, however the Group does not have an executive function and is not in a position to directly implement any of the initiatives arising out of the strategy.

A number of actions to be taken as part of the strategy fall exclusively within the executive remit of specialised agencies (e.g. MITTS has the responsibility for the security of Government's network, the MCA has responsibility for the public electronic communications regulatory framework), whereas other activities, such as critical information infrastructure protection and awareness raising, have a cross-sectoral reach. In both cases, however, actions at a national, and international level need to be coherent and coordinated. Annex F includes a list of local institutions having eSecurity related competencies.

Given this scenario, it is felt that an independent institutional structure with the necessary mandate to coordinate the activities of a large number of distinct organisations, to provide independent advice and education on managing access to online content, as well implement nationwide initiatives of a cross-sectoral nature, is required.

It is proposed that the strategy will address the question of institutional structures with a view to ensuring an effective ability to address national eSecurity on an ongoing basis.

8.0 Next Steps

This call for input will run until the end of March 2007.

This will be complemented by a series of working meetings with interest groups to be held during the 1st Quarter of 2007, with a view to soliciting direct feedback on the topics raised in this paper and any other matters that the interest groups may consider relevant to the subject in hand.

During this period, a first data-gathering exercise focusing exclusively on security issues will also be undertaken.

The Detailed Strategy and Action Plan will be developed on the basis of input received in response to this call and the feedback provided at the above-mentioned working meetings. This will be published for consultation in the beginning of September 2007, with a view to adoption of the strategy early in 2008.

9.0 Consultation Framework

The eSecurity Working Group invites comments from interested parties regarding this Consultation Paper. The consultation period will run until 16:00hrs on Friday 30th March, 2007. Comments should be sent to:

Celia Falzon
Core Team Member
National eSecurity Working Group
Valletta Waterfront
Pinto Wharf
Valletta VLT 01
Malta

Tel: +356 21 336 840
Fax: +356 21 336 846
Email: cfalzon@mca.org.mt

Written representations will be made public unless respondents request that their submission remains confidential.

Annex A: Supra-national organisations addressing eSecurity

The following is an overview of those supra-national organisations that play a direct role in eSecurity as well as those initiatives that are laying the groundwork for action at an international level.

The United Nations and the World Summit on the Information Society (WSIS)

In December 2001, the UN General Assembly endorsed the World Summit on the Information Society (WSIS) that was held in two phases. The first phase took place in Geneva in December 2003 and the second phase took place in Tunis, in November 2005.

The objective of the first phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake. The second phase was intended to put the Plan of Action developed in Geneva into motion.

The Partnerships for Global Cyber-security Initiative

The Tunis Agenda requested the ITU to act as a facilitator in implementing the WSIS Action Line on eSecurity. As a result, the ITU has initiated the Partnerships for Global Cyber-security Initiative.

This Initiative is currently focusing on three main areas:

National Strategies: The development of a generic model framework or toolkit that national policy-makers could use to develop and implement a national cyber security or CIIP (Critical Information Infrastructure Protection) programme.

Legal Frameworks: Capacity-building on the harmonization of cyber crime legislation, the Council of Europe's Convention on Cyber-crime, and enforcement.

Watch, Warning and Incident Response: Information sharing of best practices on developing watch, warning and incident response capabilities.

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN is responsible for the global coordination of the Internet's system of unique identifiers. These include domain names (like .org, .museum and country codes like .mt), as well as the addresses used in a variety of Internet protocols. Computers use these identifiers to reach each other over the Internet. Careful management of these resources is vital to the Internet's operation, so ICANN's global stakeholders meet regularly to develop policies that ensure the Internet's ongoing security and stability.

Within ICANN's structure, governments and international treaty organizations work in partnership with businesses, organizations, and skilled individuals involved in building and sustaining the global Internet. Innovation and continuing growth of the Internet bring forth new challenges for maintaining stability. Working collectively, ICANN's participants aim to address those issues that directly concern ICANN's mission of technical coordination.

An international Board of Directors, which oversees the policy development process, governs ICANN. Over eighty governments closely advise the Board of Directors via the Governmental Advisory Committee.

