POLICY RECOMMENDATIONS FOR CYBER SECURITY

GREEK CYBERCRIME CENTER

Greek CyberCrime Center

August 2015

www.cybercc.gr

PREFACE[1]

Dear Reader,

Our objective in this booklet is to provide you with guidance on a delicate issue of major importance: cybersecurity in the information age. Members of the Greek Cybercrime Center drafted it with care, in order to give you a feeling of comfort about such a key issue.

It is routine talk to say that cybercrime occurs very often and that it affects all of us. It affects, firstly, businesses, which need to derive a security policy and to safeguard their assets. Also, individuals are affected by security flaws and gaps, as hackers are targeting their private information. And finally, governments and public entities may suffer damages, e.g., by DOS attacks and other intrusive actions, while critical infrastructure may be targeted by cybercriminals.

We thus believe that the understanding of security threats, needs and measures in order to ensure and promote cyber security is a necessity for all users of information systems and that can only be achieved when awareness is high and guidance is provided by specialized experts in the field. That is why, we gathered all necessary information on the issue of cyber security in this booklet.

The first part of the booklet is devoted to a description of the ever changing landscape in information and communication technology, and the emerging security risks. It is followed by an in depth analysis of the legal landscape at European and national level as it dynamically evolves in recent years. Next, top level security principles for business are offered but also more specific everyday tips for professionals and individuals. An effort to identify gaps and provide recommendations for policy makers follows, along with a description of the main actions of the Greek Cybercrime Center.

It is our hope that this guide will serve its purpose of enlightening all relevant stakeholders in this crucial area.

[1] This research was performed with the financial support of the Prevention of and Fight against Crime Programme of the European Commission – Directorate-General Home Affairs (project GCC). This publication reflects the views only of the Author and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

CONTENTS

AUTHORS

Meltini Christodoulaki, *FORTH and SafeLine*

Paraskevi Fragopoulou, *FORTH and Tech. Ed. Inst. of Crete*

Nikos Frydas, *SafeNet*

Ioannis Iglezakis, *Aristotle University*

Evangelos Markatos, *FORTH and University of Crete*

CONTRIBUTORS

Elias Athanasopoulos, *Vrije Universiteit*

Philippe Jougleux, *European University of Cyprus*

Stefanos Malliaros, *KEMEA*

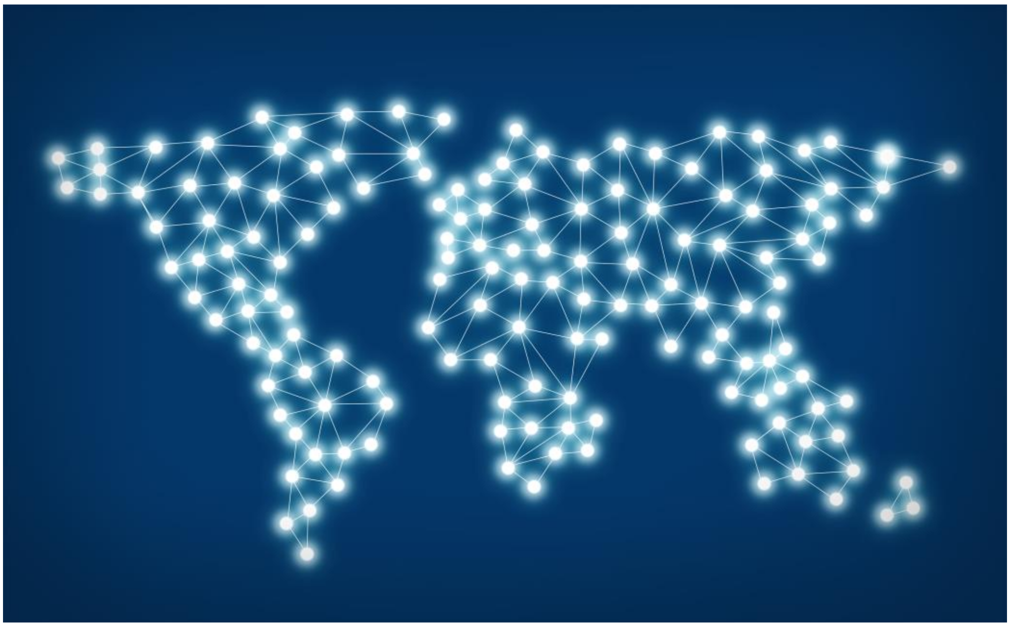
Lilian Mitrou, *University of the Aegean*

Tatiana Synodinou, *University of Cyprus*

1 INTRODUCTION

1.1 The Landscape of Information and Communication Technology

It is commonplace that we live in a networked world, in which Information and Communication Technology (ICT) plays a key role in manipulating and line-streaming the voluminous flows of information. As our ICT-dependence is growing, however, so is the vulnerability of our information assets and other personal and business assets. Over the past few years rapid technological developments have radically changed the way we work, cooperate, communicate and live: The cloud, the personalization of devices, the Internet of Things, the Web 2.0, the electronic identity systems and the move towards a digital-only world.



The Cloud – Nowadays, interconnection is a pertinent aspect of almost every system and it is accompanied with an ever growing need for exchange of information between different entities. Moreover, a distribution of information storage has taken place, as individuals and major organizations store information in the cloud, that is, in third party data centers and not in their own facilities.

Ubiquitous personal communication devices – Camera/video enabled mobile phones are now used as media players, games consoles, location aware devices, and interfaces to payment systems. Individuals can also become themselves publishers permitting audio-visual recording of personal data to be collected and transferred to the Internet for limitless onward transfer and persistent storage.

The Internet of Things and Services – Communications networks and changes to the core architecture of the Internet and its protocols (e.g. Internet Protocol version 6, IPv6) permit many more physical objects to have an Internet address, paving the way for a wide range of devices to be connected, such as vehicles, white goods and clothing. Combining these technologies with Radio Frequency Identification (RFID) affects the exposure of information to third-parties.

Web 2.0 – A series of services are developed: web-based communities, hosted services, web applications, social networking sites, video sharing sites, wikis, blogs, mashups and folksonomies. Users are enabled to interact with other users or to create content, websites.

Electronic Identity Systems (eIDs) – They are used both in the private and public sectors: mostly in the form of smart cards or biometrics. In the private sector, eIDs are used to control access to workplaces, travel and payment as well as for identification and authentication. In the public sector, eID technology is being used in identity management applications that enable access to government services, provide efficiency gains by reducing the administrative burden for government back-office functions, and support the fight against organized crime and terrorism.

Everything is getting digital – Over the past few years we have migrated a significant percentage of our activities on-line. Entertainment, Information retrieval, travel management, and a wide variety of other activities have moved partially, or completely, from the traditional dusty paper-based world to the glamorous world of digital computers. It is actually hard to imagine any kind of activity that does not involve (or will not soon involve) a strong digital component. As a result, users have increased their dependency on the Internet and aggressors are presented with a wider variety of opportunities for attacks.

