MALTA | NATIONAL CYBER SECURITY STRATEGY GREEN PAPER

2015

MALTA | NATIONAL CYBER SECURITY STRATEGY GREEN PAPER

Supporting Document

mita
MALTA INFORMATION TECHNOLOGY AGENCY

Contents

List of Figures and Tables

Part One

Introduction

1 Purpose and Scope

This document aims to serve as background information and rationale for the strategic approach proposed within the Green Paper: National Cyber Security Strategy

It draws upon various published sources to assess cyber security:

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

(ii) From a domestic perspective, particularly with respect to

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

(iii) From a stakeholder perspective, as it is understood that apart from technology, cyber security impacts upon all of country's political, legal, economic and social well being. Hence, the document also identifies the strategy's stakeholders with their corresponding interest.

Part Two

The Global Cyber Threat Scenario

2 What is meant by a Cyber threat

A cyber threat is defined as:

> **The possibility of a malicious attempt to inflict damage or disruption within cyber space, through cyber attacks.**

It can be conducted, mainly through automated means, individually or corporately. A key characteristic of a cyber threat is its asymmetric nature. Thus, a cyber attack may be conducted:

- Anywhere, as long as there is digital interconnectedness
- In one vulnerable area, leading to potential attack into more well protected systems
- Instantaneously, leaving no time for an appropriate response to be mounted
- With very minimal traceability or detection, thus making it hard to locate response by the defence.

The following sections identify a number of cyber threats along with their perpetrators.

3 Cyber Threats and their Agents

The findings shown in this Section are based mainly upon the *Threat Landscape* drawn by ENISA for the year 2014[1].

3.1 THE CYBER THREATS

Table 1 identifies the top 15 threats, menacing cyber space by end 2014, ten of which are noted to be on the increase.

Top threat	Observed current trend
Malicious code	↑
Web-based attacks	↑
Web application/injection attacks	↑
Botnets	↓
Denial of service	↑
Spam	↓
Phishing	↑
Exploit kits	↓
Data breaches	↑
Physical damage / theft/ loss	↑
Insider threat	↑
Information leakage	↑
Identity theft/ fraud	↑
Cyber espionage	↑
Ransomware / Rogueware / Scareware	↓

Table 1 – Top Cyber threats for 2014

An explanation for each of the cyber threat identified is given below.

Malicious code

Over 50% of malware is undetected by antivirus solutions due to its dynamics, complexity, sophistication and stealthiness. Malware detections are also noted to be predominant in open environments, mainly academia and education (at 40%), where access to a variety of users, who do not necessarily maintain robust end-point security, is high.

Web-based attacks

The threat is especially predominant in web browsers and is potentially enabled by malicious URLs.

Web application attacks/ Injection attacks

The threat consists mainly of feeding vulnerable servers and/or mobile applications with malicious inputs or unexpected sequence of events so as to alter site content, breach information or inject malicious code. Cloud computing as well as mobile applications and unsupported Web software are seen as most likely victims of such a threat.

Botnet

A serious cyber threat, accounting for 34% of attacks and ranking first in attack statistics. Although the number of botnet-infected computers has decreased from 3.5 million to 2.3 million during 2014, mainly due to successful law enforcement activity, its decline cannot be taken for granted due to a noted increase in sophistication and stealthiness in the technology.

Denial of Service (DDoS) attacks

A threat that is evolving in sophistication, stealthiness and unpredictability. In most cases, DDOS attacks are noted to be launched in combination with other attacks as a means of distraction. The main objectives of collateral attacks assessed are: virus and malware installation/activation, data theft, loss of intellectual propertyand financial theft.

Spam

Although it has decreased due to succesful spam blocking practices and take downs of large spam bots, it is still considered as serious mainly due to often succesful attempts by spammers to create user confidence in their messages through social media and mobile devices.

Phishing

Technical deception, through spoofed emails and counterfeit Websites as well as social engineering significantly contribute to phishing. Social networking sites as well as the proliferation of new technologies having vulnerabilities and weak security controls are also likely to enable phishing, leading to information theft or leakage. End-user behaviour and awareness may help in defending against phishing.

Exploit kits

They are increasingly complex and sophsticated automated tools applied by a number of threat agents that mainly detect vulnerabilities at user end-devices so as to download and manage malicious content. It is noted that organisations deploying vulnerability management, based upon mature and formal methods, are less likely to be infected from exploit kits.

Data breaches

It is a result of successful cyber-attacks or erroneous unintentional user activities, all leading to disclosure of confidential information. Due to their impact and their long term consequences, data breaches are among the most thoroughly managed and investigated cyber incidents. Security preparedness for new technologies, such as for mobile and cloud computing, is still in its early maturity phases, with challenges arising with respect to data ownership in off-premises environments. However it also needs to be kept in view that over 50% of data breaches are attributed to a lax regard to security controls and procedures by end-users.

Physical damage, theft and loss

Various cyber-security incidents, mainly data breaches and identity theft, may be a result of such a threat. Theft and loss of end user ICT devices rank high in related statistics.

Insider threat

Top most information types that have been breached by organisation insiders are intellectual property, customer data and financial records, whilst the top five activities of insider misuse assessed include privilege abuse, non-approved hardware, bribery and email misuse and data mishandling. Such an attack is possible due to the inherent ability to bypass existing security controls through available access rights, insider knowledge of existing protection and the awareness of an organisation's weaknesses and vulnerabilities. It could also be due to user error; potentially resulting from user negligence [2]or lack of employee security training[3].

