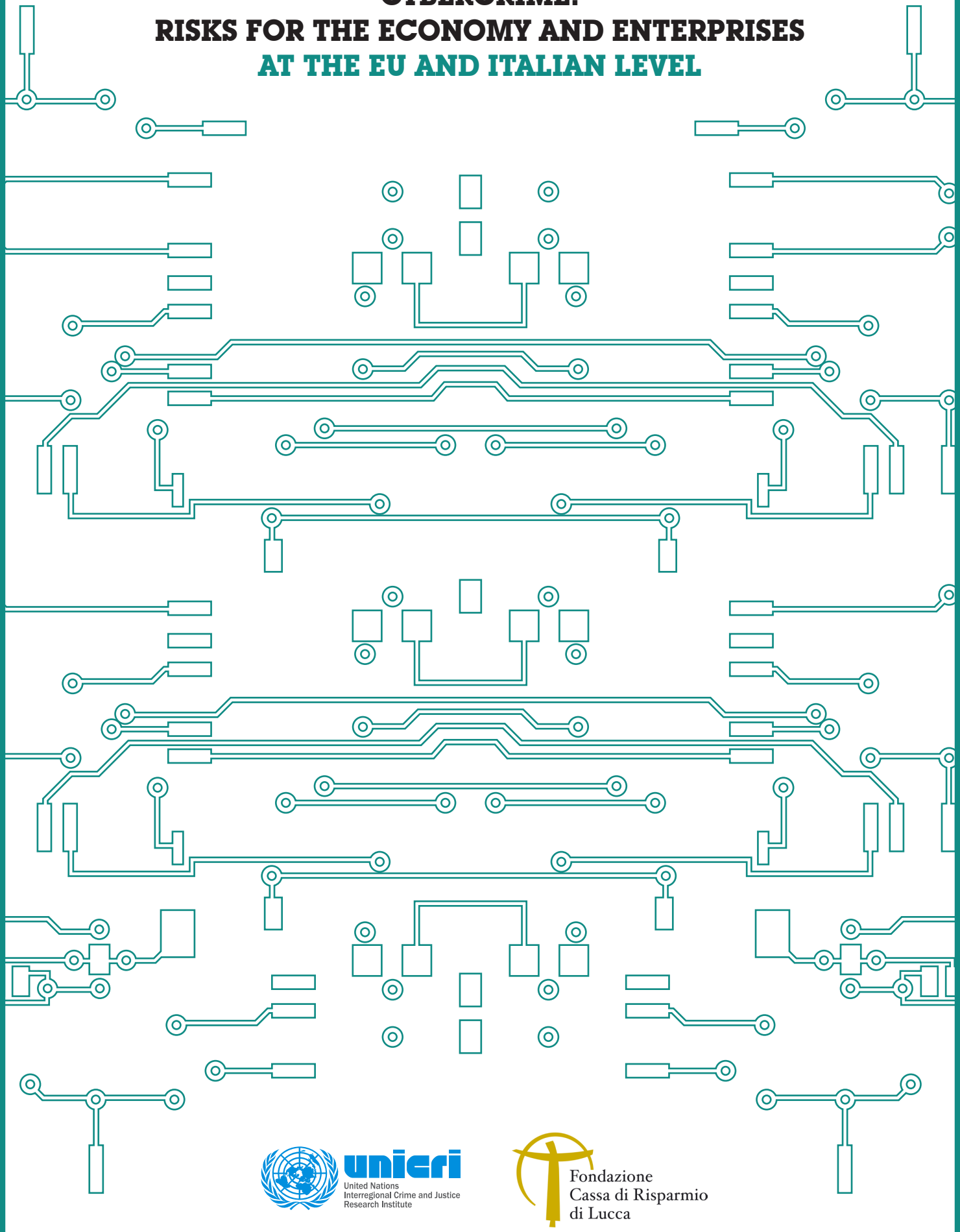
CYBERCRIME:
RISKS FOR THE ECONOMY AND ENTERPRISES
AT THE EU AND ITALIAN LEVEL



unicri
United Nations
Interregional Crime and Justice
Research Institute

Fondazione
Cassa di Risparmio
di Lucca

RESEARCH PROJECT

Cybercrime: Risks for the Economy and Enterprises at the EU and Italian Level

This study was conducted by Dr. Flavia Zappa.

Disclaimer

The views and opinions expressed in this study are those of the author and do not reflect the opinion of UNICRI or the UNITED NATIONS in general.

Copyright

United Nations Interregional Crime and Justice Research Institute (UNICRI),
Viale Maestri del Lavoro, 10
10127 Turin
Italy
Tel 011-6537 111 / Fax 011-6313 368
Web site: www.unicri.it
E-mail: documentation@unicri.it

© UNICRI, 2014

All rights reserved. In order to reproduce any part of this document, authorization from UNICRI is required.

"Without security, there is no privacy; nor true freedom.
You have no private life if your house has no walls;
you are not free to walk the streets if it is not safe to do so."

Neelie KROES, Vice-President of the European Commission
Responsible for the Digital Agenda,
A secure online network for Europe,
Cyber security conference Brussels,
28 February 2014

Preface

In recent years cybercrime has become one of the most pervasive growing phenomena, raising the concerns of governments, citizens and the private sector. Data breaches and cyber-theft are accruing in all sectors, affecting security and development in societies all over the world.

Cyber crime is no longer confined to isolated attacks committed by individuals. In recent years this type of crime has evolved into a very profitable and often very low risk activity for criminal organizations. Modern information technology society has become a borderless field of operation for criminals who have been targeting the financial and business sectors in particular.

Cyber attacks involve unpredictable economic and productivity losses, but are not limited to these types of losses. Affected companies need to bear the costs of malware cleanup, investigation and post-incident management. Furthermore, companies may not recover from all cyber-attacks; data loss or the theft of trade secrets can prove fatal for industries that rely heavily on the quality and secrecy of their manufacturing. Many companies will also have to address their loss of credibility and market positioning.

Cybercrime's zeroing in on the financial sector and small and medium enterprises comes at a delicate time, particularly in Europe where businesses hit by the recession are trying to cope with tight austerity measures and low revenues.

The research focuses on the impact of cybercrime at the international, national (Italian) and local level. Targeted interviews and case study analysis have been conducted to provide an overview of the tools currently used by criminals, the most common reasons that lead to these criminal acts, and the major risks and vulnerabilities for businesses. Interviews with institutional players and companies have helped to clarify key problems and suggest a need for a coherent strategy for SMEs to defend themselves against cybercrime.

The information collected in the research study allowed UNICRI to design and create a strategy that will allow for the creation of networks of experts to promote a culture of security at the various levels of the society. We are engaged to advance from understanding to undertaking, from knowledge to action.

Jonathan Lucas

UNICRI Director

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

We would like to thank all of the people who contributed to this research by providing valuable material and interviews for the insights and observations obtained. In particular, we thank Deputy Prosecutor (*Sostituto Procuratore)* Alberto Perduca and Deputy Prosecutor (*Sostituto Procuratore)* Giuseppe Riccaboni from the Prosecutor's Office of Turin (*Procura della Repubblica di Torino)*; Deputy Prosecutor Andrea Cusani from the Prosecutor's Office of Florence (*Procura della Repubblica di Firenze)*; Dr. Stefania Pierazzi, Assistant Deputy Prefect of Post and Telecommunications of Florence (*Vice Questore Aggiunto della Polizia Postale e delle Telecomunicazioni di Firenze*), and Chief Inspector (*Ispettore Capo)* Franco Bozzi of the Public Prosecutor's Office (*Procura della Repubblica)* at the Public Court of Lucca, for their willingness to clarify legal rules and procedures within this field. We also thank the Postal Police *(Polizia Postale)* of Florence and the Public Prosecutor's Office of Florence for the data they provided.

Many thanks to all the companies, and their respective representatives, who were surveyed: Elena Polacci of Giorgini Maggi, Tiziano Pieretti, Simone Antonetti and Marino Ninci of Industria cartaria Pieretti, Franco Pasquini and Alessandro Burresi of Lucart, Luca Landucci of Lucense, Annarita D'Urso, Matteo Fava and Santo Natale of Tagetik.

In addition, we would also like to thank Director Claudio Romiti and Daniele Chersi of Assindustria Lucca, Monica Pellegrino of ABI Lab, Veronica Borgogna of Consorzio Bancomat, Domenico Raguseo of IBM, Deputy Prosecutor Giuseppe Ledda of the Public Prosecutor's Office of Florence, Dr. Paolo Passeri, the SME, Small and Medium Enterprises Knowledge Center, and Intesa Sanpaolo, for the information provided and for their cooperation.

EXECUTIVE SUMMARY

Cybercrime is on the increase annually. In order to implement valid countermeasures, it needs to be studied in depth. It is not a phenomenon that affects only large companies, but increasingly also those of small and medium size. Its impact on the economy of a country is huge, and given that the European and Italian economic and social fabric is strongly represented by SMEs, the purpose of this research is to investigate the degree of risk for the economy and businesses resulting from this phenomenon.

The methodology chosen was 'bottom-up', meaning from the bottom to the top, with a focused investigation in the Province of Lucca, including targeted interviews addressing the real situation that small and medium sized enterprises are facing every day. In order to study the economic risks that SMEs face in regard to cybercrime and to provide the skills needed to implement the appropriate countermeasures, the decision was made to make inquiries with relevant companies and institutions that work closely with SMEs. This was done in order to understand the real needs of SMEs and their relationship and reactions to cyber crime events.

Generally, cyber security is managed and dealt with by using a top-down approach, with experts and specialists suggesting and implementing various technical solutions and best practices, but for this research project, a different methodology was decided upon which keeps in mind the precise objectives specific to SMEs.

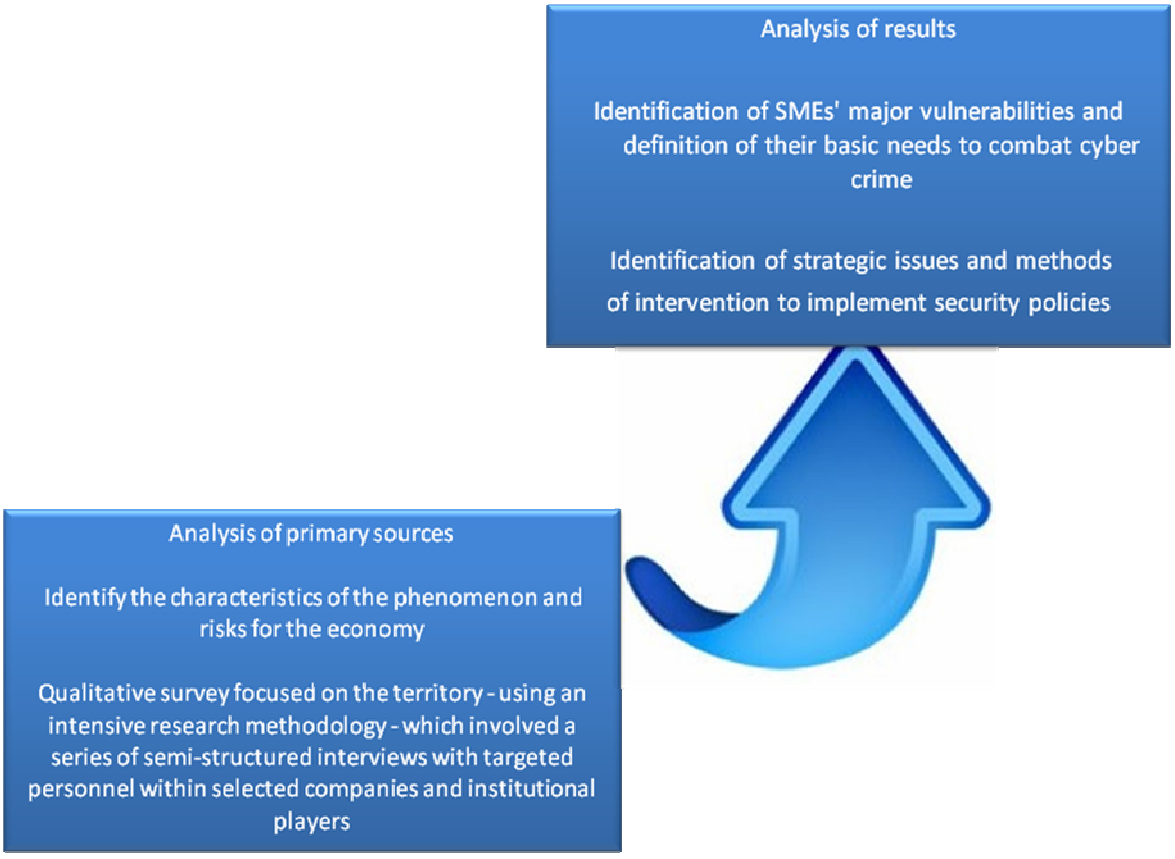


Figure 1 - Graph explaining the methodology used for the research

The decision was made to investigate the characteristics, needs and risks of SMEs and the adequate measures that need to be put in place. The focus on the Province of Lucca and its SMEs is, for this reason, instrumental in understanding the existing gaps with regards to combating cybercrime. We also conducted interviews with managers of institutions such as *Assindustria*, prosecutors and law enforcement agencies, and private companies such as *ABI Lab*, IBM and *Consorzio Bancomat*. The representatives of SMEs and trade associations are often not involved in the implementation process of defense against these threats and often do not put effective solutions in place.

In order to obtain a clearer picture of the phenomenon of cybercrime, comprehensive analysis of the context through the study of the main characteristics (actors, tools, threats, and types of risks) involving SMEs in the cyber field will be addressed in the first chapter. Cybercrime is a wide-ranging issue, much more dangerous than traditional crime, and having the ability to amplify the capabilities and the danger of the criminal subject. Information Technology is a means to commit various types of crimes: bullying, pedophilia, and industrial and international espionage.

In this study the impact of cybercrime on the economy will be addressed in reference to SMEs. In the second chapter, the risks and vulnerabilities that cybercrime poses at the international, Italian and local levels are examined through a focus on the subject matter. The characteristics relating to the international, European, and national dimensions are discussed in the third chapter. In the fourth chapter, the most current statistics in the field and implemented countermeasures are looked at, with a focus on the Province of Lucca. This chapter also explains theory in regard to countermeasures and proactive action.

LIST OF ACRONYMS

ACSC	Advanced Cyber security Center
ADI	*Agenda Digitale italiana*
AgID	*Agenzia per l'Italia Digitale*
AISE	*Agenzia Informazioni Sicurezza Esterna*
AISI	*Agenzia Informazioni Sicurezza Interna*
APP	Application
ATM	Automatic Teller Machine
BI	Business Intelligence
BMBF	*Bundesministerium für Bildung und Forschung*
BOD	Board of Directors
BYOD	Bring Your Own Device
CEPOL	European Police College
CERT	Computer Emergency Response Team
CERT –EU	Computer Emergency Response Team of European Union
CERT –PA	Computer Emergency Response Team Public Administration
CI	Critical Infrastructure
CISP	Cyber security Information Sharing Partnership
CISR	*Comitato Interministeriale per la Sicurezza della Repubblica*
CNAICIP	*Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche*
CNCPO	*Centro Nazionale per il Contrasto alla Pedofilia Online*
CNP	Card Not Present
COPASIR	*Comitato Parlamentare per la Sicurezza della Repubblica*
CP	*Codice penale*
CPM	Corporate Performance Management
CSES	Center for Strategy & Evaluation Services
DDoS	Distributed Denial of Service
DIS	*Dipartimento Informazioni per la Sicurezza*
DoS	Denial of Service
EAST	European ATM Security Team
EC3	European Cybercrime Center
ECI	European Critical Infrastructure
ECTEG	European Cybercrime Training and Education Group
EFTA	European Free Trade Association

EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
ERP	Enterprise resource planning
EU	European Union
EUCTF	European Union Cyber-crime Task Force
EUROPOL	European Police Office
FBI	Federal Bureau of Investigation
FSP	Federation of Small Businesses
GDF	*Guardia di Finanza*
GDP	Gross Domestic Product
GPRS	General Packet Radio Service
GPS	Global Positioning System
IBAN	International Bank Account Number
IC3	Internet Crime Complaint Center
ICT	Information and Communication Technology
IOCTA	Internet Organised Crime Threat Assessment
IOT	Internet of Things
IP	Internet Protocol address
ISCOM	*Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione*
ISP	Internet Service Provider
IT	Information Technology
ICT	Information and Communication Technologies
J-CAT	Joint Cybercrime Action Taskforce
MISE	*Ministero dello sviluppo economico*
MTA	Metropolitan Transportation Authority
NCA	National Crime Agency
NGO	Non-governmental Organization
NIS	Network and Information Security
NRA	National Regulatory Authority
NYPD	New York Police Department
OPMI	*Osservatorio Piccole e Medie Imprese*
OS	Operating system
OSINT	Open Source Intelligence
PA	Public Administrations

PC	Personal Computer
PDF	Portable Document Format
PEBKAC	Problem Exists Between Keyboard and Chair
POS	Point of Sale
ROI	Return on Investment
SBA	Small Business Act
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SIMU	*SIEM für Klein und Mittelständische Unternehmen*
SIPAF	*Sistema Informatizzato Prevenzione Amministrativa Frodi Carte di Pagamento*
SME	Small and Medium Enterprises
SMS	Short Message Service
TOR	The Onion Router
USB	Universal Serial Bus
VPN	Virtual Private Network
WEF	World Economic Forum
WEP	Wired Equivalent Privacy
WPA e WPA2	WI-FI Protected Access

CHAPTER 1

THE RELEVANCE OF CYBERCRIME AS A THREAT TO SME'S AND THE ECONOMY

1.1 The need for a small and medium enterprise (SME) focus

In recent years cybercrime has played an increasingly important role among the risks that citizens, businesses, and governments are facing. Media attention, however, is often focused on events involving governments and corporations, and it often doesn't take into consideration the impact of this phenomenon on the economy, especially for small and medium enterprises (SMEs).

SMEs are at the heart of the Italian and European social fabric and the role they play is important, both economically and for global security. SMEs and citizens make up the majority of the victims of targeted cyber attacks.[1]

The term "Small and medium enterprises" refers to companies with fewer than 250 employees[2] and a turnover or balance sheet total of less than 50 million euro or 43 million euro[3], respectively. Within the category of SMEs, small and micro enterprises are further differentiated, meaning small businesses that employ fewer than 50 people and whose annual turnover or balance sheet does not exceed 10 million euro, and micro-enterprises which employ fewer than 10 people and whose annual turnover or total annual budget does not exceed 2 million euro.

[1] *EISAS – European Information Sharing and Alert System A Feasibility Study 2006/2007*, available at: <http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf> (retrieved 1-11-2014).

[2] In the United States, SMEs refers to companies with fewer than 500 employees. For more details, see: *The new SME definition. User guide and model declaration. Publications of the Directorate-General for Enterprise and Industry 2006*, available at: <http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_en.pdf> (retrieved 1-11-2014).

[3] These thresholds are applied only to data relating to independent companies. A company belonging to a larger group may be required to also include data, turnover and balance sheet total of the group. *Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises* [Official Journal L 124 of 20.05.2003], available at: <http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_en.htm> (retrieved 1-11-2014).

Enterprise Category	Headcount	Financial Ceilings	
		Turnover	Or Balance Sheet Total
SMEs	< 250	≤ € 50 Million	≤ € 43 Million
Small	< 50	≤ € 10 Million	≤ € 10 Million
Micro	< 10	≤ € 2 Million	≤ € 2 Million

Table 1 - Definition of Small and Medium sized Enterprises in the European Union
Source: Based on Evaluation of the SME definition, CSES, 2012[4]

The role that SMEs play in the European economy is very important. They also represent a considerable number of Internet users. It is estimated that SMEs make up 99.8% of all enterprises in the EU,[5] employing 86.8 million people - equivalent to 66.5% of the workforce. They produce more than half of the total turnover of European companies.

SMEs in Europe are also represented mostly by micro enterprises. 92.1% of over 20 million European SMEs are micro enterprises, and when added to small enterprises, represent over 50% of jobs for EU citizens.

	Number Of Enterprises		Number Of Employees		Value Added	
	Number	%	Number	%	Million €	%
Micro	18.783.480	92,10%	37.494.458	28,70%	1.242.724	21,10%
Small	1.349.730	6,60%	26.704.352	20,50%	1.076.388	18,30%
Medium	222.628	1,10%	22.615.906	17,30%	1.076.270	18,30%
SMEs	20.355.839	99,80%	86.814.717	66,50%	3.395.383	57,60%
Large	43.454	0,20%	43.787.013	33,50%	2.495.926	42,40%
Total	**20.399.291**	**100,00%**	**130.601.730**	**100,00%**	**5.891.309**	**100,00%**

Table 2 - Data relating to Small and Medium sized Enterprises in the European Union in 2013
Source: Eurostat, National Statistical Offices, DIW, DIW econ, London Economics, 2013

Considering SMEs as the core of the European economy based only on their number and the employment derived from it is an understatement. They are often innovators in their field and have strong strategic capabilities regarding market enterprise.

[4] *Evaluation of the SME Definition September 2012*, Final Report Framework, Center for Strategy & Evaluation Services, available at: <http://ec.europa.eu/enterprise/policies/sme/files/studies/evaluation-sme-definition_en.pdf> (retrieved 6-11-2014).

[5] *A recovery on the horizon? Annual Report on European SMEs 2012/2013*. European Commission, available at: <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2013/annual-report-smes-2013_en.pdf> (retrieved 11-11-2014).

Despite being more fragile than larger businesses in the face of market imperfections, and therefore requiring greater protection and support for their development, between 2003 and 2010 the number of SMEs in Europe increased by almost 11% to around 21 million, and the number of people employed by SMEs increased by 7.5 million (about 6%).

In 2008, SMEs proved to be much more resistant to the crisis than large companies in terms of employment, even if later on the period 2010-2012 proved quite challenging. At the EU27 level, SME employment is relatively stable and forecasts for job growth and added value are moderately optimistic. In 2014, it is expected that the level of employment derived from SMEs will return to the same positive levels of 2008.[6]

Within the EU, the country with the largest number of SMEs is Italy. The Italian SME sector is currently made up of nearly 3.7 million businesses, representing more than 18% of the European total[7].

	Number Of Enterprises		Number Of Employees		Value Added	
	Number	**%**	**Number**	**%**	**Million €**	**%**
Micro	3.491.826	94,40%	6.930.947	46,10%	185.000	29,80%
Small	183.196	5,00%	3.236.764	21,50%	136.000	21,90%
Medium	19.265	0,50%	1.861.089	12,40%	101.000	16,30%
SMEs	3.694.288	99,90%	12.028.799	80,00%	420.000	68,00%
Large	3.196	0,10%	3.013.012	20,00%	198.000	32,00%
Total	**3.697.484**	**100,00%**	**15.041.812**	**100,00%**	**620.000**	**100,00%**

Table 3 - Data relating to Small and Medium sized Enterprises in Italy in 2013
Source: Enterprise and Industry Italy SBA Fact Sheet, European Commission, 2013

Italy is a hub for SMEs, with 99.9% of all companies being small and medium enterprises. Our industrial system is based on micro businesses, often consisting of family members. These micro businesses often specialize in manufacturing, focusing on areas such as fashion, decor, food, and the mechanical industry. With over 200 industrial districts,[8] many of these products hold the famous trademark *Made in Italy*, which represents excellence worldwide[9]. 68% of Italian wealth is produced by 12 million people who work in small or medium enterprises.

[6] *Annual report SMEs 2013 Source: Eurostat, National Statistical Offices, DIW, DIW econ, London Economics*, available at: <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2013/annual-report-smes-2013_en.pdf> (retrieved 6-11-2014).

[7] *Enterprise and Industry 2013 SBA Fact Sheet ITALY*, available at: <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/countries-sheets/2013/italy_en.pdf> (retrieved 6-11-2014).

[8] Quadrio Curzio A. and Fortis M. (2002, ed.), *Complessità e Distretti Industriali. Dinamiche, Modelli, Casi reali*, Il Mulino, Bologna.

[9] Phenomenon completely absent, in similar proportions, in other industrialized countries.

Micro enterprises in Italy, which represent 94.4% of the total, have a weight of 46.1% in terms of employment, compared to 21% in Germany, 22% in France and 27% in Britain.[10]

Despite this data, attention regarding cybercrime cases is generally placed on events that involve large companies such as Sony, Google, Amazon, Twitter, etc., and not on SMEs, which, as we have seen, hold strategic importance in the European economy, especially in Italy. Therefore, the perception of risk is lowered, and with it the perceived danger level. In contrast, however, is the cost of information security, with basic measures still considered to be too high for SMEs compared with large companies that have a bigger budgets.

Given the enormous contribution of SMEs to economic growth and the creation of jobs, constant support from the EU Member States and the European Community is required. European policies adopted in the Small Business Act (SBA)[11] are designed precisely to improve the conditions for growth of SMEs and to mitigate the effects of the economic crisis, with policies in their favor in order to encourage job growth in the European Union.

Despite this, SMEs are supporting the weight of the economic crisis better than large enterprises. This requires a high commitment to the development of policies in support of a major push to economic recovery. In addition to these policies regarding conditions of access to finance, the labor market, and the cutting of red tape, is strategic support development with targeted projects focused also on the technological environment and policies of protection from cyber threats. Inasmuch, companies with modern infrastructure and technologically advanced sectors with a highly skilled workforce are more competitive and able to recover much faster, returning to the same performance levels held before the crisis at a faster rate.

In a time of economic uncertainty like the present, smaller businesses do not have sufficient disposable income to invest in greater cyber defense, even though the violation of their systems would result in losses greater than the initial investment. Many companies do not realize that in most cases a significant increase in security is possible with minimal investment.

Small businesses have become an attractive target for cyber attackers because of their weak security and inadequate protection. The fact that a company is small does not necessarily mean it is unlikely to be attacked. In fact, hackers are able to attack thousands of small businesses simultaneously exploiting the vulnerabilities of software and using tools previously reserved for large companies[12], which can now be easily purchased and sold on the Internet. One other aspect not to be underestimated is that given the growing economic engagement in cyber security of large companies, criminals are moving their attack attempts to SMEs as a vehicle to hit the bigger

---

[10] Ricciardi Antonio (2010), *Le Pmi localizzate nei distretti industriali: vantaggi competitivi, evoluzione organizzativa, prospettive future*, in Quaderni di ricerca sull'artigianato N°54 Rivista di Economia, Cultura e Ricerca sociale dell'Associazione Artigiani e Piccole Imprese Mestre CGIA Edited by Centro Studi Sintesi, available at: <http://www.quaderniartigianato.com/wp-content/uploads/2011/05/Quaderni-N%C2%B054.pdf> (retrieved 11-11-2014).

[11] *"Think Small First" A "Small Business Act" for Europe*, Commission of the European Communities, Brussels, 25-6-2008, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0394:FIN:EN:PDF> (retrieved 6-11-2014).

[12] Michael Fey said that small businesses are attacked because they often do not keep their software up to date, or keep track of their financial data. *McAfee CTO: Cyber Criminals Target SME's,* February 2014, by Kevin Wright, available at: <http://www.itgovernance.co.uk/blog/mcafee-cto-cyber-criminals-target-smes/> (retrieved 6-11-2014).

and better protected enterprises - therefore, they also play a crucial role in the defense of the entire industrial system. Small suppliers and contractors are becoming the weak link in a huge market exploited by cyber criminals - the networks of larger companies. In the case of Target[13], in fact, the flaw that allowed the breach of the system was traced to a supplier. The company admitted that hackers had used the credentials of a seller to access the system and steal 40 million credit card numbers and 70 million user accounts, with an estimated loss of 5.3%.

Customer data on the server of one company can be used to access other services, for example when cyber criminals tried to attack Yahoo Mail, Yahoo said that the list of user names and passwords had probably been obtained by a third-party database made up of hackers.

The risks that SMEs face are varied and range from loss of intellectual property, sensitive data exposure, loss of competitiveness, loss of jobs, and costs relating to the destruction of services, to damage to corporate reputation. Other costs are those of compensation to be paid to customers in the event of a data breach (or penalties arising from the agreement) and those required for countermeasures and insurance payments - for the implementation of strategies to mitigate risks and recovery in the case of an incident.

1.2 Cybercrime as a threat to SMEs

Cybercrime has been a topic of great interest over the last ten years and is currently considered one of the most serious threats worldwide. Every aspect of daily life, both private and work related, is now highly computerized. All the world's economies use the same basic infrastructure, the same software, hardware, and standards - with billions of connected devices.[14]

According to a recent survey by the World Economic Forum (WEF), risks from cyber space are considered as among the greatest perceived risks in terms of impact and likelihood of occurrence [15], as can be seen in Figure 2.

[13] The US department store chain, in late 2013, had suffered the theft of sensitive data related to 40 million customer credit cards. For more details, see: *Clonati 40 milioni di carte di credito, i grandi magazzini Target si fanno perdonare con uno sconto del 10% sulla spesa*, 21-12-2013 Il Sole 24 Ore, available at: <http://www.ilsole24ore.com/art/tecnologie/2013-12-21/clonati-40-milioni-carte-credito-target-si-fa-perdonare-uno-sconto-10percento-spesa-165410.shtml?uuid=ABj2HVl> and *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores,* 19-12-2013, target Pressroom, available at: <http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores> (retrieved 7-11-2014).

[14] Rod Beckstrom: *"Anything connected to the Internet can be hacked. Everything is being connected to the Internet So everything is becoming vulnerable and a new dynamic of cybercrimes countered by security measures, countered by new criminal efforts, and so forth, is now unleashed"*, London Conference on Cyberspace, 2 November 2011, available at: <https://www.icann.org/en/system/files/files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf> (retrieved 7-11-2014).

[15] The report has been prepared based on interviews with more than 250 among experts and business leaders.

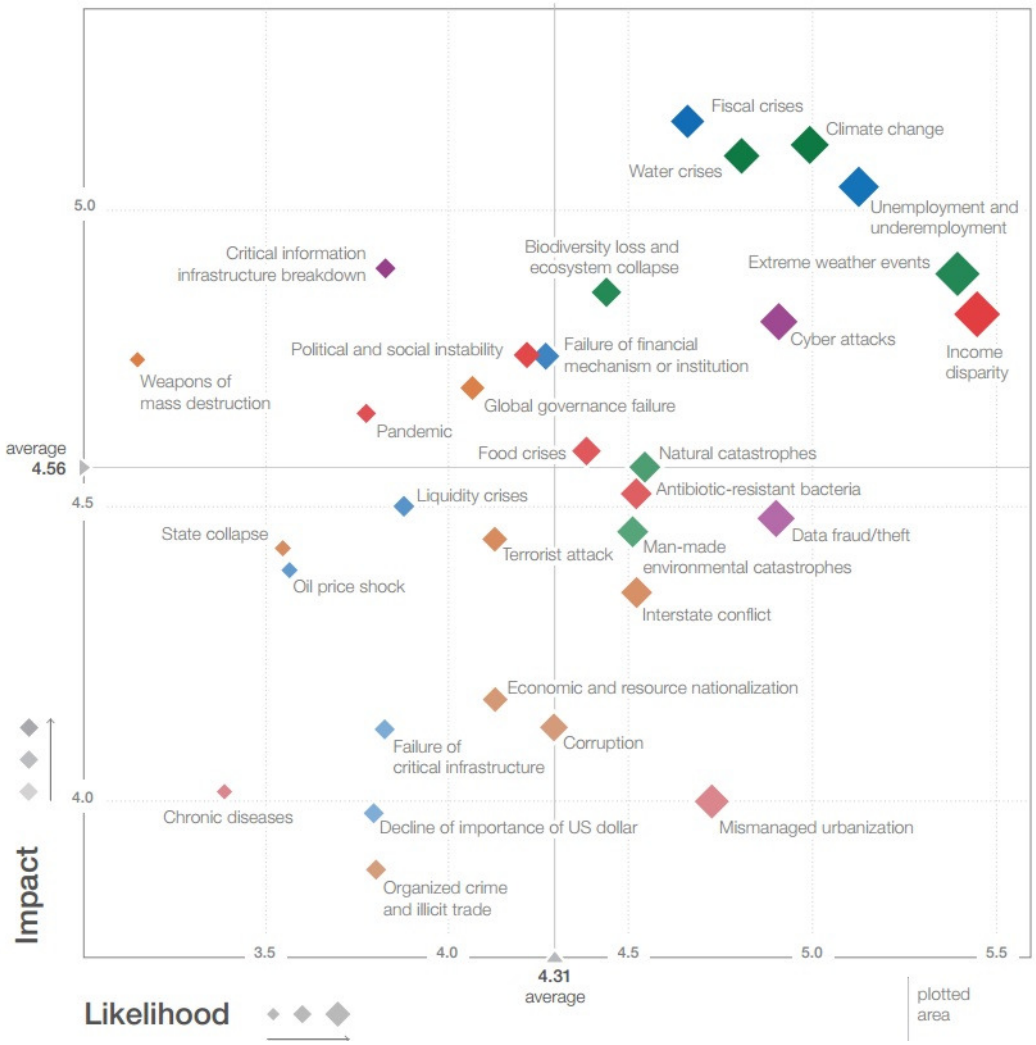


Figure 2 - The Global Risks Landscape 2014

Source: Global risks Ninth edition, World Economic Forum, 2014

The report also shows that if businesses and governments do not develop adequate defense policies, and if they do not do so quickly, the economic losses caused by cyber attacks could be up to 3,000 billion dollars by 2020.[16]

The WEF has often highlighted the interdependence of IT systems, introducing new vulnerabilities and flaws with unpredictable consequences and emphasizing the macroeconomic impact of IT risks in terms of growth of GDP. In its latest report the WEF emphasizes the delicacy of this cybercrime, explaining that if not addressed promptly and taken into account by all stakeholders (governments, businesses and civil society), it could lead to serious consequences and to a scenario in which the Internet could suffer the mistrust of users, no longer be a free resource and research tool, and no longer be used for ecommerce.

Despite all of this, there is still no shared legal definition that determines cybercrime in a consistent and exhaustive manner - due mainly to differences in the laws of various countries[17].

[16] World Economic Forum - Global risks 2014 Ninth edition, available at: <http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf> (retrieved 6-11-2014).

[17] Often dating back to the 19thCentury.

This entails additional difficulties at the international level for the construction of a concerted response. The Commonwealth of Independent States Agreement, for example, without explicitly using the term "cybercrime," defines the crimes perpetrated through technological means as a "criminal act of which the target is computer information," while the Shanghai Cooperation Organization Agreement defines cyber attacks as 'the use of information resources and (or) the impact on them in the informational sphere for illegal purposes.'[18]

We can, however, generically define cybercrime as a set of illegal operations that take place on the Internet. Cybercrime should not be considered an alien phenomenon or different from the types of crime that we are used to dealing with, but simply as a crime perpetrated by other means - through cyber space. It is an effective method, which is revolutionizing traditional crimes and making it easier and cheaper for criminals to commit them. The most characteristic aspect of this phenomenon, and the thing that differentiates cybercrime from traditional crime, is the fact that there are no physical boundaries, and geographical distances are not a factor. In addition, the fact that it can be perpetrated from any part of the planet without any kind of human contact, makes it easier to do, nullifying the perception of the consequences of a criminal act. The concept of Buckminster Fuller's principle of 'ephemeralization' (or 'to do more with less'), explored and proposed more than 70 years ago, can be applied in reference to the technological process today[19]. Cybercrime is estimated to have a very high ROI. Unlike the space for ordinary Internet users, cyber criminals inhabit untraceable spaces out of reach of search engines. This space is not easily accessible, and is commonly called "deep web".