1.2 Security Risks

Cyberspace provides easy access to offenders, which can reach a huge number of potential victims, taking into account the number of users connected to the Internet, which is more than 3 billion or 40% of the earth population. The fact the Internet is a network that can be accessed anonymously is an advantage for perpetrators. The networked nature of modern ICT means that tracing of communications is extremely difficult and asserting jurisdiction over illegal acts is hard to accomplish.

Thus, security incidents are constantly increasing. Clearly, no system exists that is impenetrable, but rather it is a fact that security incidents sooner or later happen. These range from intrusion into PCs (viruses and other malware) to more sophisticated attacks against information systems and critical infrastructure, resulting into immense damages.

The history of infecting computers and computer systems is long. So, e.g., the ILOVEYOU virus in 2000, which was actually a computer worm, attacked tens of millions of Windows PCs, starting from Philippines and wide spreading throughout the entire world via email systems. Similarly, a series of viruses, Trojans and worms have become a plague for plain and corporate users of ICT.

Besides that, a series of security threats are evolving. So, e.g., hackers recently developed a technique to gain wireless control, through the Internet, to vehicles, using software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission. Even new IT products such as smart watches are not safe from security issues, but also baby monitors, which may become targets for a hacker attack[2].

> *"There are only two types of companies left in the United States: those that have been hacked and those that do not yet know they have been hacked"*
>
> The New York Times

Since such security threats cannot be ignored, we should develop not only technical defenses, but also an integrated security strategy that would include awareness raising among users of ICT.

[2] See, e.g., http://www.mirror.co.uk/news/uk-news/baby-monitor-hacking-how-criminals-3470243

2 THE REGULATORY LANDSCAPE

2.1 Overview

Cybersecurity, i.e., the protection of networks, computer systems and data from cybercrime, has become a national policy priority in many countries that realize its importance; new cybersecurity strategies are being developed to provide protection against cyber-threats and safeguard economic and social prosperity.[3] The aim of such strategies is to enhance governmental co-ordination and define roles and responsibilities with regard to tackling cybercrime, but also to underpin cooperation of public and private entities, particularly Internet Service Providers, and international cooperation.

Although most European Member States have published a cyber security strategy, there are many discrepancies between the Member States themselves mostly as far as Network and Information Security (NIS) is concerned. Indeed, while some Member States have shown clear advancements in this field, there is little cooperation among the Member States and there is no effective mechanism at EU level for cooperation and for official trusted information sharing on security incidents and risks. As we'll see below, however, some actions have already been taken at EU level and mainly two organizations should be mentioned: the E3C (European CyberCrime Center) related with the Interpol organization and the ENISA (European Union Agency for Network and Information Security).

Also the Article 35 of the Budapest Convention requires Parties to establish 24/7 contact points with the option of international preservation requests. However, it is established that this option is underused, because of unclear legal basis and complex procedures in some countries, unclear role of 24/7 contact points and limited knowledge and routines in the use of procedure and other channels are used[4]. Most recently, the European authorities have also created ENISA[5] (European Union Agency for Network and Information Security) as the "EU's response to the cyber security issues of the European Union"[6].

[3] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[4] Cybercrime Convention Committee (T-CY), Assessment report Implementation of the preservation provisions of the Budapest Convention on Cybercrime, Adopted by the T-CY at its 8th Plenary (5-6 December 2012), p.17, http://www.coe.int/en/web/cybercrime

[5] By Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013.

[6] https://www.enisa.europa.eu/about-enisa

The current regulatory framework in the EU requires only telecommunication companies to adopt risk management procedures and report security incidents (Directive 2002/21 and Directive 2009/136, amending Directive 2002/58). Insofar that personal data processing is taking place, data controllers and processors do have also security obligations under the Data Protection directive (Directive 95/46).

In other sectors, where ICT plays an important role, e.g., in e-shops, there is no legal obligation of providers to take appropriate measures to tackle with cyber security issues. The fact that there are different levels of preparedness within the EU is illustrated by the absence of any regulation in some States, while others have an advanced status of NIS. Some uncertainty also prevails as to the application of the existing legislation on critical infrastructure on Internet's infrastructures.

For example, in Germany, in July 2015 a new law was adopted to regulate cybersecurity (the IT-Sicherheitsgesetz)[7], which imposes several obligations to German corporations: (i) Critical German corporations need to establish a minimal set of security measures; (ii) they need to prove that they have implemented those measures by conducting appropriate security audits; (iii) they should identify a point of contact for IT-security incidents and measures; and (iv) they should notify severe hacking incidents to the federal IT-security agency, the BSI (Bundesamt für Sicherheit in der Informationstechnik[8]). In addition to these general principles, specific regulations apply to the telecommunications sector, which has to deploy state-of-the-art protection technologies and inform their customers if they have been compromised. This new law also obliges telecommunications providers to warn customers when their connection was abused, e.g., in a botnet attack, and provides for data retention, i.e., storing of traffic data for up to six months for investigative purposes. Similarly, strict regulations also apply to nuclear energy companies, which have to introduce higher security standards.

In France, three high-level policy documents should be mentioned, which serve as a comprehensive strategy in regard to cyberspace: a) White Paper on National Defence and Security of 2008[9], b) France's Cyber Strategy 2011[10]; and c) White Paper on National Defence and Security of 2013.[11] In 2009, the National Network and Information Security Agency (ANSSI) was established, who is now the main entity in charge of cyber security in France.

To address the lack of an effective mechanism at EU level for effective cooperation and information sharing in the field of cyber security, the EU has taken the following steps:

- ✓ The European Commission issued a Communication in 2001: Network and Information Security (NIS): Proposal for A European Policy Approach (COM(2001) 298 final), in which it outlined the increasing importance of NIS.

- ✓ The above Communication was followed by the adoption in 2006 of a Strategy for a Secure Information Society (COM(2006), 251).

[7] http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf

[8] https://www.bsi.bund.de/

[9] http://ow.ly/T7y7H

[10] *http://ow.ly/T7ypp*

[11] *http://ow.ly/T7yhC*

- ✓ The Commission further adopted a Communication on Critical Information Infrastructure protection in 2009 focusing on the protection of Europe from cyber disruptions by enhancing security. The Communication launched an action plan to support Member States' efforts to ensure prevention and response. The Action Plan was endorsed in the Presidency Conclusions of the Ministerial Conference on CIIP in Tallinn in 2009.

- ✓ On 8 December 2009 the Council adopted a Resolution on 'A collaborative European approach to network and information security'.

- ✓ The Digital Agenda for Europe (2010), and the related Council Conclusions highlighted the shared understanding that trust and security are fundamental preconditions for the wide uptake of ICT and thus for achieving the objectives of the 'smart growth' dimension of the Europe 2020 Strategy.