Information leakage

It relates to a set of threats that emerge due to unintentional or maliciously triggered exposure of sensitive data, mainly through technical or organisational weaknesses to an unauthorised party. Software application vulnerabilities resulting in areas such as their coding or implementation are also cited as sources for informatin leakage. Social media is also reported as a major channel for information leakage that can be used in other attacks. Proper security controls are also necessary to ensure protection of data in transit or at rest on mobile and cloud computing technology.

Identity theft, fraud and cyber espionage

Identity theft is a cyber threat that aims at collecting personal identifying information (PII) which includes credentials, personal profiling, details of financial identification/authentication methods, credit card information, various access codes, technical identification data, etc. An increase in identity theft/fraud incidents has led to consumer mistrust in using digital means to perform financial transactions.Increased interoperability within the consumer market may increase the likelihood of such threat, particularly if one vulnerable application falls victim to it.Emerging yet security - immature technologies, as well as older technologies having poor security controls are envisaged as likely targets for identity theft. Sophisticated methods are increasingly being used to target both large organisations as well as small to medium sized enterprises.

Ransomware, rogueware and scareware

Although this threat belongs to the family of malware, it may still be considered on its own merits, due to recently introduced features which enable it to infiltrate mobile devices.

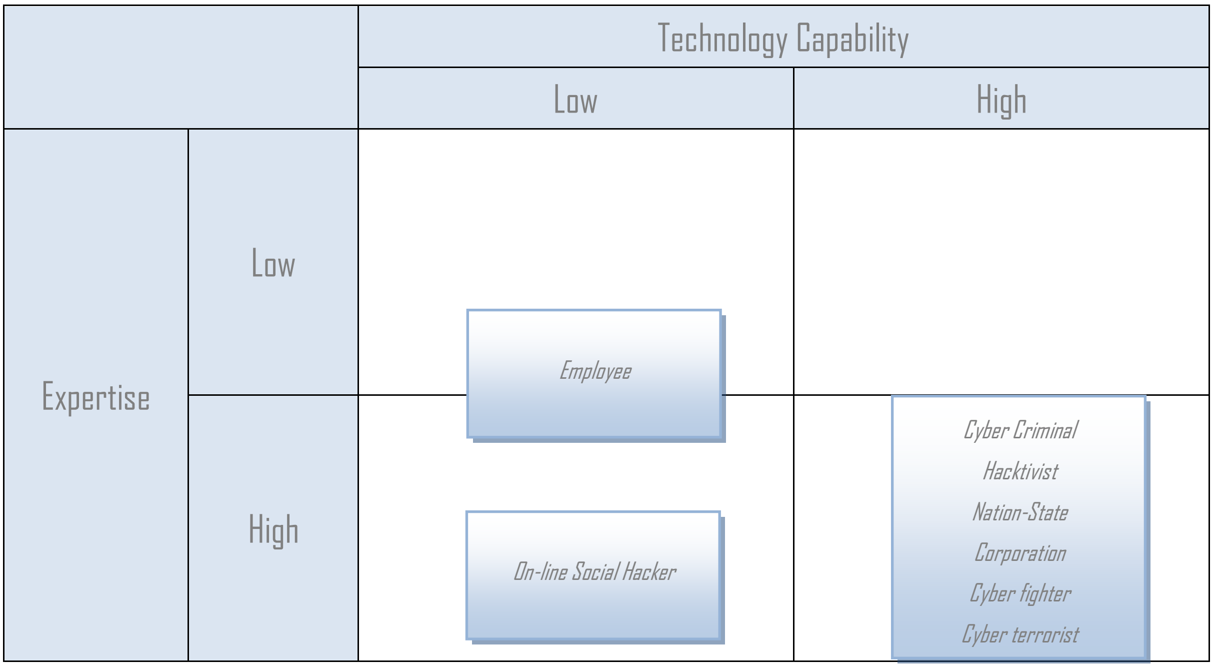
3.2 THE CYBER THREAT AGENTS

This section attributes cyber threats to an identified number of threat agents. Table 2 identifies the various threat agents along with the likely key motive for their activity.

Threat Agent	Motive
Cyber criminal	Profit oriented - in criminal activities
Online social hacker	Criminal
Hactivist	Socially motivated citizens
Nation state	Espionage
Corporation	Espionage
Employee (current, former)	Revenge, sabotage, extortion or profit
Cyber fighter	Nationally motivated citizens
Cyber terrorist	Ideological
Script kiddy	Thrilled about past achievements, considered outrageous/skills of tech saavy individuals

Table 2 – Threat Agents

The level of sophistication in terms of expertise and technology capability for each of the identified threat agents can also be noted by the Figure below.



		Technology Capability	
		Low	High
Expertise	Low	Employee	
	High	On-line Social Hacker	Cyber Criminal Hacktivist Nation-State Corporation Cyber fighter Cyber terrorist

Figure 1- The level of sophistication of each threat agent

Table 3 highlights the most likely threat agent for each of the top cyber threats. It indicates a widespread involvement of cyber criminals, followed by hactivists and nation-states[4] in such forms of activities. Identity thefts or frauds, information leakages and phishing are the predominant threats originating from any of the threat agents identified.