Governmental Advisory Committee to ICANN (GAC)

In setting up ICANN, it was acknowledged that the world is not uniform. Each country and distinct economy has different laws, different attitudes, and different policies. The Governmental Advisory Committee to ICANN was established in order to ensure that ICANN incorporates these diverse views in its activities. Participation in the GAC allows countries and distinct economies to influence policies concerning the management of the Domain Name Server (DNS) and related functions, which are important to the overall operation of the Internet.

Internet Governance Forum (IGF)

One of the outcomes of the WSIS was a mandate to set up the Internet Governance Forum. The Forum comprises representatives of governments, intergovernmental organizations, the private sector and civil society and includes various technical and academic communities.

The first meeting of the group took place towards the end of October 2006. The mandate for this forum covers a number of topical issues, including:

- Public policy issues related to key elements of Internet Governance in order to foster the sustainability, robustness, security, stability and development of the Internet;

- Exchange of information and best practices;

- Identification of emerging issues;

- Critical Internet resources; and

- The use and misuse of the Internet, particularly issues concerning everyday users.

European Network and Information Security Agency (ENISA)

At a European level a number of initiatives are underway in the field of eSecurity, both from a standardisation point of view, as well as from a policy and institutional perspective. In 2004 the European Network and Information Security Agency (ENISA) was set up with the aim of giving advice and recommendations to the European Commission and the Member States, to conduct data analysis, as well as to support awareness-raising and facilitate cooperation between EU bodies and Member States, using its expertise to stimulate cooperation between actions from the public and private sectors. Building on national and Community efforts, the Agency aims to become a **Centre of Excellence** in this field.

Among other things, the Agency provides assistance to the Commission and Member States in their dialogue with industry regarding security-related problems in hardware and software products. The Agency also follows the development of standards, promotes risk assessment activities and interoperable risk management routines by the Member States and produces studies on these issues within public and private sector organisations. It has already published a number of documents of value to this national strategy, in particular 'A Step-by-

Step Approach on how to Set up a CSIRT' and 'A User's Guide: How to Raise Information Security Awareness'. A brief overview of ENISA's strategy for the next 5 years is provided below.

Overview of ENISA Strategy 2007 - 2010

This strategy lays down the strategic orientations for ENISA for the coming years. It serves as the Agency's guideline for the development and implementation of activities, as defined in its annual Work Programme and Communication Strategy and the Communication Action Plan.

ENISA's contribution to the European objectives is focused on four domains.

- **Raising awareness and building confidence**

In the light of the generally poor appreciation of security stakes by business and individuals, ENISA will strike to present a fair balance between the security threats, which the users must be aware of, and the safeguards, which are available and often easy to implement. The aim is to present network and information security not as a burden and constraint, but rather as a virtue and an opportunity, with the double prospect of helping citizens becoming more confident in what they are doing as users, and of giving the enterprises operating secure information systems a competitive advantage to the benefit of their consumers.

- **Facilitating the working of the Internal Market for eCommunication**

The overall objective will be to guarantee integrity and robustness of the European eCommunication systems and also to provide European users with the best conditions of usage.

- **Mastering emerging technologies and services**

A natural tension exists between the networking community, which strives to create complex and heterogeneous systems, and the security community, wishing to take enough time to be able to identify, in depth, potential new risks and the corresponding safeguards. A general objective will be to strengthen the R&D capacity in Europe and to foster its position as a competitive supplier in products and services for network and information security.

- **Bridging security gaps in Europe**

A more common approach to the development of network and information security policies all over Europe will contribute to the effectiveness of each specific policy. The overall objective is to provide valuable material to help responsible authorities adequately define their specific IT security policies, justify the investment and control the evolution of the network and information security level in their environment.

A work programme for 2007 is currently being put together. This will start implementing relevant tasks related to these objectives.

- **Others**

This Annex has provided a brief overview of the key supra-national organisations and initiatives that contribute directly to the development and implementation of

international policy influencing eSecurity[23]. There are other organisations that contribute to the international debate on this subject, including the Organisation for Economic Co-operation and Development (OECD) and myriad specialised organisations and interest groups that deal with particular aspects of eSecurity, such as The Forum for Incident Response and Security Teams (FIRST), which is a global forum for CERTs.