- ✓ In its Conclusions of 27 May 2011 on CIIP, the Council stressed the pressing need to "make ICT systems and networks resilient and secure against all possible disruptions, whether accidental or intentional, to develop across the EU a high level of preparedness, security and resilience capabilities, to upgrade technical competences to allow Europe to meet the challenge of network and information infrastructure protection, and to foster cooperation between the Member States by developing incident cooperation mechanisms between the Member States".[12]

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013PC0048

2.2 EU Legal Acts in the Area of NIS

It is important to note that the EU has already established an agency for information security, i.e., the European Network and Information Security Agency (ENISA), which was established under Regulation No 460/2004, with the aim of contributing to ensuring a high level and developing a culture of NIS within the EU.[13] The agency has recently received new responsibilities and powers in order to better assume its duties[14].

Furthermore, Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, a procedure for identifying and designating European critical infrastructures (ECIs) is established. At the same time, it provides a common approach for assessing these infrastructures, with a view to improving them to better protect the needs of citizens. The Directive applies without prejudice of the 'European Programme for Critical Infrastructure Protection (EPCIP)', which sets out the overall 'umbrella' approach to the protection of critical infrastructures in the EU.

A Directive on attacks against information systems (2013/40/EU) was adopted on 12, August 2013, which establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.[15] The Directive uses the terminology adopted by the Convention of Budapest while at the same time modernizing the legal framework. Mainly, the DOS attacks are expressly referred as an offence (the illegal interference to a system) and the criminalisation of hacking is limited to the case of violation of technical measure of protections, in order to protect the fundamental freedom of individuals.

To tackle cybercrime, the Commission adopted a Communication on the establishment of a European Cybercrime Centre (EC3) on 28 March 2012. This Centre was established on 11 January 2013 and is part of the European Police Office (EUROPOL); it acts as the focal point in the fight against cybercrime in the EU.[16] EC3 is intended to pool European cybercrime expertise to support the Member States in capacity building, provide support to Member States' cybercrime investigations and, in close cooperation with Eurojust, become the collective voice of European cybercrime investigators across law enforcement and the judiciary.

The European Institutions, agencies and bodies have set up their own Computer Emergency Response Team, called CERT-EU. At international level, the EU works on cybersecurity at both bilateral and multilateral level.

[13] https://www.enisa.europa.eu/

[14] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004.

[15] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF

[16] https://www.europol.europa.eu/ec3

2.3 The Proposal for an EU Directive

To deal with the issue of NIS on EU level, the Commission submitted a proposal for a Directive in 2013; namely, a Directive concerning measures to ensure a high common level of network and information security across the Union (COM(2013) 48 final).[17] In the Explanatory Memorandum for this Proposal, it is mentioned that the aim of the proposed Directive is to ensure a high common level of network and information security (NIS).

The objective is to improve the security of the Internet and the private networks and information systems that support vital functions of the society and the economy. This will be achieved by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures, such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc), as well as public administrations to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

The Draft Directive:

- ✓ lays down obligations for all Member States concerning the prevention, the handling of and the response to risks and incidents affecting networks and information systems;
- ✓ creates a cooperation mechanism between Member States in order to ensure a uniform application of this Directive within the Union and, where necessary, a coordinated and efficient handling of and response to risks and incidents affecting network and information systems;
- ✓ establishes security requirements for market operators and public administrations.

In particular, it provides for a national framework on NIS in every Member State. To achieve that, it states that each Member State should adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security. This strategy should address certain issues, such as the definition of the objectives and priorities of the strategy based on an up-to-date risk and incident analysis, a governance framework to achieve the strategy objectives and priorities, including a clear definition of the roles and responsibilities of the government bodies and the other relevant actors, the identification of the general measures on preparedness, response and recovery, including cooperation mechanisms between the public and private sectors, etc. The national NIS strategy should include a national NIS cooperation plan.

Of central importance is the obligation of Member States to designate a national competent authority on NIS with the objective to monitor the application of the Directive at national level. The competent authorities will have the power to require market operators and public administrations to: a) provide information which is necessary to assess the security of their networks and information systems and b) undergo a security audit carried out by a qualified independent body or a national authority. They should also have the power to issue binding instructions to market operators and public administrations, and to notify incidents of a

[17] http://www.ipex.eu/IPEXL-WEB/dossier/document/COM20130048.do

suspected criminal nature to law enforcement authorities; they should work in close cooperation with data protection authorities.

In addition, each Member State would be obliged to set up a Computer Emergency Response Team ("CERT") responsible for handling incidents and risks according to a well-defined process. The requirements and tasks of the CERT are laid down in Annex I of the Directive.

A cooperation network should be established between the competent authorities and the EU Commission with the aim to cooperate against risks and incidents affecting network and information systems. The ENISA should also assist the cooperation network, if requested. With this network, the competent authorities should, inter alia, circulate early warnings on risks, ensure a coordinated response, publish non-confidential information on on-going early warnings and coordinated response, jointly discuss, etc.

The Draft Directive also provides for the provision of early warnings within the cooperation network on risks and incidents that grow rapidly or exceed national response capacity or affect more than one Member state and for a coordinated response, following an early warning.

It also aims to ensure that a culture of risk management develops and that information is shared between the private and public sectors. Companies in specific critical sectors and public administrations will be required to assess the risks they face and adopt appropriate and proportionate measures to ensure NIS. These entities will be required to report to the competent authorities any incidents seriously compromising their networks and information systems and significantly affecting the continuity of critical services and supply of goods.

Finally, it should be mentioned that under the Directive, Member States should lay down rules on sanctions in case of infringements of the national provisions adopted pursuant to the Directive.

2.4 The Legal Landscape in Greece

In Greece, there is no comprehensive legal framework on Cyber Security. In the Criminal Code the following cybercrimes are included: computer fraud (art. 386a) violation of secrecy of computer programs or data (art. 370B), unauthorized use of software, (art. 370c para. 1) unauthorized data access (art. 370c paras. 2 & 3), child pornography (art. 348a), grooming (art. 337). However, Greece signed, but did not ratified the Cybercrime Convention and its legislation does not provide for legal sanctions in case of attacks against information systems.

The Data Protection Act (Law 2472/1997, art. 10 para. 3) provides for the obligation of the data controller to take technical and organizational measures for the protection of personal data. In addition, Law 3471/2006 (Article 12) transposing Directive 2002/58 provides for the obligation of telecom providers to take technical and organizational measures to ensure the security of its services and of the public electronic communications network. Telecom providers are also under the obligation to inform subscribers if there is a risk of security breach. In case there is a breach of security related to personal data, telecom providers should inform the competent authorities. As it is obvious, the ambit of these regulations is restricted.

With Law 3115/2003 the Hellenic Authority for Communication Security and Privacy (ADAE)[18] was established and the framework for the protection of the confidentiality of communication was laid down. The procedure for lifting and assuring the secrecy of confidentiality is described in the Presidential Decree 47/2005. On November 17, 2011, the Authority issued the Regulation for Assurance of Confidentiality in Electronic Communications (decisions No. 165/2011).[19]

The Law on electronic communications (Act No 4070/2012) also provides rules for the security and integrity of electronic communication networks and services. It is noted that in case of a breach of security or integrity the provider is under the obligation to notify the National Authority for Telecommunications and Post and the latter may notify the National Authority for the Protection of Secrecy of Communication and ENISA.