		Threat Agents								
		Cyber criminal	On-line social hacker	Hacktivist	Nation state	Corporation	Employee	Cyber fighter	Cyber terrorist	Script kiddy
Top threats	Identity theft fraud	■	■	■	■	■	■	■	■	■
	Information leakage	■	■	■	■	■	■	■	■	■
	Phishing	■	■	■	■	■	■	■	■	■
	Data breaches	■	■	■	■	■	■	■	■	
	Malicious code	■		■	■	■	■	■	■	
	Web-based attacks	■	■	■	■	■		■	■	
	Web application / injection attacks	■		■	■	■		■	■	■
	Exploit kits	■		■	■		■	■	■	■
	Physical damage /theft/ loss of data	■		■	■	■	■	■	■	
	Insider threat	■		■	■	■	■	■	■	
	Denial of Service	■		■	■	■		■	■	
	Cyber espionage				■	■	■			
	Spam	■	■							■
	Botnets	■		■						
	Ransomware / rogueware / scareware	■								

Table 3 –The likely threat agent for each cyber threat

The cyber agent scenario is however not complete without also identifying the friendly cyber agents – the agents who positively contribute to a safe and secure cyber space – who are listed in Table 4.

Cyber Agent	Motive/ Sector
Security Agent	National Security
Ethical Hacker	Market
Law enforcement Agent	Law enforcement
Researcher	Research community
Cyber soldier	Military

Table 4 – The friendly cyber agents

Emerging technologies, such as smart environments[5], may create possibilities for malicious activities, and thus the establishment of new cyber threat agents who may target smaller user communities. Such malicious activity may even cost human lives and should thus not be discounted for consideration particularly in the near future. The next Section amplifies further on this area of cyber security concern.

4 The emerging threat landscape

The following is a list of emerging technology areas whereby their level of maturity in cyber security and their subsequent emerging threat are outlined for consideration.

4.1 THE EMERGING TECHNOLOGY AREAS

Cyber Physical Systems

Cyber Physical Systems (CPS) are seamlessly integrated engineered systems which interact with computing equipment so as to control, manage and optimise physical processes in a number of applications[6]. Such systems are expected to undergo a high degree of innovation and hence they pose an emerging issue.

Mobile Computing

The increasing role of mobile devices in next generation ICT architectures coupled with their contribution towards technology convergence make them a key asset both for their users as well as for operators of related application services. Hence mobile devices are increasingly being targeted by threat agents. The secure development of mobile applications is also another area in its very early stages of maturity. The reuse of code libraries and binary code protection are two areas that also expected to be further developed, so as to minimize cyber threats such as data leakage and identity theft.

Cloud Computing

Cloud computing is another area of concern to users and security experts. Innovative usage models, attack scenarios and security control implementations for cloud computing are envisaged to fall under increased focus within the realm of cyber security in the future.

Trust infrastructure

Trust infrastructure and authentication infrastructure, are two vital components for cyber security and for which a heightened level of attack has been reported by ENISA in 2014. Such attacks are however seen as an opportunity for dynamic changes, introduction of good practice and potentially innovations within the area.

Big Data

Big data is essentially a valuable asset and is therefore targeted by cyber threat agents. It also turns out to be a very powerful tool for security professionals, given that it significantly contributes to building intelligence about threats and incident management.

Internet of Things/ Interconnected devices/ smart environments

Interconnected devices from areas such as smart home, smart vehicle exchange information that may be of a highly sensitive nature. Home automation through the Internet of Things concept may potentially lead to cyber cases of harassment, abuse, sabotage and bullying[7].

Network virtualisation (NV) and Software defined networks (SDN)

Network virtualisation builds virtual networks whilst software defined networks (SDN) perform changes to virtual networks according to user needs. Although both technologies pose opportunities towards quality of service, performance and efficient network management, yet, existing standards and released technology are still in the very early stages of adoption and maturity. Hence the need for more detailed security assessments for such technology is evidently necessary.

4.2 THE CORRESPONDING EMERGING THREATS

Table 5 lists out the corresponding likely cyber threats for each of the emerging technologies identified. Except for two cyber threats which are noted as stable within the Trust infrastructure area, most threats are noted to be on the increase during 2014. It can also be noted that the cyber threats featuring across all of the six emerging technologies, albeit at varying intensity, include:

- Malicious code or malware
- Phishing
- Web application or injection attacks
- Identity theft or fraud
- Information leakage
- Physical damage or theft or loss of data

		Threat Trend	
		↓	↑
Emerging Technology areas	Cyber Physical Systems		Malicious Code Web based attack Spam Phishing Physical damage/theft/loss Insider threat Web application attacks Information leakage
	Mobile Computing		Malicious Code Physical damage/theft/loss Phishing Web application attacks Web based attack Information leakage Identity theft Exploit kits Ransomware/rogueware/scareware
	Cloud Computing		Malicious Code Web based attack Web application attacks Botnets Denial of Service Insider threat Data Breach Cyber espionage Identity theft Information leakage
	Trust Infrastructure	Web based attack Denial of Service	Phishing Malicious Code Web application attacks Information leakage Identity theft Physical damage/theft/loss Exploit kits Cyber espionage
	Big Data		Data Breaches Information leakage Identity theft / fraud Insider threat Cyber espionage Web based attack Physical damage/theft/loss Phishing
	Internet of Things / Interconnected devices / Smart environments		Malicious Code Web based attack Phishing Exploit kits Information leakage Insider threat Web application attacks Physical theft/damage/loss Identity theft Denial of Service
	Network Virtualisation and Software defined Networks		Denial of Service Malicious Code Web application attacks Phishing Exploit kits Insider threat Physical theft/damage/loss Identity theft

Table 5 – Cyber threats from emerging technology

5 Insights on Cyber Security

5.1 CYBER SECURITY IS A CONTINUOUS PROCESS

The Cyber security scenario is a highly dynamic and complex one. Sophistication of cyber threats continues increasing.

