# ENCOURAGING THE ADOPTION OF CYBERSECURITY

An initiative of:





In collaboration with:


# Encouraging the Adoption of Cybersecurity

Authors:

Gianluca D'Antonio
Adolfo Hernández
Enrique Fojón Chamorro
Manel Medina

Translated by: APWG.EU and Telefonica
November 2014

Gianluca D'Antonio is CISO of FCC Group, cofounder and President of the Information Security Advancement Society (ISMS Forum Spain). Since 2009 he is member of the Permanent Stakeholders' Group (PSG), which give advises to the European Union Agency for Network and Information Security (ENISA). He is also member of the Certification Committee of the Cloud Security Alliance. He has been granted the following certifications: CISM; CISA; CGEIT; L.A.; ISO27001; CCSK; CBCI and CDPP.

Adolfo Hernández is computer engineer from Autonoma de Madrid University. His professional skills have been certified in the CISSP, CISA, CISM, ITILf, CDPP programmes. Before joining the Cybersecurity Services Global Product Management Team of Telefonica Digital and Eleven Paths, he has been the Manager of the Governance, Risk & Compliance area of Ecix Group. He is the co-founder of the think-thank Thiber, member of ISMS Cybersecurity Centre, member of the Spanish Chapter of (ISC)2.

Enrique Fojon Chamorro is Computer Engineer. He is co-founder of the think tank THIBER and member of ISMS Cybersecurity Center.

Manel Medina is full Professor at the Politecnic University of Catalunya (UPC), and founder and Director of esCERT-UPC, Spanish UPC Computer Emergency Response Team. He is President of the Scientific Committee of the European Chapter of the AntiPhishing WG (APWG).
Former Head of CERT relations Unit and Deputy Head of TCD at ENISA (European Network and Information Security Agency). He has been founder of several spin-off companies as well as the cybersecurity advisor of several organisations.

# Table of Content

The Information Society, as we know it today, is highly dependent on the 'digital ecosystem'

# 1. Introduction

# 1. Introduction

During the last decade, the Internet has gone from being a useful communication tool for individuals and organizations to become essential digital infrastructure for economic development and the welfare of society as a whole. This assertion, included in a recent study by the Organisation for Economic Cooperation and Development (OECD) on cybersecurity[1] highlights the unstoppable transformation of a world increasingly dependent on Information Technology and Communications (ICT). Indeed, this dependence is a risk factor that cannot and should not be ignored, as has been reflected since 2011 in the World Economic Forum, in which Global Risk Map[2] a list of potential incidents related to cyberspace and the use of ICT were introduced.

The Information Society as we know it today, has a high dependence on a "digital ecosystem", whose access and use stands as a legitimate interest of the citizens, but that has not yet been fully recognised as a right. If our society cannot be understood without the availability and use of these "digital infrastructures", the natural evolution of this situation is the development of a legal and organizational framework for the promotion, protection and enforcement of measures for its adoption.

With this study, THIBER, the cybersecurity think tank (hereinafter THIBER) and the Spanish Cybersecurity Institute (hereinafter SCSI) aim to foster a debate on measures of legal and organizational nature that could make possible the generation of a secure and resilient digital ecosystem.

## 1.1 Cybersecurity: a shared responsibility

Encouraging the actions and attitudes aimed to improve the level of resilience of the European enterprises, changing business practice in cybersecurity, and to increase the level of general awareness are the pillars of the most effective approach to achieve the goals herein proposed; the development of a Society able to protect its interests, its citizens and its enterprises from threats involving the use of new technologies.

The key points on which the approach advocated in this paper is based are:

1. Cybersecurity policy making at a Turning Point. OECD. http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf
2. Global Risk 2014. Ninth Edition. World Economic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

1. Sharing cybersecurity costs amongst all stakeholders, i.e. citizens, industry and even public administrations.
2. Rewarding organizations committed to the protection of information systems.
3. Promoting cybersecurity push in order to enlarge products and services Market.
4. Stimulating demand for computer security tools by users and organizations.
5. Promoting research and development in cyber security solutions and products.
6. Stimulating the resilience of the entire cyberspace ecosystem.

Summarising, this approach encourages and fosters a culture of Security and Defence in the cyberspace, as a common and shared responsibility amongst all actors of the Society.

## 1.2 Paradigm shift

In Continental Europe tradition has made us feel comfortable with a disciplinary and punitive paradigm as a method to achieve the stated objectives. However, these sanctions should be mitigated according to the cybersecurity preventive capacity of the organization concerned, supporting them against inevitable attacks and punishing only those who have not acted with due diligence and are still vulnerable to trivial or easily avoidable cyber-attacks.

During the last decade the number of European and national regulations in the field of cyberspace have proliferated, focusing more on fines and penalties, rather than in defining incentives or best practice recommendations.

The differences between the two paradigms are not just philosophical, but crucial for the effective achievement of the objectives described in the Cyber-Security Strategy. It is therefore necessary to create a scenario where organizations will consider the resilience and security in the cyberspace as a value and an investment rather than a cost.

In this regard, this document proposes an incentive program, with the aim of encouraging the adoption of best practices in cybersecurity.


SALES BY CATEGORY
DAT
BID
ASK
PRO
QUA
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC

## 1.3 Why incentives are necessary?

In the current economic macro and micro context, where the first signs of recovery from crisis are in internal Market sales and industrial production, a policy of incentives would support private initiatives in the mission of protecting customers, users and information assets. In many EU countries, their Economy is based mainly on services, energy and industry sectors. Those sectors, which can account up to 90% of Gross Domestic Product (GDP)[3] in those countries, have a common feature: a strong dependence on Information Technology and Communications (ICT). This dependence on new technology channels is what needs to be treated as an investment factor, from the perspective of improving the consumer experience, and the user confidence in the security of the systems used for contracting services or buying products.

According to a recent survey conducted by a consultant in several developed countries, half of surveyed Spanish companies had been victims of cybercrime in the last two years[4].