Furthermore, the National Intelligence Service has been designated as the National CERT, which is responsible to deal mainly with cyber threats and attacks against Greek public institutions and critical infrastructures, in accordance with Law 3649/2008 and Presidential decree 126/2009.[20]

Finally, it should also be mentioned that there is a Draft National Cyber Security Strategy, which is in line with international best practices. It provides for, inter alia, the creation of a National Authority on Cyber Security that will be responsible to implement the National Strategy on Cyber Security, and a National Council for Cyber Security.

[18] http://www.adae.gr

[19] http://www.adae.gr/fileadmin/docs/nomoi/kanonismoi/ADAE_REGULATION_165.2011.pdf

[20] http://www.nis.gr/portal/page/portal/NIS/NCERT

3 SECURITY PRINCIPLES

In this Chapter, we will introduce & briefly discuss the following Eight Security Principles:

1. Know & Comply with the Law (§3.2.1)
2. Assess & Manage Risks (§3.2.2)
3. Cultivate Safety & Security Culture (§3.3.1)
4. Invest in a Cost-Beneficial Way (§3.3.2)
5. Consider Outsourcing (§3.3.3)
6. Improve Continuously (§3.3.4)
7. Develop an Information Security (§3.4.1)
8. Develop a Disaster-Recovery Plan (§3.4.2)

3.1 Eight Security Principles

Europol described 2014 in numbers, as following: [21]

- ✓ *"122,789,003,063 e-mails sent*
- ✓ *5,491,878,373 mobile phones in use*
- ✓ *3,019,132,565 Internet users worldwide*
- ✓ *761,258,985,941 Google searches*
- ✓ *2,232,291 blog posts written today*
- ✓ *1.393 billion monthly active Facebook users*"

It is obvious, from the above, that *cyber*[22] world is growing at a very high rate. In fact, "*over time, the world has been decisively shaped by three waves of technological innovation, each as unstoppable as the mightiest tidal force. The first was the agricultural revolution and the second the Industrial Revolution. The third is the information revolution that is engulfing us now and which presages a new way of living*"[23].

[21] GILLEN, P. (2015) *Presentation by Head of Operations & Cyber Intelligence, EC³* International Cyber Security Strategy Congress, February 4, 2015, Leuven, Belgium.

[22] The term is extracted from *cybernetics*, which comes from the Greek word *κυβερνητική*".

[23] WEBSTER, F. (1995) Theories *of the Information Society 3rd* edition London and New York: Routledge.

Cybercrime in 2014 numbers, again by Europol: [21]

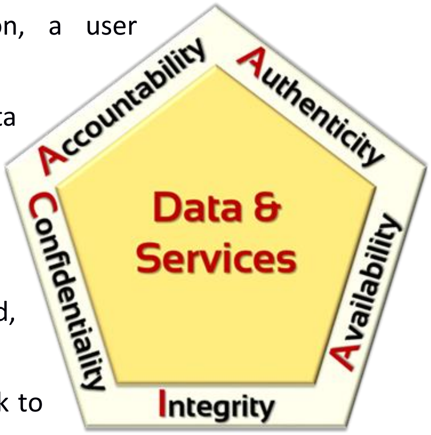
- *"19% Android users encountered a mobile threat*
- *15,577,912 malicious mobile apps worldwide*
- *38% of computer users subjected to at least one web attack*
- *123,054,503 unique malicious objects detected*
- *over 5 cyber threats every second*
- *1,432,660,467 attacks launched from online resources*
- *Cybercrime costs $445 billion/year, or ~1% of global income"*

Europol's prediction[21] for 2015 is the "*increase in the size and scope of cyber threats and the emergence of new attack vectors*".

Whether we like it, or not, we live in a world where we do many things online and we will do more in the future. This is the Knowledge Society, or Information Society, which offers unparalleled opportunities for growth, not only to nations but also to companies and even individuals. This development has boosted the value of Information and Knowledge. Like the physical world, the Knowledge Society suffers from crime. *Cybercrime*[24], is mainly after information, your information!

The three basic services, offered to users by cybersecurity, are known as the **CIA triad**:

- **C**onfidentiality: Access is denied to information, a user considers private.
- **I**ntegrity: Systems, Programmes, Information & Data may only change in an authorized way.
- **A**vailability: Access and normal use of a System is guaranteed to any authorized user.



Frequently, two more services are added to the CIA triad, above:

- **A**ccountability: Actions of a user can be traced back to him.
- **A**uthenticity: Confidence in the validity of a user ID, or of a Message.

[24] For a good definition of *Cybercrime*, see European Commission (2007) *Towards a general policy on the fight against cyber crime* COM(2007) 267 final.

It then becomes clear that either we use reliable Information Systems, or we do not use them at all. As the latter is no choice in today's world, there is only one way forward for any Director: **To take measures for the defense of the Organization against Cyber-Risks,** i.e. **to take the initiative and have the overall responsibility for the Organization cybersecurity**[25].

Security principles may be ordered in various ways. For example, the Information Systems Security Association (www.issa.org) published the Generally Accepted Information Security Principles[26], while Aaldert Hofman & Ben Elsinga[27] follow a different approach. A discussion of the above two categorizations can be found in GvIB Expert Letter / Sep 2006[28]. Furthermore ENISA categorizes its 25 security principles in 7 categories (domains).

In the following, we will classify the Eight Security Principles under

✓ Director Responsibility (top level)

✓ Management Responsibility (middle level)

✓ IT-Staff Responsibility (operational level)

[25] The terms *security* & *cybersecurity* will be used interchangeably.

[26] Published in Aug 2003 and available in http://all.net/books/standards/GAISP-v30.pdf (last accessed on 25-10-15).

[27] HOFMAN, A. & ELSINGA, B. (2004) *Security Principles* available in http://hillside.net/europlop/HillsideEurope/Papers/EuroPLoP2003/2003_HofmanEtAl_SecurityPrinciples.pdf (last accessed on 25-10-15).

[28] Accessed on 25-10-15 in https://www.pvib.nl/download/?id=6259884.

3.2 Director Responsibility

3.2.1 Know & Comply with the Law

What is the problem?

Knowledge Society is based on the cyber-world which is borderless. Nevertheless, each country has its own legislation to regulate the use of Internet. Please read through Chapter 2, THE REGULATORY LANDSCAPE, for a comprehensive introduction to the subject.

This legislation creates statutory obligations for every Organization and its CEO, who may become liable to prosecution in case of noncompliance.

What can you do?

Make sure that you

- ✓ understand the legal & regulatory requirements about obtaining & storing data (customer data is a very sensitive area),
- ✓ comply with relevant legal & regulatory requirements &
- ✓ understand the penalties/sanctions associated with noncompliance.

3.2.2 Assess & Manage Risks

What is the problem?