Trust infrastructures face massive stress as their basic security constituents have been challenged. Other emerging technologies such as big data, social media, mobile computing and interconnected devices if not properly applied and/or protected constitute a perfect knowledge base for cyber criminals, allowing for covert, well planned, human and/or technical means of targeted attacks. Additionally, related standards and technology applied may still be in the very early stages of adoption and maturity , hence increasing the vulnerability risks.

Furthermore, the unknown number of breaches and security incidents is a major concern for cyber security experts and law enforcement officials, calling for the need of breach notification at various business areas/sectors, possibly through regulation. Governments are challenged to follow up on related developments with regulation and legislation; seeking to establish a balance between what is technically possible and what is legally transparent in the process.

New, sophisticated attacks call for development of new defences, such as through new detection techniques and new security controls. In effect, such requirements for innovation call for research and development efforts and investments involving Government, business as well as the academia.

5.2 CYBER CRIMINALITY IS EXTENSIVE, COMPLEX AND ADVANCED

Cyber criminals are increasingly more effective in targeting their attacks. They are being more successful in exploitation of vulnerabilities (human and technical) through effective application of malicious tools and attack methods. Breached or leaked data is considered as one of the key means to achieve this goal. New attack techniques and practices also allow for lack of detection and traceability of the perpetrator.

The nature and efficacy of the cyber crime market does not exclude having specialised roles such as administrators, specialists in varous areas of cyber crime, intermediaries, brokers and vendors. Interactions of cyber criminals with cyber terrorists is not excluded either.

5.3 CYBER THREATS MAY ALSO ARISE FROM BUSINESS PARTNERS

The need for organisations to take heed of insider threats through their employees is critical. However consideration also needs to be taken of business partners. It is reported that financial institutions are increasingly concerned about their ability to combat threats that can arise from sharing networks and data with business partners, with 41% of respondents stating that they detected incidents perpetrated by third parties with trusted access. A number of organisations within healthcare and the utilities industry also admit to forging strategic business relationships without consideration to robust due diligence, regulatory policies or deployment of monitoring and detection controls, on third parties with whom they share sensitive information[8].

5.4 NO INDUSTRY CAN DO WITHOUT A ROBUST CYBER SECURITY PROGRAM

The public sector is reported to be the primary target of cyber attacks, accounting over 75% of more than 63,400 incidents reported worldwide during 2014[9]. However, one cannot discount the vulnerability of any other organisation – public sector or otherwise – from any cyber attack.

The Healthcare industry payers and providers report that information security incidents increased by 60% in 2014, and that costs attributed to such incidents increased to 282%[10]. For example, identity theft and fraud is particularly noted within the healthcare industry, with an estimate of around two million US citzens envisaged to spend over $12 billion as a result of such an incident alone. Cyber attacks against power and utilities organisations have also transitioned from *speculative* to *indisputable* [11]. Article 2.3 of the European Commission's European Energy Security Strategy, in particular, states that: "The EU has started to develop a policy to address the physical protection of critical infrastructure (against threats, hazards) which includes energy infrastructure. Increasing attention should be given to IT security"[12]. Within the Finance sector, its regulators are increasingly expecting the effective implementation of robust security programs from its operators.

Ultimately, the crux of it all is not simply having a cyber security program, but that its implementation does not lag behind. ENISA specifically reports in 2014, that falling behind in cyber security continues to be the number one reason for security incidents such as data breaches.

5.5 A RISK-BASED GOVERNANCE MODEL TO CYBER SECURITY IS NEEDED

As highlighted earlier, the uses of technologies - and in particular, emerging ones - present opportunities and pose risks too. Hence the need for thorough risk assessments, prior to their deployment is necessary. Possibly with the aid of widely accepted frameworks, consideration needs to be given to closely link technologies, processes and personnel skills with enterprise risk management within an organisation. The purchase of cyber insurance to help mitigate financial losses of cyber-attacks[13] may also contribute further towards a healthy risk based approach.

5.6 RESPONSIBILITY, COMMITMENT AND ACTIVE SUPPORT FROM TOP MANAGEMENT IS CRUCIAL FOR CYBER SECURITY

Cyber security is indeed a responsibility of each and every employee within an organisation. However, as in any other initiative within an organisation this is likely to falter, potentially leading to earlier reported negligence unless it is not continuously and actively communicated and supported by top management. Ongoing cyber security training and awareness programmes may help in this regard.

5.7 EFFECTIVE CYBER SECURITY DEMANDS THAT NO ORGANISATION SHOULD OPERATE IN ISOLATION

Threat analyses and achieved results, performed by various organisations, are rather complex. The challenge faced may be eased by effective sharing of information on threat intelligence and response tactics.