[23] The European Union is also contributing directly to this debate through its Strategy for a Secure Information Society – "Dialogue, partnership and empowerment". This strategy was discussed in section 4.

Annex B: Extract from the WSIS outcomes

The United Nation's Plan of Action for eSecurity – The Geneva Plan of Action identifies confidence and security among the main pillars of the Information Society.

Under this Action line, the UN undertook to promote cooperation among governments at the United Nations and with all stakeholders at other appropriate fora to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.

The following key actions to be undertaken by governments, in cooperation with the private sector, were identified:

- prevent, detect and respond to cybercrime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective, mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.

- actively promote user education and awareness about online privacy and the means of protecting privacy.

- take appropriate action on spam at national and international levels.

- encourage the domestic assessment of national law with a view to overcoming any obstacles to the effective use of electronic documents and transactions, including electronic means of authentication.

- further strengthen the trust and security framework with complementary and mutually reinforcing initiatives in the fields of security in the use of ICTs, with initiatives or guidelines with respect to rights to privacy, data and consumer protection.

- share good practices in the field of information security and network security and encourage their use by all parties concerned.

- invite interested countries to set up focal points for real time incident-handling and response and develop a cooperative network between these focal points for sharing information and technologies on incident-response.

- encourage further development of secure and reliable applications to facilitate online transactions.

- encourage interested countries to contribute actively to the ongoing United Nations activities to build confidence and security in the use of ICTs.

In the Tunis Agenda, the United Nations further expressed its commitment with respect to eSecurity. The following is the relevant extract:

39. We seek to build confidence and security in the use of ICTs by strengthening the trust framework. **We reaffirm** the necessity to further promote, develop and implement, in cooperation with all stakeholders a global culture of cybersecurity, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks. This culture requires national action and increased international cooperation to strengthen security, while enhancing the protection of personal information, privacy and data. Continued development of the culture of cybersecurity should enhance access and trade and must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

40. We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. **We further underline** the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, *inter alia*, law-enforcement agencies on cybercrime. **We call upon governments,** in cooperation with other stakeholders, to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "*Combating the criminal misuse of information technologies*" and regional initiatives including, but not limited to, the Council of Europe's *Convention on Cybercrime*.

41. We resolve to deal effectively with the significant and growing problem posed by spam. **We take note** of current multilateral, multi-stakeholder frameworks for regional and international cooperation on spam, for example, the APEC Anti-Spam Strategy, the London Action Plan, the Seoul-Melbourne Anti–Spam Memorandum of Understanding and the relevant activities of OECD and ITU. **We call upon** all stakeholders to adopt a multi-pronged approach to counter spam that includes, *inter alia*, consumer and business education; appropriate legislation, law-enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation.

Annex C: i2010, the EU eSecurity Strategy and related activities

In June 2005, the European Commission launched the initiative "i2010 - A European Information Society for growth and employment"[24].

This strategy establishes an integrated approach to Information Society and audio-visual media policies in the EU. It seeks to facilitate digital convergence and to respond to the challenges associated with the Information Society, including those related to security.

One of the three main thrusts of the Strategy is the creation of a Single European Information Space, offering affordable and secure high-bandwidth communications, rich and diverse content and digital services.

With this objective in mind, the initiative identified the need for a safer internet as a key challenge. This is being addressed through the European strategy for a secure European Information Society. This strategy recognises that achieving this objective requires an effective legal framework aimed at ensuring the right level of security in public electronic communications networks and services.

It therefore set the scene for a review of the current legal provisions governing the security of public electronic communications networks and services. The current provisions and the proposed changes are discussed below.

The EU Legal Framework

The review of the current legal framework for security and privacy in electronic communications networks and services

The key provisions of the EU framework for security and privacy in public electronic communications networks and services are established in Directive EC/56/2002. This directive places a number of obligations on undertakings in the public electronic communications sector. It provides that a service provider must take appropriate technical and organizational measures to safeguard security, if necessary in conjunction with the network provider.

Furthermore, a service provider is require to inform subscribers of any possible breach to security that cannot be addressed through the measures taken directly by the service provider and the remedies available to the subscriber, as well as the likely associated costs.