"Half of surveyed Spanish companies have been victims of cybercrime in the last two years"

This finding highlights the need for changes in public policies, without them, the lack of means and professionals needed to ensure the security of the above mentioned sectors will remain unchanged.

3. http://economy.blogs.ie.edu/archives/2014/02/estructura-de-la-economia-espanola-por-sectores-economicos-y-el-empleo-1970-2013.php
4. http://www.delitosinformaticos.com/06/2014/delitos/fraudes-y-estafas/la-mitad-de-las-empresas-

## 1.4 The Spanish case: the need to define a general framework for cybersecurity

On December 5th 2013, the Council of Ministers, at the request of the National Security Council, approved the Spanish National Cyber Security Strategy (Estrategia de Ciberseguridad Nacional, ECN)[5]. This text, whose genesis started two years back, develops the National Security Strategy released in May 2013 in the field of cybersecurity, one of the twelve policy areas identified in that document, reflecting current as well as future scenarios.

Approved under a highly restrictive budgetary scenario, the actual implementation of the action lines, whose achievements and success certainly require an investment funded through both public and enterprises contributions, should go through a policy of incentives and supporting actions, targeting organizations committed to the protection of information systems and technology infrastructure.

Therefore, it will be through taking advantage of every opportunity, like this one, that the claim for a legislative and regulatory framework in this area will find the adequate promoters.

one, that the claim for a legislative and regulatory framework in this area will find the adequate promoters.

5. National Cyber Security National Strategy (Estrategia de Ciberseguridad Nacional, ECN)
http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

# 2. Main lines of action

2.1 Legal incentives

2.2 Access to funding

2.3 Market incentives

2.4 Cyberinsurance

2.5 Public recognition

2.6 Ease of public procurement

2.7 Prioritization of technical assistance by the State

## 2.1 Legal Incentives

In the preface to the National Cyber Security Strategy, the Prime Minister of the Spanish government referred to the unavoidable need to "dedicate all necessary means" to achieve cybersecurity. The dependence on new technologies of our welfare society requires a strong commitment to "secure cyberspace".

This acceptance of responsibility and leadership from the highest institutions of the State, represents a crucial starting point for citizens as a whole, assuming the cost of this training process. And, as the document states, "... the competitiveness of our economy and the prosperity of Spain depends on the investment made in terms of management talent and resources to develop the necessary capabilities to meet these challenges."

Countries like the United Kingdom, India and the United States have launched tax incentive programs or privileged funding to boost this market, and at the same time, supporting companies that are committed to effectively protect their information systems and assets. In the case of the State of Maryland, in the United States, these tax incentives can be up to $ 250,000 per company and fiscal year. The aid is addressed at companies supplying cybersecurity products and services establishing their offices in that State[6].

In the case of India, the framework of deployed incentives, according to declarations made by his telecommunications minister, they are addressed to those companies investing in technological protection measures[7].

At European level, in the UK has launched a program of incentives for innovation called innovation voucher to support SMEs interested in launching new products and technological services.

In the same direction, the Irish government has launched a campaign to support the registration of intellectual property in the field of new technologies to promote increased scientific knowledge and their national market through patents[8].

These initiatives demonstrate an increasing interest from many governments to boost cybersecurity as a vector of economic growth through the following guidelines:

6.http://business.maryland.gov/fund/programs-for-businesses/cyber-tax-credit.http://www.choosemontgomerymd.com/programs-incentives/financial-tax-incentives/local-cybersecurity-investment-incentive-tax-credit-supplement#.VDbA2bF1yn8

7. http://khabarsouthasia.com/en_GB/articles/apwi/articles/features/2013/07/19/feature-01

8. http://www.enterprise-ireland.com/en/Research-Innovation/Companies/Source-licence-new-technologies/

1. Developing the industrial sector of suppliers of cybersecurity related products and services.
2. Increasing the number of cybersecurity products patents.
3. Improving cyber-protection in the private sector.
4. Training a highly skilled workforce in cybersecurity.
5. Increasing employment rate of highly skilled workers.

After analysing several national initiatives around the world, their main tax and legal incentive policies can be summarized in the following three blocks:

1. Support in reducing tax rates. The effectiveness of tax incentives to promote cybersecurity depends on the ability of governments to identify the activities granting rights to benefit from those incentives, since those should effectively encourage operational expenditure (OPEX) and investment (CAPEX), whether in services or technologies. The definition of "eligible costs", acceptable costs for task reduction, would be decisive. However, the access to these tax credit lines may require the involvement of various public sector actors and the development of regulations, as well as possibly a certification scheme for projects, services and technologies.

Moreover, launching cybersecurity goods and services in the internal market constitute a commercial activity that will generate benefits to suppliers, and VAT collection thanks to the purchased products.

However, if companies do not apply cybersecurity mechanisms, potential losses associated with cyber incidents can cause economic losses (between 2 and 4%, depending on the economic sector) that will impact on GDP and corporate balance sheets, reducing proportionally government tax income.

2. Reduction of administrative taxes and fees in the national register of patents, for those related to the cyber-protection, as well as an improvement of protection of technology patents.

3. Cyber-security regulation and legislation. Despite the existence of many technical recommendations and standards promoting the adoption of certain security controls, they are unevenly implemented, and even inconsistently applied. This creates regulatory uncertainty that can lead companies to face high risk levels of incurring financial, legal and reputational loss.

The adhesion of companies to voluntary programs of Cybersecurity, or total or partial implementation of controls, could provide greater legal certainty, acting as a mitigating measure or even full reduction of their liability in case of cyber-threat [9], especially when they are not subject to specific laws or administrative regulations.

## 2.2 Access to funding

To feed this industrial ecosystem and turn it into an incubator of entrepreneurship, enabling opportunities in this growing market, it is essential to solve the problem of access to capital.