Part Three

Domestic cyber security concerns and preparedness

6 An Outline of European-wide Concerns

6.1 CYBERCRIME

The Euro barometer Survey specialising on cyber security for 2014 specifically states that "*85% of Internet users across the EU agree* that the *risk of becoming a victim of cybercrime is increasing".* The levels of concern about *each specific type of cybercrime*[14] are also considerably higher than in 2013[15]. Compounded to such concern, is a high level of agreement among European citizens that they still do not feel well informed about cyber crime risks.

> **"Cybercrime undermines consumer confidence in the use of Internet, hampering both our digital economy and our online lives. Our priority is to create a safer Internet for all users by preventing and combating cybercrime in all its forms, to enable users to reap the full benefits of the digital internal market and to exercise their fundamental rights online …"**
>
> **Dimitris Avramopoulos, European Commissioner for Migration, Home Affairs and Citizenship.**

6.2 NATION-STATE ACTORS

Of equal concern is a noted increased 'alarm' over nation state actors[16] as evidenced by cyber-security simulation exercises being conducted. The European Network Security Agency (ENISA) conducts EU-wide 'simulation exercises' to prepare for better cooperation against the threat of critical systems from hostile cyber agents[17]

7 Experiences and concerns of the Maltese citizen

A number of indicative traits or concerns on cyber security issues among Maltese citizens have been extracted from Special Euro barometer public opinion surveys on cyber security conducted across the European Union for years 2012[18], 2013[19] and 2014[20] for particular consideration. Table 6 presents a number of incidents reported by the Survey's Maltese respondents for 2014 with an indicative trend from the previous year based upon the percentage of responses.Table 7 lists a number of concerns expressed by the Maltese respondents with respect to various aspects of cyber security. A detailed explanation and analyses for each of the factors listed is given further below.

Experiences	Trend (2014)
Having hindered access to online services due to cyber attacks	↑
Avoid disclosing personal information on-line	↑
Account hacked	↑
Accidentally encountered material of racial hatred etc.	↑
Reported cyber related incidents to Police	↑
Identity theft	↓
Received fraudulent emails	↓
Online banking fraud	↓
Online fraud (e.g. unfulfilled online purchases, false advertisements)	(higher relative to EU)

Table 6 – Indicative trend of cyber incidents among Maltese (2014)

Legend	
↑	Increasing
↓	Decreasing
—	Stable

Concerns	Trend (2014)
Being victims of cybercime	↑
Being victims of identity theft	↑
Being victims of account hacking	↑
Not having access to online services	↑
Receiving fraudulent emails	↑
Bank card or online backing fraud	↑
Security of online payments for banking or purchasing activities	↑
Use of Internet for activities like online banking or purchasing	↑
Personal information not kept secure by public authorities	↑
Discovering malicious software	↑
Encountering offensive material online	↑
Personal information not kept secure on Websites	↓

Table 7 – Indicative trend of cyber related concerns among Maltese (2014)

Legend	
↑	Increasing
↓	Decreasing
—	Stable

7.1 CYBERCRIME

Similar to the overall EU scenario, there is an increasing level of proportion of Maltese respondents who express their strong concern of becoming a victim of cybercrime - from 69% in 2013 to 85% in 2014. The following are a number of cybercrime variants encountered or perceived to occur within the Maltese context.

7.2 ACCESS TO ONLINE SERVICES

The overall confidence to use the Internet for online services (e.g. banking, public services) has decreased from 74% in 2012 to 73% to 2013 across the EU.

A proportional increase is noted in 2014 in the level of concern expressed by EU respondents in having access to online services, through the Internet, as a result of cyber attacks. In Malta's case, the findings indicate an increase from 44% in 2013 to 61% in 2014. This could be potentially attributed to an increase in the proportion of the Maltese respondents, from 7% in 2013 to 10% in 2014 who complain of related incidents.

7.3 ONLINE FRAUD

Overall, almost all respondents within the EU member states attribute the use of Internet to access e-mail. The Maltese respondents who receive fraudulent emails have decreased significantly from 53% in 2012 to 39% in 2013 and have remained so (39%) in 2014. However, the percentage of those who are concerned of receiving fraudulent emails has increased from 55% in 2013 to 58% in 2014.

Furthermore, Malta ranks high within the EU in the proportion of respondents (16%) who claim on-line fraud in terms of unfulfilled purchase of goods, counterfeit goods, or falsely advertised products; although the percentage has remained locally stable since 2013. The level of concern has however sharply increased in proportion from 55% in 2013 to 67% in 2014.

7.4 ONLINE BANKING FRAUD

Concern on bank card or online banking fraud appears to be on the rise across the EU in 2014, relative to 2013. In the case of Malta, the findings indicate an increase in level of concern from 62% to 71%. Such proportion of concern is considered relatively high in Malta compared to the rest of Europe in 2013 and tends to remain so, albeit to a lesser extent, in 2014.

On the other hand, although there is a 1% increase in proportion of EU respondents who claim such fraud during 2014, there is a corresponding decline within the Maltese case - from 6% (2013) to 5%.

7.5 SECURITY OF ONLINE PAYMENTS

During 2014, there again appears to be a rise in concern amongst the Maltese respondents (27%) on the security of online payments for banking or purchasing activities. This follows a previous decline from 29% in 2012 to 24% in 2013.