Risk, **R**, is defined to be the product **R** = **P** x **C**, where **C**, is the potential Cost, from a cybercrime and **P** is the Probability, of that cybercrime taking place. So Risk is ever-present (R>0), as in our discussion we consider only cybercrimes which have a cost (C>0), while P, the probability of an Accident (i.e. of a cybercrime taking place), cannot be guaranteed by anybody that it may become zero, i.e. nobody can guarantee that an Accident will never happen, whatever security measures are taken.

Hence, as all business people know, every Action has risks. What is the response when we are confronted by the Risk of a specific Action?

A. Accept the Risk, which means that management has decided to gamble.

B. Avoid the Risk, which implies avoiding the Action.

C. Transfer the Risk, which can be materialized by taking an insurance, or outsourcing.

D. Mitigating the Risk, which means that Security Controls[29] will be designed and applied, in order to reduce the Risk to acceptable levels.

What can you do?

From solutions A-D, above it is clear that A & B are not solutions. Why?

- ✓ DO NOT just "Accept the Risk": It is irresponsible to gamble an operation, unless Risk is very low, i.e. at an operationally acceptable level. It is advisable to make Risk **ALARP**, i.e. **A**s **L**ow **A**s **R**easonably **P**ractical and it is also advisable to apply any Controls available, that are cost-beneficial, without any further consideration.

- ✓ DO NOT cancel the Action in order to "Avoid the Risk": Being Risk-conscious does not mean that we should 'kill' our operations, unless Risk is high in spite Controls introduced. Security should not be allowed to obstruct new business initiatives. Security is not about Risk avoidance, but about Risk Management.

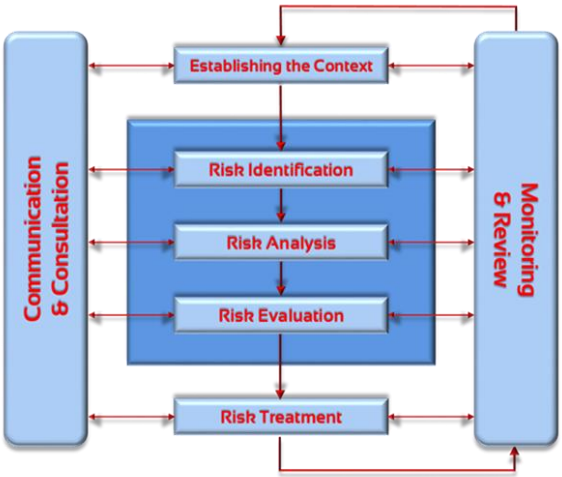


Figure 3.1: The Risk Management (RM) Process

The way forward is to Manage Risks, as shown in the block diagram of Figure 3.1. The diagram illustrates the process of Risk Management, as recommended by the ISO 31000 Standard[30].

[29] Security Controls, or simply *Controls*, are the security measures applied for a specific Action.

3.3 Management Responsibility

3.3.1 Cultivate Safety & Security Culture

What is the problem?

Some Organizations tend to view security in a purely technological way, thinking, for example, that state of the art security technology will do the job. Then there is a security breach because a careless employee lost his laptop, or an even more careless one lost his laptop which was not protected by password, or even worse that laptop contained critical company information.

To create a parallel with the physical world, what is the point of investing in sophisticated burglar alarm and security doors and locks for your house, if you do not use the alarm when you are out, or even worse if you also leave a couple of windows open to “air the house” and “after all you just go next door for ten minutes”?

Definitely then, security is not only about technology, it is also about people and processes that are respected. In the discussion above it becomes clear that people must understand what security is about and learn to respect relevant procedures.

Organizations then must not neglect to convince staff of the value and need to respect security procedures and of the consequences of a security incident[31] & accident[32].

It is not enough to have in place top security technology and procedures, if your staff do not know how to use it, do not understand why it should be used, do not care if it is used or not and they are not affected by their performance on this front.

You also need to look after your people and develop a security culture and awareness.

What can you do?

- ✓ Train/Inform your staff about the importance of cybersecurity and about the consequences of potential accidents.
- ✓ Explain to your staff the technology and procedures in place.
- ✓ Explain to your staff the legal framework.
- ✓ Motivate your staff to respect security procedures and to be on alert. Make them understand that what happens to the Organization, affects the individual, as well.

[30] “International Standard ISO 31000: Risk management — Principles and guidelines”, 1st edition, 2009-11-15.

[31] An *Incident* is an undesirable event. An *Event* is the occurrence, or change, of a particular set of circumstances.

[32] An *Accident* is an incident which has harmed the Computer System, or its users.

3.3.2 Invest in a Cost-Beneficial Way

What is the problem?

Cybersecurity comes at a price, like physical security (locks, security personnel, alarms, reinforced doors & windows, access controls, etc.). Any temptation to cut expenditure there, may be greatly regretted (there are countless examples). What is worse, there is no perfect security[33].

On the other hand, one may be tempted to keep increasing the security budget until he ‘feels’ secure, which may well be in the region of diminishing returns.

It is very frequent that an Organization overspends in one domain and underspends in another. Both scenarios result in net losses.

As discussed in §3.3.1, above, an Organization may over-invest in security technology and under-invest in people’s mind. The latter will annul the former.

What can you do?

- ✓ Obtain expert advice for a holistic approach to cybersecurity.
- ✓ Assess your Risks.
- ✓ Develop cost-effective control measures for each such Risk (in some situations, a control measure may have negligible cost!).
- ✓ Hence, create the Security Procedures.
- ✓ Train & Motivate your staff to follow the Security Procedures.
- ✓ Monitor compliance.
- ✓ Review annually (or bi-annually).
- ✓ Hence, improve your Procedures.

[33] … because Risk is never zero, as cost is not zero and probability cannot become zero.

3.3.3 Consider Outsourcing

What is the problem?

Cyber-threats and cyber-control measures demand expertise, which your own staff cannot be expected to possess, or maintain.

In addition, good security solutions may prove to be expensive, although they were not a few years ago.

What can you do?

- ✓ Cyber-world is evolving fast and Threats, Controls and Opportunities do likewise.
- ✓ Consider outsourcing part of your cyber-defense, like for example hosting.
- ✓ Consider seeking expert advice, on a need-to-know basis, for example to create a Disaster Recovery Plan, etc.
- ✓ If you do outsource though, stay satisfied that they treat your data with at least the same respect that you would.

3.3.4 Improve Continuously

What is the problem?

All Management Systems require continuous improvement. There is one extra reason why this is necessary for Cybersecurity: Cyber-world moves very fast, and that includes Cyber-threats.

Frequently there is very little time left to become alerted, devise relevant Controls and embody them in the Organization Procedures.

What can you do?

- ✓ Rely on expert advice, even outsourced.
- ✓ Be informed (there are many sources of reliable and timely information on emerging cyber-risks).
- ✓ Keep challenging yourself.

3.4 IT-Staff Responsibility

3.4.1 Develop an Information Security Management System

What is the problem?