But what exactly is the deep web? It is nothing more than a submerged layer of the web, invisible to normal every day users using traditional programs. As you can imagine, it is very difficult to gain an idea or gather statistics regarding the true size of the deep web, but many experts agree that it is hundreds of times larger than that of the common Internet. In common thought, the deep web is associated exclusively with trafficking, and criminal and illegal activities, but in reality it is not only a hiding place for these activities. More and more NGOs, political dissidents, and bloggers use the deep web as a resource, in search of information or as a space in which to express opinions, meet, exchange data and support 'good causes' whilst trying to escape censorship and controls. Frank La Rue, UN special envoy for freedom of expression, clarified before the assembly of the United Nations that "*anonymity and secure communication are crucial to an open and democratic society*"[20]. Even Edward Snowden and activists of the Arab Spring have used the deep web to spread confidential documents denouncing illegal actions by governments.

---

[18] Commonwealth of Independent States Agreement, Art. 1(a) and Shanghai Cooperation Organization Agreement, Annex 1, in *Comprehensive Study on Cybercrime,* UNODC, February 2013, available at: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (retrieved 15-11-2014).

[19] Gori Umberto (2012) "*Riflessioni propedeutiche alla cyber intelligence"* in "*Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale"* edited by Umberto Gori and Luigi Sergio Germani. Franco Angeli.

[20] *Tutti i segreti del deep web*, Arturo di Corinto, Repubblica.it, available at: <http://www.repubblica.it/tecnologia/2014/04/20/news/tutti_i_segreti_del_deep_web-84053410/> (retrieved 11-11-2014).

Documents published by Julian Assange of Wikileaks for example have been recovered through the deep web. There are also a number of virtual markets, such as the famous Silk Road, where they sell drugs, weapons, and false documents, which are then delivered to your home anonymously. The FBI estimates that Silk Road carried financial transactions of 1.2 billion dollars, earning 80 million dollars in commissions between February 2011 and July 2013.[21] The site was closed by the FBI but later reopened at another address. Even traditional gangs resort to deep web markets to conduct their trades, confirming that cybercrime is not a new type of crime, but a new way to commit traditional crimes. The sites of the deep web are not reachable by normal browsers, (programs to surf the Internet such as Internet Explorer, Firefox or Safari), because the pages are not indexed by search engines like Google or Bing. Access to search engines and navigation through the classic link is inhibited and typically, addresses at which you can reach the sites hosted in the deep web change very quickly. In the deep web some sites are accessible only through a Virtual Private Network (VPN), meaning direct encrypted links between two computers. The easiest way to navigate the deep web is through a secure connection for which you must have The Onion Router (TOR), software created to allow navigation in countries where the Internet is censored. TOR encrypts data navigation by passing the communication through different proxies or nodes, changing the IP address each time you go to a page, creating a sort of chain from which it is difficult to trace the real geographic location of the user. Due to the limited amount of search engines within the deep web, navigation is almost 'on demand' and it is possible to visit many sites only by invitation by a member of staff or a member of community who already has access. One of the most famous search engines is HiddenWiki, which collects links to websites provided by users. The illegal trade in the deep web is based, for the most part, on the use of Bitcoin as a currency through which cocaine, weapons, and pornographic material are sold. Being a virtual and encrypted currency, both the buyer and the seller remain anonymous so it is the perfect currency for this type of activity.

Cybercrime is certainly a danger that continues to increase. According to a study conducted by the Ponemon Institute[22], the cost of cybercrime has increased by 78% compared to 2009, but the biggest concern is the time it takes to solve a problem, which has also increased by 130% over the same period. Data theft is the cause of the biggest losses, approximately 43% of total costs attributable to cybercrime, while damage to business and loss of competitiveness account for 36%.

According to the 2014 Symantec Report[23], 2013 was the year of the "mega breach" because the total number of data breaches[24] increased by 62% from the previous year. On top of

[21] *Feds Arrest Alleged 'Dread Pirate Roberts,' the Brain Behind the Silk Road Drug Site,* by Kim Zetter in Wired 10/2/2013, available at: <http://www.wired.com/2013/10/silk-road-raided/> (retrieved 6-11-2014).

[22] *The 2013 Cost of Cybercrime Study*, Sponsored by HP Enterprise Security Independently conducted by Ponemon Institute, October 2013, available at: <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf> (retrieved 6-11-2014).

[23] *Internet Security Threath Report 2014*, Symantec, Volume 19, Published April 2014, available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (retrieved 7-11-014).

that, there were eight cases of violations that involved over 10 million users - with a total annual violation of identity exceeding 550 million individuals (+ 493% compared to 2012).

Overall cybercrime has an underestimated turnover of around 12 billion dollars per year[25], and the cost of cybercrime in Europe is calculated at over 750 billion euro[26] per year, which includes direct losses, loss of time, loss of business opportunities, and costs to repair damage. To this the damage of image and reputation must be added, which last for a far greater period of time[27].

The threats from cyber space are, without doubt, the most strategic the contemporary world is facing. The tools used in cyber space are not physical, but their effects are unpredictable and dangerous. This includes the difficulty in predicting when the cyber attack was successfully launched, how it is spread, and how it can evolve over time. This highlights a disturbing aspect: IT has many side effects. It can unpredictably hit other systems or networks that are not considered targets and even hit the attacker himself. The widespread management of companies through IT is what represents the major vulnerability in terms of cyber security. The most technologically advanced companies, a condition necessary to be competitive in the global market, are more attackable objectives. Internet, social networks, and online banking are becoming more and more widespread, both in private life and in the workplace.

It is important to understand this phenomenon, which has evolved over time. The romantic idea of the hacker as seen in our imagination, whose desire for a challenge is his motivation, has given way to organized crime and to a multiplicity of players with different motivations. This situation is worsening exponentially and rapidly. Today, the boundary that differentiates these threats is extremely weak.

Initially, cyber threats were mainly viruses, worms and trojans, but over time cyber criminals began to use techniques relating to social engineering - such as phishing – targeting employees who have direct access to databases containing confidential business information, and also pharming, credit card fraud, DDoS attacks, identity theft, and data theft. According to a Special Eurobarometer, commissioned by the European Union,[28] the majority of Internet users across the EU do not feel completely secure about their ability to make purchases online or use online banking and have no idea how to navigate the Internet safely. Many respondents claim to know about cybercrime from newspapers or television, but do not feel informed about the risks

---

[24] Credit card numbers, names, birth dates, login, password, identity card, address, medical insurance, phone numbers, financial information, email, etc.

[25] INTERPOL speech Opening remarks by INTERPOL President Khoo Boon Hui at the 41ST European Regional Conference. Israele, Tel Aviv 8-5-2012, available at: <http://www.Interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (retrieved 6-11-2014).

[26] *Interpol Ups The War Against Cyber Crime* di Daniella Cheslow, Huffingtonpost 05-08-2012, available at: <http://www.huffingtonpost.com/2012/05/08/Interpol-cyber-crime_n_1499734.html> (retrieved 6-11-2014).

[27] See for example: *Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit*, by Jason Mick, available at: <http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm> (retrieved 6-11-2014).

[28] *Cyber security Report,* Special Eurobarometer 404, *2013, European Commission,* available at: *<http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf> (retrieved 6-11-2014).*

that may be experienced. Their lack of awareness about their vulnerability is exploited by cybercrime and is what determines the ease of implementation.

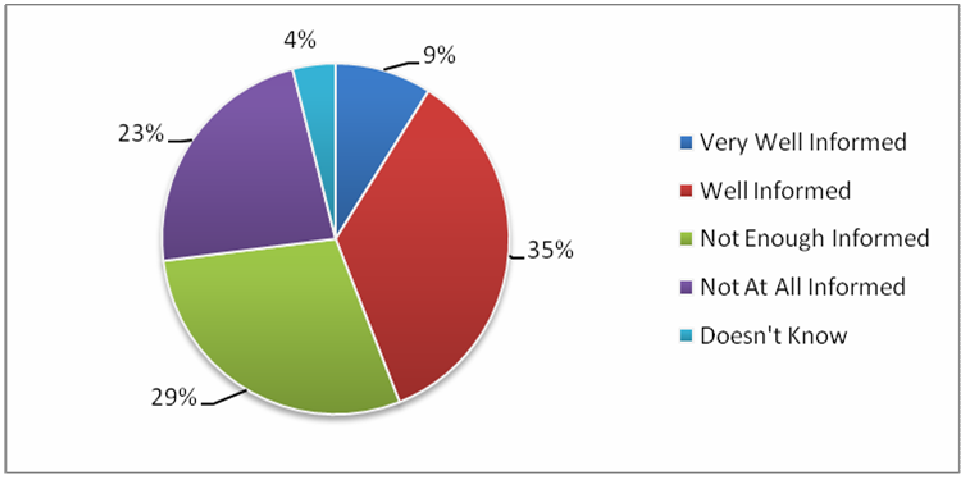


Figure 3 - Statistics on the perceived level of information for EU citizens about cybercrime, May-June, 2013, EU27
Source: Special Eurobarometer 404 Cyber security Report, 2013

In addition to the above, more than a third of Internet users claim to have received at least one email scam and feel concerned about their sensitive data online. If we add the increasing number of citizens in possession of at least one smartphone device, (currently impossible to protect), which are increasingly being used as a business tool, we realize how cybercrime today has more than fertile ground in which to operate and grow. With time, the cyber threat of several years ago has changed. It has not only multiplied by the means through which it is perpetrated[29], but has evolved into cybercrime, cyber terrorism, cyber espionage, cyber war, cyber warfare, and the phenomenon of hacktivism.

The universe of cybercrime is huge and includes different types of attacks, attackers, risks and threats.

In the next section we will analyze the main types of attackers and attacks found in cyber space. These lists are not intended to be exhaustive of all the threats in cyber space, but to offer an overview in order to understand the full extent and dangerousness of the most relevant and potentially harmful threats to small and medium sized enterprises - the core of this research. The increasing computerization of every aspect of our daily lives makes us more vulnerable to threats from cyber space, in particular identity theft, theft of sensitive data, and financial fraud - aimed not only at organizations and governments, but increasingly at companies and individuals. Cybercrime is becoming a new additional source of risk for companies, alongside traditional threats.

It was considered essential to produce an overview of the tools currently used by these criminals, the most common reasons that lead to the realization of these criminal acts, and the major risks and vulnerabilities faced by businesses. How is a cybercrime attack committed? What is the methodology and which tools are used? And what is the motivation or purpose? Knowing

[29] Exploit, Buffer overflow, Shellcode, Cracking, Backdoor, Port scanning, Sniffing, Keylogging, Spoofing, Trojan, Viruses, DoS, Social engineering, Social Network Poisoning, CMD through Browser, only to name a few.

the basics regarding the threats that SMEs face can help increase the level of attention during everyday activities. Being aware of the threat undoubtedly aids in the implementation of simple actions in order to avoid falling victim to the most common risks, and in turn make a big difference overall.

Extremely important is the constant updating of software due to the rate at which these tools are evolving. In its report Threat Landscapes 2013, The European Union for Network and Information Security Agency (ENISA)[30], identifies 16 major IT security threats, highlighting what has been the trend for the past year. The following chart, drawn from the report, summarizes the main threats directly involving SMEs, such as mobile and cloud. As you can see, with the exception of botnets and spam, which have remained at the same level of the previous year, all other threats are increasing in almost all the most sensitive areas.

[30] ENISA *Threat Landscape 2013 Overview of current and emerging cyber-threats,* 11-12-2013, available at: <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport> (retrieved 6-11-2014).

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas				
		Mobile Computing	Social Networ-king	Cloud Compu-ting	Trust Infrastr.	Big Data
1. Drive-by Downloads	↑	↑	↑		↑	↑
2. Worms/ Trojans	↑	↑	↑	↑	↑	↑
3. Code Injection	↑	↑	→	↑	↑	↑
4. Exploit Kits	↑	↑	↑	↑	↑	↑
5. Botnets	→	↑	↑	↑		
6. Physical Damage/Theft /Loss	↑	↑	↑	↑	↑	↑
7. Identity Theft/Fraud	↑	↑	↑	↑	↑	↑
8. Denial of Service	↑			↑		
9. Phishing	↑	↑	↑	↑	↑	↑
10. Spam	→		↑			
11. Rogueware/ Ransomware/ Scareware	↑					
12. Data Breaches	↑	↑		↑	↑	↑
13. Information Leakage	↑	↑	↑	↑	↑	↑
14. Targeted Attacks	↑				→	↑
15. Watering Hole	↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Table 4 - Summary table of the main trends relating to cyber threats
Source: Trend Landscape Report, ENISA, 2013

1.3 Types of threats

The threats which SMEs are exposed to in cyber space are the same as those encountered in the real world, but for criminals the web is a simpler and more user friendly way of conducting

these threats. This, therefore, multiplies the number of potential attackers that a company is exposed to - making even traditional threats more subtle and difficult to detect.

As a result, it is essential to understand their interests (direct or indirect), goals, motivation (money and information, anger) and attack strategies (targeted and non targeted, mass and individual). The following can be considered a basic, but exhaustive, list of information regarding the types of attackers, attacks, risks and vulnerabilities that SMEs may face. This could be considered the first level of protection from this type of threat.

1.3.1 Fraud

Fraud is the act of entering computer systems without permission in order to unlawfully access the services provided by the victim company. There are two main ways in which the attacker has access to these services. The first way is by gaining possession via different techniques (such as phishing or social engineering) of the credentials of an administrator or an employee of the company. The second is by coming into possession of credentials of a legitimate user. This fraud can also be perpetrated as an intermediate step in order to achieve a more challenging goal. The objective could also be to intercept or divert data, which passes through POS, in order to steal credit card information or hijack payments to a bank account controlled by the attacker.

One of the fastest growing trends, as of late, is scam, in which the criminal asks for the payment of a small sum of money to be advanced by the victim in exchange for big gains, such as foreign funding, lottery winnings, inheritance, etc.[31]

1.3.2 Identity theft

Identity theft is a scam in which the objective is to steal the identity of a person or company in order to obtain resources, information, or unlawful authorization.

Within an enterprise, this threat takes shape in two different ways. The first and more traditional way is when an attacker steals the identity of a person within the company (employee or manager) in order to obtain valuable information directly from an unsuspecting colleague. In this case the identity theft is an intermediate step for a further objective. The second and more dangerous way is when the attacker steals the identity of the entire company (logo, production, projects, catalogues, etc.) in order to use them in an illegal way in a foreign country (for example China). The same products sold by the victim company are produced and then entered into the market as counterfeit goods.

1.3.3 Theft of sensitive data and intellectual property

The theft of sensitive and confidential data is one of the biggest risks to the world of small and medium sized enterprises. The most valuable assets of a company are the know-how and the

[31] Computer scam known as the “Nigerian fraud”.

intellectual property. These are the intangible assets, which result from human creativity. These are found in SMEs and are invented by the entrepreneur himself and include architectural projects, industrial inventions, utility models, product designs, brands, and recipes. Without these, there would be no company. These assets are increasingly economically important, especially at the moment with the effects of the current economic crisis. It is easy to understand how the theft of a not-yet-launched fashion collection, a recipe for a new pharmaceutical drug, or an architectural project tender could severely damage a company.

The theft of sensitive data covers both internal data (production of goods, innovations, and employee and financial information, etc.), and the data of customers and suppliers (personal identity, credit card numbers or bank accounts, login credentials to the service offered by the victim company, email accounts, passwords etc.). According to Symantec, in 2013 the top ten pieces of stolen information were: personal data, date of birth information, identity cards, personal addresses, medical data, phone numbers, financial information, email addresses, usernames and passwords, and insurance data. Attacks of this kind have a tremendous impact on a business. In the case of internal data theft, there may even be a stop or fall in production. In the case of theft of external data (such as customer information) there may be a decline in sales due to the loss of customer confidence in the company, as well as potential legal damages for negligence in failing to preserve sensitive data. This represents, by far, the greatest threat to an SME, especially in Italy where it is difficult to repair the damage caused by a loss of the brand or of the product catalogue.

1.3.4 Espionage

Industrial espionage is an activity in which the main objective is to illegally obtain corporate and business information.

The methodology by which this type of attack takes place usually involves a direct attack through social engineering activities and/or the installation of malware on the victim company's system - giving the hacker control. This kind of attack is usually committed by a competitor with the objective of finding a gap in production or in the business. This type of attack requires an IT expert or disloyal employee.

1.3.5 Sabotage

Sabotage is an action that aims to slow down or block the activities of the victim company through the hindrance of normal operations - using means such as destruction of important material or equipment used by the victim company. Again, there are several methodologies, both social and technological, with the same players, objectives, and means as those used for espionage.

1.3.6 Demonstrative attacks

Individuals or groups of people usually cause this type of attack as a protest against the victim company accused of misconduct by end users or private citizens. These attacks usually come in the form of defacement or DDoS attacks intended to interfere with the normal work of the company and create propaganda for their point of view and as a way to display their anger.

1.3.7 Extortion

Information extortion is a criminal act in which the perpetrator installs software such as malware or ransomware on the victim's computer without the victim's permission. Through this software, the criminal remotely locks the victim's computer or encrypts the company data on it making it impossible to use. The victim is asked to pay a sum of money in order to unlock the PC or to decrypt data. The installation of malicious software is generally done through the use of fraudulent links sent by email (spam) on social networks (in which the victim clicks on the link) or through simple careless navigation.

This type of attack has increased considerably in the last year by as much as 500%[32] ,with particular interest in SMEs as preferential victims especially in Russia and in Europe in general.[33] The sums required for the ransom are reaching up to 3,000-4,000 dollars, which is often paid by the victim who would prefer to pay the money instead of losing the data or report the attack. The estimated damage is around 75 million dollars annually[34].

Below is an example of CryptoLocker's screen alerting the victim of the occurred encryption of all data and asking for a ransom for the return of said data within a set time.

[32] *Internet Security Threat Report 2014*, Symantec, available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (retrieved 6-11-2014).

[33] "*Ransomware criminals attack SMEs using strong file encryption, ESET warns Summer surge in complex attacks"* by John E. Dunn, available at: <http://news.techworld.com/security/3470388/ransomware-criminals-attack-smes-using-strong-file-encryption-eset-warns/> (retrieved 6-11-2014).

[34] *Europol, FBI, NCA and others disrupt the Gameover Zeus botnet — claim a 2 week window for users to get clean,* available at: <http://itsecurity.co.uk/2014/06/774/> (retrieved 6-11-2014).

Figure 4 - Image of the warning screen of CryptoLocker ransomware
Source: CryptoLocker Virus, example from Comodo.com[35]

It follows that there are many hidden risks in cyber space for SMEs which may impact on different aspects of business life, not only those directly related to information technology, but also on more important business and corporate assets: the data, people and services. The risks to the economy stemming from cybercrime are numerous and include mere money theft from bank accounts or credit cards, damage to the corporate network and machinery of the production system, damage to the company image, loss of safety, loss of production, and loss of intellectual property (for example the theft of patents).

Defense against the threats of cyber space offers companies an advantage in terms of competitiveness. This principle plays a key role in improving the economic factors of a country and translates into jobs and economic growth. A cyber attack on the SMEs is an attack on the whole economy of a country.

For this reason, an SME should not make the mistake of thinking it is immune to cyber attacks because it is small. The size of a company is not relevant[36]. They are, in fact, easy prey for cyber criminals who want to hit more than one company, and this is why SMEs today run a greater risk of losing confidential information from an attack than large companies[37]. Italian SMEs also face a further risk - the heaviest of any fraud or loss of data - that is, the loss of patents and know-

[35] *CryptoLocker Virus. Best Practices to Ensure 100% Immunity*, 25-10-2013, by Kimberly Reynolds, available at: <https://blogs.comodo.com/it-security/cryptolocker-virus-best-practices-to-ensure-100-immunity/> (retrieved 6-11-2014).

[36] According to the Symantec Report 2014, SMEs are as much as 30% of the victims of spear phishing.

[37] This is demonstrated by a study conducted in 2013 in the UK by the Government Department of Business and Innovation, available at: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (retrieved 6-11-2014).

how that makes the company so important and attractive: Made in Italy, a foundational aspect of our economy. In this context the formation of the management of SMEs becomes the first defense against this phenomenon.

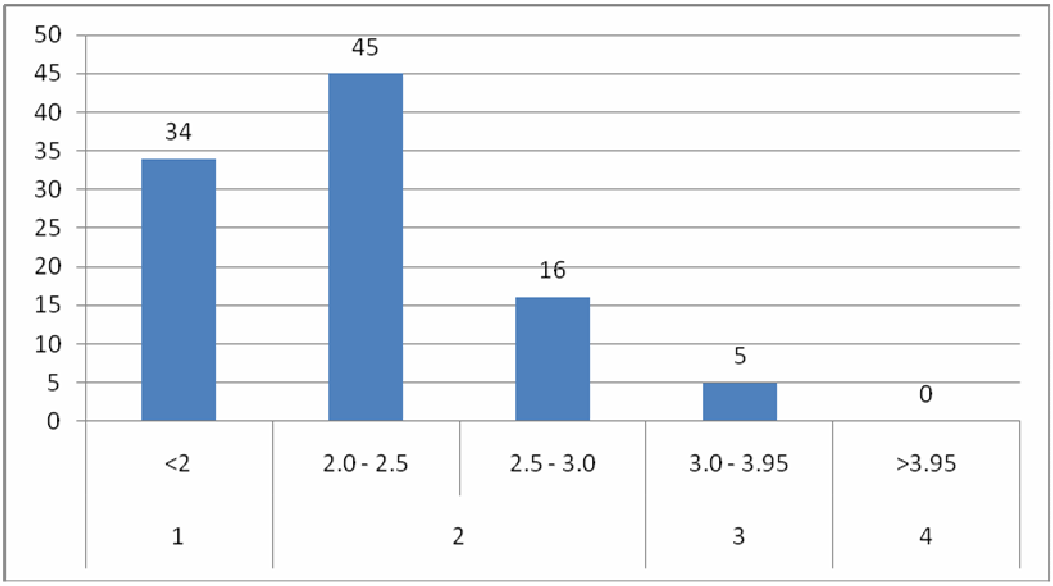


Figure 5 - Distribution of the degree of maturity of risk management regarding IT risks
Source: Risk and Responsibility in a Hyperconnected World, World Economic Forum, 2014

Out of 100 companies involved in the study of the World Economic Forum, Risk and Responsibility in a Hyperconnected World[38], it emerges, however, that corporate risk management is not very mature regarding IT risks. The report divides the degree of preparation of risk management into four levels: the lowest "nascent maturity" (1), "in development" (2), "mature" (3), and the highest "robust" (4). This investigation showed that no company examined has a robust level of risk management and only 5% were mature. As many as 34% are still at the lowest level showing the total unpreparedness of a third of companies. The remaining approximately 60% has a level of preparation in development. This level is in turn divided into two sub-levels and 45% of all enterprises are still in the initial stage of the implementation of information security practices. In the study the size of the companies in the sample are not specified but we can easily imagine that the level of maturity of risk management of a company is directly proportional to its size, so in relation to SMEs the data is absolutely alarming and shows how both necessary and urgent the implementation of training programs on cyber threats is.

Also, the smaller the size of the enterprise, the lower the ability to identify an attack immediately as compared to a larger company - for lack of specialized technical departments or simply because they are less accustomed to consider the threat. Compared to 65% of large companies and 43% of average size, only 22% of small businesses have a formally defined ICT

[38] *Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience*, World Economic Forum, available at: <http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf> (retrieved 6-11-2014).

policy. Moreover, another fact to emphasize is the prolonged recovery time companies spend on restoring attacked systems before resuming activities.

SMEs often make the mistake of considering themselves out of the reach of cybercrime. In fact, in a research study[39] conducted by Alliance of 1,000 SMEs, more than half of the respondents believed they knew how to protect corporate data and that of customers but did not have any type of corporate security policy governing the use of unprotected wireless corporate devices by employees or regulating the actions to be put in place in response to a theft of financial data or customer data. As many as 85% believe that large companies are the only target and that SMEs have less chance of being attacked by hackers. Any organization that can be easily hacked is a target of cybercrime and is viewed as profitable - be it for economic profit, for data, or for patents. Therefore, there is no discrimination concerning the size of a business. The research conducted by Alliance also shows that 65% of companies surveyed kept data about customers on their computer systems and 43% kept financial records. As many as 33% kept sensitive data relating to credit cards and corporate accounts and 20% kept data concerning intellectual property on their network - along with other sensitive corporate data. Also, as many as 75% of respondents said they had not provided more than three hours of training or an update about corporate network security or mobile devices in the last year, and almost half admitted to not providing any kind of training.

In short, it is clear that the perception of awareness regarding cyber threats is still very low especially among SMEs, which are now more likely to fall victim than large companies, who register increased investments in security policies and related budgets. This pushes the criminals to seek simpler, but equally as profitable, targets.

1.4 Types of attacks

The different types of cyber attacks perpetrated by attackers in order to damage companies, for purposes we have just analyzed, can be divided into two different dichotomies:

- Online attacks: the majority of attacks for both the number and different type (such as spam and phishing), and offline attacks: often result from incorrect employee behavior, whether it be deliberate or not - damaging the company by creating internal problems, or accidently through the improper use of company machines for personal use.

- Targeted attacks: in which the attacker hits a very specific company, selected for its specific characteristics such as product category or geographical area; and untargeted attacks: in which the attacker hits one or more companies that are vulnerable to the threat developed by the attacker.

[39] *National Small Business Study*, National *Cyber security* Alliance e Symantec, available at: <http://eagleintelligence.com/wp-content/uploads/2009/12/NCSA-SB-Study-Factsheet.pdf> (retrieved 6-11-2014).

1.4.1 Hacking

Hacking is the act of illegally accessing a system in order to achieve a high degree of knowledge and gain information regarding both the operation and the data it contains, in order to adapt it to the hacker's needs. The term hacking has acquired numerous identities during the period in which the cyber world has developed, gaining both negative and positive connotations.

The use of techniques and methods of hacking - with the goal of making a gain - are direct and material, indirect (by stealing information in order to resell the item or product), or with the purpose of damaging the victim company (called cracking). In our imagination, the hacker is a curious and solitary person motivated by challenge and personal interests, but the reality is different. The figure of the hacker is now groups of organized criminals who, through hacking, pursue economic motives for profit.[40]

1.4.2 Spam

Spam is the term for sending junk messages, usually advertising material, typically through email. The main goal of spam is advertising and the sale of illegal goods with false and/or illegal origin, leading you to the real scams. Generally, spam for companies is simply considered a waste of time but in reality the Internet traffic generated by spam is around 70% of all email traffic[41] and causes extensive damage, especially with the evolution of phishing and spear phishing. As confirmed by Symantec, spam had a volume of up to 66% of the total email traffic for the year 2013. Also confirmed by Symantec was that on average one in every 196 emails contains malware.[42]

1.4.3 Phishing

Phishing is an Internet scam attempt in which the attacker tries to trick the victim into providing sensitive personal information. They often send an email that simulates the graphics of a Post Office or Bank website and request login credentials or credit card numbers (explaining that the victim must supply said information in order to avoid incurring penalties or possible problems). Within this email is a link ("bait") that the victim needs to click in order to solve the problem. This link, however, leads the victim to a fake website in which they enter their personal data -

---

[40] The analyst Lillian Ablon, author of the study "*Markets for Cybercrime Tools and Stolen Data: Hackers 'Bazaar'*", underlines how cyber crime today is a crime more profitable and easier to perform than the drug traffic and that now is in the hands of real criminal organizations, available at: <http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf> (retrieved 6-11-2014).

[41] *More Than 70% of Email Is Spam*, Kaspersky Lab, available at: <http://usa.kaspersky.com/about-us/press-center/in-the-news/more-70-email-spam> (retrieved 6-11-2014).

[42] *Internet Security Threat Report* 2014, Symantec, available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (retrieved 6-11-2014).

delivering it directly to the criminal. The term phishing comes from fishing ("to fish" in English) and alludes to the attempt to "fish" for personal and financial information and passwords of a user. This type of attack is experiencing steady growth. From 2011 to 2012 it grew by 59% across Europe.[43]

A new variant of phishing, which for some years has been spreading, especially in English-speaking countries, is vishing. The scam is carried out by phone but is the same as phishing. Using deception and persuasion techniques, the criminal tries to get access credentials for online banking by posing as a call center operator or assistance. This new type of scam relies on the increased confidence that the victim puts in a person with whom he has direct and more personal contact with (and who appears to have permission to make the said contact) and is requesting such information - instead of just an email.

This threat should not be underestimated. Verizon data[44] shows that it is more effective than some might think. The following graph illustrates the fact that on average for every 14 phishing emails received one is successful.

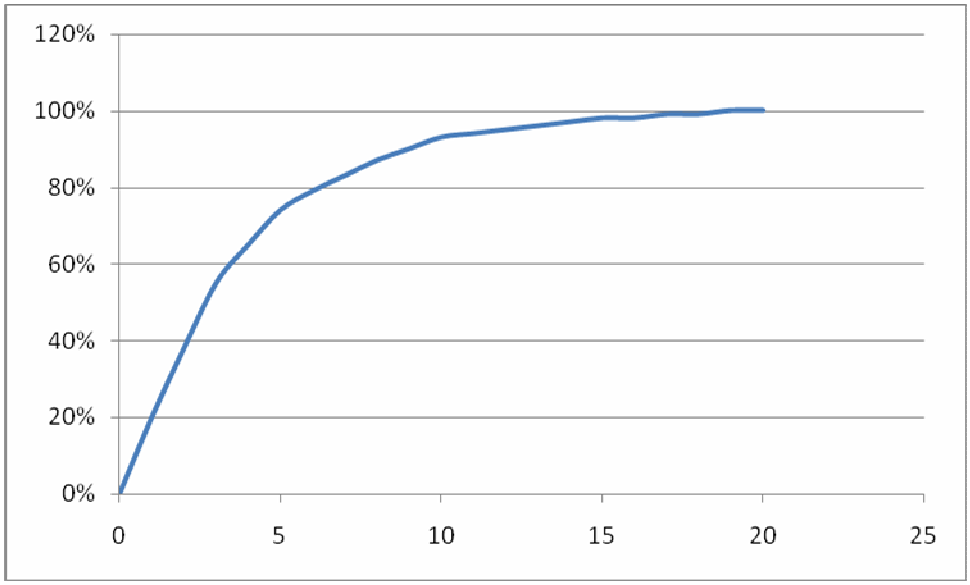


Figure 6 - Percentage of successful phishing campaigns
Source: Based on 2014 Verizon Data Breach Investigation Report

1.4.4 Spear phishing

Spear phishing is basically an evolution of phishing. The main goal remains the same: to steal sensitive data from the victim. The main difference between the two threats is that spear phishing does not send email to a multitude of random users but instead focuses on a few victims, calibrating the attack precisely. For example, in the case of SMEs, the attacker can send emails

[43] *The Year in Phishing*, January 2013, available at: <http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf> (retrieved 6-11-2014).

[44] *2014 Data Breach Investigation Report*, Verizon, available at: <http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf> (retrieved 15-11-2014).

that simulate the graphics of the bank of the victim (traceable via the IBAN posted on the company website) or a regular supplier. In this case the risk is very high as the hacker can be granted confidential data of the victim company with potentially serious economic losses. According to the 2014 Symantec Report, SMEs make up as much as 30% of the victims of spear phishing.

1.4.5 Pharming

The objective of pharming is the same as phishing. The hacker directs the victim to a fake website specifically designed to steal personal data. Unlike phishing however, pharming does not require user action, instead intrusion techniques are used on the user or ISP in which the attacker directs the victim to a site controlled by him.

1.4.6 Defacement

Defacing (or defacement) is the act of illegally changing the homepage of a website or one or more internal pages by unauthorized persons. It is usually a symbolic act of vandalism and is performed by attackers (often novices) as a demonstration of their skills and can also be used to defame or discredit the victim. In an enterprise the damage caused by these attacks is mainly to the company image as a website can be considered a "window" to its customers and/or partners and its damage may have a negative effect. In the case of ecommerce websites, damage is not only caused to the site's reputation, but also affects its economic aspect - both for the lost revenue for the period under attack and also for the future as it could discourage potential customers from entering their personal data into a "hacked" website.

1.4.7 DoS

Known as Denial of Service (DoS) or Distributed Denial of Service (DDoS), a "denial of service" attack is carried out by an attacker on a website or IT system with the precise aim of denying service provided by the attacked system. Again, like defacement, the main damage caused is to the image (in the case of a website attack), but it can also result in economic damage if the attacked system is a server that manages all business operations (email, accounting, administration, etc.).

1.4.8 Malware

The term malware ("malicious software") generically identifies all the software threats that can affect a PC. Within this family there are viruses, worms, spyware, trojans, backdoors, and many others. Using various techniques and methodologies, the aim of malware is to create serious damage to the infected machine and in some cases to replicate into the machines connected to it, in turn damaging them. In an enterprise, the loss of important data also often involves significant

delays in the supply chain and, in severe cases, the inability to continue to provide the service offered.

The main defense against such attacks consist of having antivirus software and firewalls properly configured and up to date, personnel being aware of the risks and being careful in the daily use of computer systems, and keeping backup copies of vital company data. The installation of malware can occur either online, such as by clicking links or downloading attachments received via email, or off-line, for example through the use of infected USB devices by an employee.

Many experts compare computer viruses to outbreaks of biological viruses. The main similarity between the two is that in addition to damaging the victim, it becomes a carrier of the infection itself - spreading the threat in its proximity. Obviously biological infections are spread by physical proximity (contact, air, etc.), while computer infections are spread by close connections (emails, cell phones, trusting relationships in the workplace, etc.). The second similarity is that a virus remains latent for some time and then can infect a victim for which it was not specifically created. In fact, even long after their implementation and launch, viruses can be found in the network and cyclically infect systems. An example is Stuxnet[45], which years after its launch continued to infect critical infrastructure systems in various countries around the world.

1.4.9 Botnet

A botnet or "robot network" is a network of computers called "zombies" connected to the Internet and infected with malware, which can be used without the knowledge of the legitimate owner of the machine by attackers who have obtained control - in order to carry out DDoS attacks, spam, or phishing.

The computers that are part of corporate networks are the most interesting for those who want to use this attack because on average they are on for long periods of time without being restarted, they are part of networks with multiple computers that can be easily infected and rarely is the end user concerned about the slow pace of the machine - erroneously blaming the machine's age even though it is actually a symptom of an illicit "job".

1.4.10 Social engineering

Social engineering is the set of techniques that exploit human behavior in order to obtain information. This method is able to circumvent any obstacles that are encountered by the hacker when appropriate security measures have been put in place. Through deception and identity hiding, or posing as another person, the hacker is able to obtain information that one would not be able to get otherwise. It is the exploitation of weaknesses of human behavior such as curiosity or empathy before the real attack takes place. The attacker often preys on low-level employees, by posing as someone of a higher level (internal or external) who requires information immediately, exploiting the fear within a working environment.

[45] For more details, see: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99> (retrieved 6-11-2014).

The attack techniques mentioned are not usually used individually. Often the attack is conducted using a combination of techniques in order to obtain the desired result as easily as possible.

1.5 Types of attackers

Attacker profiling has become more and more important in recent years because it helps in understanding the reasons and motivations behind the crimes.