Comparatively, USA and Asian companies benefit from better funding tools, in general. As evidenced by a recent study of A. T. Kearney[10], Countries such as China, South Korea and Japan fund their technology companies either directly through financial incentives and tax reduction, or indirectly through market barriers measures, that facilitate the contracts of services and products offered by them.

In the US case, the presence of a strong investment infrastructure of venture capital, offers easy access to funding for new businesses, while Europe has a heavily regulated banking sector and increased resistance to accepting risks. The Venture Capital is the main economic actor for financial support. Not to mention that in certain sectors, such as defence, the USA protecting policies pursue the direct support of USA national companies.

Traditionally, European governments have opted for giving priority to funding scientific-theoretical projects, rather than product development and market analysis. This factor, which could be referenced as cultural, should be added to an already low investment in R&D&I, in order to complete the differences between European and USA/Asian scenarios of investment.

This approach, based on the promotion of the culture of cyber-protection, could serve as an opportunity for organizations. On the one hand, by adopting cybersecurity best practices and control measures; and

9. http://www.ismsforum.es/ficheros/descargas/la-responsabilidad-legal-de-las-empresas-fente.pdf
10. The future of Europe's Hi-tech Industry, Kearney, 2013.

on the other, boosting the supply chain in the market, enabling the creation of industrial centres aimed at providing goods and services to meet the demand for cybersecurity.

In the European case, the governments could follow the example of the German one, which recently created a venture capital fund, specialized in information technology called Hi-Tech Gründerfond, with a budget of around 400 million euros. Similarly, it should also be taken into consideration the implementation of tax benefits for the deployment of venture capital funds investing in European cybersecurity projects and companies.

Cybersecurity has been introduced into the political agendas of most advanced nations, to be a priority in national security and defence strategies. However, dependence on foreign suppliers in building the different components of national cybersecurity strategies, is a weakness that must be mitigated. The initiatives being undertaken in other countries of our geopolitical environment highlight the urgency of agreeing on a comprehensive plan at national and European level, boosting and supporting private initiatives to invest in a professional way in development of mid- and long-term project to create and improve cybersecurity products and services.

"Cybersecurity has been introduced into the political agendas of most advanced nations"

In order to make realistic this goal, credit lines to industry must be created, and access to public funds and private investments should get incentives. The five-year and ten-year plans developed by the Chinese government have proved effectiveness to achieve results in this field. The short-term policies are not able to guarantee enough funding and investment in an area which requires high levels of training of human resources profiles capable of performing long term research and development.

The above proposed initiatives have a triggering priority its coordination by governments at European, national, regional and municipality levels, in order to ensure the uniformity of the processes and implementation objectives, without which the ecosystem cannot succeed.

## 2.3 Market incentives

With the aim of promoting the creation of a mature market in services and solutions related to security and defence in the cyberspace, it is important the creation industrial technological parks enable synergies through the entire cybersecurity supply chain, from manufacturers of technology solutions to specialized service providers.

To do so, in order to attract both domestic and foreign investment in this sector, the governments can create tax incentives, e.g. through credits deductible from the income or societal tax, for both private and corporate investors, as well as the funded companies, matching the eligibility criteria formally defined, such as:

a. The granted company is based in the national territory.

b. It is organized for profit and its corporate purpose is mainly the creation of cyber-protection technologies and services.

c. It should remain active for a minimum of five years and have a minimum number of employees.

d. It has actually satisfied all of its tax obligations and it has no contractual relationship with the Government at the time of receiving the aid.

Moreover, once these companies have met the criteria stated in this incentive, they could also be candidates for programs supporting the internationalization, e.g. through trade missions sponsored by foreign trade offices, chambers of commerce, supporting initiatives to progress in the internationalization of their target market for security technology.

Similarly, these two incentives should be supported through programs enabling access to credit and financial resources to SMEs in the initial stages of access to cybersecurity market, as already mentioned in the previous section. Another choice could be to follow the examples of Israel or USA, i.e. to allocate budget to the creation of a National Cybersecurity Investment Fund, acting as a government seed capital fund, aimed at the creation of start-ups, incentives to technological innovation, and specialized incubators.

## 2.4 Cyber risk policies

So far, most of the strategies to reduce corporate cyber risks are based on the concept of reducing the probability of success of a cyber-threat, through trying to reduce their exposure to it. Not so many of them address the complementary approach of risk reduction through measures to minimize the impact of the attack on the organization and its critical services.

It is in this scenario, cyber incidents insurance products are key elements for risk transfer. Through them, organizations get an insurance to cover the risk of pre-identified threats, and transfer its impact to the insurance company, which in turn gets an insurance premium.

The cyber-insurance, as they are also known, have a heterogeneous coverage, which primarily protects organizations from own damage (cost of recovering data, restoring public image, disinfection, legal expenses, independent experts, operating costs, profit loss, etc.) and damage to third parties (offenses to honour, intellectual property of others, failure in the duty of confidentiality, breach of contract, etc.).

These products are growing up as a strategy to promote more robust cyber-protection measures, through the insurance premium reduction as a "reward" to their adoption, much like what happens with car insurance. Insurance companies often focus on the awareness of its insurance holders, as they tend to relax in the implementation of controls, since they feel safe knowing that the loss risk has been transferred to a third party.

Consequently, insurers can play a key role in improving cybersecurity market maturity because:

1. Customers may be required to meet compliance and minimum safeguards for security as a prerequisite for the acceptance of insurance coverage, including e.g. the adoption of a framework of good practice.
2. Insurers can offer premium discounts to entities demonstrating an appropriate level of maturity in security, in ways that reduce the risk of loss transferred to the insurer.
3. Insurers can implement, advise or support handling of cyber incident response procedures, on behalf of the insured customer, improving a coordinated response to it.
4. Since insurers need reliable data to guarantee adequate

quantification of covered risks by subscription departments, allowing them to implement cost effective pricing policies. The growth of cyber-insurance Market could lead to a better understanding of the threat patterns and improvement of information exchange between the government supervisor and insured companies.