There is no problem, the requirement is clear: All Organizations have Policies on matters of Quality, Environment Protection, etc. The same applies to Security, cyber-, or physical-. The requirement for such a Policy stems from a hypothesized Vision on Cybersecurity. Not to have such a vision is irresponsible. To have a vision, but do nothing for it, is even worse.

What can you do?

Again, you need expert advice and a layered approach to cybersecurity. See Fig. 3.2 for an illustration of what cybersecurity is about.

Elements of such a Policy may well be: [34]

- ✓ Physical security: Layered measures to secure loss and theft of devices. For example, servers are locked in the Computer Room, mobile devices (laptops & tablets) are stored in a drawer when user is away, mobile phones are always with their owner, etc.

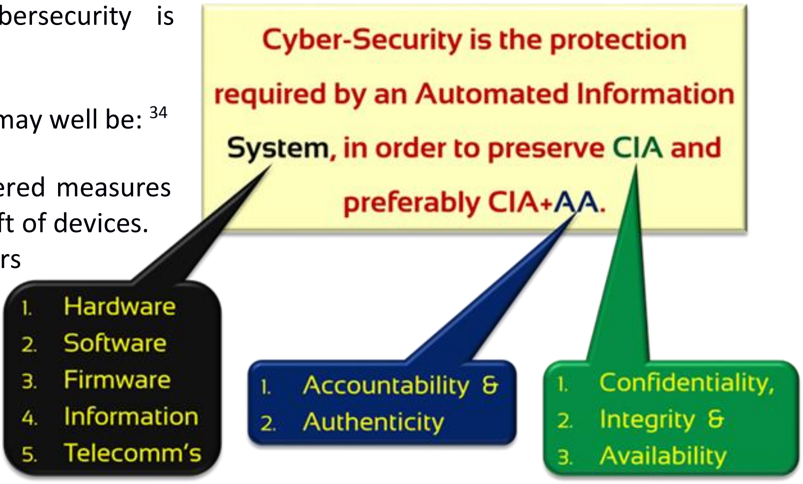


Figure 3.2: What is Cybersecurity

- ✓ Availability provision: Measures to improve Availability[35] may include: Power back-up (batteries and even generator), communications feed back-up (cable & wireless feed and perhaps double provider option), storage back-up, server back-up and others.
- ✓ Anti-virus[36] & anti-malware[37] software
- ✓ Defense against intrusions by using a well-configured firewall.
- ✓ Employee awareness & training

[34] After *A Practical Guide to IT Security*, prepared by UK's Information Commissioner's Office (www.ico.org.uk) in 2012, found in https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf (last accessed on 25/10/15).

[35] One of the Cybersecurity ***CIA triad*** (**C**onfidentiality, **I**ntegrity, **A**vailability).

[36] "*Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation*" (http://www.microsoft.com/security/pc-security/virus-whatis.aspx).

[37] *Malware* means malicious software and is "*a catch-all term to refer to any software designed to cause damage to a single computer, server, or computer network, whether it's a virus, spyware, et al*" (https://technet.microsoft.com/en-us/library/dd632948.aspx).

- ✓ Segmentation (for example, do separate payments from web browsing).
- ✓ Device hardening: Remove unused software, keep software up-to-date, etc.

A more rigorous approach is proposed by the ISO/IEC 27001 International Standard on "Information technology – Security techniques - Information security management systems – Requirements".

ISO 27K specifies an Information Security Management System (**ISMS**) for an organization. The Organization is responsible for developing its own ISMS (with expert – normally external – advice) and is then certified by Accredited Registrars. The certification process comprises three stages:

- ✓ Preliminary review of the ISMS
- ✓ Formal compliance audit
- ✓ Review audit(s)

ISO/IEC 27001:2013 specifies the following security control objectives (security measures)[38]:

A5. Information security: Management direction.

A6. Organization of information security: Internal organization, Mobile device & Teleworking.

A7. Human resource security: Prior, During, at Termination and at Change of employment.

A8. Asset management: Responsibility for assets, Information classification & Media handling.

A9. Access control

A10. Cryptography

A11. Physical and environmental security: Secure areas & Equipment.

A12. Operations security: Operational procedures and responsibilities, Protection from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management & Information systems audit considerations.

A13. Communications security: Network & Information transfer

A14. System acquisition, development and maintenance

A15. Supplier relationships

A16. Information security incident management

A17. Information security aspects of business continuity management [39]

A18. Compliance

[38] Taken from Annex A of ISO/IEC 27001 (2013) *Information technology - Security techniques - Information security management systems – Requirements*

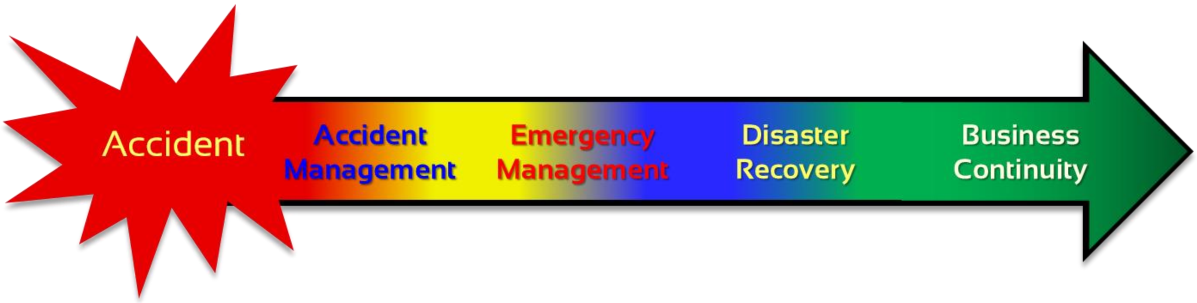
[39] See also §3.4.2 ("Develop a Disaster-Recovery Plan"), below.

3.4.2 Develop a Disaster-Recovery Plan

What is the problem?

As explained earlier on (see for example §3.2.2, “Assess & Manage Risks”, in p. 19), there is no guarantee on security. Hence, it is expected that you will have many security incidents, fewer near-misses and few accidents[40].

Hence you should be prepared to handle them.



What can you do?

Seek expert advice to prepare a Disaster Recovery Plan:

- ✓ Have your Organization’s files up-to-date and secure at a different physical location.
- ✓ Think of alternative IT hardware, in case yours is stolen / destroyed / burnt / etc.
- ✓ Have a procedure in case you become the victim of online blackmail.
- ✓ Have back-up solutions for power disruptions, air-conditioning malfunction, telecommunications provider problems, etc.

[40] An *Incident* is an undesirable event, an *Accident* is an Incident which has harmed the Computer System, or one of its users and a *Near-Miss* is an Incident which did not result in Accident, out of pure lack.