1.5.1 Organized crime

Organized groups of criminals, often international, whose motivation is mere economic profit and whose main targets are companies and banks. They target victims with both individual and mass attacks (phishing, botnets). The low level of cyber protection makes SMEs an easy target for criminals.

1.5.2 Insider

An employee or former employee with the objective of damaging his current (or former) company directly (by damaging systems) or indirectly (by selling the information to a competitor). This individual can be driven by motivations such as anger towards colleagues or management, personal dissatisfaction, or frustration at work.

Organized crime and industrial espionage are the major threats faced by SMEs, especially in Italy where "Made in Italy" and the production of quality products is endangered by the theft of intellectual property.

It should be emphasized that, as evidenced by the CISCO Report in the graph[46], we can divide cyber criminals into a kind of pyramidal hierarchy that is headed up by the most capable innovators in the field of attack techniques and codes, those in the middle that leverage the existing infrastructure of attack and/or sell such instruments, and the basic attackers that can be considered almost non-technical, but are in any case criminals in this area by pure chance, users of the programs and infrastructure put out by others.

1.5.3 Industrial spies

Industrial spies are individuals whose only motivation is that of indirect personal profit by sale of confidential information of a company to a competitor or blackmailing the victim for non-disclosure of stolen confidential information. They target companies and corporations.

[46] *Annual Security Report*, 2014, CISCO, pag.10, available at: <http://www.cisco.com/web/offer/gist_ty2_*asset*/Cisco_2014_ASR.pdf> (retrieved 6-11-2014).

1.5.4 Hacktivists

Hacktivists are groups of people with ethical, civil and political motivations and whose objective is to demonstrate their ideals and views. The term was coined to define civil disobedience protagonists and indicates the practices of those who, through the network, attack governments and multinationals accused of inappropriate behavior towards citizens or users. The attacks, mostly defacement and DoS, but sometimes even more serious, are the transposition of direct action conducted through the medium of technologies: DDoS, such as processions and massive emails of participation and protest, such as leafleting and graffiti, which are represented by temporary defacement of websites. This type of attacker is less interested, as a rule, in hitting SMEs and therefore in theory constitutes a lesser threat - unless the small or medium enterprise is in a close business relationship with the target company.

1.5.5 Wannabe lamer, script kiddie

Cybercrime is not a prerogative only of those who have highly developed technical or special skills. Thanks to the increasing computerization of all aspects of daily life, even the concept of the hacker has undergone development. Among the different profile types of hackers we can distinguish those most concerned with SMEs, (the most dangerous when considering this field of study), who are known as "wannabe lamers," and "script kiddies." These are two profiles that identify often young, less experienced and less capable hackers who act in the name of trend, as an outlet for their anger, or to demonstrate their abilities, without any real motivation relating to the victim. Whether through an act of boredom or vandalism, due to limited experience they damage the systems of end users and SMEs because they do not have the skills to aim for bigger goals. Their lack of experience makes them potentially very dangerous because they can cause serious damage due to incapacity rather than voluntarily actions. This type of attacker affects SMEs or end users who have lower defenses. An attentive approach to cyber security significantly helps combat this kind of attacker.

1.6 Risks

The types of attacks and attackers listed above ensue different types of risks for companies arising from technical and human vulnerabilities that will be discussed later. The risks hidden in cyber space for SMEs may impact different aspects of business life, not only those directly related to information technology, but also on the most important business and corporate assets: the data, the people, and the services.

Loss of data or integrity can lead to pure and simple direct economic loss (through the loss of credentials, spam, or due to extortion and fraud), and to damages resulting from the theft of intellectual property and the damage of image and reputation. In fact, information today often has

the same economic value of money and can translate into customer databases, corporate financial data, financial details of customers and suppliers, pricing information, product designs and manufacturing processes. This type of risk is particularly strategic, especially for SMEs, not only because it is difficult to estimate but above all because it is related to the core business and creates damage which is difficult to repair. When damage is caused to a single and specific area of a large solid multinational or company which produces a wide range of products, it is easier for them to manage the situation than it is for a SME that bases its entire business on the production of one single asset. It is easy to imagine how an attack of this kind can cripple an SME and what kind of impact it can have in terms of jobs and the local economy.

The second type of damage that SMEs may suffer as a result of a cyber attack is related to physical impact damage, that is the kind of attacks that affect the integrity of the equipment, systems, networks and control instruments, slowing or effectively blocking the production and damaging the company's business or preventing access to the web and to all corporate information systems. To restore systems, an investment of money and time is required, which further aggravates the direct damage of the attack.

The third and final type of damage concerns damage to the services provided or used by a company that can affect the quality of the goods produced or the safety of employees or users.

1.7 Technical vulnerabilities

Every company has its own vulnerabilities, both technical and human, which when identified, can be exploited by cyber criminals. In most cases, the attack techniques used are widely known and often simple and are aimed at the company's weak spots: code errors, failure to install security patches for programs or systems used by the victim, failure to update antivirus and anti malware, the incorrect configuration or failure of devices and corporate networks, or the use of repetitive passwords or passwords which are too simple. These are all vulnerabilities that could be easily erased with proper preparation by technical management and a greater knowledge of best practices by all users of the systems at risk. These simple practices make it more difficult to obtain the result desired by the attackers.

Today’s technology, enterprise-wise, is increasingly pervasive and consists of fast developing innovations in every area. These two features lead users to use technology, which has not always been researched or developed with security in mind. Even a wealth of technical knowledge is not always sufficient for the safe use of these tools. The availability of the Internet is now constant through wireless networks, which are often unprotected or poorly protected. These networks often have default passwords or passwords that are too simple, do not have their devices and internal networks properly configured, and use non-secure protocols such as WEP and WPA instead of the more secure WPA2. This has given rise to many tools, which until recently, have been considered unthinkable - this in turn, leading to a number of new security problems regarding data and information.

The first intrinsic risk factor is derived through the online exposure of devices, including the type of connection used and of the connections in general, offering the possibility of different types of attacks. For example, in recent years, both in private and corporate usage, the phenomenon of cloud computing, primarily for economic issues, has become evident. In short, cloud computing is the ability to use IT services through the web. More simply, this allows for the availability of files and data anywhere you have an Internet connection. Files and data can be shared across multiple platforms (home PC, office, smartphone, Smart TV, etc.) but, and in more articulate terms, can also allow exploitation of web applications by sharing them with other people over the Internet.

In fact, protecting information, which as we know is the real "money" of cyber space, is much more complicated if it can be viewed via the Internet by its legal owner. An example is the person who accesses company files from his home PC because he has to work late in order to meet a strict deadline. It is very difficult to reconcile the demands of mobile and security needs because in doing so the information can also be accessed by an attacker who, despite not having the right to that information, is competent enough to reach it, and his task is often made easier by the user's superficiality or incorrect system configurations.

This type of care is considered mandatory as defense against both internal and external attacks (made by people who may, for various reasons, want to damage, steal or resell data that they should not have access to, or in order to perform more harmful operations). At the corporate level, it is therefore essential to have prevention "rules" governing the use of mobile devices, both corporate and personal, when connecting to free wireless networks offered by stores, bars and restaurants, or while entering sensitive corporate data (bank accounts, passwords, corporate credentials) while browsing on unsecured free Internet wireless.

Together with cloud, another ongoing concern is mobile devices, such as smartphones and tablets, the sale of which has already far exceeded that of traditional PC desktops and laptops,[47] and the use of which is increasingly widespread.

[47] The global smartphone market reached a new milestone in 2013 with a billion units sold in just one year, for the first time, an increase of 38% compared to 725 million units sold in 2012. For more details, see: a *IDC Worldwide Quarterly Mobile Phone Tracker, January 2014*, available at: <http://www.idc.com/tracker/showproductinfo.jsp?prod_id=37> (retrieved 6-11-2014).

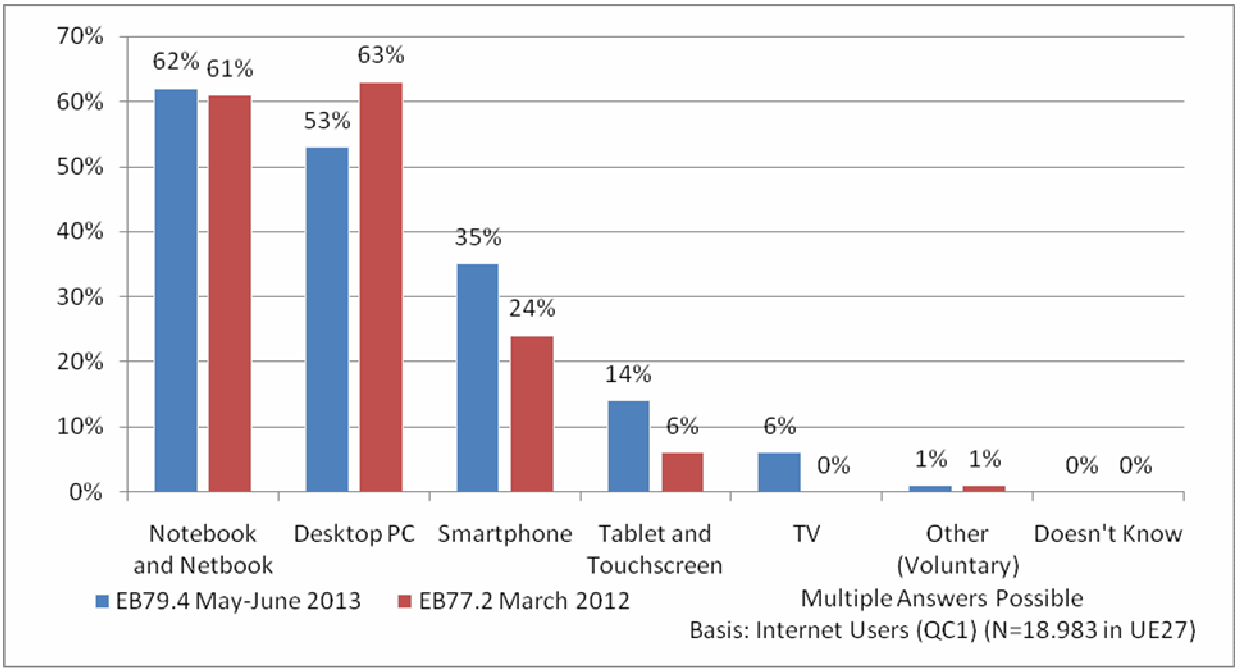


Figure 7 - Statistics on the use of devices for accessing the Internet in Europe
Source: Special Eurobarometer 404 Cyber security Report, 2013

The chart above shows several interesting points. First of all, while there has been a 10% decline in the use of desktop PCs, the use of the laptop remains stable in first place as the device primarily used to access the Internet.

The second interesting fact is the appearance of Smart TV, which has begun to carve out its share in the device market for web surfing - the first step to the Internet of Things (IoT)[48].

The last, but most interesting finding is the increased use of tablets and touchscreen devices, which has more than doubled - with 11% more smartphones. Unfortunately, the data relating to the spread of mobile devices is not encouraging if we look at the estimates of Symantec, which in its report emphasizes that 44% of adults are not conscious about the security of their mobile device. Just think of how careless teenagers can be, and they represent a significant percentage of smartphone and tablet users. This type of inattention brings risks when using the device, such as: loss of privacy, text messages or phone call logs being read, GPS tracking, calls and messages being recorded, email being read, video and photo theft, stolen social network accounts, and theft of installed applications.

Unfortunately, the high diffusion of these devices not only attracts the interest of cyber criminals who are increasing their efforts to exploit the vulnerabilities of these systems, it is also counterproductive from the point of view of security - as they are extremely difficult to protect. The main difficulties are:

- Manufacturers: the technology is still young, the design does not consider security, slow-release of patches and updates, and official store security;

[48] For more details, see: *Internet of Things* by Hermann Kopetz, available at: <http://link.springer.com/chapter/10.1007/978-1-4419-8237-7_13> (retrieved 6-11-2014).

- Users: the incomplete knowledge of the use of the device, sensitive data that is stored on them in a superficial manner, the lack of attention regarding updates, and the failure to install anti-virus and anti malware software.

The above-mentioned difficulties are only a few of the important ones. The consequences and risks are obvious. As well as risk of infections of viruses and malware, there is also social media fraud and phishing. Moreover, in this area in 2012 there was a huge acceleration in the increase of malware samples for mobile devices, which quintupled compared to 2011. This increase is due to the constant growth of banking transactions made through mobile devices. According to Gartner, the volume of mobile transactions globally will grow by an average of 42% per year between 2011 and 2016[49]. In regards to this, Kaspersky highlights how mobile banking trojans are evolving.[50]

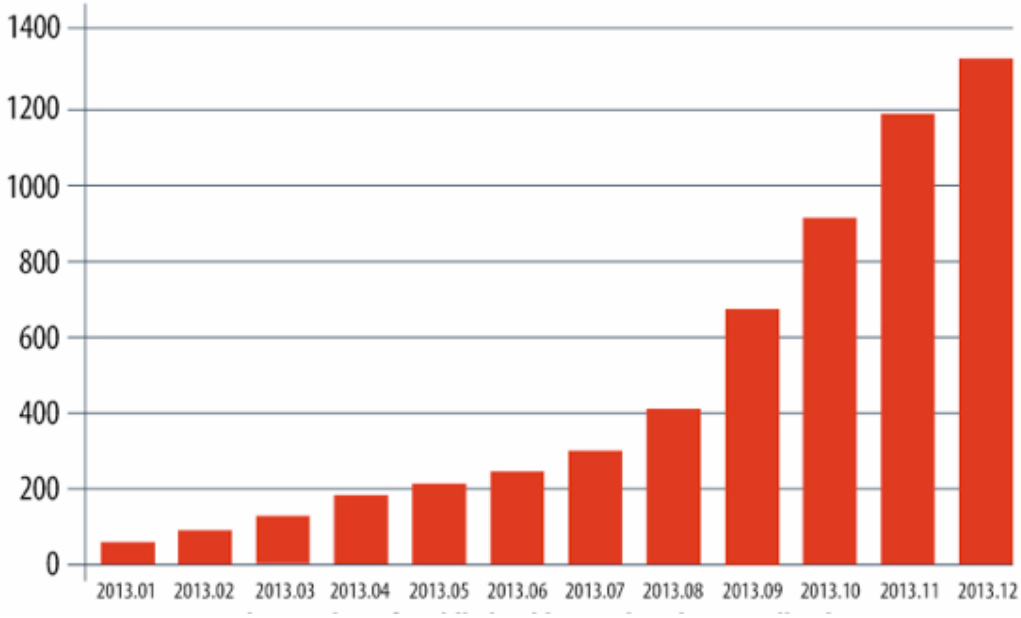


Figure 8 - Data relating to the increase of the number of trojans that target banking transactions made through mobile devices
Source: Mobile Malware Evolution, Kaspersky, 2013

The following graph, also by Kaspersky, shows that Android is the Operating system for mobile devices most affected by malware, with over 98% of detected threats. However, the most interesting factor is actually what is not present. That is the total absence of iOS - the Apple Operating system, which is now apparently immune to this threat.

[49] *Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $171.5 Billion,* available at: <https://www.gartner.com/newsroom/id/2028315> (retrieved 6-11-2014).

[50] *Kaspersky Mobile Malware Evolution: 2013,* 24-2-2014 by Cassie Bodnar, available at: <https://blog.kaspersky.com/mobile-malware-evolution-2013/> (retrieved 6-11-2014).

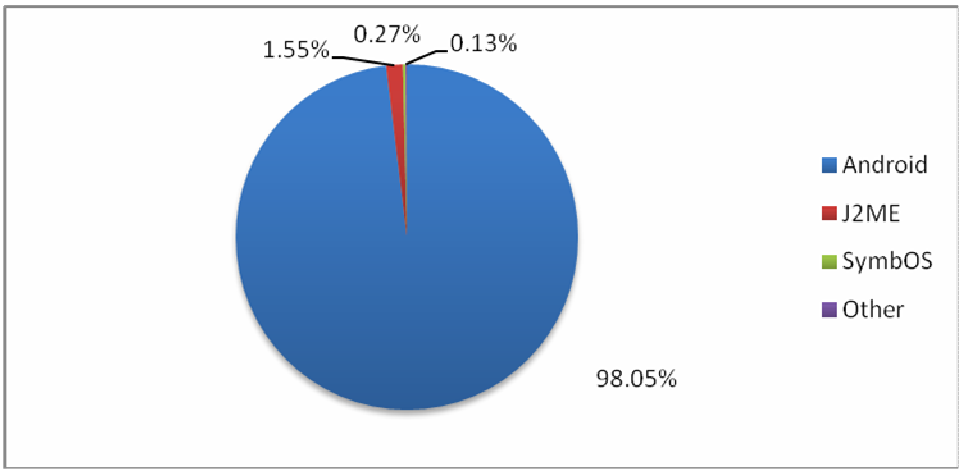


Figure 9 - Data on the percentage of spread of malware for mobile devices O. S. Source: Mobile Malware Evolution, Kaspersky, 2013

The spread of mobile devices has also contributed to an increase of the practice of BYOD, and the lack of security of these devices immediately makes companies less secure. While encouraging the use of personal devices to access corporate systems, in many cases companies underestimate the need for higher security standards to protect their sensitive data - such as the use of VPN or data encryption.

The survey IT Security Risks 2014 by Kaspersky Lab[51] shows that a further risk is the increase of the physical theft of mobile devices with a consequent risk of loss of sensitive data, corporate materials, and access to business services, which is up 25% compared to 14% in 2011. In addition, this risk is compounded by the fact that the employee who suffers the theft of his device usually reports it to the company with an average delay of between 2 to 5 days, reaching a dangerous response time to this threat. The vulnerability in these cases is not only technical, but mostly human, because employees tend not to alert business managers quickly of the occurred theft. As many as 38% of employees reported the theft of their device after 2 days, and 9% after 5 days, while only half of employees reported the incident the same day - a decrease compared to 2013 (60%).

The most worrying fact is that 19% of companies said they had lost sensitive corporate data following the theft of a mobile device[52]. Alongside the increase in the spread of the use of mobile devices in enterprises is the increase of theft and risks for companies - but the level of danger felt by employees has decreased. All over the world, as considered by the Kaspersky survey, the number of employees who report such cases is decreasing with time[53]. Despite the steady increase

[51] Survey targeted at information security professionals in enterprises and organizations on a global level. *IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats*, Kaspersky Lab, available at: <http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf> (retrieved 6-11-2014).

[52] Data is based on the contribution of 3,900 IT security managers of companies and organizations of all sizes and in 27 countries worldwide, of which 198 have contributed from Italy.

[53] In other areas of the world there are different rates of decrease; in North America, for example, the rates are slower. Only 43% of employees report the theft on the same day in which it occurred. In Asia, there has been the most significant change in just one year. 47% of employees in 2014 reported the theft of the device in the same day, while in 2013 the percentage was 74%.

of the use of mobile devices in the workplace, more than half of the respondents admitted to being more concerned with risks than in the past, and 43% believe the risks outweigh the benefits in terms of comfort.

As for SMEs, another factor that contributes strongly to making companies less secure is the use of out of date, and therefore unsafe, operating systems, programs, and applications - both client and server. For example, the failure to move from Windows XP to a recent version of the Microsoft operating system (often for lack of corporate funds for the purchase of expensive licenses) is an extremely relevant vulnerability, especially since April 2014 when Microsoft definitively decided to end support for this product.

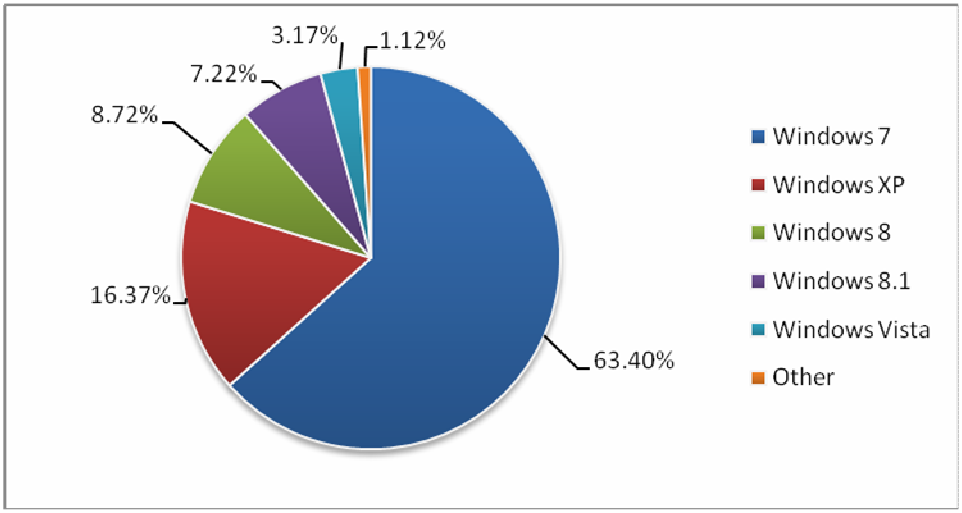


Figure 10 - Windows XP usage in June 2014, two months after the end of the official security support by Microsoft
Source: Windows usage & vulnerabilities, Kaspersky Security Network Report, 2014

As illustrated by Kaspersky Lab, among the users participating in the survey[54] regarding the use of Windows, it is evident that two months after the end of official support for Windows XP from Microsoft, over 16% of users were still using this O. S.[55], which dates back to 2001 - so 13 years ago. In information technology terms, that corresponds to an enormous amount of time. This finding is significant when considering the potential implications for the security of information. Having an outdated version of an operating system creates major risks arising from the possibility of exploitation by cyber criminals of unpatched vulnerabilities. The report also examined the percentage of users who still use Windows XP in individual countries, and Italy is in fifth place with 20.31% - the first among Western countries and represents a significant percentage in regards to information security. If we consider the percentage of users who have made the transition to the new operating system in recent months, analyzed by individual countries, the leaders are the United States (16.27%), Canada (13.52%), Germany (11,17 %), the

[54] *Kaspersky Security Network Report: Windows usage & vulnerabilities Version 1.0*, August, 2014, available at: <https://securelist.com/files/2014/08/Kaspersky_Lab_KSN_report_windows_usage_eng.pdf> (retrieved 6-11-2014).
[55] As confirmed by Statcounter.

United Kingdom (10.79%) and France (10.31%). The outsiders are Italy (8.1%), Russia (5.14%), and India (2.91%).[56]

In addition to the vulnerabilities arising from the use of outdated operating systems, the careless use of programs such as PDF readers (Adobe Reader, Foxit Reader), rarely updated office suite programs (Microsoft Office, LibreOffice, OpenOffice), and online services (Facebook, Twitter and all the applications offered by Google) all of create risks to the security of users.

1.8 Human vulnerabilities

The human factor is undoubtedly a key factor in the entire system of corporate security. In fact, very often the first breach in the security of a system is achieved not by technical means, but simply by taking advantage of aspects of standard human behavior: distraction, superficiality, negligence, altruism, confidence, and curiosity - which are the basis of many types of attacks. Attacks such as phishing, pharming, fraud, identity theft or theft of sensitive data, are based on the probability that the operator on the other side of the PC may be prompted to click on a suggested link, led by simple curiosity, because he believes he knows the sender of the email or because he is convinced they can solve problems with his credit card.[57] The social engineering technique is more complex because it uses the phone, email, information released on social networks, and direct physical contact, to get the necessary information directly from the target, in order to commit the attack using technological tools. It is therefore necessary to understand the mindset of the attacker, his attitude, his motivations, and how he collects information about the target - basically hacker profiling and the ethics that motivate them.

In July 2014, Goldman Sachs[58] asked Google[59] for the removal of a confidential email containing classified company information and customer data, which was sent in human error from a contractor of the investment bank to a wrong email address (gmail.com instead of gs.com, which is the Goldman Sachs corporate domain). This is an example of an extremely basic error that risked compromising sensitive data and consequently high profile business relationships.

---

[56] *16.37% Users Still Run Windows XP*, Kaspersky Lab Statistics Say, August, 2014, available at: <http://www.kaspersky.com/about/news/virus/2014/16-37-per-cent-Users-Still-Run-Windows-XP-Kaspersky-Lab-Statistics-Say> (retrieved 6-11-2014).

[57] In an ironic way, information technology has coined the term PEBKAC which means "Problem Exists Between Keyboard And Chair", to indicate that in information technology problems often are caused by the user himself.

[58] *Goldman says client data leaked, wants Google to delete email* by Jonathan Stempel, 2-7-2014, available at: <http://www.reuters.com/article/2014/07/02/us-google-goldman-leak-idUSKBN0F729I20140702> (retrieved 6-11-2014).

[59] On June 26, Google declared that email could not be eliminated without the order of the Court. The Case is Goldman, Sachs & Co. V. Google Inc. New York State Supreme Court, New York County, No. 156295/2014.

A recent study reveals that 80% of IT Professional respondents see employees as the weakest link in the IT security chain and paint a picture of the SME sector as being flooded with cyber threats.[60]

1.8.1 Vulnerability arising from the use of social media

This type of vulnerability is placed in the "human" category because the high risk that Internet users face through the use of social networks is not derived from programming errors of platforms such as Facebook, Twitter, LinkedIn etc., but from the incorrect use of these tools, and by malicious applications and the external plug-ins connected to them. These are made by cyber criminals and redirect users to malicious sites or fraudulent links with deceiving advertising - by inviting the user to click on false applications for games or viral videos, offering the ability to see who has visited a person's social profile, or to change the color of the template. In fact, in 2012 a large percentage of spam and phishing moved to this type of platform, making it increasingly insidious and difficult to recognize these threats. In 2013, Symantec confirmed the emergence of new threats that take advantage of the increasing popularity of social networks. Social connectivity in recent years has had unprecedented growth. It is estimated that 71% of adults using the Internet have a Facebook account[61], which alone has increased from one million users in its first year to more than 1.15 billion today. Social networks are increasingly important for global business, especially in the mobile phone market. When a new social network reaches an appropriate level of popularity it inevitably triggers the attraction of more and more users - and in turn, more and more criminals who gain interest and find new ways to exploit the platform for illegal purposes.

It is therefore important to emphasize that in order to address this growing threat, it is necessary to increase efforts relating to awareness policies and the education of people regarding prudent use of the web and social networks, rather than by technical tools alone. This would certainly lead to benefits at a corporate level also because it would be replicated in the workplace regarding the potentially incorrect attitudes we have towards the use of mobile devices, the superficiality with which we use USB devices or smartphones, and open emails from unknown senders or download unsafe pirated software.

---

[60] *2015 State of SMB Cybersecurity,* CloudEntr by Gemalto, available at: <https://app.box.com/s/2mf328i6a7j0z2tbdv07?src=undefined> (retrieved 15-11-2014).

[61] *The Internet Oranized Crime Threat Assessment (iOCTA) 2014*, EUROPOL, available at: <https://www.Europol.europa.eu/sites/default/files/publications/Europol_iocta_web.pdf> (retrieved 6-11-2014).

CHAPTER 2

CYBERCRIME: AN INTERNATIONAL AND EUROPEAN PERSPECTIVE

2.1 Cybercrime as an international threat

Globally, risks of various kinds have become more and more important due to the intensification of globalization. In this scenario, cybercrime is an even more dangerous threat. The consequences of the new risks have become international, and are potentially devastating and unpredictable. Global interconnectedness makes any national economic production system vulnerable. As we have seen, cybercrime is a phenomenon that affects all the countries of the world - especially the most industrialized and computerized.

There are hundreds of different sources that provide data about the scale of cybercrime, but the statistics are insufficient and fragmented. However, when conducting an analysis, of a major report from the field, the data is very discouraging.

In a recent report drawn up on the basis of interviews among 250 industry experts and business executives, the World Economic Forum warns that over the next six years cyber attacks could cause economic losses of up to 3 trillion dollars if we are unable to act effectively in order to fight this threat. That could, according to the same study, also lead to a slowdown in the use of innovative technology solutions in the coming years.[62] As many as 78% of companies surveyed, in fact, had postponed the use of solutions such as cloud computing for fear of being a victim of a hacker attack and suffer the loss of sensitive data. According the WEF study, the adoption of proactive actions by companies and governments would not only lead to a limitation in the number of attacks, but could also lead to generation of economic value in terms of technological innovation - which in turn would generate a profit to the global economy of between 9 and 21 trillion dollars in a decade.

The annual cost of the damage inflicted by cybercrime is difficult to estimate for several reasons: companies do not always share information as they often do not realize they have been attacked until months or years later, and in some cases it can be difficult to estimate the actual loss suffered. In this type of crime, the fact that there is no legislation at the international level should be taken into consideration. It is also difficult to define which actions are considered offenses in different nation states in order to draft reliable international estimates.

In addition, numerous reports drawn up by private IT security companies all suffer the limitation of not being able to take advantage of the full data compiled at the level of the

[62] *Risk and Responsibility in a Hyperconnected World*, World Economic Forum, available at: <http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf> (retrieved 6-11-2014).

individual nation state. Only an official report drawn up by a government body could provide more details on the final statistics. In any case, these reports by IT security companies give an indication of the severity and the trends recorded in recent years regarding cybercrime. All reports, in fact, point out that the risk of cyber attacks is constantly increasing and that the impact on the global economy is increasingly worrying, and this should be enough to encourage SMEs, civil society and governments to take this threat more seriously and to cooperate in order to limit damage.

According to Kaspersky, the impact of cybercrime on the global economy is sadly destined to multiply over time, with the most feared attacks being those to critical infrastructure. What is also worrying is the significant increase in crimes against businesses, such as fraud or identity theft. At the Dublin Web Summit this year, Eugene Kaspersky said that the impact of cybercrime on the global economy has been estimated at one hundred billion dollars, but that today this value should be considered multiplied many times over[63].

The more conservative estimates of McAfee[64] and CISCO assess the gap of the annual cost of cybercrime to the global economy at between 375 and 575[65] billion dollars a year, potentially even a trillion dollars - but still growing steadily due to the large and easy returns compared with very low risks for criminals. McAfee also noted that companies tend to underestimate the severity of cyber risks and their growth rates.

The gap between the increased ability to attack and the defense systems of companies is constantly increasing[66]. This problem becomes greater when considering SMEs, who, for obvious reasons, have smaller budgets dedicated to defense instruments than large companies - which are often too small in terms of the required security measures. It is estimated that in 2013 alone, there was a loss of over 800 million records - a cost to businesses of 160 billion dollars a year. In 2013, more than 3,000 companies in the US were victims of cyber attacks, two banks in the Persian Gulf lost almost 50 million dollars, a British company lost more than a billion dollars, and in Brazil millions of dollars were stolen from customers. Between 2011 and 2013, Indian CERTS[67] claimed that cyber criminals had violated more than 300,000 websites.

One of the most extensive studies on the impact of cybercrime on users, the Norton Cybercrime Report 2012, estimates that each year cyber crime directly affects, on average, over

---

[63] *Online fraud costs global economy 'many times more than $100bn'*, The Guardian, 30-10-2013, available at: <http://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars> (retrieved 6-11-2014).

[64] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies June 2014*, available at: <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (retrieved 6-11-2014).

[65] Even the smallest of the estimates is still higher of revenue of many National States.

[66] According to Gartner, global spending on cyber security products and services was around 70 billion dollars in 2013, an increase of 16% over the previous year, while estimates of the Ponemon Institute indicate the direct and indirect losses caused from cybercrime are estimated at 500 billion dollars, 26% more than in 2012. It is therefore evident that economic investment in IT security is not sufficient to counter or at least stem the advance of the threat posed by cybercrime.

[67] The acronym CERT is the historical name for the first team (CERT Coordination Center CERT-CC) at Carnegie Mellon University in Pittsburgh (Pennsylvania), established in 1988 in response to the Morris worm, available at <https://www.cert.org/about/> (retrieved 10-11-2014).

500 million people[68]. Given their greater level of computerization, more industrialized nations suffer the most losses, but the situation is expected to increase in less developed countries as they increase their computerization. The United States, China, Japan, and Germany, alone, have registered 200 billion dollars of annual losses.

The report presents the average estimates of the costs which companies incur when they suffer an attack - in six analyzed countries: the United States, Germany, Japan, France, the United Kingdom and Australia. The difference between the national data could depend on both the frequency and previous experience of attack and on the level of importance that each company places on this specific threat compared to others.

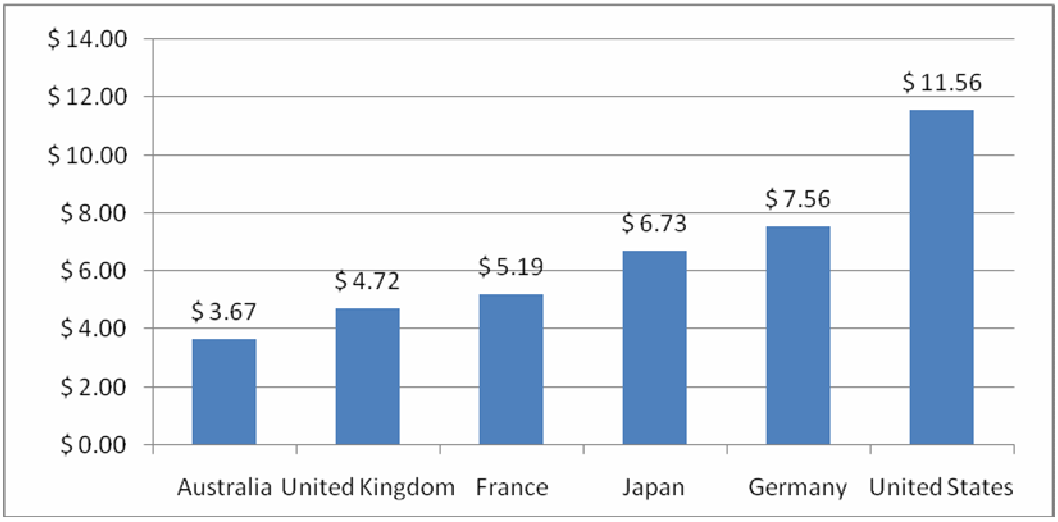


Figure 11 - Data related to the total cost of cybercrime in six nations, expressed in millions of dollars
Source: Cost of Cybercrime Study Global Report, Ponemon Institute, 2013

Other types of losses, as we have seen, are much harder to quantify. For example, losses from theft of intellectual property are difficult to estimate in the short term but they are a huge cost for companies in the long run, not only as a direct loss but above all in terms of cost recovery, loss of business, and loss of jobs.[69] Cybercrime has a serious impact in terms of employment within a country and the greatest damage to companies is the effect that an attack can have on the business, specifically: customer relations, compensation to be paid or contractual penalties, recovery costs relating to image damage, countermeasures to mitigate the loss, disaster recovery plans and insurance, damage to reputation, and effects in terms of competitiveness. In the US alone, there was a loss of employment of at least 200,000 jobs, while in Europe it is estimated that the losses could be around 150,000 - not only employees of companies closely related to the IT world, but also employees of companies suffering difficulties following huge economic losses.

[68] Estimate made based on a sample of 13,000 users from 24 countries.

[69] A British company admitted to have suffered losses of 1.3 billion dollars due to a theft of intellectual property and, subsequently, suffered significant disadvantages in its business activities. *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies June 2014*, available at: <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (retrieved 6-11-2014).