5. The insurers themselves may develop monitoring mechanisms aimed to assess the state of cyber-risk of their customers markets, playing an important role in early warning of incidents.

While it is highly recommended to keep the cyber-insurance market completely private, government agencies could encourage the adoption of these products through creation of action lines such as:

1. Reduction of the insurance premium by transferring part of the insurance coverage (risk) to public reinsurance programs.

2. When risks are considered "uninsurable" by the private insurance market, it could be considered by the governments to take the risks in order to stabilize the private market, for example, through specific compensation programs. E.g. in the Spanish case it could be driven it through the Insurance Compensation Consortium.

3. Recognize the adoption of cybersecurity frameworks, with a certain level of maturity, as an example of due control, being thus its implementation a mitigating agent to protect from potential attacks and limiting the extent civil and even criminal liability of attacked organizations.

## 2.5 Public recognition

Despite the existence of abundant legislation which is referenced mandatory for all companies to report "significant events" and these mainly fall on listed companies. Moreover, these regulations are focused on the principle of complete or full disclosure [11] with relevant facts, which favours certain reluctance to comply with them. For this reason, and given the difficulty and lack of resources to audit and detect such incidents, notification thereof becomes a corporate commitment to society in general, and especially to its "Stakeholders": customers, investors and market agents.

By virtue of this principle, companies are required to publicly provide "accurate, complete, effective and timely information to enable investors to build their own view on the status of the company, and to contribute to the smooth functioning and transparency of the stock-market."

Understanding that "any information not known to the stock-market that may substantially affect the price of the affected shares, is likely to constitute a relevant fact" [12], we could think that a cyber-incident which internal and/or external impact was significant, should be considered a relevant fact, and consequently, had to be publicly notified.

For this reason, the Governments should incentive companies to clearly and diligently communicate cyber incidents of particular relevance to Society, thus recognizing their corporate social responsibility. For example, the proof through a regulated process and the inclusion in the corporate annual report of evidences of the commitment of the company with transparency in reporting cyber incidents, could a basic criteria to grant companies the right of contracting with the Public Administration or to go public.

"Governments should incentive companies to clearlyanddiligently communicate cyber incidents"

Countries like the UK [13]

11. Cachon JE White, Securities Market Law, Madrid, 1992, vol. II.
12. Internal Regulations. CNMV. https://www.cnmv.es/docportal/Legislacion/resoluciones/RRI_CNMV.pdf

or Australia [14] have reacted to that need to regulate a growing market, with guarantees of professionalism and quality. The Governments and non-profit organizations could become the reference for the creation of a consolidated cyber-security industry in their countries. Public recognition of the commitment of companies and professionals with cyber-security, could be achieved through the creation of certifications and a public list of certified companies. These lists act as centralized public point of reference in the market by providing:

1. A positive business impact and reputation for companies and professionals listed there.
2. An evidence of the level of security of processes and procedures, and a validation of the expertise of certified organizations.
3. A guidance, through standards and challenges, to share and improve knowledge.
4. A quick way to get into the Market of cybersecurity skills, services and technologies.

## 2.6 Ease to public procurement

The Public Administrations (PAs) have a dual role: a) as providers of critical services to Society and b) as regulators of the market and the economy. This dual responsibility also offers the ability to set the minimum requirements to be met not only by the suppliers of their services, but also of those considered critical to Society, following the example of the European Directive on Services Trust. [15]

This Regulation capability has a dual function:

1. Define the thresholds over which organizations' security plans must be placed.
2. Help security managers to get the resources needed to implement the minimum required security mechanisms stated in the Regulation.

An example would be the definition of a standard criteria for classifying information, standardizing systems needed to efficiently and satisfactorily handling Governments' information. This standardisation would, both a)

13. Crest. http://www.crest-approved.org/
14. Crest Australia. http://www.crestaustralia.org/
15. http://ec.europa.eu/digital-agenda/en/trust-services

unify procedures for accreditation of providers' products, giving them a European dimension in terms of requirements to fulfil; and b) it would it would set up international accreditation requirements for systems aiming to qualify for handling classified information. Thereby reducing cost and time required to validate security products by both providers and public institutions.

Accreditation of organizations capability to offer services to Public Administrations has always been a controverted practice, since the lack of uniformity and harmonization of criteria with those of other European administrations constitutes an unfair administrative barrier.

Defining selection criteria based on internationally recognized standards and good practices would encourage its adoption, as it would facilitate the accreditation of skills to qualify for the provision of services to any European Public Administration.

In fact, this is one of the objectives of the European Commission with Directives and Regulations, to achieve the "single market", removing administrative barriers.

These capabilities can make reference to both the management of security processes, such as the preservation of personal data, as well as the capabilities of staff involved in the service provision. In this regard the European Commission asked the European Union Agency for Network Security and Information Security (ENISA), in the European Cyber Security Strategy of 2013, to draft a roadmap for the implementation of standardized training services for a Network and Information Security Driving License, thus extending the already internationally recognized European Computer Driving License (ECDL).

## 2.7 Prioritization of technical assistance by the Government

Prioritized technical assistance is a measure whose proper implementation would be a clear incentive for the adoption of internationally recognized cybersecurity good practice frameworks by business organisations, regardless of their size.

This incentive, although it should be conceptualized as a basic government service, is proposed as a benefit of higher level of service and speed, for organizations meeting cybersecurity requirements. However, it should be interpreted as a complement, i.e. not a replacement, of other cybersecurity mechanisms companies should implement with their own resources, such as cyber self-protection, as well as real time information exchange with governmental cyber-security institutions.

This provision of technical advice tailored to the specific circumstances of each applicant organization, both promptly during an incident, as well as on a regular basis. It could be performed by governmental CERTs and CSIRTs offering public services, such as established sectorial bodies, if any, providing immediate and flexible response, increasing resilience to cyber threats.