In addition, the EU framework places an obligation on Member States to ensure the integrity of public telephone networks and the continued availability of fixed telephone services, even in cases of *force majeure*.

The European Commission recently published for consultation a set of proposals outlining proposed changes to this framework. It is to be noted that any changes adopted as part of this review are expected to become effective in Member States in around 2010.

[24] COM(2006) 173: i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All.

Proposed changes

The Commission is proposing that the updated framework would clarify what technical and organisational measures should be taken by service providers to secure their networks and services and strengthen the obligations on electronic communications to include:

- the implementation and maintenance of security measures to address security incidents and to prevent or minimise the impact of such incidents on customers and on other interconnected networks. The framework would include a liability clause for not taking appropriate security measures;

- an obligation to comply with any guidance issued by regulators in conformity with Community law on the practical implementation of such measures; and

- an obligation to include a specific clause in contracts with consumers, which would inform them of specific actions that could be taken in reaction to security/integrity incidents and in prevention of known security threats and vulnerabilities.

The consultation papers also propose that providers of electronic communications networks and services should be required to:

- notify the national regulatory authority of any breach of security that led to the loss of personal data and/or to interruptions in the continuity of service supply;

- and notify their customers of any breach of security leading to the loss, modification or destruction of, or unauthorised access to, personal customer data.

With respect to obligations related to network integrity, it is being proposed that these will be extended beyond the traditional public telephone network, to cover mobile and IP networks used for public services.

EU legal framework re SPAM

Directive EC/58/2002 also regulates unsolicited commercial messages. It prohibits the marketing by electronic communications to natural persons unless these have opted in to receive such messages. The regime covers not just email but also fax, SMS, MMS and others.

The Commission has established a Contact Network of Spam Authorities (CNSA) that meets regularly and uses online facilities to exchange best practices and cooperate on enforcement across borders.

The review of the regulatory framework for electronic communications discussed earlier will assess whether any additional regulatory provisions are necessary.

The 2001 Council of Europe Convention on Cybercrime

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

This subject requires Member States to make provision for the following offences to be punished by effective, proportionate and dissuasive criminal penalties:

- illegal access to information systems;

- illegal system interference (the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data);

- illegal data interference.

Electronic identification in the EU

Significant developments related to electronic authentication methods are taking place in the US and in a number of organisations, including the Transatlantic Secure Collaboration Program (TSCP) and the International Identity Proofing & Vetting Framework. A number of European Governments are already taking an active part in these activities.

The i2010 eGovernment Action Plan suggested a European electronic identity management (eIDM) framework, intended to lead to a single pan-European specification for interoperable eIDM.

The need for improved and interoperable electronic identity mechanisms is highlighted in the EU *Strategy for a Secure Information Society* of July 2006; identity theft is gaining an additional dimension, not only in Europe, but across the world, mostly in the light of the fight against illegal immigration, terrorism, and organised crime. In view of this, ENISA is also considering putting greater emphasis on Identity Management in its 2007 Work Programme.

Annex D: Overview of the international activities of the Cyber Crime Unit

Overview of the Cyber Crime Unit

The Cyber Crime Unit was officially launched in February 2003. Prior to the establishment of this unit, all incidents involving IT were handled by the Malta Police IT Services Section. The main objectives of the Cyber Crime Unit are to:

- Assist in the investigation of all crimes in which computer and computer systems are used as the target of an attack, and/or used as the medium to launch an attack on any entity;

- Be in a position to collect and preserve evidence and to present the same evidence before judicial authorities;

- Be in a position to provide a 24X7 level of support to international law enforcement agencies, either assisting in investigations or preserving evidence that would be required as evidence before a Court of Law;

- Monitor local Internet use to identify any potential production, dissemination/ collection of prohibited materials such as child pornography, race hate etc;

- Develop a network amongst the local IT industry striving to harness support in combating related crime and generating awareness amongst local communities, particularly safeguarding against possible targeting of young Internet users;

- Monitor and document any developments related to legislation that may be required on both the local and international platform.

The Malta Police Cyber Crime Unit is an active participant in a number of European Union and international law enforcement initiatives.