7.6 PERSONAL ONLINE DATA PRIVACY AND SECURITY

Over a three year period, there also appears to be a variation in the trend of Maltese respondents who seek to avoid disclosing personal information online. It has significantly declined from 95% in 2012 to 80% in 2013, but has almost returned to the original level, increasing to 93% in 2014.This may similarly reflect an increase in 2014, in stated concerns with respect to the

- Use of the Internet for activities like online banking and online purchases – an increase of 12%. This percentage indicates an increase of 12% from 2013. Malta also registers the highest proportion of respondents registering such concern across the EU, at 34%.
- Personal information not kept secure by public authorities – with proportion of respondents varying from 65% in 2012 down to 62% in 2013 and increasing again by 4% (66%) in 2014.

On a positive note however, a declining trend is noted in the level of concern regrding online personal information not being secured by websites – from 74% in 2012 to 71% in 2013 and declining further to 69% in 2014.

7.7 IDENTITY THEFT

The proportion of Maltese respondents who have experienced identity theft has declined from 11% to 5% between 2013 and 2014[21]. However, this does not dispel the increasing level of concern of experiencing such an incident as stated across the EU, including Malta – from 59% in 2013 to 74% in 2014.

7.8 ACCOUNT HACKING

During 2014, a significant proportion of the Maltese respondents (71%) relative to the EU average (60%) express their concern of having their social media or email account hacked. In addition, there is also an increase in proportion of Maltese respondents who claim that their social media or email account has been hacked – from 12% in 2013 to 16% in 2014.

7.9 MALICIOUS SOFTWARE

In 2014, a significantly high proportion of Maltese respondents (76%) have also stated concern of discovering malicious software on their ICT devices. 40% of Maltese respondents have also reported discovering malicious software. The survey also refers to a direct correlation between those who installed anti-virus software and those who discovered malicious software.

It is noted that during the same period, the proportion of Maltese respondents who claim to have installed anti-virus software stands at around 40%, increasing to 60% by end 2014.

7.10 OFFENSIVE MATERIAL

Across the EU, respondents are more likely to state that they have encountered material which promotes racial hatred or religious extremism online; with an increase of 11% from 2013. Indeed, in the case of Malta, the level of related concern has increased from 37% in 2013 to 50% in 2014. A sharp increase, in the case of Malta is noted in the percentage of those who accidentally encountered such material – from 12% in 2013 to 25% in 2014.

Similarly, an increase of 9% is noted between 2013 and 2014 in the number of Maltese respondents who are concerned with accidentally encountering child pornography online.

7.11 ON-LINE HARASSMENT

In 2013, when compared to the highest EU level of 9%, only 4% of Maltese respondents report that they have been personal victims of on-line harassment. Additionally, only 1% of the Maltese respondents claim to have child victims of on-line harassment, compared to the EU's highest proportion of 5%.

During the same period, it is noted that on-line harassment is consistent among EU states and is higher among:

- Frequent internet users
- Respondents aged 15-24 years
- Multiple (rather than single) households with children

Notably, in 2014, Malta ranks amongst the top:

- four EU countries where 52% of respondents take steps to protect children when they are online
- five EU countries where 31% of respondents monitor children's Internet usage

Specifically, at 23%Malta rates highest amongst the EU respondents who state that they adjust security settings for children.

7.12 FEELING INFORMED ABOUT THE RISKS OF CYBERCRIME

On a more positive trend, the percentage of Maltese internet users who feel well informed about the risks of cybercrime has increased from 45% in 2013 to 54% in 2014. This similarly reflects an EU trend, with a decrease from 59% to 53% during 2012 -2014 among those who do not feel well informed about the risks of cybercrime.

This may potentially explain one behavioural trait reported in the Euro barometer 2014 survey whereby a significant proportion of the Maltese respondents, relative to their EU counterparts (48%) claim that they are most likely to visit only known Websites.

Significantly encouraging is that despite the overall cyber security concerns, it appears that a fewer proportion of Maltese respondents (6%), compared to European ones, deem it likely not to buy goods or services online.

7.13 REPORTING CYBERCRIME

On an EU –wide perspective (including Malta), the Police are most frequently contacted in case of cyber crime such as for identity theft, online banking fraud, child pornography. This indicates the key role that the Police force is perceived to play within the cyber crime area. However the survey findings also suggest that a higher level of knowledge on cybercrime leads to a preference to contact website or vendor organisations rather than the police.

8 Current domestic scenario in cyber security

At this stage, current domestic on cyber security aspects in Malta has been largely noted from on-line publicly available sources as follows:

8.1 DIGITAL AGENDA FOR EUROPE

As an EU Member State, Malta is expected to align itself to Europe 2020, the 10-year strategy proposed by the European Commission on 3 March 2010 for advancement of the economy of the European Union through smart, sustainable, inclusive growth" with greater coordination of national and European policy. The Digital Agenda for Europe (DAE), adopted by the European Commission in May 2010, is one of the Strategy's seven flagship initiatives that aim to increasingly facilitate the deployment of high-speed internet and reap the benefits of a digital single market for households and firms. Along with other related Council of the European Union Conclusions, the DAE highlights a shared understanding that security and trust are the necessary prerequisites for the wider uptake of ICT. The Implementation of the DAE, focuses, among others, on four action items pertaining to Trust and Security, namely:

- Action 38 – Member States to establish pan-European Computer Emergency Response teams
- Action 39 – Member states to carry out cyber attack simulations
- Action 40 – Member States to implement harmful content alert hotlines
- Action 41 – Member States to set up national alert platforms

Reference to the latest status for the action items can be found at http://daeimplementation.eu/member_states.php?id_pillar=45&id_country=18.