Thus, assistance activities could be classified as follows:

1. During an incident:

a. Support real-time resolution.

b. Coordination with ISPs, CERTs, governmental Law enforcement Authorities and others.

2. On a regular basis:

a. Supporting the implementation of the protection mechanisms of the selected framework.

b. Training and awareness.

c. Generating cybersecurity security operation and incident response document templates.

In any case, certain aspects should take into consideration by the Government for effective adoption of this incentive:

• Scalability and costs: the program, being funded by central government bodies, could be facing a scalability problem of both personnel and technical nature, since the number of enterprises and organisations meeting the requirements giving them the right to have access to this service could quickly grow.

• Prioritization criteria: facing a potential lack of public resources to provide services to too many enterprises, one option could be to prioritize eligible companies by sector (e.g. favouring operators of certain critical infrastructures).

• Advertising and competence with the private sector: it is necessary to complement the deployment of this mechanism with a communication campaign, spreading a message of completeness and proportionality. It could be shown as a service addressed mostly to those companies with fewer resources available. Similarly, it should be emphasized that these measures are in no way replacing other mechanisms, so the private cybersecurity providers should not feel displaced. In fact, public support should be proportional to private investment, so that whoever does not adequately invest in their own security, neither should receive this public support.

• Reputational impact: it is necessary to mitigate, through a strict duty of confidentiality, the risk of "stigmatization" of companies using the technical assistance, if certain incident details are disclosed to the Market. The claim of support by governmental cybersecurity providers by private organizations, could be encouraged through service level agreements ensuring confidentiality of public service provider and null or positively controlled media impact in its sector.

• Monitoring eligibility. This measure is not a substitute and, therefore, the eligibility of the recipient companies should be supervised. There is some risk of irresponsibility on the side of businesses, of them not acting diligently and not taking, by extension, the minimum measures (due care) to secure their systems, relying on government institutions to properly react to a cyber-attack.

# 3. Analysis of initiatives at the international level

3.1 Europe

3.2 USA

3.3 Israel

## 3.1 Europe

Cybersecurity is one of the priorities of the European Union since the creation in 2004 of his agency ENISA (European Union Agency for Network and Information Security) which aims to encourage and advise governments of Member States in the implementation of legislation and regulation on cybersecurity, trying to harmonise the 28 governments' conditions and legal incentives for the implementation of security measures.

Later on, other European institutions were created:

- The Computer emergency response team of the European Institutions (CERT-EU) in 2012. It is aimed to advice and support responses to cyber-attacks to the European institutions, encouraging the application of preventive measures in them, and being an example for similar national organizations.
- The European Centre for Cyber Crime (EC3), subordinated to EUROPOL, in 2013. Heir to the cyber-crime division of EUROPOL, it is responsible for planning and coordinating all the European LEA (Law Enforcement Authorities) cyber-crime related actions. It concentrates in detecting and prosecuting supranational cybercrime, and in developing tools and methodologies for national LEA to improve quality and responsiveness to cyber-crimes.

The Parliament and Council of the European Union have developed several policies and regulatory plans for direct application or (indirect) transposition into Member States legislative framework:

a) The European Cyber-security Strategy, adopted on February 7, 2013[16] , sets out five strategic priorities:

1. Achieve the cyber resilience, creating coordination mechanisms and encouraging the publication of data from cyber incidents.
2. Drastically reduce cybercrime.
3. Deploy policy and cyber-defence capabilities related to the Common Security and Defence Policy.
4. Develop technological and industrial resources for cybersecurity.
5. Establish a coherent European policy for international cyberspace and promote core values in the European Union.


16. JOIN (2013) 1 final "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber-space".

b) European cybersecurity Directive[17], aimed to standardize the minimum level of network and information security in Europe, establishing a common regulatory framework and cooperation mechanisms, through exchanging information in a cooperative network and establishing incident reporting mechanisms, with the aim of improving efficiency in incident management.

This cooperation will optimize resources, avoid duplications and thus reduce the costs of implementing basic security mechanisms, such as risk analysis, governance, awareness and incident prevention.

c) Research and Innovation Project Financing Programme: Horizon 2020. In late 2013 the eighth framework for research and innovation of the European Commission (EC) program "Horizon 2020" was approved. With this initiative, EC aims to co-finance mainly innovation in the implementation of security measures, promoting the use of developments already made that need their implementation in use cases and demonstrators, showing their efficiency and helping other organizations to implement them: with the minimum resources, avoiding mistakes and taking advantage of the lessons learned in previous public funded projects.

## 3.2 USA

Obama's Administration, in response to the rising number of cyber-attacks on their governmental information systems and critical infrastructures, has prioritized the resilience of their public administration, financial and other critical services, strengthening defences against cyber threats through implementation of technical standards and early response guidelines.

President Obama, failed to get Congress approval of legislative demand to companies to improve protection of their ICT infrastructures, mainly required by critical infrastructure operators. The members of the congress argued that it would require a number of legal reforms and a strong financial program. For this reason Obama's government issued a special Executive Order, known as EO13636 that focused most of in effort in

17. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

incentives for cybersecurity industry.

This executive order signed on February 12, 2013, empowered agencies and federal governments to develop cybersecurity standards for private sector industries, and propose new procurement rules, if needed. Its primary objective is to help the federal governments to protect critical infrastructures[18].

The executive order states that the Homeland Security Department will be the cyber threats information hub. It will be responsible of sharing it with the several governments and private companies with responsibilities for the protection of critical infrastructures. This order also required NIST to develop a cybersecurity framework, based on voluntary incorporation of companies responsible for critical infrastructure, which was published in February 2014[19].

To accelerate the adoption of the good practices framework and trying to mitigate the economic impact of its adoption by private companies, launched parallel ambitious plan of tax, market and financial incentives for operators of critical infrastructures and the cyber-protection market.

With some flexibility and federal autonomy, certain states such as Maryland, have fostered the creation of industrial poles, similar to those of their Israeli partners, concentrating ciber-security technology and services companies.