- Interpol – Malta has been an active member of Interpol since 1971. Since 2003 Malta is continuously participating in a drive to prevent the manufacture and distribution of child abuse images over the Internet. The Cyber Crime Unit is available 24x7 to ensure prompt and effective response to intelligence and information collected by law enforcement globally. A conference entitled "Interpol Conference on Information Technology Solutions to the Identification of On-Line Victims of Child Abuse" was hosted by the Cyber Crime Unit in Malta during September 2006. This was an important conference, bringing investigators from all Interpol members, to discuss and exchange new strategies, best practice and investigational tools.

- Europol – The Cyber Crime Unit cooperates with Europol in respect of high-tech crimes and child pornography. Police Officers from within the European Union share intelligence and coordinate initiatives, focusing on dismantling organised crime groups and activities.

- G8 High-Tech Crime – This agency facilitates communication between over 40 Member States allowing for rapid response in cases related to cybercrime incidents. The G8 High-Tech Crime Group also allows for exchange of expertise amongst law enforcement agencies.

- COSPOL – The COSPOL group, an initiative launched by the Chiefs of Police of the European Union, is focused on dismantling Internet user groups sharing child abusive material. The main role of the group is to coordinate and promote joint operations amongst its members. Malta has participated in a number of such joint operations. The Cyber Crime Unit hosted the COSPOL group in Malta in May 2006.

- The Unit has established a number of bilateral agreements, both formal and informal, which ensure that the Cyber Crime Unit has direct access to law enforcement resources and investigational tools. This reciprocal exchange of information and tools ensures that law enforcers are kept updated about new *modus operandi* and potential security risks.

Legislation

Specific computer misuse legislation was introduced in Malta during 2001 and is embedded within Chapter 9 of the Laws of Malta. Articles 337c and 337d of the Criminal Code outline the offences related to this category of crime. The legal framework is practically divided into two categories.

The first category deals with unauthorised access to, or use of, information. According to article 337c of Chapter 9, it is an offence whenever a person, without authorization, does any of the following acts:

a) uses a computer, or any other device or equipment to access any data, software, or supporting documentation held in that computer, or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;
b) outputs any data, software, or supporting documentation from the computer in which it is held, whether by having it displayed, or in any other manner whatsoever;
c) copies any data, software, or supporting documentation to any storage medium other than that in which it is held, or to a different location in the storage medium in which it is held;
d) prevents or hinders access to any data, software, or supporting documentation;
e) impairs the operation of any system, software, or the integrity or reliability of any data;
f) takes possession of, or makes use of, any data, software, or supporting documentation;
g) installs, moves, alters, erases, destroys, varies, or adds to any data, software, or supporting documentation;
h) discloses a password or any other means of access, access code, or other access information, to any unauthorised person;
i) uses another person's access code, password, user name, electronic mail address, or other means of access or identification information in a computer;
j) discloses any data, software, or supporting documentation, unless this is required in the course of his duties or by any other law.

The second category, article 337d of Chapter 9 of the Laws of Malta, safeguards against damage to computer hardware and makes it an offence for any person who without authorization:

a) modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network;

b) takes possession of, damages or destroys a computer, computer system, computer network, or computer supplies used or intended to be used in a computer, computer system or computer network, or impairs the operation of any of the aforesaid.

Any person found guilty of breaching any of the above provisions is liable on conviction to a fine (*multa*) not exceeding Lm 10,000, or to imprisonment for a term not exceeding 4 years, or to both such fine and imprisonment. However, when the act is detrimental to any function or activity of the government or any public service or utility, or is committed by an employee to the prejudice of his or her employer, then the punishment for such an offence is increased to a fine (*multa*) of not less than Lm 100 and not exceeding Lm50,000, or to imprisonment for a term from 3 months to 10 years, or to both such fine and imprisonment. This same punishment is also applicable when a person commits a subsequent or more offences.

One important aspect of Maltese legislation is that it has remained technology-neutral. This is important, given the ever-changing *modus operandi* used by computer-related crime offenders. The law is focused on whether the individual has sufficient authorisation to carry out any of the activities described above.