8.2 ITU REPORT – CYBER WELLNESS PROFILE

Malta is a member of the International Telecommunications Union (ITU)-the United Nations specialized agency for information and communication technologies.

The ITU has embarked the Global Cyber security Agenda (GCA); a framework for international cooperation aimed at enhancing confidence and security in the information society. The CGA is based upon five domains for a country's cyber security development, namely Legal Measures, Technical Measures, Organisation Measures, Capacity Building and Cooperation. Information on Child Online

Protection, a key ITU initiative, is also covered. A Cyber Wellness profile has been established by the ITU for each its member states, as a means to assess their level of cyber security development.

Reference to the most recent Cyber Wellness Profile can be found at http://www.itu.int/en/ITU-D/Cyber security/Documents/Country_Profiles/Malta.pdf

8.3 OTHER SOURCES

Other sources that have been noted include:

- Digital Malta–National Digital Strategy 2014-2020
- eCommerce Malta-The National e-Commerce Strategy 2014-2020
- Malta Critical Infrastructure Protection[22]
- MITA Strategy 2015 -2017

Part Four

Stakeholder overview

9 Identification and assessment of Stakeholders

Table 8 broadly identifies the stakeholders for a Malta Cyber Security strategy.

Stakeholder	Requirements	Potential players in Malta
National leading authority on cyber security	Lead in the overall implementation of a National Cyber security strategy.	To be identified
Computer Security and Incident Response Teams (CSIRTs)	Lead and contribute to specific relevant aspects of the cyber security strategy. Incident and Risk handling.	Top level coordinating CSIRT and other
Public Authorities related to national cybercrime, defence and security	Lead and contribute to specific relevant aspects of the cyber security strategy. Take appropriate measures to manage the risks posed to the ICT which they control and use in their operations.	Public Sector functions responsible for ● handling cybercrime on a national basis ● national defence, security, critical infastructure protection
Key Market operators that include: ● Providers of information society services ● Operators of critical information infrastructure (CII) ● Operators of critical infrastructure that provide essential or critical services to CII.	Lead and contribute to specific relevant aspects of the cyber security strategy. Take appropriate measures to manage the risks posed to the ICT which they control and use in their operations.	Public sector functions and private sector organisations responsible for ● Information Society services[23] ● Critical information infrastructure services such as those in communications, ISPs, etc ● essential or critical services to critical information infrastructure
Legal	Contribute to the legislative aspect (including law enforcement) of cyber security strategy.	Public Sector functions responsible for legal matters and other legal respresentations

Stakeholder	Requirements	Potential players in Malta
International and EU Affairs	Contribute to international and EU aspect of cyber security strategy.	Public Sector functions responsible for EU and international affairs
Academia and Research and Development	Contribute to capacity building/research.	Public Sector functions and potentially private sector organisations responsible for education training, skills development, research and development
Other market operators[24]	Participate and contribute to specific cyber security strategy related activities, as appropriate. Need awareness	Private sector respresentations for various business areas
Civil Society	Participate and contribute to specific cyber security strategy related activities, as appropriate. Need awareness.	Various representations of civil society, such as those for children, youths, elderly and pensioners, families, workers, education, NGOs, political parties.

Table 8 – Indication of Stakeholders for Malta Cyber Security Strategy

Within the local context, it is likely that the Public sector and regulated industries, such as those in banking and finance, electronic (mobile) telephony, ISPs are key leaders in cyber security; given that they:

- Use the Web and mobile channels extensively for their services
- Handle sensitive data
- May already be expected, as critical infrastructure owners / operators to undertake related security measures
- May likely have more human and financial resource capacity and capability to mount robust cyber security measures

A brief review of some **local** indicators, such as the highest percentage contribution to GDP in 2013[25], further suggests that the following sectors need to take particular active consideration of cyber security in Malta:

- Services (76.4% contribution), which apart from Finance notably includes Gaming, Education, Real-estate services' ,Hospitality and Tourism, Transport and storage, Professional, Scientific and Technical activities, ICT activities
- Industry (22.2% contribution)
- Agriculture (1.4% contribution)

Additionally, as also indicated within the Table, consideration also needs to be made of cyber security related updates to regulation and legislation, international cooperation, capacity building, education and awareness.

Part Five

Conclusion

10 Concluding Note

Such findings, provide various indications of areas where further attention needs to be further expended with respect to cyber-security. Above all, they clearly show that cyber security cannot be treated as a monolith. Cyber threats are not all the same and resulting impacts are not to the detriment to technology only, but to organisations,processes and ultimately to the end-user.

Ultimately it is not only the public sector alone that is impacted upon. Given today's digital interconnectedness between Government, the private sector and civil society, it is thus necessary for a continuous and well planned concerted effort so as to ensure updated security in place so as to minimise cyber threats as much as possible.