And if we consider SMEs, the data is even more alarming. According to the Symantec Internet Security Threat Report 2014, cyber criminals will focus their resources on attacks against small and medium sized enterprises, and they will descrease those against large companies. In addition, the report stresses that the methodologies used are becoming increasingly sophisticated and are composed mainly of the use of phishing, social engineering (often used together), and ransomware.[70]

Data concerning the impact of cybercrime on employment and infringement of intellectual property is not easy to estimate, but it is certainly not to be underestimated. The variables are more severe for the economy of a country - especially for countries like Italy where SMEs are the backbone of the national economy. Losses from theft of intellectual property affect the income, production and employment of a company. When considering the economic impact of cybercrime, it is easy to see how the main damage to companies consists of intellectual property theft[71]. This is damage that affects a company internally, but which has a rippling effect both nationally and internationally. All this acts as a brake on business growth and the growth of a country as a whole by preventing the expansion of national and global economies, which are so important in the international development - above all in these years of deep economic crisis.

Although the losses caused by this type of violation are not immediately apparent, they should not be seen as insignificant when compared to the loss of banking and economic data - which are easier to calculate in the case of a cyber attack. Millions of people and businesses have become victims of credit card data theft and illegal levies on their bank accounts - so much so that it is becoming a global phenomenon. In 2013, in the UK alone, a series of large-scale attacks on (mainly) targeted companies caused losses of 850 million dollars; in Australia, losses amounted to about 100 million dollars.[72]

In the UK, the National Cybercrime Unit of the National Crime Agency (NCA) has launched a new campaign to raise awareness of the dangers of inadequate online protection, asking users to be "cyber streetwise" and to adopt security measures to protect their data. According to the Office of National Statistics, there were more than 10,000 victims of computer viruses in the UK last year - 80% of which could have been avoided by simply upgrading security programs and installed software.[73] The objective of this new campaign is to reduce the number of attacks caused by fraudulent email, the use of infected USB sticks, and to combat the lack of attention when downloading from the Internet and when updating programs. These are cited as the most common problems among users. The campaign also highlights how both savings and personal data of users are at risk. The statistics that led to the creation of this initiative, to which 860 million

---

[70] *Symantec Internet Security Threat Report 2014*, available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (retrieved 6-11-2014).

[71] *2014 McAfee Report on the Global Cost of Cybercrime*, available at: <http://csis.org/event/2014-mcafee-report-global-cost-cybercrime> (retrieved 6-11-2014).

[72] Data by McAfee-CSIS.

[73] *10 Steps to Cyber security Executive Companion CESG The Information Security Arm of GCHQ*, available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf> (retrieved 6-11-2014).

pounds has been allocated over a five year period, are those related to the percentage of adults who do not install or update security software (40%).

Unfortunately, this trend in cybercrime is only getting bigger. There is a low risk index for hackers to be caught. It is extremely easy for a cyber criminal to commit this type of crime in the face of very low risk and huge gains. Industry studies estimate that the Internet generates a volume of business for the global economy that varies between 2 trillion and 3 trillion dollars a year, and that given the high growth of computerization, it constitutes a market that is steadily increasing. This aspect could help boost global economic growth, if it were not so vulnerable. Cybercrime is a tax on the value of the economy estimated between 15% and 20%, with an impact on global GDP ranging from 0.4% to 1.4%, and with serious implications on growth and employment - reducing the rate of investment in innovation by companies.

From the data provided for this research by Dr. Paolo Passeri, who has been analyzing the major cyber attacks that occur globally for years, we note that cybercrime is always the main motivation behind the attacks against the public and private sectors.

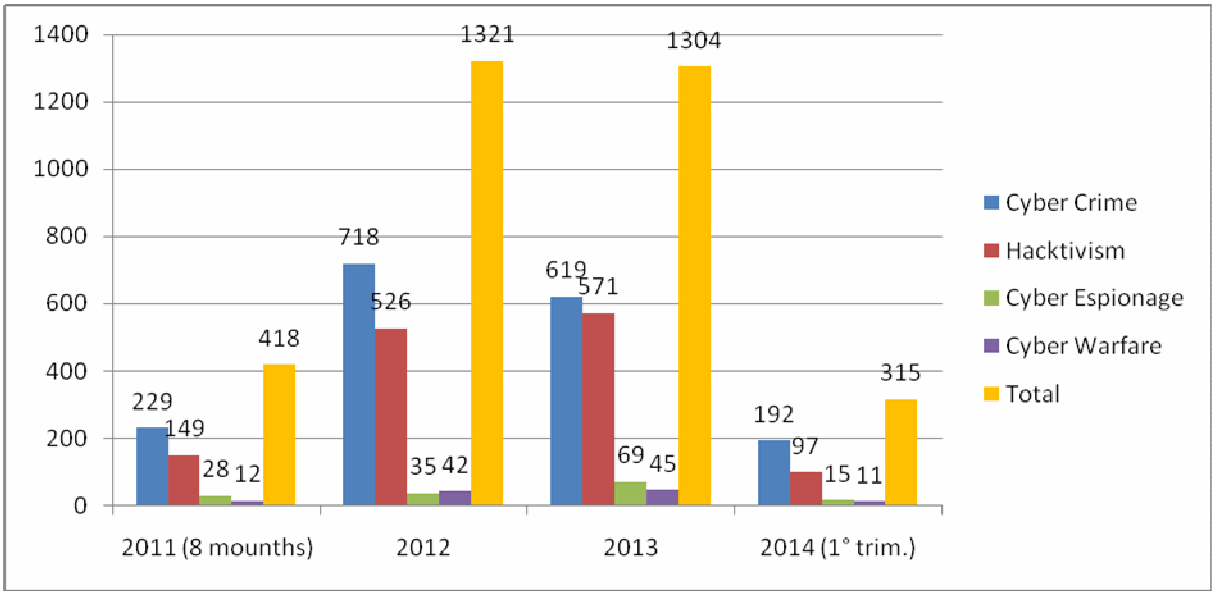


Figure 12 - The motivation at the basis of most cyber attacks in the world, 2011-2014
Source: Based on data provided for this research by Dr. Paolo Passeri, 2014

Another aspect that characterizes the phenomenon of cyber crime, and what makes it so insidious, is that being strongly linked to technology, it is a phenomenon with a high growth potential - parallel to the increase of the digitization of every aspect of daily and business life and the exponential increase of Internet users.

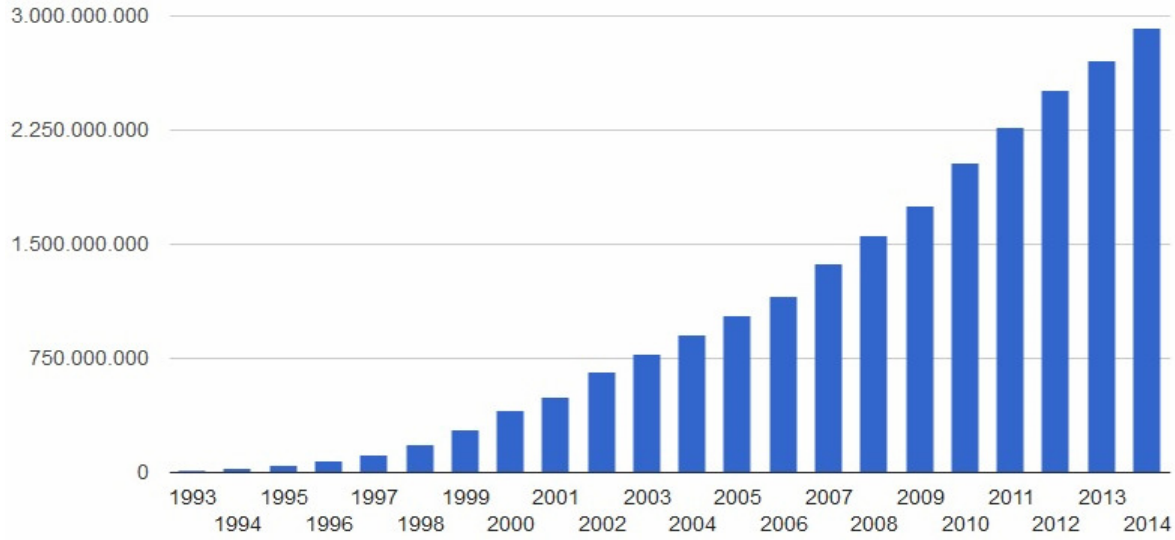


Figure 13 - Overall number of Internet users
Source: Internet Live Stats[74], 2014

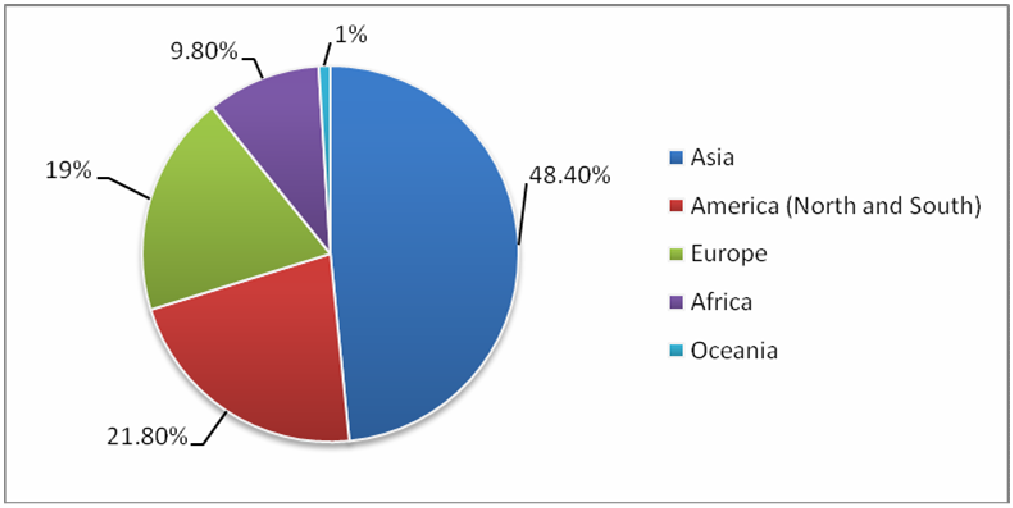


Figure 14 - Internet users in July 2013 by Continent
Source: Internet Live Stats, 2013

Offenses against mobile devices are increasing: targeting smartphones, tablets and the customers who use them; the crimes perpetrated through social media on which many companies have a public profile; attacks through Internet banking services; attacks on corporations by hacktivists who exploit the enormous audience that the web provides for their demonstrative acts around the world. The exponential growth of data that is made available on the Internet will increase alongside the ability and knowledge of cyber attackers with the aim of stealing the new currency of the Internet: information.

According to The 2013 Cost of Cybercrime Study, carried out by the Ponemon Institute, the cost of cybercrime has increased by 78% compared to four years ago. Also worrisome is the data concerning the amount of time required to solve a problem - which increased by 130% over the

[74] Internet users in the world, available at <http://www.Internetlivestats.com/Internet-users/> (retrieved 6-11-2014).

same period. Data theft is attributable to major losses of 43% of total costs, while damage to the business and the loss of competitiveness account for 36%.

Also, according to research by the Ponemon Institute[75], last year the average total cost for data breaches worldwide increased by 15% to 3.5 million dollars; and for each record the percentage has increased by more than 9% from $136 to $145. The importance of this finding is that the data is not hypothetical but rather actual estimates provided directly by the companies involved in the study[76] who suffered such damage and who recorded losses from 2,415 to just over 100,000 compromised records. The highest average cost paid for this violation was $201 for a single record for US companies and $195 per record in Germany. In Germany and France the report also shows greater investment in the activities of detection and evaluation with respect to data breaches, with budgets of 1.3 million dollars and 1.1 million dollars, respectively.

At a global level, cybercrime is becoming increasingly serious issue for businesses, citizens and governments, and they are beginning to develop strategies to combat it.

In Australia in 2012, 5.4 million people were victims of computer crimes, with an estimated cost to the economy of 1.65 billion dollars. This required a significant response to security. The cyber threat was identified as one of the main risks in the country's national security strategy. In Canberra, in May 2014, a new Cyber Security Center (ACSC) that uses the expertise of the best IT security experts of the nation was established. The center will be the focus of efforts in the field of information security, and the government will increase the capacity of the nation's defense against cyber attacks. The ACSC includes the major operating units of the Australian Defence Intelligence and Security Organisation, the Department of Emergency Response Team Australia, the Australian Federal Police and the Australian Crime Commission all in one location. The center will analyze the nature and extent of cyber threats and will guide the government's response in the event of an incident. The work is done in close contact with the critical infrastructure sectors and enterprises of the country in order to protect networks and national systems, creating a kind of epistemic community in order to cope with such threats. The center also provides advice and support for the development of prevention strategies to counter cyber threats.

Another interesting example of how cybercrime can be dealt with is the cyber security strategy issued by Canada in October 2010. In addition to guidelines on security and protection systems within government and critical infrastructure, the Canadian strategy also involves an innovative aspect not evident in other nations. That being, that it supports the planning of actions to raise education and awareness of the Canadian population about cyber threats and the proper use of the web. The strategy involves collaboration with other governments and IT companies to ensure that IT systems vital to Canadian security, economic prosperity, and quality of life are protected.

---

[75] *2013 Cost of Cyber Crime Study: Global Report*, Ponemon Istitute, available at: <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf> (retrieved 6-11-2014).

[76] 1,690 individuals from 314 companies have participated, interviewed during a ten-month period, representing the following 10 countries: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, UAE and Saudi Arabia.

Increasingly, governments are investing in preventative measures within the IT field through the implementation of policies for combating cybercrime, an issue considered a danger to national economies. Indian defense officials have said that India is preparing to face an escalation of attacks and that is why in 2012 they developed a plan to recruit up to 500,000 cyber specialists over the ensuing 5-year period[77]. India has also signed a non-binding protocol with the United States for technical and operational cooperation in the face of cyber threats[78].

The United States is confirmed as one of the nations most affected by cybercrime. In the last ten years, Americans' awareness about the importance of cyber threats coming from other nations, terrorist organizations, criminals and other entities has grown, leading to the formulation of one of the first strategies in the IT field. In May 2011 the White House presented its international strategy for cyber space, and in November 2011, according to the National Defense Authorization Act, the Defense Department reported that the US has the right to respond to any "significant cyber attacks directed against the US economy, the government or the military" with military force. According to unofficial estimates, organized transnational cybercrime amounts to 12 billion dollars a year, with direct and indirect damage to the amount of almost 400 billion dollars. Added to this is about a trillion dollars a year - the result of industrial espionage (private and government) and misappropriation of intellectual property and sensitive data. Within this context, in 2012, the US government created CyberCity - a real training camp for technicians. It is a virtual environment where 15,000 people live, engaging in their normal social behavior, and contains all services such as banks, hospitals, power stations, bars, restaurants, universities, SMEs, and Wi-Fi zones, etc. CyberCity has a special feature: it is constantly under attack and therefore defended by hacker-soldiers.[79] President Obama said that "*the cyber threat is one of the most serious challenges to national and economic security that we face as a nation*" and that "*the economic prosperity of the United States in the twenty-first Century will depend on cyber security*."

Recently in the city of New York, which in 2013 saw a sharp increase in data breaches that mainly affected business and commercial activities, a collaborative relationship was developed between the FBI, New York Police Department (NYPD) and the Metropolitan Transportation Authority (MTA) to respond specifically to financial crimes committed through the use of new technology. Working also with foreign federal agencies, this new task force will focus on financial crimes in the New York area - theft of credit cards, fraud, and attacks on payment systems and trading platforms. While crimes of a financial nature are the most common, they are also those with the greatest impact on the economy of a country. The IT security departments of private companies will work with the newly formed task force to share information about cyber incidents. This collaboration between local, federal and international agencies is needed to tackle cyber crime, which has the particular characteristics of having no boundaries or territoriality. In 2013,

---

[77] *India training half a million cyber security experts*, available at: <http://www.timeslive.co.za/scitech/2012/10/16/india-training-half-a-million-cyber-security-experts> (retrieved 6-11-2014).

[78] *India to greenlight state-sponsored cyber attacks. Gov agencies will get the nod,* by Phil Muncaster, available at: <http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/> (retrieved 6-11-2014).

[79] To understand the best strategies for IT security, it is necessary to enter into the mindset of the attacker, to be able to predict and thwart his moves. Psychological and sociological aspects become essential.

the Internet Crime Complaint Center (IC3) produced 262,000 complaints, representing more than 781 million dollars in losses.[80]

According to a McAfee survey, out of 1,000 companies, nearly 90% of SMEs in the United States do not use data protection for information about customers and partners, and less than half protect corporate emails to avoid scams such as phishing. The International Center for Strategic Studies in Washington estimated that cybercrime and cyber espionage cost the US economy 100 billion dollars a year, and the global economy about 300 billion dollars. SMEs are still unaware of the threat. In fact, two-thirds believe their data and devices are safe from hacker attacks, and only 9% protect their employees' smartphones.

In the last few years several countries have begun to develop IT security policies, including support for innovative SMEs directly involved in this sector. France, the US and the UK promote opportunities for SMEs dealing with innovative IT products and allow them to have an active role in making cyber space a safer place.

As mentioned above, it is necessary to point out that at present most of the reports that provide data and statistics on cyber crime are drawn from IT companies; however, it is not very often that statistics are compiled from official and national sources. This would be useful not only to understand the real impact of this phenomenon on the economy at the national level, but also to create international databases that measure, according to their national legislation, local, regional, national, and international cybercrime - in order to organize law enforcement efforts. Aggregate global data often contributes to a lower perception of cybercrime at the local level. Individual citizens and SMEs, with no official figures of how widespread cybercrime is in their localized area, may run the risk of underestimating the real danger and interpret global data as relating only to the world of big multinational companies or confined to countries such as the United States, or simply feel it is distant from their daily lives. It would also be useful to have official estimates and data at the national level from each individual State in order to compare global trends.

2.2 Cybercrime as a threat within Europe

In Europe, the situation is certainly not any better. According to estimates by Interpol, cybercrime is a 750 billion[81] euro a year business[82].

[80] *2013 Internet Crime Report*, IC3, available at: <https://www.ic3.gov/media/annualreport/2013_ic3report.pdf> (retrieved 6-11-2014).

[81] *Opening Remarks by INTERPOL PRESIDENT KHOO BOON HUI.* At the 41ST EUROPEAN REGIONAL CONFERENCE (ISRAEL, TEL AVIV, 8 MAY 2012), available at: <http://www.interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (retrieved 10-11-2014).

[82] At the end of 2012 a group of cyber criminals launched malware that, by restricting access to the infected computers, earned about 1 million euro for each attack.

At the European level, recent Eurobarometer research[83] confirms that European citizens consider information security as a subject of enormous concern. The data reveals that 89% of respondents claim to be concerned about the security of their personal information accessible online, and 74% think that the risk of being a victim of cyber crime has increased over the previous year. The most interesting data in the report indicates that 10% of European users surveyed are certain to have suffered online fraud, and 6% have been the victim of identity theft.

The possibility of becoming a victim of an Internet crime is a fear that is beginning to take hold, but even this does not diminish the level of ease with which many users share their personal information online, regardless of prevention or security measures - thus allowing cyber criminals to have easy access to a considerable amount of personal data. In addition, 50% of the sample admitted that they had not changed passwords for online services in the last year, and 52% are either not well informed or misinformed about cybercrime. 12% experienced a block of access to the Internet, and another 12% had their social network accounts hacked, while 7% had suffered the theft of credit card information.

Only half of Europeans put in place acceptable protective measures to tackle this type of crime.

In the UK in 2013, 93% of large companies and 76%[84] of SMEs reported a cyber attack[85] with costs ranging from 110,000 to 250,000 pounds for large companies and between 15,000 and 30,000 pounds per SME.[86] It is believed that the estimates may actually be much higher since the incidents of fraud reported are less than those that have actually occurred because one does not always realize that a fraud has taken place (and therefore it might not be reported).

The English Federation of Small Businesses (FSB) has published an interesting study on the costs of cyber crime as suffered by SMEs in the UK and has revealed an increase in the phenomenon[87]. In addition, approximately 30% of its members have been victims of fraud, over 50% of UK SMEs have been hit by malware, 8% were the victim of hacking, and about 5% had suffered a security breach. To address this issue, the English Action Fraud Center has developed a section on its website dedicated to raising awareness about the problem and provide information about prevention against attacks and data protection for SMEs concerning the weak points of companies such as customers, suppliers, employees and assets. Within the site there is a section for online reporting of attempted fraud attempts.[88] The report, which highlights how to protect

---

[83] Cyber Security Report Special Eurobarometer 404, available at: <ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf> (retrieved 6-11-2014).

[84] 87% according to the McAfee 2014 Report.

[85] *2013 Information security breaches survey Technical Report*, available at: <https://www.pwc.co.uk/*asset*s/pdf/cyber-security-2013-technical-report.pdf> (retrieved 6-11-2014).

[86] The costs of the worst security breaches can range anywhere from 35,000 to 65,000 pounds for SMEs, and from 450,000 to 850,000 pounds for the largest companies. For more details, see: *SMEs face increased risk of cyber attack***,** available at: **<**http://www.prweb.com/releases/2014/09/prweb12147240.htm> (retrieved 6-11-2014).

[87] *Cost of cybercrime for UK Small Businesses*, by Pierluigi Paganini in Security Affairs, available at: <http://securityaffairs.co/wordpress/14628/cyber-crime/cost-of-cybercrime-for-uk-small-businesses.html> (retrieved 6-11-2014).

[88] *ActionFraud is the UK's national fraud and Internet crime reporting center*, available at: <http://www.actionfraud.police.uk/> (retrieved 6-11-2014).

SMEs from cybercrime, serves as a strategic document for defending large corporations as well ,and therefore the country's economy.

According to the estimate of the FSB, which projects data relating to small businesses nationwide, the cost of cybercrime is more than 18.8 billion pounds.

In the UK there are around 4.8 million SMEs and despite the impact of cybercrime and the high frequency of damaging events, nearly 20% had not taken any countermeasures to mitigate threats[89]. Cyber security, for the British government, is a very important topic for the growth of the UK. Minister James Brokenshire[90] said the results suggested by the study is what stimulated action and a proactive approach to cybercrime is being adopted. The British government has also enacted the Data Protection Bill, which will force companies to report all cyber incidents and violations suffered. The strong support of the government and of major businesses is essential to support the growth of a security culture that could help reduce the effects of cybercrime.

Another interesting initiative of the British government relates to a new partnership with companies to share information on cyber threats. The Cyber Security Information Sharing Partnership (CISP) involves the construction of an online platform through which you can exchange real-time information about threats and vulnerabilities.[91]

Germany has seen significant financial damage and loss of value creation and confidence arising from industrial espionage. A study by the Corporate Trust states that industrial espionage affects German Industries for an amount of about 4 trillion euro per year. The largest German telecommunication company, Deutsche Telekom, claims to suffer about 450,000 attacks per day and that number is increasing. Security of IT systems is a factor that undoubtedly slows the economic and social development of Germany.

A study by BITCOM, taking into consideration all German companies, says that in the year 2012 over 39% of companies were the victims of a cyber attack such as data theft, violation of patents and intellectual property, espionage, fraud, wiretapping, and damage to systems.[92]

The severity of the situation is confirmed by the data about German SMEs, 96% of which have experienced cyber incidents and related damages.[93] Consequently, since 2009 the Federal Ministry of Education and Research (*Bundesministerium für Bildung und Forschung*) and the Federal Interior Ministry have been supporting research in the field of information and communications security, "IT Security Research," for the development of new technologies in this field.

---

[89] Recent research has found that only 12% of companies surveyed have invested in insurance against cyber threats.

[90] Minister of State for Security and Immigration.

[91] *Government launches information sharing partnership on cyber security*, available at: <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security> (retrieved 6-11-2014).

[92] The Federal Office of Criminal Police declared an increase in cybercrime of 3.4% in 2012, with a total of 87,871 cases. The offenses involving corruption of data and computer sabotage (+133.8%) are becoming an increasing hazard.

[93] *Cybersecurity research to boost Germany's competitiveness*, available at: <http://www.bmbf.de/en/73.php> (retrieved 6-11-2014).

SMEs primarily use basic security systems such as firewalls and antivirus software, which are often not enough to ensure an adequate level of protection. The project "SIEM *Mittelständische für Unternehmen und Klein*" (SIMU)[94] is therefore studying how to adapt more complex security systems and Security Information and Event Management (SIEM) used by large businesses to SMEs, which are often not economically accessible to small businesses.

Although the data provided in the various reports examined up to now give useful information on how cybercrime is evolving over time for citizens and companies (despite the difficulty in quantifying the magnitude and the damage that this phenomenon involves), it must be noted that for the most part these data are provided by private security companies, and there are no official estimates by the various governments and supranational entities that could give a more accurate and comparable international picture.

2.3 The activities of the European Union against cybercrime

With the publication of the "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber Space"[95] on February 7, 2013, the European Union acknowledges that cyber space is an increasingly important dimension at the international level and wants to start an intensification of its actions in this field by defining roles, responsibilities and required actions, based also on the protection and promotion of the rights of citizens. Making cyber space safer and combating digital illiteracy have become priorities that the EU can no longer afford to ignore. The European Union has structured its system of governance based on three structures.

The first structure, founded in 2005, is the European Network and Information Security Agency (ENISA), which identifies causes and creates dialogue and awareness and provides information and best practices to EU Member States.

The second structure covers the issue of protection against cyber threats through the establishment of the European Center on Cybercrime (EC3)[96], of which more will be discussed later on.

In the third structure, launched in 2010 in conjunction with the Digital Agenda for Europe[97], the European Union has adopted a series of laws and initiatives that promote the development of

[94] Part of the program "Innovative SMEs" of the BMBF.

[95] European Commission *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* 7/2/2013, available at: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> (retrieved 6-11-2014).

[96] The European Commission decided to establish a European Cybercrime Center (EC3) at Europol. The Center will be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crime. "The EU Internal Security Strategy in Action", adopted on 22 November 2010, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF> (retrieved 6-11-2014).

[97] *Digital Agenda for Europe* is one of the initiatives of the Europe 2020 strategy, which defines the objectives of growth that the European Union aims to achieve by 2020. The Digital Agenda aims to exploit information and

social and economic opportunities in the digital world, such as the protection of intellectual property, the development of broadband coverage, e-commerce, and electronic signature. Even the European Parliament, assisted by the European Data Protection Supervisor, is a key player in the governance of information security of the EU in order to balance the three structures.

As mentioned, the first of the three structures around which the European Union has organized its system of governance is ENISA, established in March 2004.

Acting within the European Union, ENISA promotes the development of a security culture for citizens, businesses and public organizations, helping the European Commission, Member States and IT companies to avoid and deal with information and network security problems. The agency's objective is for its website to constitute a European "hub" for the exchange of information, best practices and knowledge in the field of information security. Since 2007, ENISA has also been in charge of promoting the development of security policies targeted at SMEs, given their considerable importance in the European economy.[98] In 2009, the European Union established that ENISA Member States should annually report on incidents involving the electronic communications sector.

The European Commission has invited ENISA to conduct a feasibility study on a system of sharing at the European level in order to raise awareness of IT security and to fill gaps in the coverage of such information, especially for citizens and SMEs. In its recent report, *Annual Incident Reports 2013: Analysis of Article 13a*[99]*,* which contains data on significant incidents relevant to the communications sector and reported in accordance with Article 13a of the Framework Directive (2009/140/EC)[100] by the national regulatory authorities (NRAs) of the different EU Member States, ENISA makes a pooled analysis of incidents that resulted in serious disruption of services across Europe.[101]

Another particularly relevant political initiative of the European Commission is represented by the communication on the protection of critical information infrastructure[102] that emphasizes how critical information infrastructures are vital for the economic and social growth of the

---

communication technologies (ICT) to stimulate innovation, economic growth and progress, available at: <http://ec.europa.eu/digital-agenda/digital-agenda-europe> (retrieved 6-11-2014).

[98] *ENISA Deliverable: Information Package for SMEs*, available at: <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/information-package-for-smes/at_download/fullReport> (retrieved 6-11-2014).

[99] *Annual Incident Reports 2013 Analysis of Article 13a annual incident reports September 2014*, available at: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport> (retrieved 6-11-2014).

[100] The reform of the EU regulatory framework for electronic communications, which was adopted in 2009 and was implemented by most countries in the EU in May 2011, adds article 13a of the Framework Directive. Article 13a concerns the security and integrity of public electronic communications networks and services.

[101] This year, 19 countries have reported 90 accidents, while 9 countries have reported no significant incidents.

[102] European Commission, *Protecting the Critical Information Infrastructures. "Reinforcing preparedness, security and resilience to protect Europe from cyber attacks and disruptions"* COM (2009) 149, 30 March 2009, available at: <http://europa.eu/legislation_summaries/information_society/Internet/si0010_en.htm> (retrieved 20-11-2014).

European Union and establishes a plan of action to strengthen security and resilience, and which has contributed to increasing the role of ENISA at the tactical and operational level within Europe.

The European Information Sharing and Alert System (EISAS) seeks to improve the cooperation of the Member States to reach citizens and SMEs through collection, processing and dissemination of relevant security information.[103] It aims to empower European citizens and SMEs by developing the required knowledge and skills to protect themselves from cyber threats, and to implement the capabilities of Member States through cooperation between national CERTs.[104] The 2012 project involved a sample of more than 1,500 people made up of citizens and SMEs across Europe and highlighted data regarding very low awareness about the main vectors of attacks and the preferred contact in case of difficulties: friends and family rather than IT professionals.

ENISA also organizes and coordinates Europe-wide exercises to test the ability of Member States in response to a digital attack.[105] On October 4, 2012 a simulation of a cyber attack was carried out on a European scale and for the first time saw the participation of Banks and IT companies[106]. Four hundred specialists in the private and public sectors faced 1,200 cyber incidents in order to assess the response and cooperation, as if a true joint attack on public websites and major European Banks was taking place. In August 2013, ENISA published a report of the results of the exercise, concluding that the lack of transparency and information on incidents made it difficult to understand the overall impact, causes, and possible security legislation interdependencies. This type of exercise is carried out every two years.

This year, the largest European exercise ever conducted took place. The exercise, called Cyber Europe 2014[107] and coordinated by the European Network and Information Security Agency, was attended by more than 200 organizations from 29 European countries, 26 EU Member States and three from the European Free Trade Association (EFTA), with the ultimate aim being to test the abilities of individual countries in countering cyber threats and cooperating at the national and international level across public and private sectors. The simulation contained more than 2,000 different cyber security incidents including DDoS attacks, defacement, publication of sensitive

---

[103] *EISAS - European Information Sharing and Alert System, A Feasibility Study 2006/2007*, available at: <http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf> (retrieved 6-11-2014).

[104] *EISAS Basic Toolset 1.0 Feasibility Study of Home Users' IT Security*, available at: <http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas-basic-toolset/at_download/fullReport> (retrieved 6-11-2014).

[105] European Commission Vice-President, Neelie Kroes declared, on the occasion of the recent exercise: "The sophistication and volume of cyber-attacks are increasing every day. They cannot be countered if individual states work alone or just a handful of them act together. I'm pleased that EU and EFTA Member States are working with the EU institutions with ENISA bringing them together. Only this kind of common effort will help keep today's economy and society protected.", available at: <http://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today> (retrieved 6-11-2014).

[106] *Europe tests cyber security capabilities in simulation* by Andrew Wagaman, available at: <http://www.neurope.eu/article/europe-tests-cyber-security-capabilities-simulation-today> (retrieved 6-11-2014).

[107] *Biggest ever cyber security exercise in Europe today*, ENISA, available <http://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today> (retrieved 6-11-2014).

information and attacks on critical infrastructure, such as energy and telecommunications.[108] This exercise also saw the collaboration of more than 400 experts from the public and private sectors, such as cyber security agencies, CERTs, Ministries, telecom operators, companies in the energy sector, financial institutions, and Internet service providers, and among other issues, cooperation at the European level and escalation procedures were tested[109]. The results of this exercise will be published in the coming months through a report drafted by ENISA.

Also a part of the critical security infrastructure is the communication on "critical information infrastructure protection"[110] which reaffirmed the central role of ENISA regarding the protection of CI and called on Member States to implement their own national CERTs.

At the end of 2012, the Computer Emergency Response Team (CERT-EU)[111] was established within the European institutions in order to meet the growing number of cyber threats and to support the work of the national CERTs whose institution is strongly supported and recommended by European Digital Agenda. The team consists of IT security experts from the main EU institutions (European Commission, Council Secretariat, European Parliament, and Regional and Social committees) and collaborates with other CERTs in Member States and with IT security companies. It operates under the strategic supervision of an inter-institutional steering committee[112]. There is still a lot to do because at the European level we have encountered considerable difficulties in the implementation of effective operational national CERTs, and this is a gap that needs to be filled.

The European Union does not have a single approach to IT security. In general, the responsibilities of internal security remain the prerogative of individual national governments. But the presence of different regulations, which are in some cases are altogether different from one nation to another, makes the implementation of a European coordinated protection system complex[113]. Different organizations and directives responsible for filling this gap manage IT security at the EU level.

Under the second structure, the European Commission established a European Cyber Crime Center (EC3) at Europol in January 2013. The center is responsible for sharing information,

---

[108] Italy has participated in this simulation with 10 organizations of the public and private sectors, for a total of about 50 technical experts in the field of IT security.

[109] European Standard Operating Procedures (EU-SOPs), a set of standard tools that includes the list of National Contact Points, operational templates, workflows, best practices, and guides on how to manage major cyber incidents.

[110] European Commission, *on critical information infrastructure protection "Achievements and next steps: towards global cyber-security"* COM (2011) 163, 31 March 2011, available at: <http://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-163-EN-F1-1.Pdf> (retrieved 20-11-2014).

[111] CERT-EU About us, available at: <http://cert.europa.eu/cert/plainedition/en/cert_about.html> (retrieved 6-11-2014).

[112] Press release, European Commission, 12 September 2012, *Cyber security strengthened at EU institutions following successful pilot scheme*, available at: <http://europa.eu/rapid/press-release_IP-12-949_en.htm> (retrieved 6-11-2014).

[113] *The European Cyber security Strategy: Too Big to Fail?,* by Neil Robinson, available at: <http://www.rand.org/blog/2013/02/the-european-cyber-security-strategy-too-big-to-fail.html> (retrieved 6-11-2014).

awareness and assistance in the investigation of cyber crimes and is designed to be the reference point in the fight against cybercrime in the European Union and to speed up the response in cases of online crimes. The EC3 has the task of addressing the following areas of cybercrime:

- Crimes committed by organized groups capable of generating large criminal profits from offences such as online fraud;
- Cyber crimes that cause serious damage to victims such as the sexual exploitation of minors;
- Attacks against critical infrastructure and information systems in Europe.

The EC3 can rely on the existing infrastructure of Europol, but has a staff that is too small for the tasks assigned to it - such as to support Member States and the European Union in the development of operational capabilities and analysis for the investigation of cybercrime.

From September of this year, the Joint Action Cybercrime Taskforce (J-CAT), a European task force against cybercrime, has been in operation. It is based at the EC3 and acts in coordination with other international organizations. The task force, which is led by Andy Archibald, Deputy Director of the National Cybercrime Unit of the National Crime Agency of the United Kingdom (NCA), is composed of experts and liaison officers of Police of EU Member States and other countries. To date, this task force is composed of Austria, Canada, Germany, France, Italy, the Netherlands, Spain, the United Kingdom, and Ireland. The United States, Australia and Colombia are also involved in this initiative. The objective of this new structure is not only strategic, but also operational, with the aim of fighting online crime more effectively by involving the police forces of the different EU countries in order to coordinate investigations and cooperate in the face of cybercrime.