## 3.3 Israel

The continuous and important geopolitical changes taking place in the Middle East added to the proliferation of state and non-state actors with advanced cyber capabilities in the area, place Israel in a situation of permanent risk.

This has meant that since the mid-1990s successive Israeli governments have prioritized the development and competitiveness of domestic cybersecurity industry, with especial emphasis in the national program of technology incubators and internationalization of cyberspace technology sector policy.

18. ExecutiveOrder -- Improving Critical Infrastructure Cybersecurity.
http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
19. Framework for Improving Critical Infrastructure Protection.
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

In 1991, the Israeli Ministry of Industry created the national program of technology incubators[20] with the aim of transforming ideas into innovative technology companies. Moreover, these incubators have as secondary objectives: to promote R&D in strategic capabilities for security and defence of the country[21], creating an enabling ecosystem for the private sector to invest in new businesses, and a culture of entrepreneurship in the country.

"the Israeli Ministry of Industry created the national program of technology incubators"

In 2014 the budget allocated by the government of Jerusalem to its program of technological incubators reached the amount of 40 million euros. Companies that are part of one of the 22 technology incubators scattered across the country -of which an estimated 10% dedicate their activity to cybersecurity - will receive during the two years of sponsorship in the incubator an annual grant ranging between 350,000 and 600,000 euros. On top of that, during these two years the entrepreneurs will receive deep training on business administration and management, as well as legal and regulatory aspects. After finishing their stay in the incubator, companies successfully integrated in the markets must reimburse the government for 85% of the received amount, during the next twenty years; in the event of cessation of business entrepreneurs see their debts forgiven. Another important aspect of the national program of technology incubators is the fact that foreign firms may also be beneficiaries of it.

The policy of internationalization of Israeli cybersecurity industry has leaded the country to become one of the major world leaders in the sector, stimulating exports and encouraging foreign companies' settlement in Israel, with very advantageous fiscal policies. It is estimated that 7% of global turnover in Cybersecurity[22] is generated by Israeli companies, many of them from the national program of technology incubators.

In summary, Israel is a world power in cybersecurity, thanks to inclusive and incentives government policies.

20. http://www.incubators.org.il/article.aspx?id=1703
21. http://www.moital.gov.il/NR/rdonlyres/5E7A4322-4D0F-4320-953C-83F94024E7AA/0/RDspreads.pdf
22. http://www.asdnews.com/news-53610/Global_Cyber_Security_Market_to_be_Worth_$76.68bn_in_2014.htm


Detailed information of changing business activity of subdivisions of main company
Subdivision 1
Subdivision 2
Subdivision 3
Best subdivision value
Value of all subdivisions
Product placement in different
Subdivisions

# 4. Spanish cybersecurity incentive program (PICE)

4.1 Reference Framework

4.2 Recommended Incentives

4.3 Failure Critical Factors (FCF)

4.4 Conclusions

# 4. Spanish cybersecurity incentive program (PICE)

The Spanish National Cybersecurity Strategy (ECN) adopted in late 2013 recognizes the strategic importance of a reliable cyberspace, resilient and safe, aligned with EU policies and OECD, it encourages proper development focused on digital society and economy growth, employment and welfare.

While ECN sets its roadmap aligned with the Digital Agenda for Spain (Agenda Digital para España, ADPE)[23], some of the specific actions in achieving the abovementioned objectives for the Spanish industry are developed in the Digital Trust Plan (Plan de Confianza Digital, PCD)[24], which responds to the European Cybersecurity Strategy (EU CSS)[25], it also includes initiatives promoted by ENISA.

Whilst the primary goal is to improve the level of resilience of the Spanish industry, as already reflected in the PCD, a collateral directive is aimed to create a "[...] opportunity axis for ICT industry, intended to provide subsidies and financial incentives to companies throughout the cycle of R&D&i of products and services of digital trust, promoting technical standardization, certification and internationalization".

Thus, amongst others, it has launched an industrial cooperation initiative called: National Forum for Digital Confidence (Foro Nacional de Confianza Digital, FNCD)[26], one of which objectives is to study and propose stimulus measures and incentives to encourage investment of ICT industry and its adoption by the customers, in both the public and private sectors.

But, together with the development of cybersecurity industry, the domestic business sector -from big companies to SMEs- should first adopt and to deploy a framework for cybersecurity best practices, meeting increasing regulatory framework requirements in the field, and second, to do dynamic analysis and management of their cyber-risks; all these actions have associated some economic contribution.

23. Digital Agenda for Spain (Agenda Digital para España, ADPE) http://www.agendadigital.gob.es/

24. Plan Trust in the digital space (Plan de Confianza Digital, PCD) http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaconfianza/1.%20Plan/Plan-ADpE-5_Confianza.pdf

25. European Cyber Security Strategy (EUCSS) http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

26. National Forum for Digital Confidence (Foro Nacional de Confianza Digital, FNCD) http://www.agendadigital.gob.es/FNCD/funciones/Paginas/alcance-fncd.aspx

In this way, the proposed framework: Spanish cybersecurity incentive program (Programa de Incentivos a la Ciberseguridad Español, PICE), would have as main objective to recommend a first set of incentives, designed to adopt a framework of best practices in cybersecurity, aligned with the existing activities of promoting investment and R & D. Examples of those activities as the ones contained in the Plan to promote the digital economy and digital content[27], as well as those developed by the Technical Coordinating Committee at as requested in the Measure 6 of PCD.

The proposed incentive scheme, without aiming to be exhaustive and with a purposive interest, will additionally require specific actions:

1. Evaluation of benefits, effectiveness and efficiency of incentives aimed at improving the cybersecurity maturity level.
2. Assessment of public funding needs associated with each activity.
3. Identification of which of these incentive actions require extraordinary legislative or regulatory efforts.
4. Creation of a micro-economic conceptual model to take into account the probability of adoption of the proposed framework in the Spanish cybersecurity sector, as well as in the public administration itself, considering marginal benefits and costs.