References

Cabinet Office-United Kingdom (2011), *The UK Cyber Security Strategy- Protecting and promoting the UK in the Digital World*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Commonwealth of Australia (2009) *Cyber Security Strategy*, https://www.ag.gov.**au**

Commonwealth Telecommunications Organisation, *Commonwealth Approach for developing National Cybersecurity Strategies*, www.cto.int

Department of Information-Malta (Dec 12, 2014), *#StopHate-The launch of a nationwide awareness campaign against cyber bullying*, Reference Number PR142913, Press Release, http://www.gov.mt/en/Government/Press%20Releases/Pages/2014/December/12/PR142913.aspx

Department of Information-Malta (Apr 30, 2015), *Digital Citizen Charter biex ħares lill-persuna digitali*, Reference Number: PR150939, Press Release, http://www.gov.mt/en/Government/Press%20Releases/Pages/2015/April/30/PR150939.aspx

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

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

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

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

European Commission (2014), European Energy Security Strategy, COM(2014) 330 final, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN

European Network and Information Security Agency (ENISA) (2014), *ENISA's efforts on Cyber Exercises–Policy Context*, Cyber Europe 2014 –Background info, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/briefing-pack/ce2014-background-information

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

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

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

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

Index Mundi (2015), *Malta Economy Profile 2014*, www.indexmundi.com

Infocomm Development Authority of Singapore (IDA), *National Cyber Security Masterplan 2018 brochure*,http://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf

Malta Critical Infrastructure Protection, *Legislation*, http://maltacip.gov.mt/legislation?l=1

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

Malta Financial Services Authority (MFSA) (2014), *Economic and Market Overview*, http://www.mfsa.com.mt

Marmon, W. (2011), *Main cyber threats now coming from Governments as 'state actors'*, http://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors

Ministry of Economic Affairs and Communications – Estonia (2014*) Cyber Security Strategy: 2014-2017*, https://www.mkm.ee

Ministry for Finance – Malta (November 2014), *Economic Survey (Malta)*, www.mfin.gov.mt

National Audit Office – UK (2013), *The UK Cyber Security strategy: Landscape Review, Report by the Comptroller and Auditor General*, http://www.nao.org.uk/report/the-uk-cyber-security-strategy-landscape-review/

National Security Authority - National Cyber Security Centre – Czech Republic (2013), *National Cyber Security Strategy of the Czech Republic for the period from 2015-2020*, https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf

National Statistics Office – Malta (2 February 2015), *Short term services indicators Q3/2014*, News Release https://nso.gov.mt/en/News_Releases/View_Current_Year/Pages/2015-[1].aspx

Presidency of the Council of Ministers –Italy (December 2013), *National Strategic Framework for Cyberspace Security*, www.sicurezzanazionale.gov.it

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

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

United States of America (February 2003), *The National Strategy to Secure Cyberspace*, https://www.us-cert.gov/sites/default/files/.../cyberspace_strategy.pdf

United States of America (May 2011), *International Strategy for Cyberspace, Prosperity, Security and Openness in a networked world*, https://www.whitehouse.gov/.../international_strategy_for_cyberspace.pdf

Verizon Security Researchers, *Data Breach Investigations Report for 2014*, http://www.verizonenterprise.com/DBIR/

Watson, M (June 16, 2015), *Second data breach at OPM confirmed*, http://www.itgovernanceusa.com/blog/second-data-breach-at-opm-confirmed/?utm_source=Email&utm_medium=Macro&utm_campaign=S01&utm_content=2015-06-17

World Economic Forum (2014), *Annual Global Competitiveness Report: 2014-2015*, http://www.weforum.org/reports/global-competitiveness-report-2014-2015

Endnotes

[1] ENISA is the European Union's Cyber research agency. The ENISA Threat Landscape 2014, can be found at www.enisa.europa.eu

[2] 50% of data breaches are attributed to this defect

[3] 48% of organisations participating in a related survey admitted to not providing such training to their employees

[4] Verizon Security Researchers, in its Data Breach Investigations Report for 2014 reports an annual three-fold increase in cyber espionage. The profile of the attacker is evolving from one of a lone hacker to one or more nation-state actors who have the sophisticated cyber attacking means to infiltrate organisations – both public and private sector.

[5] For example smart homes, smart vehicles,etc.

[6] Such as power supply systems e.g.SCADA (supervisory control and data acquisition), medical systems, telecommunication, etc

[7] Which could be potentially triggered by neighbourhood disputes, tenancy, etc.

[8] PwC (2015), Global State of Information Security Survey(2015) http://www.pwc.com/gx/en/consulting-services/information-security-survey/

[9] Verizon Security Researchers (2014), op.cit

[10] PwC (2015), op.cit

[11] Detected incidents soared six-fold from 2014 – PwC (2015),op.cit.

[12] Article 2.3 Protection of critical infrastructure-European Energy Security Strategy, European Commission COM(2014) 330 final, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN

[13] PwC (2015), op.cit.

[14] For example: identity theft; hacking of email/social media account; being a victim of bank card or online banking fraud, misuse of personal data

[15]Eurobarometer survey: EU citizens very concerned about cybercrime http://europa.eu/rapid/press-release_MEX-15-4322_en.htm

[16] http://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors

[17] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/briefing-pack/ce2014-background-information Also refer to https://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today

[18] http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

[19] http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

[20] http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

[21] Following a previous sharp increase of 6% during 2012-2013

[22] http://maltacip.gov.mt/legislation?l=1

[23] Any service normally provided for renumeration, at a distance, by electronic means and at the individual request of a recipient of services (Source: Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:217:0018:0026:en:PDF).

[24] Not falling within the scope of the key market operators

[25] Various sources have been referred to, such as: Ministry for Finance (Economic Survey 2014), National Statistics Authority (News Releases), MCA (eCommerce Strategy), and Malta Financial Services Authority (Economic and Market Overview 2013). Index Mundi , World Economic Forum (Annual Global Competitiveness Report:2014-2015)