As for law enforcement agencies, Interpol and Europol have an important role in coordinating and sharing information regarding this type of crime due to its strong transnational character. Interpol is the largest international police organization in the world and is made up of 190 Member States. It has the task of ensuring that police forces worldwide have access to the services and tools needed to carry out their work efficiently. They also conduct training projects, including those in cyber space. Founded in 1923 in Vienna as the International Criminal Police Commission, they have a central office in every Member State of the organization. Interpol works with local crime fighting organizations that are dedicated to international crime prevention. Interpol doesn't have its own operatives; it is purely coordinative.

Since 1999, Europol has been in charge of the fight against crime throughout the European Union. The main purpose of this agency is to facilitate the exchange of information among the police forces of Member States by collecting and analyzing data and communicating news and reporting crimes to the competent bodies of each European State, with the aim of facilitating and speeding up the investigation. The role of Europol is extremely important in the fight against cyber crime, as this type of crime is of a transnational nature. In 2014, Europol issued a public version of its Internet Organized Crime Threat Assessment (iOCTA)[114], the purpose of which is to provide an

[114] *Threat Assessment on Internet Facilitated Oranized Crime* (iOCTA) 2014, available at: <https://www.Europol.europa.eu/sites/default/files/publications/Europol_iocta_web.pdf> (retrieved 6-11-2014).

analysis of the impact of cybercrime in the EU and provide predictions about future risks and emerging threats.

Founded in 2001 and established as an agency of the European Union in 2005[115], the European Police College (CEPOL)[116] also supports and promotes a cooperative approach among European countries to combat major transnational crimes. It brings together senior officials of law enforcement agencies from throughout the whole of Europe. Every year Member States organize courses, seminars, conferences, and meetings, which cover many relevant issues to current law enforcement activities in Europe, including cybercrime.

In 2007, the European Cyber-crime Training and Education Group (ECTEG) was established. Its members come from EU Member States, law enforcement agencies, international organizations, universities and private industries. It coordinates training on cybercrime; discusses international activities; shares knowledge, expertise and solutions to specific problems; standardizes methods and procedures for training; and collaborates with universities and IT partners in order to extend the knowledge of this phenomenon outside national borders.

Eurojust coordinates European judicial cooperation. The unit, established in 2002[117], assists the competent authorities of the Member States when faced with international organized crime groups - enhancing the efficiency of national authorities. The staff of Eurojust is composed of approximately 200 people and comprises a designated representative prosecutor, judge or police officer with equivalent competence - for all Member States. Cybercrime is one of the main topics of the meetings, which are held periodically throughout the year and involve the judicial and investigative authorities of Member States.

In 2010, the European Union Cyber-crime task force (EUCTF) was also appointed and is composed of a group of expert representatives from Europol, Eurojust and the European Commission, in collaboration with the heads of the cybercrime units of the European Union for the fight against international cybercrime. It provides assistance for the promotion of a harmonized EU approach to the fight against cybercrime.

The third and balancing structure, presented in May 2010 by the European Commission and the Digital Agenda, and managed by DG Connect[118], contains 101 actions grouped around seven priority areas with the aim of improving Europe's ability to prevent, detect and respond to problems in IT technology. The aim of DG Connect is to strengthen the resilience of critical infrastructure, improve preparedness, and promote a culture of cyber security through the centralization of information and the creation of partnerships between the public and private sectors based on a common approach and international perspective. Its task is to ensure that digital technologies can help achieve the growth that the EU needs.[119] Among Digital Agenda's

[115] Decision 2005/681/GAI of the Council, 20 September 2005.

[116] Comes from the French "*Collège Européen de Police*".

[117] Decision 2002/187/GAI of the Council, modified with decision 2009/426/GAI of the Council, 16 December 2008.

[118] European Commission Directorate General for Communications Networks, Content & Technology.

[119] For more details, see: <http://ec.europa.eu/dgs/connect/en/content/mission-and-priorities> (retrieved 6-11-2014).

foundational pillars is IT security, because it is considered one of the fundamental requirements in the spread of new technology and the Internet as a development tool and is therefore a means by which to increase the competitiveness of European companies. For the web to be added value for enterprises, it is necessary that their approach to the digital world is one of trust. To act with the fear of the risk of suffering serious harm would create a brake on all the many opportunities the world wide web has to offer, and in turn the economy.

Moreover, it is important to continue to apply the rules of the physical world where it is common and normal practice to inquire about the reliability of a work partner (be it a customer or a supplier) or the security of a place before you visit - especially if it is unknown. These basic rules, obvious when talking about the physical world, must be applied with even greater care when it comes to the virtual world, with it being so vast, inaccessible, dangerous, and ever-changing.[120]

The European Digital Agenda plays a strategic role as it is estimated that its full implementation would increase the European GDP by 5% over the next eight years, leading in turn to an increase in investment for innovation in technology that would improve the conditions for development of all sectors, both public and private, including the job market. The risk is that without a common European framework, up to 900,000 jobs could be lost by 2020. On the other hand, with the construction of new digital infrastructure via a long-term project, 3.8 million jobs across Europe would be created.

The European Digital Agenda includes two types of actions: those in the charge of the European Commission, including legislation concerning strategies and guidelines; and those in the charge of the individual Member States, which have the task of applying concrete European level regulation.

In recent years The European Commission has been working hard to achieve the goal of effective data protection, reconciling the need for privacy with the benefits of a global "*open, innovative, unified*" network. In February 2013, the Commission presented the first European Cyberstrategy[121], which focuses on cybercrime, with the aim of implementing a defensive plan against IT tools at the community level. The report stresses the importance of increasing the resilience of networks and systems, intensifying the fight against cybercrime through the legislation already in force, strengthening of the tools to combat the phenomenon and promoting cyber security policy between Member States and in the international sphere - for an "*open, safe and secure*" cyber space. The document urges states to develop national strategic plans aimed at tackling an array of cyber threats and stressed that the responsibility for the security of cyber space is shared between all players in the global information society: individuals, companies, and the states.

International cooperation within and at the EU level, along with cooperation from international organizations, the private sector and citizens is essential in developing a secure

[120] "*People - including me - sometimes about talk about our "digital rights". But I don't think that's quite right. These are not digital rights, nor online rights: they are fundamental rights, and they apply just as much online as off. Whether it is privacy, or freedom of speech, or consumer protection. New technology can enhance our humanity: it should not override our human rights*". Neelie Kroes, *A secure online network for Europe Cyber security conference*, Brussels 28 February 2014, available at: <http://europa.eu/rapid/press-release_SPEECH-14-167_en.htm> (retrieved 6-11-2014).

[121] Drafted by the High Representative Catherine Ashton and the European Commission.

environment in cyberspace. Eithin this framework, the establishment of a public-private NIS platform is required, with participation of SMEs encouraged.[122]

Among the most important goals are the adoption of a common legal framework, the strengthening of cooperation between the agencies responsible for combating cybercrime, incentives for the creation of public-private partnerships through training, and supporting the implementation of national CERTs. Also important is the promotion of international cooperation beyond European borders, urging Member States to ratify the Convention on cybercrime known as the Budapest Convention[123], which after four years in development entered into force on July 1, 2004 and is the first international treaty on crimes committed via the Internet and other computer networks. With the aim of building a common criminal policy to combat cybercrime and promote international cooperation, it addresses the issues of infringement of copyright, computer fraud, child pornography and network security and provides for heavier sanctions, increased corporate accountability, and the provision of greater protection of personal data. It is also lays out the appropriate procedures such as searching computer systems, the interception of data, and the authorization of police forces to ask the Internet provider to freeze telematics data for six months.

The convention covers three areas: the definition of the field of application of the procedural measures provided for (Art. 14); the provision of measures for the acquisition of computer data (Art. 19, 20 and 21), and the provision of measures of constraint to obtain such data by third parties (Art. 16, 17 and 18). An important issue is that the scope of the convention includes not only purely technical crimes, but also traditional crimes achieved through technological means and crimes that can be proved by electronic evidence.

The importance of international cooperation in the fight against this type of phenomenon is also the subject of the Additional Protocol to the Convention on Cybercrime concerning the acts of racist and xenophobic nature committed through computer systems, published in January 2003[124].

The priorities of the European cyber Strategy are: to develop a level of IT resilience, to reduce cybercrime, to develop industrial and technological resources, to develop a coherent policy to counter threats by promoting the values of the EU, and above all to establish the minimum common requirements for National Information Security at national level in order to force the Member States to adopt a cyber security strategy. The strategy is also designed to designate competent national authorities on the subject, to establish a reliable operation of CERTs, and to push for real international cooperation. The Commission constantly encourages a high level of NIS throughout the European Union by adopting practices of risk management and information sharing on network security and addressing national capacities. The document stresses the need for all European countries to adopt an efficient cyber security system - considering the fact that weak links make the whole European system fragile. Each State must establish strong and

[122] NIS Platform, available at: <https://resilience.enisa.europa.eu/nis-platform> (retrieved 20-11-2014).

[123] *Convention on Cybercrime,* Budapest, 23.XI.2001, available at: <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm> (retrieved 6-11-2014).

[124] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, entered into force on 1 March 2006, available at: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&CM=8&NT=189> (retrieved 6-11-2014).

effective legislation that addresses cybercrime. Inside the European Cyber Security Strategy, the European Commission asks for the development of a national contingency plan and the realization of periodic exercises designed to test the response to large-scale network security incidents and subsequent disaster recovery.

Also presented alongside the European Cyber Strategy was a proposal for a directive on the security of networks and information that imposes obligations on Member States in relation to prevention, management and response to risks and incidents. This proposed directive would create a mechanism for collaboration between Member States and also establish security requirements for market operators and public authorities.[125]

The EU's vision can only be realized through a genuine partnership between the various stakeholders. In order to face future challenges, Member States cannot wait any longer and must define their national strategies, define their roles and responsibilities, and identify the various national dedicated bodies. The strategy should not be just a façade, but be real and efficient.

The European Cyber Strategy is essentially based on three structures, as shown in the graph below, which must be a cooperative project both at the European and national level. Given the complexity of cybercrime and the multitude of players involved, an effective response at the national level, combined with strong European involvement, is necessary as a first step.

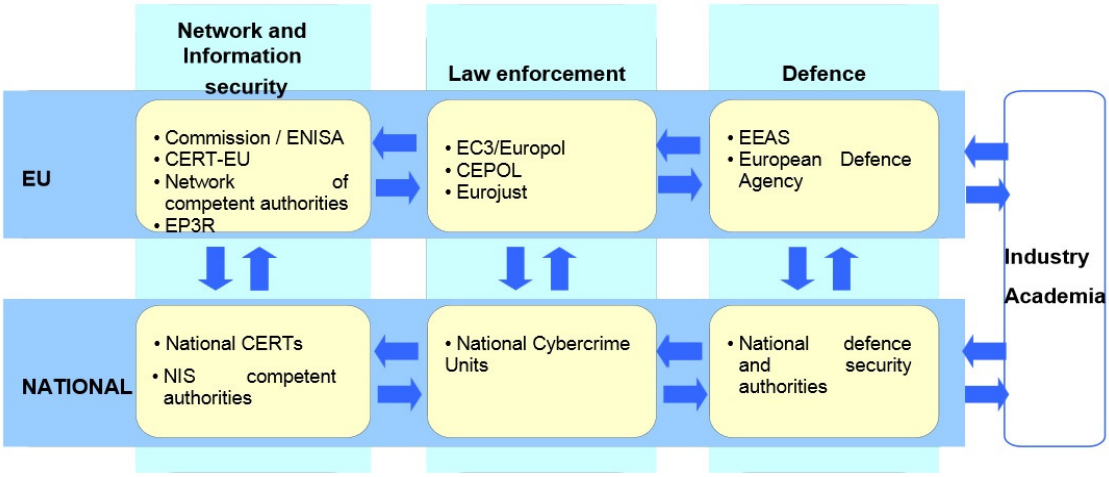


Figure 15 - Coordination of skills and distribution between the different players
Source: Cybersecurity strategy of the European Union, 2013

At the European level, the implementation of the cybercrime strategy is limited by the delays associated with the ways in which Member State adopt European directives and the differences between these policies - all of which make it difficult to achieve set goals, despite the EU's commitment to the fight against cybercrime.

[125] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security in the Union, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF> (retrieved 20-11-2014).

Further EU engagement in the fight against cybercrime is considered by Directive 2013/40[126] of 12 August 2013, which addresses attacks against information systems. It was adopted under Article 83 of the Lisbon Treaty on the Functioning of the European Union and should be transposed by 4 September 2015. It aims to unify the criminal offenses and penalties for this type of crime, and requires States to at least impose the minimum limit of the maximum sentence when cybercrime offenses involve multiple countries.

The Commission has also included cyber security and issues concerning privacy and the trust of citizens and European companies within the Horizon 2020 program[127]. The program has defined a public platform, called "NIS" platform (Network and Information Security), which aims to identify best practices for cyber security and promote and encourage new ICT solutions to improve security and risk management in information technology. Approved on 13 March 2014 by the European Parliament, the Directive on Cyber security provides for the compulsory notification of attempts to breach the systems of companies that own, manage or provide technology for critical infrastructure, but does not include providers of global services. The importance of SMEs in the European economic system requires their inclusion in the disclosure requirement system since they constitute the majority of enterprises in Europe.

The European Digital Agenda bases its actions on defining rules and setting up instruments and support platforms but does not implement actions for the measurement and evaluation of the actions taken. They also do not delegate this task to the Members States, which, for their part, are significantly late in the implementation of the suggested actions. With the exception of Action 39 concerning the implementation of simulated cyber attacks, many important actions have not yet been implemented by Member States. For example, Action 38, concerning the creation of the Computer Emergency Response Team (CERT) in every Member State, which was originally scheduled for 2012, is still in the late stage of implementation in a number of countries, including Italy. As many as 12 countries are at fault in regard to Action 40, concerning the implementation of danger alert hotlines for some of society's the most vulnerable groups, such as children (scheduled for 2013). Italy and 15 other European countries have not yet implemented Action 41, which deals with the creation of national alert platforms, planned for 2012[128].

The delays in the advancement of the agreed actions established by Digital Agenda reflects the tendency of many European countries to remain bound to a national approach to policy, and to be slow in implementing the agreed actions made at the EU level. This means a delay in the unification of policies to fight cybercrime. There are also disparities in the evaluations of the responses of the different countries because these are made by the countries themselves, revealing differences in benchmarks, thereby preventing an exact comparison between states.

---

[126] *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040> (retrieved 6-11-2014).

[127] Activities "Innovation in SMEs" is a bridge between the main activities of Horizon 2020 (research support, development and innovation projects) and the creation of an environment for growth and innovation of SMEs.

[128] *Sicurezza delle reti in Europa: il punto sui ritardi* by Nello Iacono, available at: <http://www.agendadigitale.eu/infrastrutture/718_sicurezza-delle-reti-in-europa-il-punto-sui-ritardi.htm> (retrieved 6-11-2014).

With this in mind, the approval of the European Directive that governs Member States and planned joint actions is certainly a useful tool for combating cybercrime.

The most important feature, however, is its operations because network and system security in Europe is closely linked to the adoption of all approved directives and the fulfillment of all requirements by each Member State as established by the European Commission.

Statements made by the European Commissioner for Digital Agenda, Neelie Kroes, confirm the need for a strong and truly binding directive that decisively involves all Member States in order to not hinder the efforts made so far and to not to endanger the digital future of Europe. The result of the European Digital Agenda depends very much on the willingness of Member States to create an efficient network that deals with security. The importance of these issues at European level is also confirmed by the presence of a new Vice President and Commissioner for the Digital Market, and a new Commissioner.

It is also important to consider that a further obstacle in the realization of an effective common European defense strategy in the cyber field is the differences among the individual Member States in terms of infrastructure, legal frameworks and defense. At the infrastructure level, the digital divide between countries of the Union, and in some cases even within the countries themselves and the consequent networks and information security, makes it difficult to achieve an adequate level of defense. Regarding the law, Member States do not have a common approach to certain types of IT crimes and also have completely different, independent and sometimes conflicting legal frameworks. This situation does not allow easy unification of the suitable legal measures required to reach a community response to cybercrime.

CHAPTER 3

THE IMPACT OF CYBERCRIME IN ITALY AND RELATED COUNTERMEASURES

3.1 The current state of SMEs in Italy

As illustrated within the first chapter, 99.9% of the Italian economic landscape is composed of small and medium sized enterprises. Microenterprises (enterprises with less than ten workers) account for 95% of the Italian total and have a weight of 81% in terms of employment. In its latest annual report[129], the SME Envoy stated that in 2013 the balance between the number of SMEs founded and those that ceased their activities was the worst in recent years and reached the greatest number of failed enterprises in the last decade (more than 10,000). However, the SME Envoy did highlight that even in the current crisis there are examples of positive performance, such as in the case of networking between small enterprises belonging to industries driven by medium size enterprises, specifically those of which opted for export, technology[130] and the production of high luxury goods - all traits of "Made in Italy." Some of the trends highlighted by the SME Envoy as positive future trends include an increase in the use of digital technology within the artisan sector - among companies that were able to fuse tradition with innovation, and the increase of innovative start ups - especially those founded by workshops sponsored by universities and companies. Medium sized enterprises, with a solid presence in the market and a greater level of internationalization[131], represent a great opportunity for suppliers within the industry and a push towards recovery. In reference to this, e-commerce is a useful tool for widening the pool of potential clients and aid in the exporting efforts of those micro and small enterprises that suffer from a low level of digitalization. Their presence on foreign markets can be an opportunity for those specialized Italian SMEs belonging to the manufacturing sector and represent the cream of the crop of the Italian economy ("Made in Italy"). According to the Garante data, Italy is among the top five exporting nations for 25% of the 5,500 products that make up the world's commerce. Also important is that within those 5,500 products Italy is the major exporter for 235 of them.[132]

---

[129] Relazione al *Presidente del Consiglio* articolo 17, comma 1, legge 11-11-2011 n. 180 *"Norme per la tutela della libertà d'impresa. Statuto delle Imprese"*, Rome, 06.02.2014, available at: <http://www.governo.it/backoffice/allegati/75045-9261.pdf> (retrieved 7-11-2014).

[130] Primarily mechanical and pharmaceutical industry.

[131] In the report of the SME Envoy is specified also that the latest Unioncamere-Mediobanca data indicate that 90% of medium-sized Italian enterprises exports its products abroad.

[132] Bonifazi Alberto, Giannetti Anna (2014), *Finanziare l'impresa con i fondi europei Strumenti e opportunità 2014-2020. Redazione e presentazione delle domande. Simulazioni pratiche*, IPSOA.

The figures highlighted by the Guarantor in relation to SMEs were also supported by the Observatory on the competitiveness of SMEs.[133] OPMI (*Osservatorio sulla competitività delle PMI)*[134]*,* sponsored by the Knowledge Center of *Bocconi Sda,* has stated that from 2007 until the end of 2013, of the 55,709 Italian SMEs with sales of 5 to 50 million euro, 16% have now shut down. Translated into economic terms, this signifies a loss of 120 billion euro in sales, 405,000 less jobs and the disappearance of 8,841 enterprises. The encouraging figure is derived from the 46,868 enterprises that did not shut down as a result of the economic crisis and have achieved a median annual growth of 4.28%, or 26% cumulative. Among these enterprises, 2.5%, or almost 1,165 SMEs, grew 12.4% annually (77% cumulative growth) despite the crisis. The enterprises in question are primarily in Veneto, Emilia Romagna, Piemonte and Liguria, and they belong to the manufacturing (mechanical, food and beverage, chemical and pharmaceutical) and wholesale trading sectors. These are primarily enterprises with several more years of activity behind them, and according to the report, they achieved this through their abilities to internationalize, innovate and register brands and trademarks. 9,000 more SMEs, according to the report, have the potential to increase their revenue.

Italian SMEs are in a position to play a key role for the economic recovery of the country. Riccardo Luca, of the Italian Digital Champion, is of the same opinion and has recently highlighted the importance of investing in the digitalization of Italian SMEs in order to support internationalization efforts and the use of e-commerce. He has also highlighted how crucial it is for the resurgence of the economy that SME's protect themselves from web related risks. According to Luca, culture is another strategic factor that needs to be supported in order to increase awareness regarding information technology. He stated that, "*In the 60's the economic boom was also caused by Maestro Manzi, who taught Italians to read and write on TV. Today we need a new Maestri Manzi to teach Italians about the risks and (especially) the opportunities of the web*"[135].

[133] *Empowering the knowledge of small and medium enterprises management*, Divisione ricerche Claudio Demattè Osservatorio sulla competitività delle PMI, 10 July 2014, SDA Bocconi, available at: <http://www.sdabocconi.it/sites/default/files/upload/pdf/report_PMI_10_luglio_2014.pdf> (retrieved 7-11-2014).

[134] The survey analyzes the financial statements of the 56,000 Italian SMEs since 2007 with a turnover of between 5 and 50 million euro, which, while constituting only 6.1% of Italian companies, produce 39% of GDP and employ 2.291 million people. The survey identifies 1,200 samples.

[135] Luna: "*Le startup non bastano, per la ripresa servono PMI digitali*", available at: <http://www.corrierecomunicazioni.it/job-skill/30662_luna-le-startup-non-bastano-per-la-ripresa-servono-pmi-digitali.htm> (retrieved 7-11-2014).

3.2 Cybercrime as a brake on the country's economy: an overview of cybercrime in Italy

In Italy, cybercrime is still underestimated in terms of the actual impact it has on the economy. According to PwC's 2014 Global Economic Crime Survey[136], one out of four Italian enterprises reported that they had been victims of cybercrime. The survey obviously also highlighted that the figure is probably much lower than the real figure as these types of crimes are hard to detect by the company, and if detected the company is not always willing to disclose that information.[137] The risk of one of these attacks occurring is now taken more seriously than in previous years; yet, for almost half of companies the threat assessment remains the same. The types of damage resulting from a cyber attack that are particularly worrisome to the Italian companies surveyed are damages to image or reputation (65%), damages resulting from the violation of systems (64%), direct economic damage due to IT fraud (60%), interruption of services due to hacker attacks (59%), theft and loss of sensitive information pertaining to their clients (58%), and damage resulting from the theft of company information (55%). It is notable that this type of menace is perceived to originate outside the company, usually cyber criminals being considered as individuals not belonging to one's own environment, but instead criminals who operate from foreign and faraway places. The majority of Italian companies surveyed consider cybercrime as originating from outside the company, 23% consider it both an internal and external risk and only 7% consider it a risk from within the company.

The situation described by the study *"Guadagnare dalle informazioni digitali" (Earnings from Digital Information)*[138]*,* conducted by Trend Micro regarding cyber security, is not exactly rosy. According to the said study, Italy ranked fifth among the countries with the most number of active botnets in the first trimester of 2013, and the third overall worldwide in terms of spam sent. It also ranked eighth among countries hit by malware destined for the financial sector and e-banking. Regarding the fact that Italy is considerably affected by cyber threats, it is quite telling that Italian is the ninth most utilized language for spam in the world and, in reference to the world of mobile devices, Italy is fourth among the countries with the largest number of malicious apps for Android platforms.

The EMC Data Protection Global Index surveyed more than 3,000 IT decision makers in 24 countries to create a ranking of protection readiness. The results underscore what every country must do to be confident that their data is safe.

---

[136] *PwC's 2014 Global Economic Crime Survey Le frodi economico-finanziariein Italia: una minaccia per il business Settima edizione,* available at: <http://www.pwc.com/it/it/services/forensic/assets/docs/gecs-2014.pdf> (retrieved 7-11-2014).

[137] The Global Economic Crime Survey 2014 has conducted over 5,000 interviews in a total of 95 countries . With regard to Italy, it surveyed 101 companies.

[138] *Guadagnare sulle informazioni digitali* Verifica di sicurezza annuale 2013 by TRENDLABS, available at: <http://www.trendmicro.it/informazioni-sulla-sicurezza/ricerca/trendlabs-2013-annual-security-roundup/index.html> (retrieved 7-11-2014).

EMC's Data Protection Index ranks 24 countries on the maturity of their data protection strategies and assesses the relative preparedness of their businesses. Within this index, Italy ranks in the 15th position.

Only 10% can be described as being "ahead of the curve" when it comes to data protection practices. 80% of the companies surveyed recorded an unexpected block placed on their computer systems or a loss of sensitive data, which led to a 38% loss of productivity; a 22% decrease in sales; and a 36% delay in the development of a product, all within the previous year.

Italian companies have lost as much as 9 billion dollars due to data loss in the last 12 months - a figure that rises to 14.1 billion dollars if you add the 5.1 billion dollars in unplanned downtime.[139]

Italy suffers from a lack of research studies, data and official statistics regarding cybercrime. The only available studies are the result of statistics compiled by the private sector. An association that prepares an annual report on ICT security in Italy is Clusit.[140] Clusit has had among its objectives for many years, the dissemination of ICT security culture in Italy through the promotion of information sharing about the sector through the hosting of periodical summits. According to the Clusit Report 2014[141], cybercrime is a rapidly evolving phenomenon and is increasing at an alarming rate. The seriousness of attacks has increased significantly over the years regarding the number of attacks, the value of the stolen data, and the consequences resulting from the various attacks. Furthermore, the lines between cybercrime and hacktivism have become increasingly blurred as the instruments associated with the two worlds are used simultaneously in order to achieve the same objectives and to increase the odds of success of an attack. Through the deep web, it is easy to access all the tools available to cyber criminals. For example, it is possible to purchase a botnet to launch a DDoS attack, which is usually a typical hacktivist technique. However, it is now often used in order to hide the real intent of the attack, which is the theft of sensitive data.

Another trend at the international level highlighted by the Clusit Report relates to the tendency of cyber criminals to attack suppliers of goods and services and companies, which they consider to be the weakest links within their respective networks[142]. Despite being the pulsating heart of the Italian economy, these SMEs are used as a means to an end - usually in order to reach medium and large companies. Recently in the media, there have been reports concerning the hacker attack against the American giant for home and building products, The Home Depot. The hackers managed to steal 53 million email addresses and 56 million financial records (including debit cards and credit cards belonging to US and Canadian citizens), simply by using the credentials of one of Home Depot's suppliers. Through the username and password of an outsourcer, the hackers managed to access the Home Depot network, install a piece of malware created specifically to fool the antivirus software and spread within the network, thus accessing a

[139] Emc Global Data Protection Index available at: <http://www.emc.com/microsites/emc-global-data-protection-index/index.htm#infographic-italy> (retrieved 8-12-2014).

[140] Born in 2000 in the Department of Informatics, University of Milan.

[141] *Rapporto Clusit 2014 sulla sicurezza ICT in Italia*, available at: <https://clusit.it/rapportoclusit/> (retrieved 7-11-2014).

[142] Generally exploiting their privileged accounts and VPN connections.

database of email addresses as well their record of payments and transactions. In doing so, the hackers succeeded in carrying out the greatest cyber attack ever recorded[143]. As illustrated in the first chapter of this research paper, hackers see a very lucrative shortcut via SMEs, which allows them to strike larger organizations with minimum effort thanks to the low budget and culture related to levels of cyber security which are present in small enterprises.

Regarding the Italian landscape: of the 438 companies interviewed as part of the study, 81 of whom are technology suppliers, half declared that they want to increase the budget for cyber security, while the other half intends to maintain their current budgets. (None intend to diminish them.) For SMEs: 43% would like to increase the budget dedicated to security; however, the information as to when they would actually be able to do so is not available. Despite this, the sample analyzed in the report expressed a willingness to invest in ICT security - 46.7% compared to the 26.7% declared in 2013. This could represent an increase in the level of awareness regarding this risk. According to ICT security providers, medium enterprises are the most likely to increase their investments. In general, we can detect a higher interest in ICT security compared to previous years; although, the investments in ICT security recently are primarily of a technical nature as formation activities are left for last.

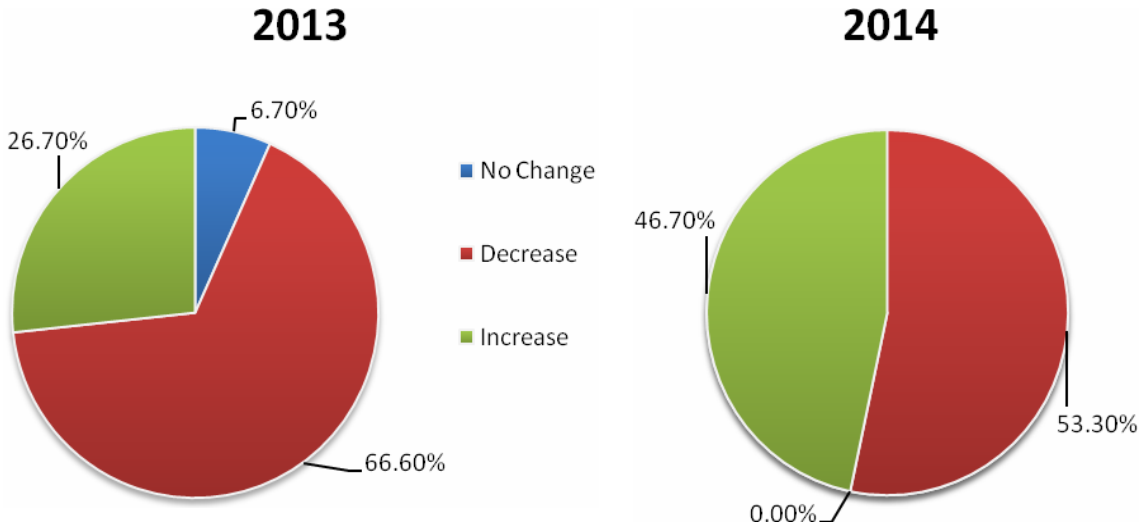


Figure 16 - Declaration of investment in ICT compared to the previous year
Source: Clusit Report 2014

A limitation of the Clusit Report regards information on the analysis of attacks in Italy in 2013. The report analyses only 35 serious cases, which obviously cannot represent a snapshot of the current state of cybercrime in Italy for two basic reasons. The first relates to the reluctance of companies to release information regarding attacks and the difficulty, which still exists, in

[143] *The Home Depot Reports Findings in Payment Data Breach Investigation*, available at: <http://www.streetinsider.com/Press+Releases/The+Home+Depot+Reports+Findings+in+Payment+Data+Breach+Investigation/9986431.html> (retrieved 7-11-2014). See also: *Home Depot Says Hackers Also Stole Email Addresses* by Nicole Perlroth, The New York Times 6-11-2014, available at: <http://bits.blogs.nytimes.com/2014/11/06/home-depot-says-hackers-also-stole-email-addresses/?_r=0> (retrieved 7-11-2014).

detecting the attacks. The second reason to consider is that serious cases are usually related to governments, political movements, police and institutional forces[144]. In this category there are more hacktivism attacks as opposed to those classified as cybercrime (respectively 83% and 17%). The nature of these attacks in themselves is such that hacktivists have an interest in their attacks being made public and use tools to make the attack obvious. Cybercriminals on the other hand tend to use less visible tools to keep their attacks hidden, and therefore the data is not complete.

This analysis is confirmed by Fastweb data contained in the report, which despite referring only to their network (more or less 10% of national coverage[145]) shows that cybercrime is the main cause of attacks, representing 60% of the total, while 24% is related to industrial espionage and only 16% can be traced back to hacktivism[146]. This fact is particularly alarming for enterprises as they are targets of both cybercrime and cyber espionage - designed to steal or copy projects, sensitive data and documents.

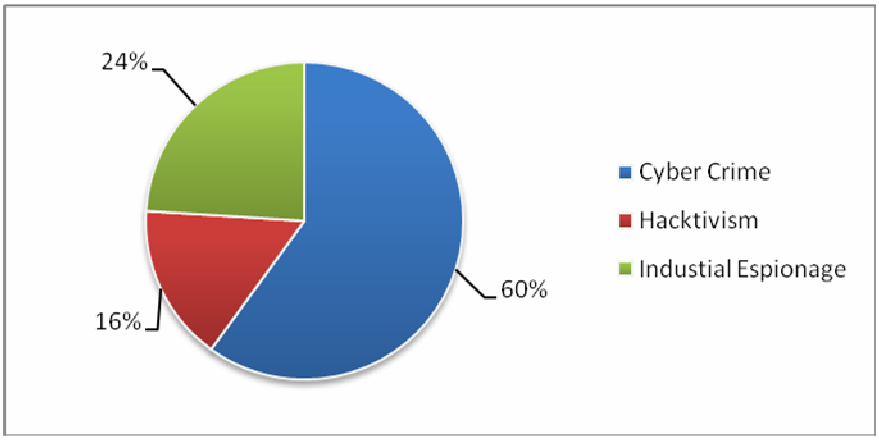


Figure 17 - The Motivations of Attackers
Source: Clusit Report 2014, Fastweb data

Regarding the origin of these attacks, for obvious reasons Fastweb takes into account the lack of reliability of information pertaining to the final IP addresses of an attack, which often belong to a botnet and are used to locate the Command and Control. In other words, the servers are utilized as a control center (activated at the request of the "botnet master"), and they act as the connection through which the criminal can command the infected computers in order to conduct the attack. Even Command and Control is a tool that can be used remotely, thus its localization does not automatically guarantee the localization of the attacker who could be controlling it from an entirely different country. This element is indicative of how cybercrime is a

[144] Among attacks considered by Clusit are those DDoS attacks made against political objectives such as the President of the Council Matteo Renzi, movements such as the Movimento 5 stelle and Casaleggio & Associati, institutions such as the Ministry of Interior, regional offices, and law enforcement. Among the cyber crime events listed, the Report also cites Alpitour, the Court of Milan and the CNR of Genova.

[145] *Agcom data: bene 3 Italia e Fastweb. Ed è boom per Lycamobile* by Andrea Biondi in Il Sole 24 Ore 7-10-2014, available at: <http://www.ilsole24ore.com/art/impresa-e-territori/2014-10-07/dati-agcom-bene-3-italia-e-fastweb-ed-e-boom-lycamobile-173237.shtml?uuid=ABdmQx0B> (retrieved 8-11-2014).

[146] Data collected on 200,000 IP addresses belonging to the Autonomous System of the Internet Service Provider Fastweb SpA, which includes both those of customers and Fastweb.

transnational phenomenon. The area with the largest number of Command and Control centers is Asia, followed by Europe and the Middle East.

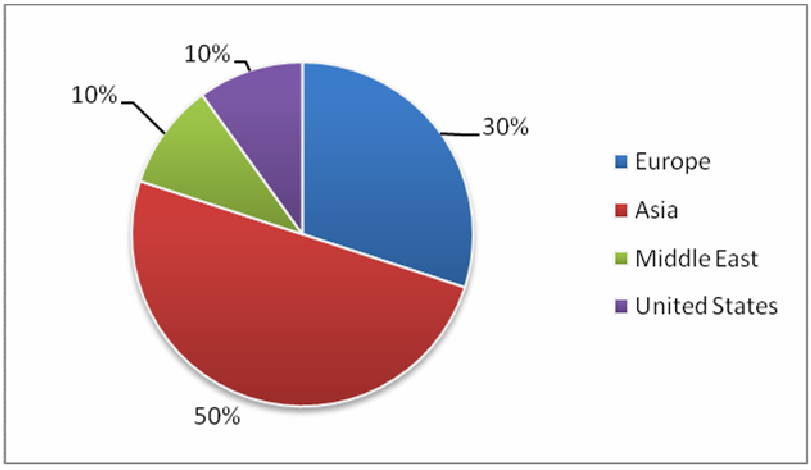


Figure 18 - Distribution of Command and Control Centers
Source: Clusit Report 2014, Fastweb data

Cybercrime, anticipating and identifying early on the best channels to exploit and maximize profits, travels at a higher speed than the awareness of informatics tools available to users. In this context, social networks and the increasing use of mobile devices represent new channels to conduct cyber attacks. In Italy, according to the latest Audiweb data (August 2014), 27.4 million Italians[147] are active online[148]. This social and technological revolution includes a growing number of Internet users who access it through mobile devices (tablets and smartphones) as opposed to PCs [149].