3.5 Other Sets of Security Principles

The following references were studied, compared & contrasted and used as an inspiration for the “Eight Security Principles” discussed above:

1. European Union Agency for Network and Information Security (ENISA) (2014) Security objectives and security measures in *Technical Guideline on Security Measures* available in https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures (last assessed in 7-11-2015)

2. ICC Belgium, FEB, EY, Microsoft, L-SEC, B-CCENTRE and ISACA Belgium *Belgian Cyber Security Guide* available in https://www.b-ccentre.be (last accessed in 25-10-15)

3. ISACA *Principles for Information Security Practitioners* available in http://www.isaca.org/Knowledge-Center/Standards/Documents/Principles-for-Info-Sec-Practitioners-poster.pdf (last accessed in 25-10-15)

4. (AUS Gov) Trusted Information Sharing Network for Critical Infrastructure Protection (Dec 2009) *Secure Your Information: Information Security Principles for Business Resilience - Summary Report for CIOs and CSOs* available in http://www.tisn.gov.au/Documents/ITSEAG+Secure+Your+Information+CIO.pdf (last accessed in 25-10-15)

5. (USA) FCC *Cybersecurity for Small Business - Advice for protecting your business, customers and data* available in https://www.fcc.gov/cyberforsmallbiz (last accessed on 25/10/15)

6. Business Insider Australia (2014) *10 Principles Of IT Security Every Small Business Should Know* available in http://www.businessinsider.com.au/10-principles-of-it-security-every-small-business-should-know-2014-11 (last accessed on 25/10/15)

7. (UK) Information Commissioner’s Office (2012) *A Practical Guide to IT Security* available in https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf (last accessed on 25/10/15)

8. ISO/IEC 27001 (2013) *Information technology - Security techniques - Information security management systems – Requirements*

4 ADVICE ON SECURITY

4.1 Tips for Business

In this section you will find a list of important tips for businesses[41] that wish to guarantee the security of their infrastructure and the integrity of their data.

✓ Analyze your risks

Understand what is your risk and exposure to network and your information security risks. For example, are your company's data important? Do you store client's data? (such as names, addresses, passwords, credit card numbers, etc.) Are they encrypted when in rest? What would your liability be if they were compromised or leaked? In case your company's normal operation depends on IT infrastructure, what would be the impact if the infrastructure is compromised? Do you have a contingency plan?

✓ Understand your liability

Try to understand your liability towards your clients and employees in case your data/infrastructure is compromised. The first step is to determine whereas some personal data have been collected and therefore if a third party had access to them. According to the situation, you might have the legal duty to inform the user and the national personal data protection authority for the existence of the breach. Then, clients can also ask for damages in a civil law action for negligence, in case your company has facilitated hacking or a virus propagation.

✓ Protect your assets

Who is responsible for the protection of your assets? Put a security policy in place. It could be useful to expressly give to your human resources manager the ability to manage complaints and inquiries regarding the company's processing of Personal Data.

✓ Protect your network

Do you have technical capabilities in place (such as firewalls) to protect your network from outsiders? You should definitely have a policy in place on who can connect to your network, especially the WiFi. In case your employees connect to the network remotely, special safety metrics (such as VPNs) should be set in place. At the same time, you have to be careful to respect the privacy of your employees. For instance, you cannot organize a general surveillance scheme of their communication. Furthermore, specific surveillance measures in case of legitimate concerns about the security of the network shall be held only with the previous information of the employee.

[41] We focus mostly on non-IT business although most of the advice applies to IT business as well.

✓ Protect your IT infrastructure

Your computers should be protected with appropriate software, such as antivirus, firewalls, NAT (Network Access Control) and vulnerability scans. There should exist a policy on what kind of software should run on the computers of your company, and on how this policy should be enforced. Some of the most important issues are the following: How is un-authorized installed software discovered? Who has access to your infrastructure? Have you considered two-factor authentication (at least for your administrators)?

✓ Protect your data

Data "at rest" should be stored encrypted and data transfers should be appropriately protected. Files and emails must be transferred over encrypted channels at all times. There should be a clear policy on the use of laptops, smartphones and portable devices outside the premises of the company. What happens if such a device gets stolen/compromised? A mandatory periodical change of user passwords together with an access to administrator's password to a very limited number of persons, could be very useful as a first means of protection. It should be mentioned that a lot of backdoors and Trojans have been installed by employees themselves, who then use them as a mean of blackmail in case of termination of their contract.

✓ Outsource

In case you need to run web servers and/or provide services to remote customers, such operations can be outsourced to specialists who guarantee not only their correct functionality, but also the continuity and security of the whole operation 24/7. However, be very careful when you outsource not only operations but also storage of data.

✓ Put an information security policy in place

You should have an information security policy in place. All relevant stakeholders must be involved to guarantee that the policy is being properly enforced.

✓ Test and monitor your systems

Systems should periodically undergo security tests. Perform penetration tests and periodic scans for open services/ports. Keep logging and monitoring of all activity to know at all times who is using your systems.

✓ Deal with emerging technologies

More and more employees tend to bring their own devices (smartphones, tablets, etc.) to the workplace. Some of them use the same device to store both personal and company data. What is your policy towards this and how does it affect your security and liability?

✓ Physical security is of paramount importance

Do you have control over who has access to your premises? You should enforce and monitor the application of this policy, and always be aware of any un-authorized persons that gain access to your premises.

✓ Be prepared

There are official entities from which you can receive authorized security services, such as CERTs. Get informed on what to do if your system is compromised. Do you know who to contact? The police? Your clients? Your collaborators? Do you know how to handle the press? A simulated "readiness exercise" would be very useful in unveiling gaps to the above questions.

✓ Provide the minimum number of services necessary for your business

Do you have installed software "in case it is needed sometime in the future?" Do you run servers which are not absolutely necessary for your core business? Make sure that you understand the risk such services impose and you weigh them against the possible benefit they may provide you.

✓ Educate your people

Do you have periodic training of your staff on security and privacy aspects of your business? Are they aware of the dangers of insecure systems and the business benefits of secure ones?

4.2 Tips for Individuals

The following constitutes a list of tips for individuals that wish to ensure the security of their devices and data.

✓ Use a secure password and never disclose it

Using a secure password to lock your computer is the first and most important safety tip that should be followed by all individuals. Use letters (lower and upper case), numbers, and special characters to derive a good blend. Create a different password for each individual account and change them regularly to ensure their security. It is also suggested that an easy way to remember a strong password is to use an acronym. For instance, “my wife's birthday is on 28 January” could become “MW’SB@izO2812!”, which would make a good passphrase.

✓ Keep your computer locked at all times when unattended

Do not leave your computer unlocked and unattended at any time and any place. The physical security of all your devices is fundamental for their security.

✓ Install an antivirus and keep it up-to-date

Installing an antivirus and keeping it current at all times by automatically installing all major updates is the cornerstone of computer security.

✓ Backup your data away from your data source

You should regularly and automatically backup the data stored in your computer to a secure data source which lies physically away from your device. A good choice is to use a secure distant cloud as a solution.

✓ Whenever possible select a two-factor authentication

Two-factor authentication tends to become a standard practice whenever extra security is required for accessing a distant recourse. Use it whenever possible.