Article 208a of the Criminal Code, although not considered a cybercrime by its very nature, is relevant for the purpose of this document as it focuses on crimes related to child pornography. Although child pornography did not originate from computers or the Internet, there can be no doubt that recent technological developments have facilitated the creation and distribution of such material. Article 208a makes it an offence for:

> Any citizen or permanent resident of Malta, whether in Malta or outside Malta, as well as any person in Malta, to take or permit to be taken any indecent photograph, film, video recording or electronic image of a minor, or distribute or show such indecent photograph, film, video recording or electronic image, or be in possession of such indecent photograph, film, or video recording or electronic image.

If a person is found guilty of such an offence, then he or she is liable, upon conviction, to a fine (*multa*) not exceeding Lm200, or to a term of imprisonment not exceeding 6 months, or to both such fine and term of imprisonment. Aggravating circumstances shall increase the punishment to a term of imprisonment from 7 months to 1 year (with or without solitary confinement).

Annex E: National ICT Strategy

The national ICT strategy for the period 2003 - 2006 identified as one of its key objectives the need to make the Internet a secure place, build confidence, trust and security in the use of ICTs.

It identified the following tactical areas to be addressed over this period:

- Educate citizens and businesses on the basics of ICT security;

- Develop and disseminate a secure electronic communication scheme amongst businesses to safeguard consumer's privacy and protection of data transmitted;

- Set up a national eCrime Working Group to serve as a discussion platform for major stakeholders to work as a team towards achieving a safer online environment for everyone;

- Collaborate with major software developing firms to ensure more security in their systems;

- Facilitate the growth and potential of the Cyber Crime Police Unit to be able to serve the public better and ensure more security in the online environment;

- Establish a Hotline to deal with cases of Child Abuse over the Internet and act as a central point of contact for Internet-related queries for the young and their parents / guardians;

- Review and amend the existing cybercrime legislation to reflect the use of technology to complete illegal and harmful acts;

- Engage into a national campaign to combat the proliferation of spam and develop a national policy in this regard;

- Explore the feasibility of a unique national smart card and investigate the possible integrating biometric authentication mechanisms with the current authentication framework;

- Develop consumer trust in electronic commerce by deploying a national eTrust scheme providing trust marks to online retailers that meet the established standards;

- Educate citizens on the respect and protection of Intellectual Property Rights and take necessary measures to reduce the growth of software piracy in the country.

- A number of these tasks have been completed, while others are currently underway. These are discussed further on in this chapter.

Annex F: Institutions with eSecurity-related competencies

Government and the National Information Society Advisory Council (NISCO)	Comprises representatives of all stakeholder groups including the private sector, NGOs, educational institutions and government agencies. Enables debate and exchange of views on matters related to the Information Society. Provides input of stakeholders; informs the national agenda for the Information Society.
MIIIT	Policy development in matters related to the Information Society.
MCA	Implementation of the regulatory framework for electronic communications networks and services. Supervisory body for electronic signature certification services. Represents Malta on the GAC, IGF, HLIG and ENISA.
Infosec Authority	Develops national polices with respect to security of public information in line with EU norms.
MITTS	Provides ICT services to the Government of Malta and a number of public sector entities and national authorities.
Cyber Crime Unit	The Cyber Crime Unit was officially launched in February 2003. Prior to the establishment of this Unit, all incidents involving computers was handled by the Malta Police IT Services Section. The main objectives of the Cyber Crime Unit are to: Assist in the investigation of all crimes in which computer and computer systems are used as the target of an attack, and/or used as the medium to launch an attack on any entity, Be in a position to collect and preserve evidence and to present the same evidence before judicial authorities, Be in a position to provide a 24X7 level of support to international law enforcement agencies, either assisting in investigations, or preserving evidence that would be required as evidence before a Court of Law, Monitor local Internet use to identify any potential production, dissemination, collection of prohibited materials such as child pornography, race hate etc, Develop a network amongst the local IT industry striving to harness support in combating related crime and

	generating awareness amongst local communities, particularly safeguarding against possible targeting of young Internet users, Monitor and document any developments related to legislation that may be required on both the local and international platform. Represent Malta on the Interpol, Europol, G8 High Tech Crime Group, Cospol. The Unit has also concluded bilateral agreements with a number of counterpart organisations.
Office of the Data Protection Commissioner	Implementation of the legal framework for data protection.