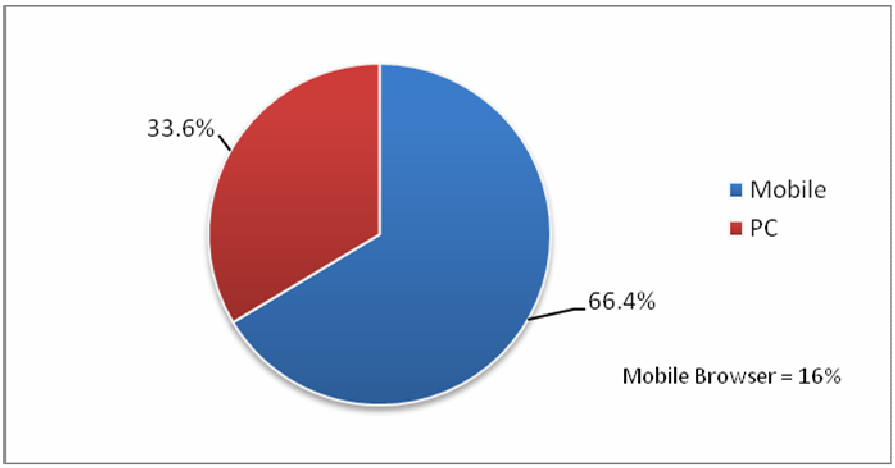


Figure 19 - Time online in relation to utilized device
Source: Audiweb data, August 2014

[147] Unique users.

[148] *Audiweb pubblica i dati dell'audience mobile e della total digital audience del mese di agosto 2014*, available at: <http://www.primaonline.it/wp-content/uploads/2014/11/Audiweb_CS_TotalDigitalAudience_03112014.pdf> (retrieved 7-11-2014).

[149] Italians between 18 and 74 years of age who every day are connected by mobile devices are numbered at 15.5 million. The online Italian audience connected via PC has been recorded at 10.5 million unique users.

This data is important to understand the changes in Italian habits and consequently identify where the greatest risks may originate from, which can influence investments and strategic choices as well as the actions of cyber criminals. From the data related to mobile navigation, it is important to highlight that 84% refers to the use of apps, while navigation through a browser accounts for only only 16%. From a company perspective, it is important to point out how the versatility of mobile devices has increased the cases of dual use, in other words, the use of the device for both work and private purposes.[150] This opens the door to a variety of other problems for companies who now have to manage the vulnerability of mobile devices and their use by individuals who are nonchalant and less vigilant, and therefore possible conduits for targeted and aggressive attacks. The vulnerability of mobile systems has pushed cyber criminals towards more sophisticated attacks targeting these devices, which are for all intents and purposes, PCs not equipped with efficient antivirus protection - making them more accessible from the outside. Via a wireless connection, for example, the data travelling from a smartphone to the network is decrypted, which makes it possible to visualize passwords and any other information pertaining to that particular connection by any cyber criminal pretending to be an access point. Furthermore, many users modify their devices by eliminating factory blocks and unlocking advanced administrative settings (Root for Android and Jailbreak for iPhone), then install "cracked" software and games downloaded from unofficial App stores, without understanding the real danger which these actions can lead to.

Another trend, which concerns the habits of Internet users in Italy - both private and work related - is the increase in the use of social networks and cloud services. The investigation conducted by AIDiM, ANVED and eCirle[151] in 2012, revealed that 75% of the 315 Italian companies interviewed used social media platforms for branding purposes, to interact with clients, attract new clients through promotions, conduct marketing schemes and to collect feedback about their products and services. The most used social network was Facebook, followed by LinkedIn, YouTube and Pinterest - so it is easy to imagine that this trend has evolved rapidly in recent years. Cloud services allow companies to use innovative tools, thus reducing administrative costs. This is especially useful for SMEs, which have more limited budgets as compared to larger enterprises. However, social networks and cloud services contain a large amount of data which is what makes them desirable prey in the eyes of cyber criminals, who then utilize techniques such as social engineering, phishing and spam to take advantage of the technical weaknesses (of cloud services and human weaknesses of social networks) to conduct their attacks.

Cybercrime should not be underestimated as it has a huge impact on the country's economy. According to the latest McAfee study on cybercrime's impact on the economy worldwide,[152] Italy suffers from direct losses of almost 875 million dollars per year, and that figure

---

[150] *Guardia di Finanza* Nucleo Speciale Frodi Tecnologiche, 2014, available at: <http://www.aracneeditrice.it/scaricabili/interventoreda.pdf> (retrieved 7-11-2014).

[151] "*Quanto è Social la tua Azienda?*", available at: <www.slideshare.net/kornfeind/quanto-social-la-tua-azienda> (retrieved 7-11-2014).

[152] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies*, June 2014, available at: <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf> (retrieved 7-11-2014).

reaches 8.5 billion dollars (equal to 0.6% of Italy's GDP) if we consider damages to image and reputation, the costs related to recovery and loss of business opportunities.

According to the Websense study 'Exposing the Cybersecurity Cracks: A Global Perspective'[153], conducted by the Ponemon Institute[154], 66% of Italian companies admit to not having the necessary tools and know-how to prevent the loss of sensitive information. 54% of interviewees did not consider their company to be sufficiently protected against more sophisticated cyber attacks and almost half admitted to having been a victim of a considerable attack in the previous year. For more than 70% of those interviewed, their tools did not identify the primary causes of the attack, and more than half of companies which have suffered an attack were not able to identify which information was stolen.

Another important aspect that surfaced through interviews with IT managers (who are considered to be the most competent figures regarding cyber security within companies) is that 80% of them think that management has difficulty in recognizing the loss of information as an economic loss. One last relevant piece of information is that half of those interviewed consider the average manager's knowledge of the cybercrime phenomenon to be insufficient.

The problem has very strong cultural connotations. Despite the fact that the number of Italian web users is almost 37 million (or roughly 60% of the Italian population)[155], the awareness of possible IT risks is still very low. According to information published by Eurobarometer,[156] 61% of Italians interviewed do not consider themselves to be well informed regarding the risks of cybercrime compared with a 52% average in Europe as a whole. The survey reveals that the majority of European citizens feel unprepared when it comes to protecting their information online. As we can see in the figure below, 33% stated that they are well informed - but this is very difficult to measure adequately. Simple habits such as periodically changing passwords are still not part of the routine of Internet users. According to Eurobarometer, more than half of Italians state that they have not changed any of their passwords in at least 12 months.

[153] *Exposing the Cybersecurity Cracks: A Global Perspective Part I Websense*, Inc. Ponemon Institute April 2014, available at: <https://www.websense.com/assets/reports/report-ponemon-2014-exposing-cybersecurity-cracks-en.pdf> (retrieved 7-11-2014).

[154] The research involves about 5,000 IT security professionals around the world, having an average experience level of about 10 years. They come from from 15 countries: Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Italy, Mexico, the Netherlands, Singapore, Sweden, the UK and the US.

[155] Italy Internet Users, available at: <http://www.Internetlivestats.com/Internet-users/italy/> (retrieved 7-11-2014).

[156] *Eurobarometer Special Surveys*, Cyber security Report, European Commission, available at: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_it_en.pdf> (retrieved 7-11-2014).

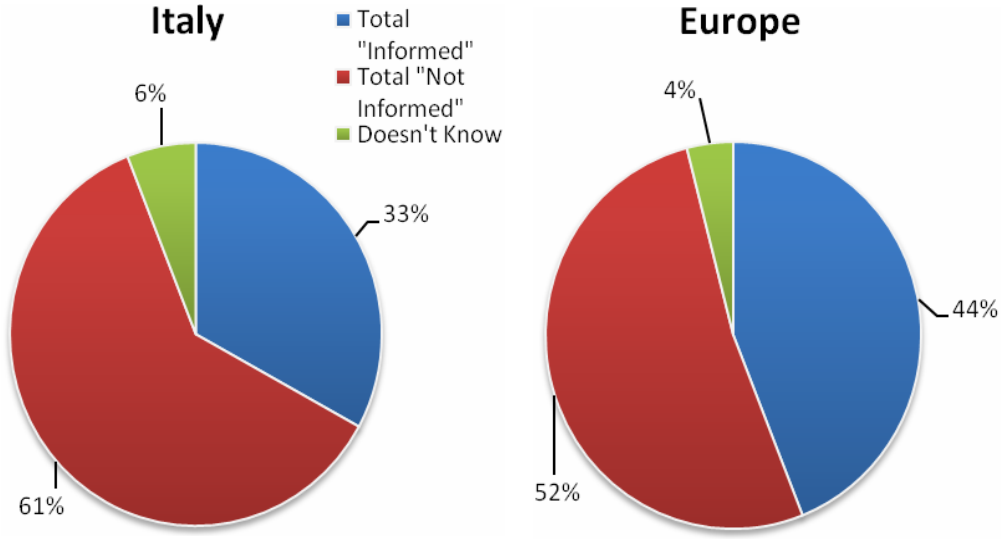


Figure 20 - Survey on perceived awareness regarding the risks of cybercrime
Source: Special Eurobarometer 404 Cyber Security Report, 2013

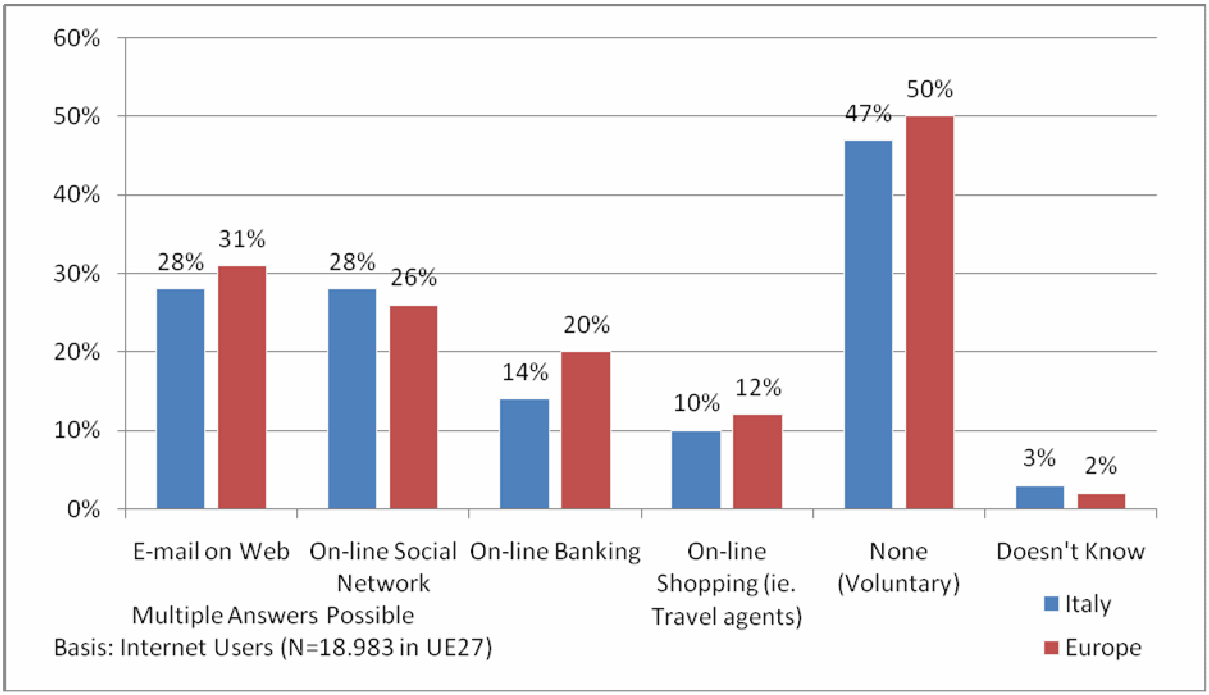


Figure 21 - Survey of password changing habits within a 12-month period
Source: Special Eurobarometer 404 Cyber Security Report, 2013

3.3 Italian cyber security policies

New laws regarding cybercrime were introduced for the first time through changes to the Penal Code (*Codice penale)* and Code of Criminal Procedures (*Codice di procedura penale)* with approval of two laws in the 1990's. Law No.547 of 23 December 1993: 'Modifications and integrations according to the Penal Code and the Code of Criminal Procedure on the subject of computer crime' ("*Modificazioni ed integrazioni alle norme del Codice penale e del Codice di*

procedura penale in tema di criminalità informatica"), and law No.268 of 3 August 1998: 'Provisions against the exploitation of prostitution, pornography, sex tourism involving children' ("*Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori')*[157], which designates the Postal and Communications Police (*Polizia Postale e delle Comunicazioni)* as the entity responsible for fighting cybercrime[158].

Concerning the delicate question of information protection, the first Italian document is the directive 'Computer security and telecommunications in public administration' ('*Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni')*[159] of 16 January 2002, which states that it is of strategic importance for the country to protect and safeguard the information contained in the databases of public administration and urges public administrations to test their levels of cyber security and take the necessary steps to ensure an adequate level of security. This area is also governed by the 'Code concerning the protection of personal data, approved through Legislative Decree' ('*Codice in materia di protezione dei dati personali approvato con Decreto legislativo)* No.196 of 30 June 2003, which regulates the management of personal information and related responsibilities of public administrations.

In order to promote these normative interventions regarding security and protection of the web, both regulatory and administrative, a Working Group was established through an Inter-ministerial Decree enacted on 1 September 1999. In 2003, the working group became 'The Permanent Observatory for the safety and protection of networks and communications' ('*Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni')* within the Ministry of Economic Development through a Ministerial Decree with the task of safeguarding and protecting the Internet and communications. Now, permanently expanded through the presence of representatives from the Ministry of Defence - The Department for Public Service, the Department of Innovation and Technology and the Ministry of Industry, this monitoring mechanism stays up to date on the technological evolution and norms regarding the different aspects of the telecommunication sector, with a particular emphasis on security[160].

This body covers the important role of being the principal national counterpart to ENISA and to the College of Communication and Information Technology, ISCOM (*Istituto superiore delle comunicazione e delle tecnologie dell'informazione)*,[161] a technical and scientific body of the

---

[157] "*Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*.", published on *Gazzetta Ufficiale* n. 185 of 10 August 1998, available at: <http://www.camera.it/parlam/leggi/98269l.htm> (retrieved 9-11-2014).

[158] Article 14.

[159] Enacted by Ministero per le Innovazioni e tecnologie, available at: <http://www.gazzettaufficiale.it/eli/id/2002/03/22/02A03219/sg%20;jsessionid=nBvFj9k-8FcOCREFNlFaag__.ntc-as1-guri2a> (retrieved 9-11-2014).

[160] *Osservatorio permanente per la sicurezza e la tutela delle reti e delle comunicazioni*, available at: <http://www.sviluppoeconomico.gov.it/index.php?view=article&catid=686%3Apresentazioni&id=2017543%3Aosservatorio-permanente-per-la-sicurezza-e-la-tutela-delle-reti-e-delle-comunicazioni-&format=pdf&option=com_content> (retrieved 9-11-2014).

[161] *Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione* operates within the *Ministero dello Sviluppo Economico*, Presentation, available at: <http://www.isticom.it/index.php/presentazione (retrieved 9-11-2014).

government within the MISE, which was established in 1907[162]. Over the years it has evolved alongside the technology of the communication and information sector. Today, ISCOM is composed of four internal divisions and employs 112 highly qualified staff members (of whom 70% are technicians and engineers) and supports the ICT sector, public administration and users through consultations focusing on services to enterprises. ISCOM also organizes national cyber security exercises and participates in the Pan-European and the joint EU-US exercises to evaluate the efficiency of information sharing between public and private sectors.

One of the first published reports on cyber security was the 'Protection of critical information infrastructure. The Italian reality,' ('*Protezione delle infrastrutture critiche informatizzate. La realtà italiana').* The report was published in 2004 by the Working Group, which was established in 2003 by the Ministry for Innovation and Technology. The Working Group was composed of representatives from various Ministries, such as the Interior Ministry of Infrastructure and Communications as well as private sector representatives, such as Telecom Italia, ABI, Wind and Snam Rete Gas. The document highlighted the strategic importance of the security of critical infrastructure for the whole country, particularly in light of their IT related interdependency, and identified those of greatest impact on the country[163]. The critical infrastructure was then classified in 2008 by the 'Identification of critical infrastructure information of national interest Decree' (*Decreto Individuazione delle infrastrutture critiche informatiche di interesse nazionale),* approved by the Interior Ministry. This report also recommended the creation of a CERT for public administration (CERT-PA), which will be discussed later on.

On 7 March 2005, Legislative Decree No. 82 Digital Administration Code (*Codice dell'amministrazione digitale)* was passed, along with law No.155 'Urgent measures to combat international terrorism,' also known as the '*Legge Pisanu*' being enacted on the 31st of July. The code is at the foundation of the process of the digitalization of administrative tasks in order to achieve real modernization within public bodies and agencies by using digital and telecommunication technology to communicate between public administrations, the citizenry and enterprises. The '*Legge Pisanu*' appointed the Internal Ministry as the entity responsible for the protection of critical information infrastructure[164] and identified the Postal and Communications Police as those responsible for implementing the laws against cyber attacks targeting said infrastructure. In 2008, under the same law, the 'National Crime Center for the protection of critical infrastructure,' CNAIPIC, ('*Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche')* was established and placed under the control of the Postal Police[165]. CNAIPIC is tasked with protecting the cyber systems of institutions, public administration, public bodies, private individuals and companies operating in areas such as international relations,

[162] Law 111 of 24 March 1907 "*sull'ampliamento e il miglioramento dei servizi postali, telegrafici e telefonici*".

[163] Specifically: electrical infrastructure, computer and telecommunications networks, infrastructure for the transport of gas, rail and road circuits, banking and financial, hospitals, and other critical infrastructure, nuclear facilities, satellite navigation systems and SCADA systems.

[164] Article 7a about IT security.

[165] "*Decreto"* of *Ministero dell'Interno* of 9 January 2008 in implementation of the law 31 July 2005 n° 155.

security, defense, finance, communications, transportation, energy, the environment and anything deemed by the Internal Ministry to be strategic to maintain order and national security. CNAIPIC and each critical infrastructure entity manage cyber security through dedicated lines and connections made in accordance with respecting agreements with the Department of Public Security (*Dipartimento della pubblica sicurezza)* and work through an operations center which is active 24/7. Through web monitoring and collaboration with law enforcement agencies and national and international ICT security companies, the center monitors, collects and analyses data relevant to monitoring and preventing cybercrime. In the case of an attack on critical infrastructure, the center can count on 20 districts and 80 sections of the Postal and Communications Police, as well as foreign and international police forces such as Interpol and Europol. As provided for by the Budapest Convention on cybercrime, within CNAIPIC resides the Italian liaison desk pertaining to transnational cyber attacks. The liaison desk, established by the G8 and expanded to the Council of Europe, operates 24/7 within the High Tech Crime network, which connects 64 countries around the world. Statistical data[166] provided by the Postal and Communications Police show the following: there were 746 attacks detected in 2013 (almost double the total from the previous year), 786 alerts were issued, 62 cooperation requests were made within the High Tech Crime network[167], 53 investigations were conducted, charges were brought against 18 people (9 of whom were arrested), and 9112 monitoring tasks were conducted.[168] Since 2006, the online portal of Commissariat of Public Administration (Commissariato di P.A) has been active.[169] This portal aims to become the point of reference for specialized users, receiving 7014 complaints in 2013 alone.

The Italian Financial Police (*Guardia di Finanza)* and another branch of the Italian Police Force (*arma dei Carabinieri)* also have centers tasked to counter this type of crime. For example, the Special Unit for fraud telematics of GdF (*Nucleo speciale frodi telematiche* of GdF), active since 2001, discharges its responsibilities to fight finance related cybercrime in collaboration with the Italian Digital Agency (*Agenzia per l'Italia Digitale)*. In addition, the Scientific Investigations Service (*Servizio investigazioni scientifiche dell'arma dei Carabinieri)* has 4 units, 29 sections and a scientific investigation group, all active in cyber security.[170]

The national process to counter cybercrime pushed Italy to ratify the Convention on Cybercrime of the Council of Europe in 2008.[171] The following year, the "*Piano e-Gov 2012*" was

[166] *Relazione annuale 2014 della Polizia Postale e delle Comunicazioni*, provided for this research by *Vice Questore* of Florence, Dr. Stefania Pierazzi.

[167] Under Article 35 of the Budapest Convention.

[168] Within the "*II Divisione del Servizio Postale e delle Comunicazioni"* also operates the "*Centro nazionale per il contrasto della pedopornografia online*", CNCPO, estalished with law n° 38 of 6 February 2006. The investigations of the center referred to the year 2013 in which 28,063 sites were monitored, 1,641 sites included in the blacklist, 430 searches conducted, 344 people charged and 55 people arrested.

[169] Accessed at the address: www.commissariatodips.it.

[170] *Carabinieri* indagini scientifiche, available at: <http://www.carabinieri.it/Internet/Arma/Oggi/RACIS/> (retrieved 9-11-2014).

[171] Ratification and implementation of the Convention on Cybercrime of the Council of Europe, Law No. 48 of 18 March 2008.

promoted by the Ministry for Pubic Administration and Innovation *(Ministero per la Pubblica Amministrazione e per l'Innovazione),* developed with the objective of increasing the level of digitalization of the country and decreasing the digital divide.

Cybercrime was elevated to the status of a proper threat to national security through the 'Report on the possible implications and threats to national security arising from the use of cyberspace' *('Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico')*[172]*.* The aforementioned report was prepared by COPASIR (*Comitato parlamentare per la sicurezza della Repubblica)* and presented on 15 July 2010. The report subdivides the risks of cyber space into cybercrime, cyber terrorism, cyber espionage and cyber war. The document goes on to propose national policies to counter these issues through the inclusion of enterprises and citizens to foster a public-private partnership and promote a cyber security culture. The relevance of this report consists in the fact that, for the first time, cyber threats were listed as risks, and the government was asked to form a coordination structure to adequately manage the policies designed to fight cybercrime and take heed of the most important aspects of cyber security.

Between 2011 and 2013, Italy took further steps in the implementation of actions geared towards tackling this phenomenon. Among these is the 'Implementation of Directive 2008/114 / EC on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection' ('*Attuazione della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione')* of 2011[173]. The directive assigned to the 'Core inter-ministerial situation and planning,' NISP[174] ('*Nucleo interministeriale di situazione e pianificazione*'), which was tasked with identifying European critical infrastructure (ECI) and to function as the national focal point for the protection of ECI at the European level, but had no assigned funds to achieve these objectives.

In 2012, with the law No. 83 of 15 June 2012[175], Italy formed the Italian Digital Agency, AgID (*Agenzia per l'Italia Digitale)* with the objective of coordinating all actions geared towards innovation and promoting the use of ICT within public administration in line with the objectives of the Italian Digital Agenda (*Agenda Digitale italiana*)[176] and the European Digital Agenda. Building Italy's broadband capabilities, ICT infrastructure of public administrations and digital development are some of the strategic actions pushed forward by AgID, with the objective of creating growth

---

[172] *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, COPASIR, 7 July 2010, available at: <http://www.senato.it/service/PDF/PDFServer/BGT/525461.pdf> (retrieved 9-11-2014).

[173] *Decreto legislativo* n° 61, 11 April 2011, of Presidente della Repubblica.

[174] Established by DPCM 5 May 2010, *Organizzazione nazionale per la gestione di crisi*, that update the *Manuale nazionale per la gestione di crisi* of 1994, based on NATO Crisis Responses System Manual and on Manual of EU Emergency and Crisis Coordination.

[175] "*Decreto"* converted in law 134 of 7 August 2012, so-called "*Decreto sviluppo"*.

[176] Established by *Decreto* of *Ministero dello Sviluppo Economico* of 1 March 2012. The measures for the effective implementation of the Agenda, are indicated in: *Decreto legge* 179 of 18 October 2012 "*Ulteriori misure urgenti per la crescita del Paese".*

opportunities for the country's economy. Since January 2014, CERT-PA, one of the active CERTs in Italy, has been operational within AgID.

Regarding cyber security, law No. 133 of 7 August 2012[177] gives the Department of Information and Security (DIS) the important role of coordinating intelligence activities to strengthen national cyber security.

In 2013, for the first time, Italy defined "*the institutional architecture appointed to national security in relation to critical infrastructure*"[178] through the DPCM[179] of 24 January, approved by the President of the Council of Ministers in order to address the need for a legal framework for security in cyber space. The DPCM is tasked with identifying the bodies to counteract cybercrime and outline an organizational structure conducive to cyber security, as well as providing common definitions of the major aspects of cyber space.

The DPCM identified three levels of interventions: the strategic and political level (to elaborate strategies, which is a responsibility of the Interministerial Committee for the Security of the Republic; the operational level, which coordinates and supports all the bodies involved, the Security Cybernetics team led by the Military Advisor of the President of the Council (*Nucleo per la Sicurezza Cibernetica)*; the crisis management level, entrusted to the Ministerial Desk for Crisis Cybernetics (*Tavolo interministeriale di crisi cibernetica*).

This document also identifies the national public bodies tasked with cyber security. The Chairman of the Board had the task of designing a 'National Strategic Framework for the security of cyberspace,' QSN ('*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*') and a national plan for cyber protection and cyber security, PN *(Piano nazionale per la protezione cibernetica e la sicurezza informatica).* The plan was adopted on December 2013 through a unanimous decision of the Interministerial Committee for the Security of the Republic, CISR (*Comitato interministeriale per la sicurezza della Repubblica*). Both documents have been operational since 27 January 2014[180], and their purpose is to define the tools and procedures for fighting cyber threats that are in the nation's interests.

Specifically, the QSN is a document that outlines political strategy to identify profiles and threats to and weakness of the national network by defining the roles of the various private and public players, and the instruments and the procedures to fight and prevent cybercrime[181]. Cybercrime is one of the four categories tackled by the QSN (the risks of cyber space together with espionage, war and cyber terrorism), and addressing these issues is considered a maximum priority for the country. The document also outlines the procedures needed to build Italian cyber capacity in six strategic directions, the primary actors of national cyber security as defined by the

[177] Amendments to the law 3 August 2007 n° 124, "*concernente il sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto*", Art. 3.1.

[178] Art. 1.1

[179] "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*".

[180] Gazzetta ufficiale n° 41 of 19 February 2014.

[181] Presidenza del Consiglio dei Ministri, QSN, available at <http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf> (retrieved 9-11-2014).

DPCM on 24 January 2013[182], and eleven operational paths. The concrete implementation of the QSN is delegated to the 'National Plan for the Protection of Cyber Security' ('*Piano Nazionale per la protezione cibernetica e la sicurezza informatica')*, which outlines the desired objectives for all the operational paths and develops strategies for the two year period from 2014-2015 on the basis of public private partnerships upon which hinges the success of the adopted policies. Unfortunately the plan does not yet have an established budget for cyber security and does include a timeline or identify those assigned with the responsibility to complete the actions indicated. The official national cyber strategy is composed of these two documents (QSN and PN). Despite the delay in the implementation of a cyber strategy when compared to more advanced European countries, the objectives of these documents are forward thinking, calling for the prevention of future cyber threats and to put in place a foundation for gradual progress on this front.

Ms. Rita Forsi, *Direttore dell'Istituto superiore delle comunicazioni Ministero dello Sviluppo Economico-Dipartimento per le Comunicazioni (ISCOM)*, confirmed that the national CERT[183] entered into force on the 5 June 2014. The CERT is the organization responsible for monitoring cyber incidents, to manage them and then help users to go back to their normal status prior to the violation. In order to reduce the risks resulting from a cyber attack, many CERTs provide their users with useful information regarding cybercrime. The role of CERTs on a national level is important because they contribute to the physical and economic security of a country by identifying the threats that could hit critical infrastructure, and they inform stakeholders of emerging threats and engage in dialogue with other national and international public and private sector CERTs.

Regarding the current state of CERTs in Italy, the list on the ENISA website[184] referencing operational CERTs in Member States is not up to date as it lists CERTs which are no longer active in Italy. According to the ENISA list, there are nine CERTs in Italy. Of these, through the consultation of websites and phone calls, we were able to ascertain that some of the CERTs such as the CERT-RAFVG Friuli Venezia Giulia region and CERT-IT are no longer active. On the other hand, and contrary to what is listed, the CERT of the Italian Post, PI-CERT, has both the First and Trusted Introducer certifications, which are certifications that attest to a high level of maturity of CERTs and allow for more dialogue. We were able to get this information from the updated lists on the official websites of the two certifications. For some CERTs, there is a lack of necessary information to understand the activities they discharge and their actual status. The following is the list we updated through our research.

---

[182] *Presidente del Consiglio dei Ministri*, CISR, intelligence, "*Nucleo per la sicurezza cibernetica"*, NISP and national CERT.

[183] For more information, please, visit: <https://www.certnazionale.it/chi-siamo/>

The establishment of CERT-GOV at the *Ministero delle Sviluppo Economico* was called for with the passage of *Decreto legislativo* 28 May 2012, n. 70 "*Modifiche al decreto legislativo 1° agosto 2003, n. 259, recante codice delle comunicazioni elettroniche in attuazione delle direttive 2009/140/CE, in materia di reti e servizi di comunicazione elettronica, e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita private"*, available at: <http://www.gazzettaufficiale.it/gunewsletter/dettaglio.jsp?service=1&datagu=2012-05-31&task=dettaglio&numgu=126&redaz=012G0091&tmstp=1338881263427> (retrieved 10-11-2014).

[184] Accessed at the address: <http://www.enisa.europa.eu/activities/cert//background/inv/certs-by-country-interactive-map> (retrieved 10-11-2014)

CERT	Date	Web Site	TI Certification	First Certification	State
Servizio Base Provider Clienti PI-CERT	I° Trim. 2013	http://www.picert.it	Qualified from 1 Jan 2001	Member	Operative
Telecom Italia CERT - TS.SOC	2004	http://www.telecomitalia.com/CERT	Not Qualified	Not member	Operative
CERT-PA	II° Quad. 2014	http://www.cert-pa.it/	Not Qualified	Not member	Operative
CERT-Difesa	Not specified	http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/ PAGE NOT FOUND	Not Qualified	Not member	Operative
CERT IT Ricerca e Formazione	I° Trim. 1994	http://security.dsi.unimi.it PAGE NOT FOUND	Not Qualified	Not member	Not Operative
GARR-CERT	01/03/1999	http://www.cert.garr.it	Qualified from 3 Dec 2013	Not member	Operative
CERT ENEL Settore Energia	Not specified	http://www.enel.it/attivita/servizi_diversificati/informatica/cert/ ENEL HOMEPAGE	Not Qualified	Not member	No information in regard
CERT-RAFVG Regione Friuli Venezia Giulia	Not specified	http://cert-rafvg.regione.fvg.it/ NOT OPERATIVE EMAIL ADDRESS	Not Qualified	Not member	Not Operative
SICEI-CERT Diocesi della Chiesa Cattolica	Not specified	http://cert.chiesacattolica.it/	Not Qualified	Not member	Operative

Table 5 - Table summarizing the actual status of Italian CERTs

Although there is still much work to be done, the development of Italy's cyber strategy was founded on the gradual understanding of the need for adequate instruments in order to face the risks coming from cyber space. These efforts will surely improve with time[185], and, in this context, promoting a cyber security culture among citizens, companies and institutions is a crucial step in achieving Italy's cyber objectives.

3.4 Empirical investigation on the impact of cybercrime in Italy

It is clear that cyber security is not only a current issue of importance, but it also requires knowledge and research to be able to stop it. The lack of research and official national statistics concerning such a phenomenon required us to utilize an empirical approach to compose this research paper. We conducted interviews - focusing on the impact of this phenomenon from a

[185] For more details, see: *Cybersecurity: Unione europea e Italia Prospettive a confronto* by Claudia Cencetti, 2014, Quaderni IAI, Edizioni Nuova Cultura.

banking and legal perspective - in order to gain a more complete picture of the various aspects that are involved in the fight against cybercrime.

3.4.1 Banking sector

One of the sectors which has always been aware of these risks is the banking sector. We conducted an interview with Dr. Monica Pellegrino, ICT Research Analyst at *ABI Lab*[186], who informed us that *ABI Lab* coordinates a veritable center for information sharing and updates banks on major cyber threats. This center, called *Osservatorio Sicurezza e Frodi Informatiche*[187] (Monitoring Unit for Security and Cyber Fraud) brings together 40 Banks and 10 specialized ICT partners and organizes periodic meetings to analyze the main trends concerning cyber fraud, logic security, and client and staff identity management. The monitoring unit also undertakes the following activities for Italian banks: monitoring of the national and international landscape, conducting ad hoc investigations and system surveys, defining guidelines for the system, designing technological solutions and organizational models for the prevention and neutralization of major threats, policy analysis regarding cyber security, promoting and developing pilot studies, and disseminating best practices. The unit has also established a mailing list, called *presidio.Internet*, which reaches more than 300 contacts in banks and at the Postal Police through whom the relevant information on new attacks, as well as monthly newsletters on the state of national and international cyber security, are shared.

ABI Lab is also a member of various international networks, both institutional and operational, in order to remain up to date with the latest trends related to cyber fraud and threats. Furthermore, the Monitoring Unit for Security and Cyber Fraud *(Osservatorio Sicurezza e Frodi Informatiche)* also conducted its annual survey. The 2014 edition of the survey saw the participation of 25 Banks (77% of the banking organizations in terms of staff). The survey uncovered that in 2013, 70% of those surveyed participated directly in a community of information sharing and other similar collaborative and inter-sectorial initiatives. Among the various initiatives, there was also the construction of a platform for information sharing managed by the Postal Police, which was designed together with *ABI Lab* under the European project Online Fraud Cyber Center and Expert Network (OF2CEN)[188].

Following an agreement between ABI and the State Police, signed in December 2010 and geared towards the prevention of cybercrime in the Italian banking sector, the collaboration

[186] Established as a project under the Technology and Security Sector of the Associazione Bancaria Italiana, *ABI Lab* was founded in 2002 as a consortium and has emerged today as the Center for Research and Innovation for the Bank, promoting collaboration among Banks, companies and institutions; information available at: <http://www.abilab.it/*Consorzio*/chi-siamo> (retrieved 10-11-2014).

[187] *Osservatorio Sicurezza e Frodi Informatiche*, available at: <http://www.abilab.it/web/sicurezza-e-frodi-informatiche> (retrieved 10-11-2014).

[188] Global Cybersecurity Center, Online Fraud Cyber Center and Experts Network (OF2CEN), available at: <http://www.gcsec.org/activity/research/online-fraud-cyber-center-and-experts-network-of2cen> (retrieved 10-11-2014).

between ABI, banks and the Post and Communications Police continued through various activities. An example is the joint participation in the European project OF2CEN, financed by the Commission and coordinated by the Postal Police. The project, concluded in October 2013, saw the foundation of an information-sharing platform with the objective of sharing information related to abnormal transactions, and with the objective of opening a secure communication channel with the Postal Police to simplify the formal process of signaling fraudulent transactions. The platform can be accessed voluntarily by all banks, which have previously subscribed to the convention with the Postal Police. By inserting the information regarding fraudulent transactions, each user contributes to the expansion of the police database and thus increases the level of efficiency of information sharing - which happens through structured and secure processes. This procedure also contributes to the efficiency and the speed of the investigations.