✓ Secure your home WiFi router

Allowing open access to your home wireless network can be a security risk, as it may allow anyone close enough to your router to connect to it. Secure your home WiFi router by changing the default router password, using a strong password and changing your SSID to a unique name. Advanced security options include disabling SSID broadcast, using encryption, enabling a firewall, allowing only https or ssh access, etc.

✓ Be aware of spam

Never open attachments of emails from users you do not know as they may hide malware that can severely damage your computer.

✓ Dangers can also hide in the body of an email

Dangers can also hide in bodies of emails. In general, be aware of email from unknown senders as they are widely used to spread viruses and malware. Do not follow links hidden in the bodies of such email.

✓ Avoid installing unauthorized applications

Avoid installing software from unauthorized sources as they may present major threats for your computer.

✓ Avoid installing plugins you do not need

Browser plugins and add-ons can damage your computer. Install them only when you really need them, keep them up-to-date at all times, and disable them as soon as you need them no more.

✓ Avoid surfing questionable sites

Surfing questionable sites can infect your computer with malware that can seriously damage it. Use extra caution when surfing the Internet. Avoid downloads from untrustworthy freeware or shareware sites.

✓ Wireless networks can be a risk

Connecting to an unknown wireless network can present unpredictable security risks for your devices.

✓ In general if it is online you can't be sure it is safe

Visiting a distant link over the Internet, downloading over the Internet could present risks. Use extra caution with online activity.

✓ Do not disable security tools

Never disable the security tools installed on your computer, on the contrary always keep them current enabling their automatic updating.

✓ Never lend your mobile device to others

Lending your laptop, or mobile device to other individuals can expose them to intentional or unintentional security risks. Always have them under your supervision and keep them locked whenever away from them.

✓ Be careful with mobile apps

Only install mobile apps from authorized, valid sources.

✓ Use secure connections

Whenever possible use secure file transfer as your data can be at risk while in transit over the network.

✓ Use desktop firewall

Use a desktop firewall for extra security and definitely disable peer-to-peer access of other devices through your computer.

✓ Use a password manager

Do you keep your passwords in scraps of papers, plain text emails or unencrypted files stored somewhere in the cloud? A password manager can help you get a long way ahead of your security issues!

✓ Stay up-to-date with the latest developments in computer security

Last but certainly not least, you should remain informed with the latest trends in computer security, tools and measures and on the emerging threats and how to avoid them.

5 GAPS AND RECOMMENDATIONS FOR POLICY MAKERS

Gap 1: As of the time of this writing (summer 2015) there is no official Greek Cybersecurity Strategy published, although many EU Member States have already done so.

Recommendation 1: Formulate a National Strategy for Network and Information Security, defining the strategic goals and the concrete policy and measures, which are necessary to achieve the defined goals.

Gap 2: There is no single Agency in Greece that deals with cyber-security-related policy issues, such as, e.g., the French Network and Information Security Agency (ANSSI, Agence nationale de sécurité des systèmes d'information).

Recommendation 2: Establish a specialized Agency (here forth: 'the Agency') with the task to supervise cyber security, promote best practices, provide advice, and conduct investigations and reviews of networks and information systems; Allocate responsibility to the authority Agency for cooperation with EU Member States and other countries in order to coordinate and efficiently tackle security related risks and incidents; provide for cooperation with data protection authorities, where security incidents concern personal data and law enforcement agencies, where unlawful acts are committed.

Gap 3: There is no comprehensive legislation in the field of Cyber Security.

Recommendation 3: Introduce legal measures to lower Cyber Security risks, as well as handle and respond to incidents & accidents; in particular, define and keep up to date the appropriate technical and organizational measures to manage Cyber Security risks.

Gap 4: There is no legislation applying to security-related incidents and accidents, with the exception of Law 3471/2006 and Law 3115/2003.

Recommendation 4: Provide for the obligation of public administration and market operators to notify all the stakeholders, including involved citizens, about security-related incidents and accidents.

Gap 5: There is no law imposing sanctions in case of infringements of cyber security, with the exception of the legislation applying to secrecy of communication.

Recommendation 5: Provide rules on administrative and criminal sanctions in case of infringements of the national provisions adopted to create a comprehensive framework for cyber security.

Gap 6: Greek Citizens do not have a clear point of contact to deal with their concerns on cyber security and to help them in case they suspect their cyber-security has been compromised.

Recommendation 6: Encourage citizens to become more security-aware. Encourage the use of suitable software to protect their computers and networks. Provide them with a point to contact when they think their system has been compromised. This would be the role of a National Agency for Cyber-Security.

6 INFORMATION SECURITY IN GREECE – ROLE OF THE CYBERCRIME CENTER

Living in a world of technology, for the users, minors or adults, and for the enterprises, big or small, privacy and information security is a very crucial issue. Similarly to other European countries, Greece needs to strengthen its framework for an adequate protection. Not only the legal framework need to be updated, but also new initiatives have to be taken in the area of science, education with the governmental support. Sufficient rules and regulation on the one hand and specific governmental bodies for addressing cybercrime cases on the other, indisputably would benefit the information security in Greece.

The Greek Cybercrime Center (www.cybercc.gr), provided a first step in the following fields:

- ✓ LEA Information and Training. The Consortium organized three 2-day seminars where Law Enforcement Agencies, judicial authorities and industry employees took part. Divided to parallel sessions, the attendees had the opportunity to choose the topic they were interested in and learn more about how to address an incident of cybercrime not only in theory but also in practice. In the seminars speakers from core scientific organizations of cybercrime, such as ENISA, Cyber Crime Unit of the Greek Police, Law School of University of Athens, Europol, Democritus University of Thrace, EC3, Hellenic Data Protection Authority, Hellenic Ministry of the Interior, Hellenic Telecommunications Organizations, ISACA, etc. were invited. Therefore, expertise from academia, LEA, industry could be combined.
- ✓ Research. The Consortium carried out research which was focused (i) on monitoring and detecting infected machines and (ii) on social forensics. Additionally, GCC through the publications in Journals and Conferences and presentations in Conferences contributed in the field of information security.
- ✓ Education at the University Level. At Law School of Aristotle University of Thessaloniki, a new course title “Legal Aspects of Cybercrime” was added in the list of modules. The module referred to crimes that occur in cyberspace and the legal framework that is currently in place.

At the national level, the Greek Cybercrime Center empowered its constituency through periodic advisory board meetings. Representatives from LEA, judicial authorities, ISPs, industry, independent governmental authorities participated and shared views and experiences with other bodies/authorities. At the international level, the Center is part of a European-wide activity to create a network of similar Centers of Excellence that will facilitate sharing of expertise and best practices. By publishing this guide, the Center hopes to contribute in raising awareness in the area of cybercrime and to identify gaps and recommendations at the policy level that can make the Internet a Safer Place for personal and professional use.

NOTES

POLICY RECOMMENDATIONS FOR CYBER SECURITY

GREEK CYBERCRIME CENTER

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission — Directorate-General Home Affairs

FORTH Institute of Computer Science

KEMEA

Faculty of Law
Aristotle University of Thessaloniki

SAFENET