Annex G: The National eID Initiative

Government has made significant steps in introducing eGovernment and in propagating the Information Society – it has, however, become very clear that this could only be done within a trustworthy framework that is complete with a secure mode of electronic authentication. The e-ID of the Citizen is an electronic version of the Identity Card. The e-ID was launched in 2004 to provide a basic homogenous authentication mechanism for all e-Government services. All ID Card holders are eligible to obtain an e-ID from any of a number of ever-increasing Local Councils that offer a registration facility from their offices.

E-ID has so far offered a basic level of secure authentication. The next level of authentication will be based on PKI Digital Certificates. The public key infrastructure will allow the citizen to literally hold a unique electronic key with which to access e-Government services, as well as sign electronic documents and emails. The infrastructure has been developed entirely for the Government of Malta by a local software company and made possible through Government's agreement with Microsoft. This infrastructure will be hosted by MITTS Ltd, who will act as Government's Certification Authority.

This Digital Certificate infrastructure is a fundamental element of the upcoming e-ID Card and e-Passports projects. The e-ID Card will replace the National ID Card with the next renewal due in 2007. The new e-ID Card will replace the current polycarbonate version, and will incorporate smart technology to offer a multitude of electronic services that will be loaded onto the card. The e-ID Card will also continue to serve as a valid travel document, by meeting the stringent security regulations that have been set for passports issued by EU Member States. PKI technology will also be used in the digital signing of e-Passports, which will also harness facial and fingerprint biometrics to produce the new generation of EU standard machine-readable travel documents.

The launch of Digital Certificates is only the tip of a broad Identity Management Strategy, whose vision is the creation of a secure identity framework for Government. Whilst the framework will respect Data Protection Legislation and norms, it will provide Government with the necessary harmonisation when processing applications and offering services to its citizens. This will be an important tool in combating social security fraud, amongst others, as well as ensuring that one's identity credentials are consistent in all Government systems and documents issued by the various departments (e.g. ID Card, Passport, Driving License etc).

Glossary

Botnet	Botnets refer to a collection of compromised machines running programs, usually referred to as worms, trojan horses, or backdoors, under a common 'command and control' infrastructure. Such compromised PCs could in turn be used to perpetrate fraud.
eSecurity	There is little agreement both nationally and globally on a formal definition of eSecurity. Different organisations hold varying views on scope of the term 'eSecurity' and quite often, it is used interchangeably with other terms such as 'Internet security', 'cyber-security' and/or 'IT security'. For the purposes of this paper, eSecurity encompasses security aspects of the information economy, including information systems and communications networks.
Malware	Software designed to infiltrate or damage a computer system, including computer viruses. Trojan horses, spyware and adware.
Phishing	Attempts to fraudulently acquire such information as passwords and credit card details by masquerading as the sender of an apparently legitimate email. Also known as "spoofing".
Spam	Unsolicited or undesired bulk electronic messages.
Spim	A type of spam where the target is instant messaging services.
Spyware	Spyware is software that is installed on a computing device and takes information from it without the consent or knowledge of the user and gives that information to a third party. Spyware may have additional negative impacts for the computer user, such as causing the computer to crash or run slowly.
Threat	A threat is a potential cause of an unwanted event which may result in harm to a system, information asset or organisation. Threats may arise from all hazards, including natural disasters or accidental or deliberate human acts. Threats are characterised in terms of source (who/what causes the threat) and target (what elements of the system etc. may be affected by the threat) and are assessed in terms of the likelihood of its occurrence.
Trojans	A trojan is a malicious program, disguised as legitimate software that installs itself on a computer and can cause harm once executed.
Vulnerability	Vulnerability is a characteristic (including a weakness) of a system, information asset or organisation that causes it to be susceptible to be exploited by a threat. Exploitation of vulnerability may cause harm to a system, information asset or organisation, and the business processes they support. The presence of vulnerability does not cause harm in itself as there must be a threat present to exploit it.

Worms	A worm is a self-replicating program that copies itself and spreads from machine to machine across the Internet, often damaging data in the process.
Zombie	A zombie is a computer that has been infected by a virus program that allows it to be taken over for remote use, without the owner's knowledge. The machine can then be used to send spam, for example. It has been estimated that this is the way most email spam is now transmitted.