For the Banks, it is important to raise the awareness of their clientele regarding fraud and cyber threats in order to make them aware of the risks of negligent use of the web. This is of strategic importance not only for an increase in the adoption of technological and behavioral protection measures, but also to increase awareness about the channels and procedures to use when signaling anomalies to banks and the police.

The survey of *ABI Lab* also highlighted that banks utilize a variety of channels available to them when discussing security related issues with their corporate clientele. Channels utilized are as follows: Internet Banking is obviously the preferred channel (100% of the sample), but also branch visits (50%) and contractual information (50%). As a result of the increase in cyber attacks on corporate clientele in recent years, in 2013 *ABI Lab* prepared, in collaboration with the Customer to Business Interaction Consortium (CBI)[189] and the Postal and Communications Police, a document containing technological and organizational recommendations with the objective of supporting banks in their activities of awareness raising of their corporate clientele on safe use of Internet banking services[190].

The Computer Fraud and Security Observatory's (*Osservatorio Sicurezza e Frodi Informatiche*) 2014 report entitled 'Security and computer fraud in the bank. How to prevent and combat fraud on the Internet and Mobile Banking' ('*Sicurezza e frodi informatiche in banca. Come prevenire e contrastare le frodi su Internet e Mobile Banking*')[191], provided for this research paper

[189] The Customer to Business Interaction Consortium (CBI) was created on 20 May 2008 in continuation of the activities managed by the Associazione per il Corporate Banking Interbancario (ACBI), established in 2001. The CBI Consortium defines, in the cooperative sector, rules and technical standards and regulations of "CBI Service", the "CBILL Service" and Node services and manages the technical connection infrastructure between the associates, to achieve, by IT, link and talk with customers, with the goal of interoperability at the national and international level. Approximately 600 financial institutions adhere to CBI (95% of the Italian banking system, the Italian Post Office and CartaLis), which now offer the CBI service in competitive mode to over 950,000 businesses, available at: <http://www.cbi-org.eu/Engine/RAServePG.php/P/250110010404/T/*Consorzio*-CBI> (retrieved 10-11-2014).

[190] Such indications, in fact, can be sent by Banks to customers in the manner considered most appropriate, such as an attachment to its communication on security, adapting according to customer needs, etc.

[191] The report contains the results of the survey conducted by *ABI Lab* on fraud via the Internet and mobile banking. Respondents to this survey included 25 organizations, specifically: banks, groups and outsourcers of banking services; however, if one takes into account the number of individual institutions associated with the respondents, the overall number rises to 153 banking entities. In terms of representation at the system level, the sample of respondents refers

by *ABI Lab*, it emerged that fraud activities are primarily detected through the use of internal tools for monitoring abnormal transactions (44%) or through clients in the retail sector ceasing their activities (39.2% of the cases). In 2013, 95% of the banks included in the report identified episodes of theft of their retail clients' Internet banking access credentials. The figure increases to 100% if we consider corporate clients in a sample of 18 out of 25 banks.

In relation to effective fraudulent transactions, the analysis shows a prevalence of illicit operations involving the successful recharging of pre-paid cards - equivalent to 58% of the actual total of fraud in the retail sector. 39.4% of operations which included a loss of money are represented by transfers, while the remaining 2.6% from phone recharges - used less for criminal activities (probably related to the limited money associated with this type of transaction).

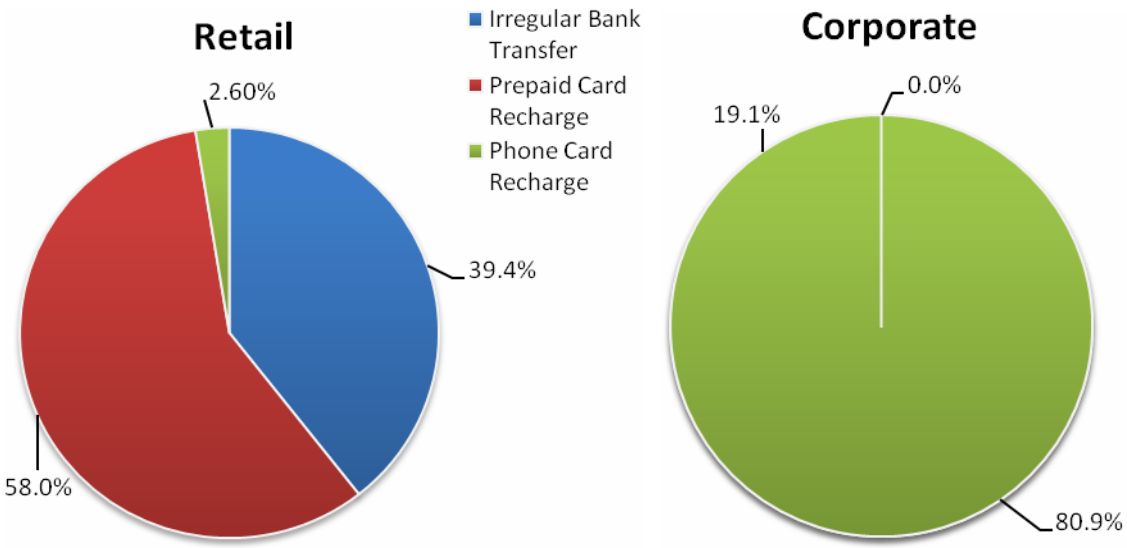


Figure 22 - Percentage breakdown of different types of effective transactions
Source: How to prevent and combat fraud on the Internet and Mobile Banking, ABI Lab, May 2014

The figures change for the corporate sector, where 80.9% of transactions are transfers, which are the most common type of transaction utilized by companies engaged in Internet banking. It is interesting to see the link between fraudulent transactions and the losses to corporate and retail clients, as well as the monetary value of these transactions. Despite a smaller number of fraudulent transactions (43.3%) committed against corporate clients, the monetary value of said transactions is 3 times larger than the amount stolen from the retail clients, 74.4% versus 25.6% of the total, respectively.

to about 77% of the employees and Retail accounts enabled and approximately 1.9 million active Corporate accounts. The data refer to the time period between 1 January and 31 December 2013 and are distinguished by customer segment, Retail or Corporate.

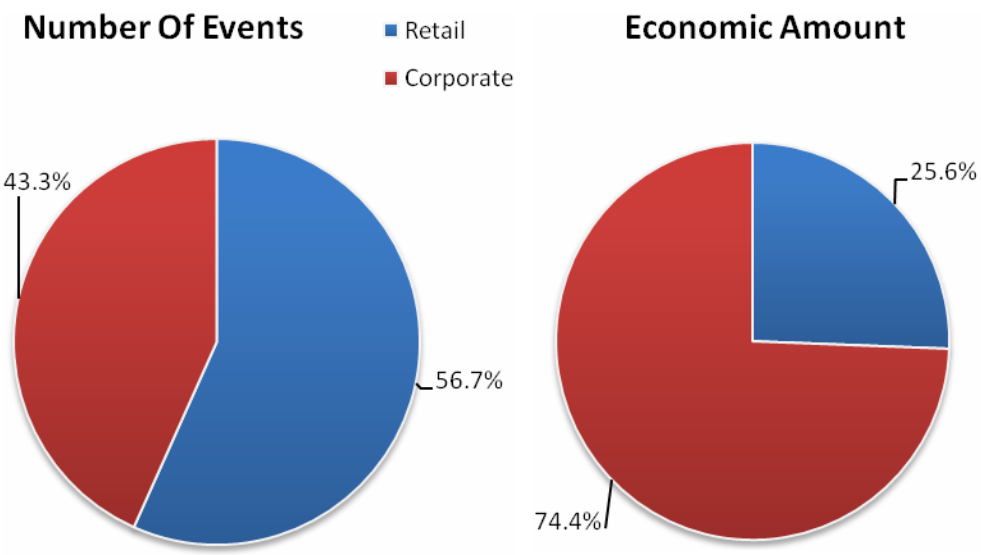


Figure 23 - The total effective transactions, divided by segments

Source: How to prevent and combat fraud on the Internet and Mobile Banking, ABI Lab, May 2014

3.4.2 Legal field

Following the 'Ratification and implementation of the Council of Europe's Convention on Cybercrime,' held in Budapest on 23 November 2001 and the adaptation of internal regulations[192] all cybercrime has since been tracked by the Prosecutor of the Republic. For this reason, we decided to conduct interviews with the Prosecutor's office, in order to better understand the issue and how these types of crimes are handled. The interviews with Deputy Prosecutor Alberto Perduca of the Prosecutor's Office of Turin and with Deputy Prosecutor Andrea Cusani of the Prosecutor's Office of Florence, both cybercrime specialists, yielded some interesting results.

There is no doubt that the web today represents an enormous opportunity for criminals. Economic transactions are taking place more frequently over the Internet, and, consequently, related predatory activities have moved to the web as well. The Internet also represents an enormous opportunity for companies, especially SMEs, which can cut the costs of many services through the Internet. In fact, many goods and services companies are moving their services to the Internet. Phishing, for both interviewees, represents almost the entirety of cases related to cybercrime that reach their desks. Phishing is almost a zero risk activity for those interested in financial crime. The problem is that the whole community - from citizens and companies to governments - are slow to adapt to the constant development of the web. According to Dr. Cusani, one of the greatest problems encountered is a huge difficulty in securing international collaboration to fight this type of phenomenon. The majority of cybercrimes are not generated by Italian perpetrators or from people residing within Italy, but primarily from Eastern European countries such as Bulgaria and Romania. Those countries, following the outsourcing of IT companies, have developed capacities that are now being utilized by cyber criminals. For these transnational crimes, once prosecutors are sure that the crime is being perpetrated from another

[192] Article 11, law n° 48/2008 published in *Gazzetta Ufficiale* n. 80 of 4 April 2008 - Supplemento ordinario n. 79, available at: <http://www.parlamento.it/parlam/leggi/08048l.htm> (retrieved 10-11-2014).

country, they need to ask for an international Letter Rogatory; this process is expensive and time consuming. In these cases, according to a realistic estimate, the country that receives the Letter Rogatory usually responds within 3 months. Considering the nature of cybercrime, this prolonged waiting period makes it hard to obtain useful and timely information. The average time for a Letter Rogatory to be processed is between six and nine months, but can take up to up to one year, or in some cases an answer is never received. Even one month of delay in this field is a huge amount of time considering the volatility of cyber data. According to Dr. Cusani, at the International and European level, there is too large of a technical competency and legal gap between countries, and this is one more obstacle in fighting this phenomenon. There are different sets of rules between countries, various offices and different procedures. Harmonizing everything and making investigations faster is very difficult. Eurojust, EC3 or other European instruments are a step in the right direction in the fight against cybercrime, but they are subject to a system of international relations based on polite declarations of cooperation as opposed to real and efficient pacts. The intent is admirable, but in reality there are processes that make the work extremely slow and complex. "*It is like chasing a thief with a Fiat 500 while he is escaping in the latest model of Ferrari,*" stated Dr. Cusani. Moreover, collaboration between countries with which there are no agreements, is obviously also quite uncertain[193].

Dr. Perduca, Deputy Prosecutor of Turin, is of the same opinion. His team generally works on fraud cases and on all cases of cybercrime that fall into the district's jurisdiction. For the Prosecutor's Office of Turin, there are approximately 4,000 cases per year, and they have a very low level of legal prosecution. Out of the 4,000 cases, 90% are dismissed. Before assigning the cases to a judge, half are dismissed due to a variety of procedural reasons: in the case that nobody is pressing charges, or if the charge is too generic and devoid of useful information, or if it concerns civil issues not addressed in court, or (more often than not) the cyber criminal cannot be found. In any case, especially in scenarios where an international Letter Rogatory is necessary, what is done is a simple cost-benefit analysis to see if prosecution is affordable.

This aspect has an enormous sociological relevance because what emerges is that the border between written procedural norms and practice can vary quite a bit, and the burden falls largely upon those tasked to uphold and interpret the law, legal norms and their application. The difference between practice and procedure is a common problem, as it the obligation to prosecute is often overlooked in various legal spheres. What happens regarding cybercrime is linked to a

[193] To contrast cyber crimes, an additional element to consider is the difficulty of determining the Court's jurisdiction since it is complex to determine the physical place where the crime was accomplished. In summary, the general rules of jurisdiction laid down by the code must be related to the individual case and therefore it is possible that for different crimes provided by law are raised different criteria for determining the territorial jurisdiction. For this reason the issue of determining the territorial jurisdiction in matters of cyber crimes cannot be tackled jointly. It is likely therefore that the applicable procedures of the different proxies for the competence can be different and also deviate sharply.

simple economic principle of being beyond the obligation to prosecute; a prognosis of failure is undertaken based upon a cost-benefit analysis.[194]

The cybercrimes logged at the Prosecutor's Office of Turin vary from unauthorized accesses to Facebook or social media in general (which are not crimes threatening wealth) to digital identity theft and online fraud. Deputy Prosecutor Perduca states that there is a steady stream of thefts from bank accounts caused by phishing and online money withdrawals using a variety of techniques, against which little can be done. This applies for reasons relating to the size of the single transfer (maybe only a few hundred euro) and for the speed of this type of offense - which makes it very difficult to investigate. What happens frequently is that the money is credited to an account or the pre-paid card of a person who does not really exist, is unreachable, or simply gives his details to allow the money to move. The classic scam perpetrated against companies, especially SMEs, consists of accessing the company email and stealing the list of clients and suppliers. Once in their possession, the hackers use the list to send an email to all the contacts telling them that the company has changed IBAN so the money needs to be sent to another IBAN, and in turn the money ends up in an account created by the cyber criminal. The client pays, thinking he is paying the right company - while the reality is that the account where he is sending his money is in another country. Usually these scams happen via phishing emails, where a client clicks on a malicious link or, in some cases, the criminals manage to crack the password of the account. The problem is in the fact that the attack can happen from anywhere in the world, and IP is not a reliable indication of location. For the Police Force and the Magistracy, this makes it very difficult to effectively fight the phenomenon.

Regarding intellectual property rights, the classic case refers to an ex-manager or employee who is fired or goes to set up his own business and steals all the data from the previous company - using the client list or accessing the company database. In the majority of cases it is an insider who accesses the system because their company accounts were not revoked. Crimes linked to hacktivism are few compared to attacks such as phishing or spear phishing, which represent real economic threats.

According to Dr. Perduca, there is a need for a larger system of prevention. Once a crime is committed, especially if it doesn't concern large sums of money, it is difficult for the current system to intervene effectively, taking into account limited resources, procedures and time needed, etc. The penal process of today is an oversized instrument in terms of costs and time. With more education and training we could increase the level of resistance.

As we know, the Postal Police is the specialized agency tasked to tackle cybercrime, but despite this, citizens and companies frequently also report crimes to the *Carabinieri* and other law

[194] For more details, see: *L'obbligatorietà dell'azione penale come un mito? Appunti sul caso italiano*, in M. Verga (edited by), Centro Universitario per le Ricerche sulla Sociologia del Diritto, dell'Informazione e delle Istituzioni Giuridiche (CIRSDIG), in "Quaderno dei lavori 2007, Terzo Seminario Nazionale di Sociologia del Diritto, A.I.S. – Sezione di Sociologia del Diritto", Working Paper n. 25, 2007, pp. 121-136, available at: <http://www.cirsdig.it/Pubblicazioni/capraia.pdf> (retrieved 11-11-2014); and Zanier M. (2009) *Tra il dire e il fare. Obbligatorietà dell'azione penale e comportamenti degli attori giuridici*, Macerata, EUM Edizioni Università di Macerata.

enforcement agencies. These police forces are not always equipped to handle statements of this nature, as they may lack the necessary training. Sometimes these statements are pasted on to the Postal Police, and in other cases, these police forces open there own investigations, but this entire process is often time consuming. Therefore, there should also be a basic training course for all police forces equipped to receive these types of statements. In doing so, the average level of preparation would be raised.

Thanks to Deputy Prosecutors Perduca and Riccaboni of the Prosecutor's Office of Turin, we were able to access and include in this report a case study concerning cyber fraud against an SME in Piemonte.

The case study relates to a company specializing in the production of animal feed. The clients of this medium enterprise are 90% foreign companies. Four companies from Asia, specifically from Hong Kong, Australia, Japan and Thailand all received an email, apparently from the Piemontese company, with an invoice for the exact amounts they owed the company, created in such a way that the accountants of the companies did not get suspicious. The email also included a change of the supplier’s IBAN (bank account number). Three out of four companies then transferred the money into the criminal’s bank account without making any inquiries. Only one out of four companies, perhaps due to company policy or suspicion of the non-Italian IBAN, called the company from Cuneo for clarifications and that is how they found out that there was a crime happening. Unfortunately, it was too late for the three companies who had already transferred more than 200,000 dollars. Following the establishment of the charges, the investigation started, but tracing the IP address was impossible. Finding out where the crime is being perpetrated from, as we have seen, is very difficult. In these cases, banks can provide some assistance by following the transfers. Following the request by the company for its bank to trace the transfers through the international banking system, it was discovered that the money was deposited in four different accounts in Tbilisi, Georgia. From these types of verifications, which are usually very efficient, especially between banks in more financially developed countries (which do not belong to the black list), it is possible to get an answer within 24/48 hours and thus block the emission or the transfer in the case of an investigation or fraud. In this particular case, Georgia does not belong to an international banking network so they responded several days later. It is plausible that Georgian banks were selected precisely for this reason.

From this information a Letter Rogatory was sent from Italy to Georgia, which usually needs to be in the language of the receiving country, in this case Georgian. Both parties agreed that it was okay to write the letter in English. Georgia answered the Letter Rogatory in a relatively short time (in more or less 3 months) and sent a dossier in Georgian. After some difficulty in locating a translator, it surfaced that the company was in contact with a young man who helped them translate food labels in Georgian. He managed to translate the response to the Letter Rogatory, from which it emerged that the receiving bank accounts belonged to three men of African origin whose documents were attached to the Letter Rogatory. In this case, Georgia was quite quick in responding to the Letter Rogatory as they had an important investigation on money laundering going on - which confirmed that the money went to the accounts in question. The

documents identified the three suspects as nationals of South Africa, England and Guinea. Based on this information, the Prosecutor's Office of Turin sent letters asking for information from the three countries, but only received a response from England informing them that the passport was a fake. They have yet to receive any response from the other two countries. If the Prosecutor's Office does not get answers from Guinea and South Africa, or if they were to respond that the passports were also fakes, the process would stop and the case would be archived against unknown perpetrators.

It is worth noting that in this case the companies not only received an email with the same letterhead and details of the Piemontese company, but also that the invoice had the exact amount that they were supposed to pay. This means that the Italian company suffered a cyber attack that they were not aware of, and nothing surfaced from the investigation regarding this. In order to not lose or damage the relationship with their Asian clients, the company reached agreements with them to split the losses.

Dr. Riccaboni says that unfortunately cases of cyber fraud and the theft of sensitive data are increasing. Cyber criminals are specializing in this type of fraud against which little can be done. The only cases for which it is perhaps more probable to get results, from an investigative point of view, are the cases of tampering with ATMs in order to clone cards. This type of crime requires the physical presence of the criminal close to the ATM and, as such, the criminal can be caught on camera and perhaps fingerprints or other traces make it possible to find the perpetrator.

Recently, the Public Prosecutor's Office of Turin received a case regarding a company in the chemical sector, very similar to the one illustrated above, with the difference that the initial violation had presumably happened to a client company in India, which received a spear phishing email quoting a change in IBAN. The transfers for the amount of 40,000 euro were accredited to an account in a bank in Turin belonging to a Nigerian person. A search and investigation on the suspect's PC yielded nothing. Through collaboration with Google and Yahoo, email providers the criminal used to create the false addresses, it was discovered that the emails were sent using a mobile device. The investigation is still on-going.

It is clear that cybercrime constitutes a risk that should not be underestimated by SMEs. Domenico Raguseo, European Security Systems Technical sales and Solution Manager at IBM, is of the same opinion. According to Mr. Raguseo, being a victim of fraud "*is not a problem of just big companies for whom it could be damaging to their image or reputation and the damage could be greater than that of an SME in absolute terms - but for Small and Medium Enterprises a cyber attack can put the survival of the company in jeopardy.*" Regarding preventing, identifying and responding to attacks: *"It becomes,"* according to Raguseo, "*an intrinsic benefit for SMEs, as important as oxygen is for a human being. Prevention is the most important part. Attacks now are more and more sophisticated and with an increasing duration*". It becomes vital to also know how to identify attacks, as these "*are designed and built specifically for the particular target they want to attack.*" Attackers have an enormous advantage because they know their victims, and the technology they use, very well. On the other hand, potential victims must defend themselves against an array of complex, and often little understood, cyber threats. Finally, it is important to keep in mind that

"*you can't consider an attack as a remote possibility - limiting the impact and containing an attack is therefore important and possible*".

CHAPTER 4

FOCUS ON THE PROVINCE OF LUCCA

4.1 Characteristics of the Territory and of the SMEs in the Province of Lucca

In order to conclude with a study which would not only give us indicators of the cybercrime phenomenon, but also provide us with qualitative information useful to make us understand which industrial assets are more at risk, and the steps needed to prevent possible effects, and what level of awareness has been reached in recent years regarding this phenomenon, we chose to conduct a series of semi-structured interviews with companies representative of the area in question, institutional actors and Police Forces tasked with fighting cybercrime.

Let us now examine some elements in order to better understand the characteristics of the territory. The Province of Lucca is the third most populated in the Region of Tuscany, with 372,244 inhabitants[195] and has 38,584 enterprises active within its territory. The workers, divided by enterprise size, are as follows: 57.1% are employees of micro enterprises (less than 10 employees), 23.4% are workers in small enterprises (between 10 and 49 employees), and 13.2% are employed by medium enterprises, while 6.3% are employees of enterprises with 250 or more employees. 93.7% of workers in Lucca Province are employees of Micro, Small and Medium Enterprises[196].

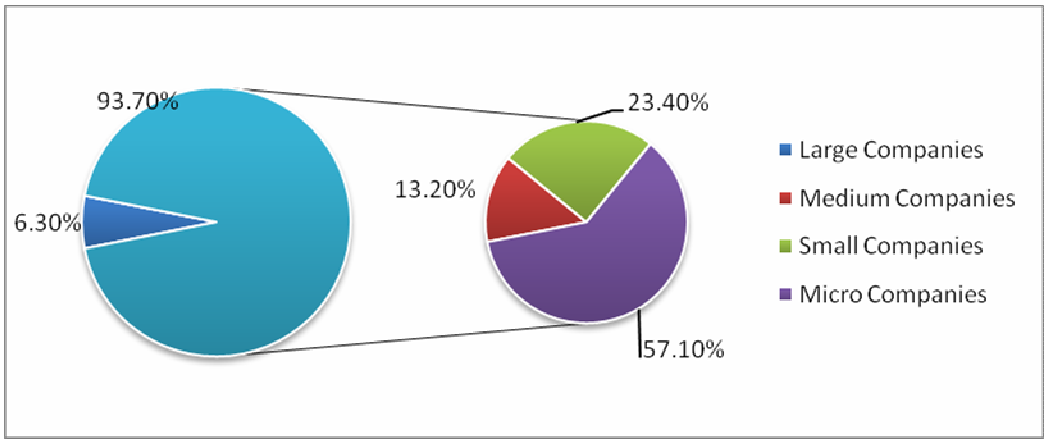


Figure 24 - Workers divided by size of enterprise year 2011

Source: L'Italia delle Province, Servizio Studi e Ricerche Industry and Banking of Intesa Sanpaolo, 2014

[195] Resident population in the Province of Lucca in 2001 Census - data by municipality. "*Elaborazioni Provincia di Lucca su dati ISTAT",* available at: <http://www.provincia.lucca.it/economia_occupazione/popolazione.php> (retrieved 11-11-2014).

[196] *L'Italia delle Province. Lucca Settembre 2014,* provided for this research by Servizio Studi e Ricerche Industry and Banking of Intesa Sanpaolo.

The percentage listed above is slightly larger than the national average, and is representative of the situation in the regions in central Italy. From the statistics, given to us by the Industry and Banking Study and Research Service of Intesa Sanpalolo bank (*Servizio Studi e Ricerche Industry and Banking di Intesa Sanpaolo)*, we can see that the economic value of exports of the companies in Lucca Province is twice that of imports, and the sector with the largest percentage of exported goods is that of paper[197], with 23.9%, followed by mechanical, other transport vehicles, leather and shoes, respectively at 17.2%, 13.7% and 9.1%. The paper sector of the Lucca district is quite important for the province; it includes more than 100 companies with sales of almost 3.5 million euro and employs more than 6,500 people. The number reaches more than 14,000 if we consider satellite activities. The district is responsible for almost 80% of the national production of tissue paper, which represents 17% of the total European figure. More than 80% of the exports of this district are destined for European markets, while for the mechanical sector the figures are more homogenous, 38.7% for Europe, 28.2% for North and South America and 33% for the rest of the world.

As can be seen from these figures, the Province of Lucca reflects the typical picture of industrial assets in central Italy. The vast presence of Micro, Small and Medium Enterprises with a vast know-how and high level of commercial relations abroad, makes this area appetizing for cyber criminals.

4.2 Consorzio Bancomat Data

Cybercrime is a fringe risk for the ATM Consortium (*Consorzio Bancomat)* as they only collect information about attacks on ATMs. Having an IP connection directly connected to the bank's network, the attacks are probably not designed to interfere with the transaction, but probably aimed at infecting the Bank's network.

The Consortium logs attacks and collaborates with Police Forces as well as participates in various groups and technical subgroups for the creation of the Automated System for the Prevention of Fraud on Bank Cards (*Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento* SIPAF), and is a national member in the European ATM Security Team (EAST), an international consortium for the management of ATMs. Within the ATM Consortium there is an anti-fraud centre, which conducts checks on the whole network of stakeholders and shareholders. This centre put in place fraud monitoring mechanisms through which banks and services flag, through real time apps, any ATM tampering attempts or other types of fraud, which are then logged in SIPAF.

[197] Back to grow the export of paper district of Capannori (+2.5% result for the third trimester of 2013), *Monitor dei Distretti Toscana Trimestrale – n. 15 Intesa Sanpaolo January 2014 Servizio Studi e Ricerche Industry and Banking* edited by: Stefania Trenti, available at: <http://www.group.intesasanpaolo.com/scriptIsir0/si09/contentData/view/content-ref?id=CNT-04-00000001B77B2> (retrieved 12-11-2014).

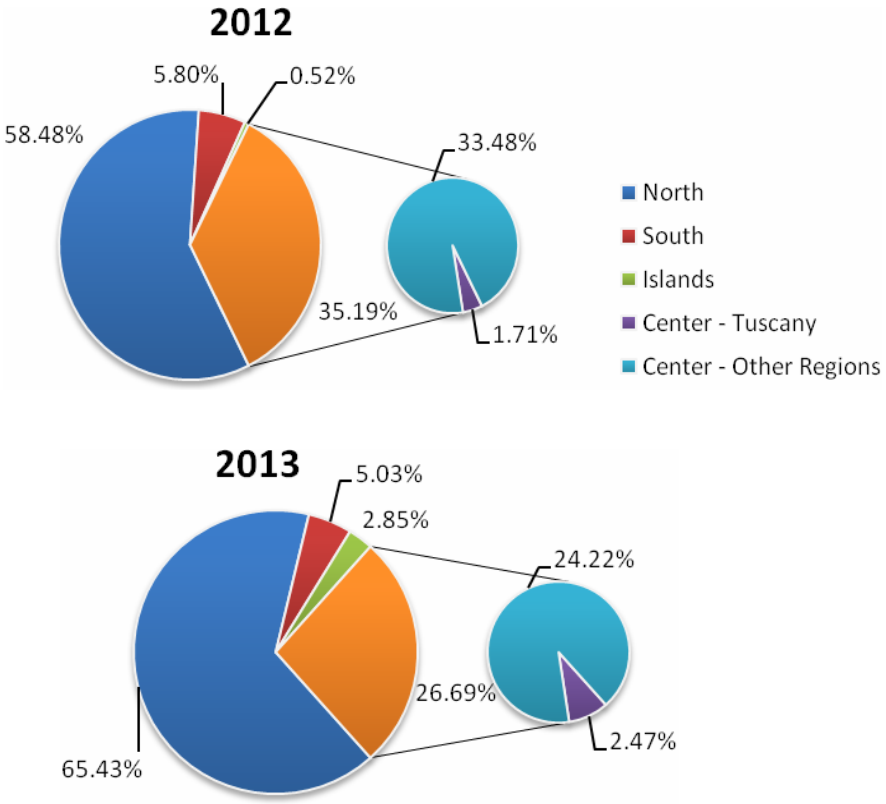


Figure 25 - Distribution of percentage of tampering per geographic area
Source: Statistics of fraudulent attacks, Centro Antifrode Consorzio Bancomat

Because it is a domestic circuit, it can only transmit within Italian borders, as such the ATM Consortium is only marginally affected by transnational cybercrime, in the sense that the cards can only be used in Italy. However, ATM cards often share the same platforms with other circuits, such as Visa, MasterCard etc., so when the tool is compromised there is a loss in their system as well.

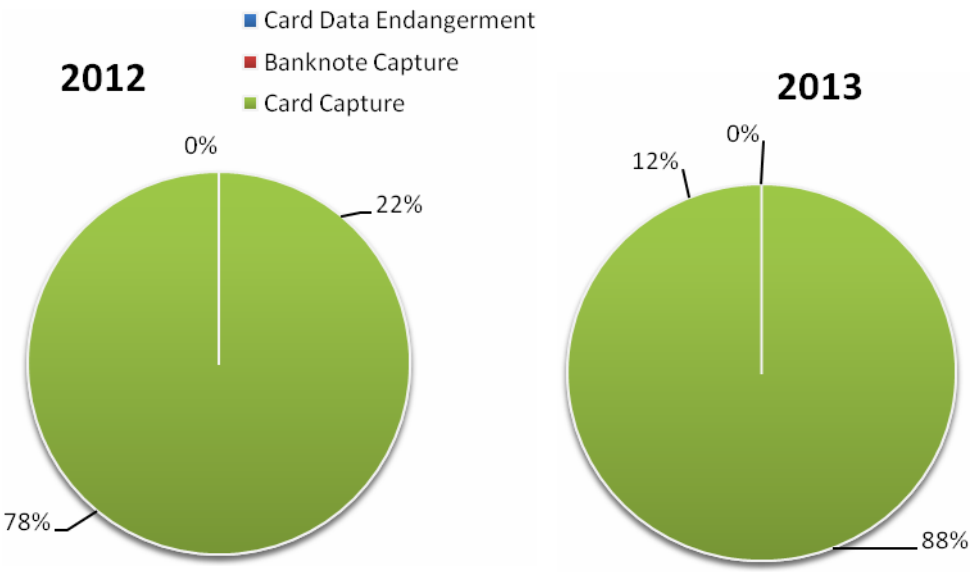


Figure 26 - Distribution of the attacks in Tuscany Region
Source: Statistics of fraudulent attacks, Centro Antifrode Consorzio Bancomat

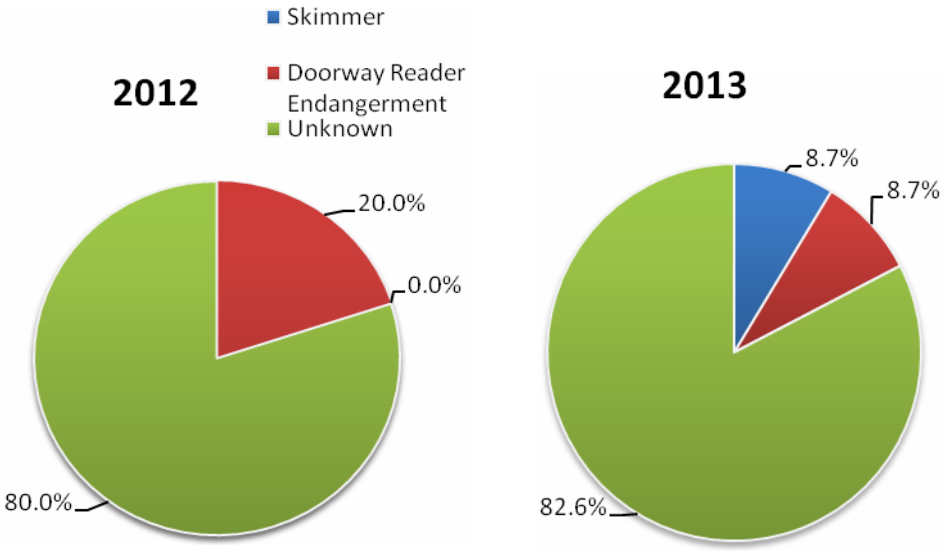


Figure 27 - Type of tampering, damage to card data
Source: Statistics of fraudulent attacks, Centro Antifrode Consorzio Bancomat

At the moment, the circuit is sufficiently protected by the current norms. Problems arise from transactions where a "card is not present," in other words for transactions done through the internet or web. For these scenarios, there is a lack of legal support, the subject matter is not clear and there are some gaps that need to be addressed.

4.3 Analysis of the interviews conducted in the Province of Lucca

4.3.1 Interviews conducted with representatives from Law Enforcement Agencies

In order to evaluate the cybercrime phenomenon in the Province of Lucca, we chose to conduct targeted interviews with two members of Law Enforcement Agencies in Tuscany, Franco Bozzi, Chief State Police Inspector at the Prosecutor's Office within the Court of Lucca (*Ispettore Capo* of *Polizia di Stato* at *Procura della Repubblica al Tribunale di Lucca)* and Stefania Pierazzi, Deputy Comissioner of the Postal and Telecomunications Police of Florence (*Vice Questore Aggiunto*[198] *della Polizia Postale e delle Telecomunicazioni di Firenze).*

As illustrated in the previous chapter, since 2008, following the Ratification of the Convention of Budapest, all cybercrimes are followed at a district level[199]. In Tuscany[200] this is done by the Prosecutor's Office (*Procura)* of Florence, where all charges collected by all law enforcement agencies converge, regardless of the fact that the Postal Police is the most equipped body to investigate these types of crimes. For this reason, we decided to conduct our first

[198] The full interview with Dr. Pierazzi is attached in the methodological appendix.

[199] Article 11, law n° 48/2008 published in *Gazzetta Ufficiale* n. 80 of 4 April 2008 - Supplemento ordinario n. 79, available at: <http://www.parlamento.it/parlam/leggi/08048l.htm> (retrieved 10-11-2014).

[200] At the district level in Florence, complaints from all the provinces of Tuscany are managed, except Massa-Carrara, which is included in the district of Genova.

interview with Dr. Pierazzi in order to understand, from an investigative point of view, the observed trends of cybercrime in the last few years. Dr. Pierazzi states that cybercrime is steadily increasing; registering a real escalation, especially in the last 3 or 4 years. Phishing and spear phishing have now reached their highest peaks ever. These, however, are not considered crimes by themselves, but only if combined with an unauthorized access to an IT system with the objective of stealing data and bank credentials of an individual or a company of any size and using them to conduct transactions. "*This trend doesn't show any signs of decreasing, it continues to develop in a constant manner over time*", stated Dr. Pierazzi.