## 4.1 Reference Framework

The first decision to address, in parallel with the design of the incentive plan, is to analyse the need for adopting an existing framework of cybersecurity best practices, acting as a reference framework in the Market. It could be complemented with industry regulations, binding the industrial, services and technologies sectors, as well as the sector for the protection of critical infrastructure. Moreover, it may also be possible to develop a specific regulatory framework, covered by public agents (as happened with the Spanish National Security Scheme, regulated in RD 3/2010 of 8 January) and/or by Standardisation bodies authorized for this purpose, as AENOR, AFNOR, BSI, CEN-CENELEC, ETSI, etc.

According to the authors of this document and given, first, the existence of a growing legislative framework and policies for cyber security and defence; and, second, the membership of Spain in two large blocks that draw our geopolitical scenario: the European Union (EU) and the North Atlantic Treaty Organization (NATO); the alignment of a new hypothetic national

27. http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-impulso-contenidos-digitales.aspx

"it is recommended the adoption of a recognized reference framework"

cyber security framework with the commitments achieved with those international organisations, would require a big effort.

For this reason it is recommended the adoption of a recognized reference framework, enabling cross recognition by our international partners. That practice would facilitate also the internal work of the Spanish companies to implement such controls, since they would be recognized in global markets, reducing the costs associated with the internationalization of enterprises. Such a framework of best practices in cybersecurity, however, could be formalised through a national standardisation schema, by an authorized body for this purpose.

To achieve cybersecurity level standardization in our territory, through the adoption of this framework of good practices, the Government should support this challenge by establishing a set of incentives with a multi-sectorial vision enabling companies to implement those measures, that will allow them to have a secure cyberspace and to respond to one of the guiding principles of the National Security Schema (Esquema de Seguridad Nacional, ESN): shared responsibility.

## 4.2 Recommended Incentives

This study elaborated between THIBER and ISMS Forum Spain, with the collaboration of APWG.EU, proposes a number of public incentives, based on the range of incentives defined in an initial review conducted before the elaboration of the Spanish cybersecurity incentive program (SCIP) has begun.

The proposed incentive plan vertebrates around 7 lines of action, materialised in the following 23 suggested incentive actions, detailed in the following sub-sections, and summarised in a table at the end of this section.

### 1. Framework of Legal incentives

1.1 Program tax incentives, reducing tax rates for companies in the acquisition of technologies and services that support the

adoption of marc n cybersecurity or established. These solutions and services must be duly justified through a process of approval and/or certification by a public official who shall also define the concept of "eligible costs" or "deductible" in both operating costs (OPEX) and investment (CAPEX).

1.2 Reduced costs and administrative fees in the national register of patents relating to the cyber-protection and improved protection technology patents in cyber-protection.

1.3 Development of regulations and specific legislation on cybersecurity for the Spanish industry and general government, unifying compliance and the potential overlap of existing requirements and supplementing Directive s Security Networks and Information (SRI)[28], the future European Regulation on Protection of Personal Data and Regulation of Electronic Identity and Trust Services. This regulation should reflect an analysis of international initiatives, recognizing equivalent foreign regulatory regulations (type Safe Harbour), reducing the burden of audit and compliance validation.

1.4 Limitation of civil and criminal liability by demonstrating an implementation of the control framework for cybersecurity mentioned, showing diligent management and proper control over business processes with regard to their cyber protection measures.

## 2. Access to finance and investment funds

2.1 Inclusion in financing instruments General Administration existing State and Official Credit Institute, new variables in credit lines granting programs and state funding on favourable terms for compliance and adoption framework of good cyber-security practices established for that purpose.

2.2 Tax incentives and financing associated with R&D&I in cybersecurity activities, mentioned in the Plan for development and innovation in the ICT Sector[29], with special emphasis on research programs linked to the promotion of technical research, extending industrial policy and creating more tractors projects within the National R&D&I related with cyber-protection, bringing supply and demand.

2.3 Government aid for investment in companies cyber national security and start-ups throughout the investment cycle, whether seed capital or venture capital for internationalization,

28. http://europa.eu/rapid/press-release_IP-13-94_es.htm
29. http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-sector-tic.aspx

supported and advised by specific interest groups and industry, being able to grant tax deductible claims on the income tax both investors and host companies which own eligibility criteria defined suits a formal guidelines taking advantage of the ecosystem and current public-private initiatives.

### 3. Cybersecurity Market growth

3.1 Specific support to access to new markets and internationalization projects by specific trade and diplomatic campaigns, with special emphasis in LATAM and Middle East, building on existing in the General State Administration and the Technological Business Internationalization Plan[30].

3.2 Creating industrial parks, acting as an incubator and business accelerator focused on cyber protection technologies. This must be the embryo of an ecosystem enabling the private sector to invest in new companies. This incentive will be the logical extension of the PDC-9 as Digital Trust Plan, as well as another line to include in the policies of the Ministry of Economy and Finance through the Ministry of Economy and Business Support.

3.3 Development of a National Investment Fund Cybersecurity (NCSIF), allowing public investment in this sector, so as to allow balancing the need for existence of niche companies in this sector, but also can contemplate reducing the current division acting as a partner a robust public investor company (called "champion") that can compete in international markets.

### 4. Ciber-insurance Market Development

4.1. Stimulation of cyber-insurance services market demand, transferring a mandatory risk coverage in contracts with Public Administration.

4.2 Campaigns to reduce costs in hiring insurance policies, through mechanisms such as:

• The recognition of the adoption of cybersecurity frameworks with a maturity level determined as a reduction mechanism own damage and third derivatives of a cyber incident.

• Reducing the cost of premiums by taking on part of the coverage from private insurers through reinsurance programs.

4.3. Creating guarantee funds to cover damages of high impact cyber-threats,, considered "uninsurable" risks, in order to replace or stabilize the private market, enabled through the Insurance Compensation Consortium,



30. http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-empresas-tecnologicas.aspx

attached to the Ministry of Economy and Finance, and through the Directorate General of Insurance and Pension Funds.

4.4 Enable the ability of the Insurance Compensation Consortium, acting as direct insurer in the event that the private market failure in the provision of cyber-insurance (e.g. for lack of insurance or insolvency of the insurer), but without competing with the private sector.

### 5. Public recognition

5.1. Preparation of a list of companies authorized to provide cybersecurity services.

5.2. Obligation to practice full-disclosure in the Corporate Annual Report of private companies, showing their activities and more Relevant benchmarks related to cybersecurity and the need to report security incidents to public agencies and the market itself.

5.3 Professionalism in the cybersecurity industry, by creating certification schemes and training for professionals and companies. Thus, the employment rate will increase with highly specialized workers.

### 6. Optimization of Public Administration procurement process

6.1. Reduction of time to sign a contract with Public Administration, as an exclusive benefit for companies that certify the adoption of the control framework.

6.2. Reduction of administrative delays associated with accreditation and approval of ICT systems used to handle restricted, classified or secret information.

6.3. Reducing bureaucracy and paperwork in skills accreditation in public tenders.

### 7. Prioritization of technical assistance by the Government

7.1 Advisory support in implementing selected controls of the cybersecurity framework.

7.2. Improvements in the level of support to cyber incidents, given that the involved company has enabled information sharing mechanisms and demonstrated due diligence in implementing cybersecurity framework, thus prioritizing provision of INCIBE's capabilities as national coordination CERT for industrial cyber-Incidents.

7.3. Definition of concise guidelines about how to implement the necessary security measures within companies and industry.

| INCENTIVES | PRIORITY |
|---|---|
| 1. Legal framework of incentives | |
| 1.1. Program tax aid | Medium |
| 1.2. Reduced costs and administrative fees in patenting | Low |
| 1.3. Development of regulations and specific legislation on cybersecurity | High |
| 1.4. Limitation of civil and criminal liability | Low |
| 2. Access to finance and investment funds | |
| 2.1. Creating a program of credit lines and financing | Medium |
| 2.2. Aid for R & D + i in Cybersecurity | Medium |
| 2.3. Government aid for investment in national cybersecurity companies | High |
| 3. Cybersecurity market momentum | |
| 3.1. Specific support in access to new markets and internationalization | Medium |
| 3.2. Creating industrial parks, business incubators and accelerators | Medium |
| 3.3. Development of a National Cybersecurity Investment Fund | Low |
| 4. Cyber-Insurance Market Development | |
| 4.1. To stimulate market demand of cyber-insurance services | High |
| 4.2. Campaigns to reduce costs in hiring insurance policies | Medium |
| 4.3. Creating guarantee funds to cyber threats high impact | High |
| 4.4. Enable the ability of the Insurance Compensation Consortium, acting as a direct insurer in the event that the private market fails in insurance | Medium |
| 5. Public recognition | |
| 5.1. Preparation of a list of companies authorized to provide cybersecurity | Medium |
| 5.2. Obligation to practice full-disclosure in the Annual Report Corporate | Medium |
| 5.3. Professionalism in the cybersecurity industry, by creating certification schemes and training of professionals and companies | High |
| 6. Optimizing procurement processes with the Public Administration | |
| 6.1. Reduction of recruitment time with public administration | Medium |
| 6.2. Reduction of administrative delays associated classified accreditation and approval of ICT systems | Low |
| 6.3. Reduction of procedures for accreditation of skills in public tenders | Low |
| 7. Prioritization of technical assistance by the State | |
| 7.1. Support the implementation of selected reference frame | Alta |
| 7.2. Improvement in the level of support to cyber incident | Alta |
| 7.3. Definition concise guidelines on how to implement the necessary measures within the company | Media |

## 4.3 Failure Critical Factors (FCF)

The authors have identified three (CFF) associated with the actual implementation of the proposed incentives. After analysing similar strategies addressed by other governments, national idiosyncrasy and peculiarities that have leaded to the success of other initiatives, the conclusion is that success (and failure) factors will not be easily replicable and transferable from one national Incentive Program to another.

The identification of these FCF is an essential first step to start up the road map towards achieving the following objectives:

1. First FCF: insufficient promotion campaign.

The program should be accompanied by a promotion policy, clear and concise communication and public dissemination of incentive framework, creating several prototypes of business case stage shown ROI derived from improved cyber security in organizations. This media campaign should have international reach through embassies, so that they act as an attractor of foreign investment capital.

2. Second FCF: short term approach for Framework implementation.

The proposed incentive framework should handed a five-year time horizon or even ten, breaking quadrennial periods of legislatures, since the focus of the strategy should be the medium to long term, although some lines of incentives are contemplated short, such as those referenced to market cyber-insurance. The short-term policies are not able to secure sufficient funding and investment in an area which requires high levels of training under the profile of human resources and long research and development.

3. Third FCF: Relevance Scope of the cybersecurity framework.

The control framework should be applied exclusively to the private sector. For the entire business value chain cybersecurity and industrial truly resilient implementation of the framework of good practice should be equitable and, by extension, also apply in the Public Administration.

## 4.4 Conclusions

The Government needs to complement the above described cybersecurity incentives, with design and deployment of a realistic plan of business incentives, in order to ensure a correct and massive application of measures cyber-protection in the industry and services, in a reasonably short time. Those plans should be based on the premise of cybersecurity costs distribution amongst all involved stakeholders.

Thus, the adoption of the proposed incentives, would be the first inclusive approach of this nature, aimed at improving the level of cyber resilience of the industry and emphasizing an emerging market of cyber-protection products and services, undercovered by cooperation, sharing of responsibility and knowledge strategies.

Please visit the following webpages for more information
www.ismsforum.es www.thiber.org

An initiative of: ISMS Forum Spain THIBER The cybersecurity think tank In collaboration with: APWG.EU Telefónica