Parallel to the increase of cyber-attacks, the tendency to rely on the competent authorities has also increased. Dr. Pierazzi, who has been working on this phenomenon for the past 15 years, noticed a real evolution taking place: "*in the first years there was a lot of embarrassment in declaring these types of crimes […] then with time it became a more and more common type of crime and people started realizing that being the victim of an attack does not diminish or tarnish your image, and does not make an individual or a company less credible. Now victims report more easily, even large companies are not afraid to go to the police to make their statement as victims of cybercrime. This surely happens a lot more than in the past.*"

A decade ago, the Postal Police heard, through the statement of a small company in Prato, about an attack directed at Google which involved several Florentine companies. Thanks to that statement, it was possible to reconstruct the size and type of the attack and find out that several other companies were involved, including some big companies. Four or five years ago a reversal of the trend occurred, thanks in part to the fact that we are talking more about this type of crime, companies are beginning to understand that it is a phenomenon that touches many and this also shows, as reported in the interview, a good level of trust towards law enforcement agencies by victims. The Deputy Commissioner (*Vice Questore)* stated that it is rare to find distrust towards them and that the victims usually collaborate fully, accepting advice, and providing their information freely.[201]

Unfortunately, it is also necessary to consider that it is true that the users rely on law enforcement agencies, but they are still not aware of the problems related to investigating this type of phenomenon, thinking that the problem can be solved quickly in the case of fraud on platforms such as e-bay, subito.it or other similar entities. The interviews, with Inspector Bozzi and Dr Pierazzi, also confirm this fact and illustrate that it is very difficult to identify those responsible for the attack because "*usually the criminals are very prepared, so they use a system that allows them to not be identified, all they have to do is use a proxy and they immediately become untraceable, or at least the attack will seem like it happened from a server abroad at which point the investigation will pretty much stop*."

As illustrated in the previous chapters, the international nature of cybercrime makes it more difficult to conduct investigations. Often the attacks come from countries which do not belong to the European Union, with whom there isn't reciprocity and an international relationship, and rogatory letters are not always activated. Moreover, in situations where one is activated, the

[201] As confirmed by: *Cyber security Report* Special Eurobarometer 404, 2013, European Commission, pag.77, available at: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf> (retrieved 6-11-2014).

necessary time to conduct the process is too long compared with the volatility of the information necessary to conduct an investigation. Regarding this, Dr. Pierazzi admitted "*Speed is of the essence in this type of crimes. They are very difficult. If we move immediately we might be able to do something, otherwise, no*." Even though there is international collaboration at an investigative level, there is a need to create a dossier and there is a need to follow standard procedures, such as use of the international rogatory letter, which are complex and tend to extend the timeline of the investigation.

Unfortunately, the damage resulting from these types of attacks is not to be underestimated. The cases recorded by the Postal Police of Florence vary from phishing and spear phishing, where there is a purely economic loss, to data loss, patents and client list theft, which are types of damage which can only be quantified at a later date. Official data, provided to us by the Postal Police Distict of Florence[202] *(Compartimento della Polizia Postale di Firenze),* relating to last year, is of 711 fraud charges, 231 unauthorized access charges and 92 cyber fraud charges.

Several interesting aspects emerged from the information provided for this research by the Chancellery of the Prosecutor's Office of Florence (*Cancelleria della Procura della Repubblica di Firenze)* related to the recorded cases in the last 3 years, not only by the Postal Police, but also by other law enforcement agencies, such as the *Carabinieri* or *Guardia di Finanza*, according to Articles 615 Ter cp[203], 615 Quater cp[204], 640 cp[205] and 640 Ter cp[206].

[202] We consider that the cases reported to the *Polizia Postale* are just part of those actually reported because many may be reported to, and sometimes even managed by, other Police Forces.

[203] Art. 615 ter codice penale. Offense of unauthorized access to an IT system "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".*

[204] Art. 615 quater codice penale *"Chiunque, al fine di Procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si Procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro".*

[205] Art. 640 codice penale. Offense of fraud "*Chiunque, con artifizi o raggiri, inducendo taluno in errore, Procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da cinquantuno euro a milletrentadue euro*".

[206] Art. 640 ter codice penale. Offense of cyber fraud "*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, Procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032".*

PROCURA DELLA REPUBBLICA OF FLORENCE				
Lawsuit	**Year of Registration**			
Arrived	**2012**	**2013**	**2014 (up to 27/10/2014)**	**Overall Total**
Known Mod. 21	**1.723**	**1.817**	**2.404**	**5.944**
Art. 615 Quater cp	19	30	46	95
Art. 615 Ter cp	246	339	574	1.159
Art. 640 cp	1.233	1.144	1.258	3.635
Art. 640 Ter cp	225	304	526	1.055
Unknown Mod. 44	**2.963**	**4.176**	**6.714**	**13.853**
Art. 615 Quater cp	50	47	41	138
Art. 615 Ter cp	991	1.701	2.940	5.632
Art. 640 cp	938	864	1.127	2.929
Art. 640 Ter cp	984	1.564	2.606	5.154
Overall Total	**4.686**	**5.993**	**9.118**	**19.797**

Table 6 - Procedures arrived against known and unknowns according to Art. 615 Ter, 615 Quater, 640 and 640 Ter
Source: Based on data provided for this research by Repubblica of Florence, years 2012, 2013 and 2014

PROCURA DELLA REPUBBLICA OF FLORENCE					
Lawsuit	**Year of Resolution**				
Resolved	**2012**	**2013**	**2014**	**Pending at 27/10/2014**	**Overall Total**
Unknown Mod. 44	**2.563**	**3.696**	**4.317**		**10.576**
Art. 615 Quater cp	28	64	36		128
Art. 615 Ter cp	715	1.457	1.758		3.930
Art. 640 cp	938	847	848		2.633
Art. 640 Ter cp	882	1.328	1.675		3.885
Known Mod. 21	**1.532**	**1.930**	**2.051**	**131**	**5.644**
Art. 615 Quater cp	10	14	41	2	67
Art. 615 Ter cp	195	351	456	5	1.007
Art. 640 cp	1.129	1.223	1.099	124	3.575
Art. 640 Ter cp	198	342	455		995
Overall Total	**4.095**	**5.626**	**6.368**	**131**	**16.220**

Table 7 - Procedures resolved against known and unknowns according to Art. 615 Ter, 615 Quater, 640 and 640 Ter
Source: Based on data provided for this research by Repubblica of Florence, years 2012, 2013 and 2014

From 2012 until today, it has been possible to notice that crimes related to cyber fraud (Art. 640 Ter cp) have gone from one third of the total fraud cases to more than half today. Another observable fact is that in the last three years, while fraud crimes (Art. 640 cp) have been more or less constant, or register a slight increase, those related to cyber fraud have increased considerably, especially those against unknowns which have reached 2,606 cases. This enormous disparity between the procedures for cyber fraud against unknowns and those against known entities is symptomatic of this type of crime, in which it is very difficult to trace back the perpetrator. These figures obviously refer to those cases in which the victims pressed charges, and

do not consider all those cases in which charges were never pressed, or where the victim never noticed the attack. To have a more statistically accurate picture, it is necessary to conduct further investigations within the enterprises.

As far as the companies are concerned, another element which surfaced from the interviews that makes it difficult to even notice if you were a victim of an attack, is that cyber criminals study the correct amount of money to ask for so as to make the request realistic and reflect the usual size of transactions. This tactic makes it difficult to detect anomalies by the banks and the companies themselves. The stolen amounts usually seem to correspond to the volume of business conducted by the company. The stolen sums are normally between 30,000 and 70,000 euro for a large company, and 500 euro and above for an SME. These attacks of a modest nature, perhaps repeated over time, rely on false orders, false invoices or by modifying banking information.

An interesting fact that surfaced from both the interviews with Dr. Pierazzi and Inspector Bozzi, is the difference of the attackers in relation to the crimes. These crimes range from purely economic crimes, such as phishing and fraud, to those related to violations with the objective of stealing reserved data. In almost all cases, the first type of attack is external to the company, while the second, more often than not, involves people from within the company, disloyal employees or disgruntled ex-employees who steal information either to hurt the company or to somehow benefit from that information. For example resell this information to criminals or start their own business, stealing know-how, customer lists, projects and patents. Among the latter, Dr. Pierazzi mentions one case which occurred years earlier in which former employees of a pharmaceutical company in Tuscany stole the recipe of a drug not yet patented and formed another company.

It is clear that both types are considerable risks for SMEs, for whom an economic fraud could cause heavy damage, and more importantly in this period of economic crisis, could put the actual survival of a company in jeopardy. SMEs very often base their business on patents, excellence, exclusive use of a specific brand and business contacts, the loss of which could be catastrophic.

However, the awareness and preparation of SMEs is still quite low. Today, they are the companies which are most exposed to risk. Small and micro enterprises tend to have obsolete PCs or do not update their hardware or software, and have few or perhaps no IT technician dedicated to security. To this we can add PCs always connected to the internet through modems which are always connected and without antivirus software or firewalls, or perhaps not updated or correctly configured.

From a technical standpoint and the maintenance of protection tools cyber security is surely a large economic investment for SMEs, but on the other hand it also requires the activation of company security policies, which can be implemented at low prices or for free. *“More often than not, they wait until their first attack before they run for cover,”* states Dr. Pierazzi, *“sometimes there are some simple things that could be done, such as changing passwords. For example if an employee who used to manage the administration leaves the company, it would be advisable to at least change the passwords and deactivate the account, but usually nothing is done for months. Sometimes there are things that wouldn’t cost anything; it might be beneficial to invest in an employee who would take care of these kinds of things, but rarely is this the case with*

the possible exception of large companies". An interesting case recounted by Inspector Bozzi during the interview for this research paper confirms what has been said. It refers to an SME in the Lucca area which suffered an attack because of a type of malware known as ransomware through which their administrative files were encrypted and a ransom of 1,000 euro was required to decrypt the files[207]. The company in question did not have an adequate security system, did not perform frequent backups and always did so on the same hard disk. Due to the difficulty of conducting an investigation, the company decided to pay the ransom[208]. The IT consultant of the company then tried to implement a solution for the future, but before he could do so, the company was once again the victim of another ransomware attack, probably by the same cyber criminals which attacked them the first time, but this time they requested a smaller amount.

From this case we can understand the intelligence of cyber criminals in tailoring their monetary requests to make it more convenient to pay rather than go the route of a law enforcement investigation. Furthermore, given the ease of action, it is plausible that it might be more profitable for cyber criminals to ask for a low ransom from more than one company, since this type of attack has a high ROI. Another shocking factor from this episode is that despite having been a victim of this type of attack, the capacity of the company to put in place protective measures was practically non existent, so it was not able to avoid becoming a victim again. The level of awareness is still so low that it doesn't allow for the identification of the most basic prevention mechanisms. Regarding the second attack, however, having performed the weekly backup, the company decided not to pay the ransom and accepted that they lost the data following the last backup.

As we were told by Dr. Pierazzi, the cybercrime phenomenon, in any case is cross cutting. Based on the charges that have been filed, tips given and the cases that have been followed, cybercrime doesn't strike a particular type of company, but it indiscriminately attacks any company, not only those in the IT sector or those which produce highly specialized goods. Now even the smallest companies have computerized at least their economic management, usually without considering the possible cyber risks they might encounter. Dr. Pierazzi stated that "*sometimes it seems that they really don't understand how vulnerable their systems really are.*" "*Sometimes they are more aware, but they still wait until some losses are incurred before putting any counter measures in place*". The interviews also highlighted that there is no type of information sharing between the companies in this field. Dr. Pierazzi confessed that, some years ago during seminars on the use of POS (Point-of-sale systems) organized by National Confederation of the Italian Traders (*ConfCommercio)* of Florence, it was noticed that the business owners and the SMEs were really uninformed and as such were completely vulnerable.

Both interviewees, when asked what tools they thought were the most effective to counter this phenomenon, highlighted the strategic importance of the cultural aspect and the value of training. What Dr. Pierazzi states concerning what is more useful for SMEs to defend themselves is

[207] In this case the cyber criminals were Russian. Russia is a country with whom there isn't a high level of cooperation with regard to cybercrime.

[208] Among other things, the company in this case obtained, following payment of the "ransom", the decryption of the data by criminals. Which does not always happen.

quite representative: "*Knowledge. Absolutely... also because a lot is based on social engineering. Man versus man. It is true that there is a machine in between, but there is a man in front of that machine. I think that the preparedness of the user, the client, the employee, is crucial. First and foremost it is important to be aware of the risks, so as to prepare even the last of the employees to face said risks, and not make stupid mistakes, such as accessing malicious sites which can infect the system. There is a need for awareness about and training on cyber tools, because there is a presumption that this tool is easily manageable. It is deceiving because it gives you the opportunity to do everything immediately. IT is amazing, really, it allows you to do some amazing things, I believe that it is truly amazing, but you have to approach it with a bit of slyness and don't rely on it with your eyes closed.*"

4.3.2 Interviews at companies

An integral part of this research was to find companies that could be representative of the Lucca territory and to conduct interviews which could yield the necessary information to understand the current status of SMEs in relation to cyber security, awareness of cybercrime and the necessary tools to face the risks associated with it. Given the characteristics of the province, we decided to interview a company with advanced know-how in machinery for the processing of marble, two paper mills in the most important district in the area and two IT companies.

Giorgini Maggi is the oldest company[209], specialized in the building of machinery for the processing of marble, stone and granite. Composed of 10 employees with 5 desktop PC stations, it has always had direct contact with its clients all over the world. The company receives, as do most commercial activities, numerous spam e-mails, along the lines of 50 per day. They rely on a local external company to provide them with e-mail service and website management. During the interview a very important element surfaced regarding an indirect experience they had had with fraud. In June of this year, Giorgini Maggi was expecting a transfer from a Greek client who is usually very punctual in his payments, so they contacted the client to see if there were any problems. They found out that the client had made the payment, but utilized a different IBAN which he had received through an e-mail from the Tuscan company. The e-mail in question was quite good, written in perfect English, with all the right references, colors and company logo, and it communicated the change of IBAN for future invoices. The amount stolen by the cyber criminals was around 4.000 euro, and luckily the client, due to a long standing relationship with the company, did not interrupt his working relationship with them. We do not know if the initial violation, which made this fraud possible, happened within the interviewed company or within the Greek one. In any case, an attack of this kind, in addition to resulting in economic losses, can also destroy the trust between SMEs. Fortunately, the company we interviewed has always kept sensitive data, and the patents for the machinery they make, on a separate computer, which is not

[209] Its origin, in fact, dates back to 1865. The company is located in Tuscany in the historical area of the white marble from the Apuan Alps where Michelangelo began his rigorous activity of marble extraction devoted to the creation of his masterpieces.

linked to the internal network and without access to the internet. Since the June event, before which the owner never thought she could have ever been a victim of cybercrime, Giorgini Maggi started a policy of changing their alphanumeric passwords every 15 days. They would like to do more for their cyber security, but they complain that they did not receive support and information on this issue, especially from the company that manages their e-mail.

This type of fraud, as we have already seen in the case illustrated in the previous chapter, is very widespread nowadays, and it is a type of targeted attack that is harder to identify than the classic form of phishing. This type of fraud is usually designed very well, has the name of the client or supplier, the related logo and invoicing information and is sent to an e-mail address deemed reliable, so without a specific check on the new IBAN or a phone inquiry of the change of IBAN, it is easy for companies to fall into the cyber criminal's trap. It was quite important to find this anecdote within the interviews, as it shows how this type of crime is not far from the world of micro enterprises which make up the economic fabric of Italy.

Following the first interview, we conducted interviews at two paper mills in the area. The two companies are of a medium-large size, and they too have both Italian and International clients. The companies in question, Industria cartaria Pieretti (ICP) and Lucart, are companies which have been dealing with cyber security for several years. Both companies have IT departments, which among other things, also deal with cyber security. They are both well-structured and have a policy of obligatory changing of alphanumeric passwords every three months for all their employees.

ICP is a company with 110 employees and clients in 60 countries, mainly in Europe, the Middle East, the United States and South America. In the paper sector since 1924, they have an IT manager who takes care of hardware, networks, connections, computers and other tools, backup, and configuration. There is also an employee responsible for internal software, Enterprise Resource Planning (ERP) and various products. Last but not least, there is also a telecommunications expert who handles marketing. The three employees are managed by Dr. Tiziano Pieretti, CEO of the company, with whom we conducted the interview. ICP represents a great example pertaining to cyber security, as it has implemented company rules on the correct use of their IT system, as well as developing a Business Continuity Plan, which is periodically verified and updated, and it respects the norms on managing personal data[210]. ICP has established an awareness in terms of security that goes well beyond the current norms. The company has also adopted quite restrictive IT policies. To this regard, even Dr. Pieretti says "*maybe we are the extreme opposite of the average, we are too careful, but if the alternative is the other then I think this is better*".

What they fear the most is the damage that an attack can cause to their systems, such as stopping production or damaging the ERP server, which would block the entire company for days.

[210] Data handling, both personal and sensitive (depending on the management of administrative tasks) within industria Cartaria Pieretti SpA is carried out following the provisions of the Decree of 30 June 2003, n. 196 following the arrangements in accordance to the technical regulations regarding minimum security measures (Annex B).

Losing one day or 12 hours to perform disaster recovery, or stopping shipments or transports is a luxury they cannot afford.

Lucart is a large sized and well-structured company[211] that has between 300 and 350 computer workstations in Italy and at least another 200 in France, all managed by the IT department located near Lucca. The company declares that it increases the budget dedicated to cyber security every year, this in addition to the expansion of the IT department in recent years. The ICT Manager believes that their level of protection according to their standard is today at 60%, but they are confident they will bridge the remaining gap in a short period of time. In addition to an increase in budget in recent years, their attention towards cyber security has also increased.

Both interviews highlighted that a restrictive security policy is not always understood and positively received by employees. "As a reaction to the limitations to web usage we received a variety of comments and concerns. There are those who hoped for it, those who understood the idea behind it, and those who complain because they do not understand," revealed ICT Manager Dr. Burresi.

"There are two types of companies," declared Dr. Pasquini, "those which already have a certain type of culture and those which are waiting to hit their head."

The last two companies interviewed are companies in the IT sector, selected for a technical opinion related to their experience with other companies within their territory and beyond.

Lucense is a non-profit consortium company, established in Lucca in 1984 with the participation of public institutions, banks and foundations, and trade associations. Its activity was geared towards the development of the economic system in the area, but over the years the market of Lucense has progressively expanded until it reached national proportions, and for certain activities even an international dimension. Since 2010, Lucense has been a research body and performs industrial research activities, experimental development, technology transfer and dissemination. Lucense has been operational since 1986, also as a technology player within the ICT sector by designing and building websites and software for the web, applications for mobile devices and multimedia installations, developing and managing networks and IT systems. Since 1995, they have also been an Internet Service Provider through their LUNET brand, and they provide hosting services, internet radio connections and cloud computing solutions. Mr. Landucci, interviewed for this research paper, stated that in the last two or three years, there are increasing reports of phishing e-mails from companies that have their domain at Lucense. The interview highlighted that recently a company belonging to the shoe sector, following an order from China, almost became a victim of spear phishing in a very similar way to the case studies analyzed in the previous chapters. Lucense often recommends its clients periodically change their passwords and to implement at least the minimum required security policies, but what they find is that there is an incredible difficulty at a cultural level, "*The attention towards simple things such as a complex passwords, seem difficult to make part of company habits*", confesses Mr. Landucci. The majority of DDoS or defacement cases are the result of the default password never being changed from

[211] Company with 1,400 employees and an IT department managed entirely in Italy. The branches in Italy number five, plus two in France. The IT department has been in existence for 20 years and currently consists of 11-12 people.

"admin". For this reason, Lucense has been including, in the applications designed by them, a mechanism for obligatory password changing every 90 days, but not for the e-mail domain as the policy was not tolerated by clients. When safeguarding sensitive companies' data within their servers, Lucense has devised a restrictive security policy that includes historic backups based on the client's needs on encrypted servers. The interview revealed episodes of defacement on some of the websites hosted by them, nothing targeted or with a particular objective, but can be traced back to Russian and Iranian hackers with low skills and only engaged in the activity as a challenge. But cases such as these, according to Landucci, do not constitute a true danger for SMEs, which frequently notice defacement on their sites only months later; the real danger is represented by phishing and spear phishing, which can cause considerable economic losses. But even in this interview, the low level of awareness of SMEs regarding this phenomenon surfaced again.

The average Lucense client, especially in this period of economic crisis, is not inclined to invest money in security and prefers to run the risk of incurring damages as a result of a possible attack, underestimating the dangers that may stem from it. It is not rare, according to Mr. Landucci, for Architects not to protect their project designs for upcoming tenders, "*without considering how much it would cost them if the design was lost*." Some Lucense clients complain about the speed of their connection, blaming the provider for poor performance, but not noticing that this slowing down is caused by an unauthorized use of the net by an employee who, perhaps during office hours, downloads dubious material which might include viruses that could infect the company's system.

When asked what could be useful to fight this phenomenon, and in line with the other interviews conducted, Mr. Landucci confirms the need to conduct seminars for companies and trade associations, during which even the practical aspects could be discussed, with demonstrations to companies that show how easy it is to conduct a cyber-attack. Over the years, Lucense, itself, has organized seminars on cloud and disaster recovery, every 2 or 3 months, with poor turnout. "*A seminar could be a good opportunity to breakdown the wall of silence and improve on the low level of information sharing regarding this topic*", concluded Mr. Landucci.

The second company interviewed from the IT sector is Tagetik, founded in 1986 and recognized in the software solutions market for the Corporate Performance Management (CPM) and the Business Intelligence (BI) that in recent years recorded one of the fastest rates of growth in its sector. Targetik has more than 600 clients worldwide, the majority of whom are abroad in Europe and overseas. Targetik has various branches in Italy, Europe and the United States. Five or six years ago their cloud department, which saw a doubling of its personnel from 3 to 6 units, has also been active. The IT department, which takes care of the management of IT systems, is composed of 4 employees.

Dr. Santo Natale, the Manager for the Cloud team, and Dr. Matteo Fava, IT Manager, both stated that the security policy had changed tremendously over the years.

"*In the beginning it was completely different. During those years I remember a successful attempt, in which someone hacked a Windows server through which they tried to attack another company, which called us and told us that our public IP address was trying to attack them. Maybe it was in 2001*." (Matteo Fava).

Tagetik is a very well structured company and is very interested in cyber security. It has a restrictive internal security policy, which includes plans for business continuity and disaster recovery on external servers, and they are planning to utilize a second cloud service to create a redundancy of their data. They do periodic penetration tests and vulnerability assessments. They also have different levels of access to data for junior and senior users, as well as for the management unit. Their greatest fear, as illustrated by Dr. Fava, "*it is the possibility that someone might access our servers where there are critical clients' data, such as unpublished balance sheets of very big companies*."

Within the cloud service, which in recent years has been garnering a lot of commercial success, they offer a package that includes software developed by them, the server which hosts it and of course security. For this reason the problem of security gets a lot of attention at Tagetik because it represents a problem for business. If some data was lost or stolen, this would damage the reputation of the company. The cloud department is ISO/IEC 27001 certified[212] and lives on restrictive policies; the rest of the company benefits as well from these restrictive policies.

As is the case for all public IP addresses on the internet, they have frequent unauthorized access attempts, although so far they have no evidence of damage to the machines. "*We see a high frequency in the attempts to infiltrate the system, spam, virus, and on the public IPs we have frequent scan attempts, from the brute force on the FTP accounts to attempts to access our e-mails with the most common passwords*." In June of this year, they detected a breach in one of their accounts, were notified by Google, and they immediately suspended it. Fortunately, the account belonged to a user with low privileges and limited access.

The perception that emerges is that awareness among SMEs is still quite low. "*Whoever says that it is safe, has no idea what they are talking about*", stated Dr. Natale in this regard.

Some big clients frequently complain about too many authentication protocols. "*Despite the fact that we do it for the client's security it is not always perceived that way and there is some resistance […] unfortunately our power to impose security policies is low, we can't do more than give advice. If the user complains our hands are tied*."

Both Natale and Fava refer to the need to raise awareness of users on cyber risks in a crosscutting manner, something which they are already trying to do, and advocating for more information sharing regarding this. "*Security should not only be seen as a cost but also as an investment*", they declared.

Information sharing is important, not only the sharing of information, but also the sharing of objectives and methods acts as a good relationship builder between IT departments and boards of directors. It facilitates the implementation of correct security policies. "*If IT is not supported by the Board of Directors you can't go anywhere*", declares Fava. Both also complain about a lack of balance at the seminars they participate in, stating that they are usually either too superficial or too alarmist.

[212] ISO / IEC 27001 is the best known standard that provides the requirements for information security management systems (ISMS), available at: <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> (retrieved 15-11-2014).

The final interview was conducted at *Assindustria* of Lucca, with Director Claudio Romiti and Manager for Economic Services, Daniele Chersi, according to whom, in general and especially for SMEs, there is no awareness of the dangers stemming from a nonchalant use of technology. During this period there has been a noticeable interest towards the cloud services because it is economical. The attitude they notice the most is that of the refusal to consider even the most basic security policies, *"until a disaster happens, they don't take into consideration even a simple password change […] there is an enormous cultural problem. The problem in addition to being cultural consists also in the fact that in the majority of SMEs there is no figure in charge of these aspects."*

Assindustria organizes annual, themed seminars on topics such as PEC, company invoicing, and broadband, but it claims there is constantly a low turnout of SMEs.

Conducting semi-structured interviews, with different institutional players and representatives of companies in the province, allowed for what can be defined as the key emerging concepts. These key concepts are useful for the correct design of ad hoc programs for SMEs in relation to combating cybercrime.

Given the nature of this phenomenon, the need to invest in information is the primary issue that surfaced in all of the interviews, together with the need to demolish cultural barriers, which hinders awareness regarding the risk of cybercrime. In fact, human weaknesses are to be considered more dangerous than the technical ones.

The cases on the rise in recent years are those which tend to have a specific target, such as spear phishing. These techniques are quite dangerous for companies because the criminals calculate the amounts to steal in such a way that it makes it hard to detect the attack.

It is also deemed necessary that not only IT departments continue to be informed about this phenomenon, but also that management, business owners, and boards of directors should also stay informed in order to establish appropriate policies and counter measures.

The total lack of information sharing and collaboration between companies highlights the need to create networks between companies in the same sector, or having the same size, in order to increase the dialogue and dissemination of best practices.

Unfortunately, security is still seen as a cost and not as a value; this inevitably makes us notice that the average level of security is directly proportional to the size of the company, to how well the company is structured and the size of the budget and the resources utilized to improve this aspect.

Protecting Italian SMEs, crucial for the Italian national economy and very valuable in terms of know-how, should be a fundamental objective, especially if we consider that SMEs are often victims of theft by insiders more than by hackers. Consequently, a good internal policy is necessary to mitigate this risk.

CONCLUSION

For the security of the nation and its economy, opposing the growing phenomenon of cybercrime is a crucial issue. Events of cybercrime are becoming increasingly widespread, and their impact on the world economy is becoming alarming.

As we have seen, the European Union, in 2013, adopted its own cyber strategy, and it invited the member states to do the same. In 2014, Italy adopted a National Strategic Plan for Cyber Space Security (*Quadro strategico nazionale per la sicurezza dello spazio cibernetico)*, but there are still delays in the implementation of some of its steps in comparison with the European average. As stated in the UNODC report[213], the majority of cyber-attacks are of a transnational nature; this means that it is difficult to fight them just locally. There is a need to come up with a global response through a shared set of rules and common technological development road maps. The implementation of cyber security policies is a prerogative of each State, but it is important to incentivize European and International cooperation, as well as public and private partnerships, regarding this phenomenon. Moreover, we should not forget that cyber space constitutes an important opportunity for the economy of the country, but it hides numerous risks which need to be identified, and we have to learn to protect ourselves against them.

The difficulty in facing this type of crime is in the discrepancy between the tools and the knowledge available to cyber criminals and the tools and knowledge available to those who have to defend themselves or are tasked with opposing this phenomenon. The tools to conduct a cyber-attack are becoming more powerful and easier to locate and use, as well as being relatively cheap. The skills necessary to conduct a cyber-attack are diminishing. With little effort, a criminal can equip himself with the necessary tools and information to carry out this task, and the development of the deep web further simplifies things. The fight against cybercrime requires strong legislative actions, mechanisms for law enforcement, adequate instruments, collaboration, but most importantly knowledge.

Law enforcement agencies and companies have the difficult task of opposing and defending themselves from every type of known cyber-attack. While on the other hand, more and more often, criminals specialize in a specific type of attack and refine their techniques to reach high levels of efficiency, and develop new ones, often unknown to those who have to oppose this phenomenon. If we look at the evolution of phishing, we are no longer in the presence of fraudulent e-mails written incorrectly and easily identifiable, but, instead, we are witnessing an increase in spear phishing and targeted actions that are extremely difficult to recognize. The results, from a prosecutorial point of view, are unclear in this field; the problem is not due to a lack of pressing charges or from a lack of personnel, but it can be traced back to the nature of the phenomenon. As such, it is easier to work on prevention. What has emerged from the interviews is that this type of crime is very difficult to prosecute, and this currently constitutes the ideal

[213] *Comprehensive Study on Cybercrime*, UNODC, February 2013, available at: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (retrieved 15-11-2014).

situation for cyber criminals. They can continue to augment their capacities, their profits and their network, as well as provide fertile ground for illicit activity and be an example for others involved in organized crime or terrorism.

There are some elements that unfortunately don't help in reducing the gap between the intensity of this phenomenon and the real capacity to defend ourselves from these attacks. Elements such as the speed with which cyber criminals reinvent themselves, their level of specialization and the quantity of resources they dedicate to their crimes will always be greater than the defensive efforts.

Furthermore, the border between the types of various cyber attackers is diminishing day by day, and there is an increase in the relationship between cyber criminality and ordinary criminality, which is now using new technologies to expand the scope of their illicit activities by collaborating directly with cyber criminals or purchasing from them the tools and necessary resources to commit cybercrimes themselves.

From the interviews, it emerged that the types of crimes committed by cyber criminals in Italy reflect the classic Italian style of fraud perpetrated through the web, such as the sale of fake or non-existent items, while the other more complex cybercrimes are primarily the domain of Russians, Chinese and nationals of several African countries.

Another factor that makes the fight against cybercrime more challenging is the difficulty in determining a singular type of victim. All web users (citizens, SMEs, large enterprises, States) are potential victims.

It is also useful to consider the psychological aspect at the basis of these crimes, the perceptions of danger in physical security and cyber security are completely different and influenced by personal experience. Physical theft is well understood, the virtual one a little less. In fact, none of us today would ever leave our front door open or a wallet unattended in a public place, but when it comes to cyber security, we are not able to see our weaknesses due to the tendency not to consider the virtual as real. Also, from a psychological point of view, the neutrality of the computer monitor destroys our ability to see the effects of our actions, both from the point of view of the criminal and that of the victim. The desensitization that occurs through the use of a PC prevents the cybercriminal from understanding the extent of the damage he is inflicting on the victim. The consequence of this is that the victim is downgraded to the status of just an IP address. The same process happens to the user, who lowers his guard on the web, loses inhibitions and underestimates the dangers of the web. This might lead him to click on a link received via e-mail or share personal information on social platforms. The ease with which we are inclined to communicate with unknown people via chat or webcam are examples of habits that we would probably never replicate as lightly in the real world. In addition, the physical distance between the cyber-criminal and the victim amplifies these aspects.

The human factor is a determining element in this type of crime, which frequently exploits human weaknesses for its own gains. Cyber criminals count on small human errors to convince a user to click on a link in a phishing e-mail that will lead to an infection of the PC, or push somebody into revealing personal information about themselves, counting on the habit of not checking the reliability of the person on the other side of the monitor. Cyber security is not a status to be acquired, but a mentality that needs to be adopted at 360 degrees in one's private life and

especially within one's company or at one's job. Only in this way can we achieve valid and long-lasting results.

To make the damage of cybercrime tangible and their victims visible, in October 2012, the first case of reparation justice in Italy took place. The objective of the case was for the culprit, who defrauded 100 people, to get to know his victims and pay back the community, not in monetary, but in "human" terms. The culprit was sentenced to serve at a soup kitchen after a plea bargaining agreement[214].

Even in the case of SMEs, the human element plays a fundamental role. Negligence in the workplace is one of the major causes, together with the system's flaws and hacker attacks, of the loss of company data, which can lead to the loss of business and a loss of trust in the company by its clients, an enormous tragedy for an SME.

SMEs often underestimate the risk of cybercrime, giving priority to their balance sheet and not considering the costs tied to those risks. The ICT budget is seen as a necessary evil because it is thought not to have an impact on profits. Today, any sector of business is influenced by ICT.

The structure of our economic system was founded upon SMEs, unlike that of other European countries. The Italian know-how is our cherry on top, and while large enterprises are starting to protect themselves from cybercrime, and banks have been living with this reality for some time, SMEs struggle to put in place adequate counter measures. Although the risk might seem intangible, the damage they cause is not. The connective tissue of our country cannot be considered a closed system, the business relationships, national and international, and the communications between companies, crucial for conducting business, can be vehicles for swift infections and potentially harm the whole economic system. The system's security depends on everybody's security measures. An SME might not think of itself as an appetizing target for a cyber-criminal, especially if they produce goods not related to ICT. In reality, it is the small and vulnerable companies which constitute an easy target, and the biggest problem is that they are not aware of that. From the interviews it surfaced that a very common attitude of SMEs regarding cybercrime is that they prefer to pay for the damages following an attack as opposed to investing in prevention. It is true that the level of awareness is slowly increasing, but what remains is the idea that investing in cyber security is too high a cost and so they choose not to do it. Then there are also perceptions about the risks of cybercrime, but they are rarely followed by proactive actions geared towards diminishing those risks.

We have to consider that it is not just the company victim of an on-line fraud attack that suffers, but indirectly the whole economic system, the market, and local institutions suffer as well. Furthermore, in the case of this crime, the victim is not sufficiently protected. As we have seen in the cases illustrated in the previous chapters, larger companies are being hit more and more through suppliers, outsourcers and companies belonging to their network.

[214] *Truffatore on-line servirà a tavola i poveri. Primo caso di giustizia «riparativa» Il giudice: così si accorge delle vittime nel mondo reale*. by Luigi Ferrarella. "Corriere della Sera" 7-10-2012, available at: <http://milano.corriere.it/milano/notizie/cronaca/12_ottobre_17/truffatore-pena-riparativa-poveri-mensa-2112290080980.shtml> (retrieved 15-11-2014).

In terms of cyber security, the reliability of Italian SMEs, especially within the industrial districts, could be a factor playing in their favor when faced with the prospect of relocation to Eastern countries. A move eatward could constitute a risk in terms of cyber security. The struggle over the issues of outsourcing and corporate relocation cannot just focus on economic concerns, as an Italian company will never be able to lower its prices to the same level as rivals from a developing country, but it could count on an offer of more reliability regarding cyber security and using it as an added value. District enterprises could then see an investment opportunity in Italian SMEs.

The real frontier that needs to be demolished is the cultural one. Many defensive strategies could be put in place, and at a low cost. Beyond internal security policies, there is a need to incentivize information sharing at the highest levels. As a preventive measure, before an attack, all the best practices and information concerning cyber threats could be shared between companies of the same network, trade associations and law enforcement agencies; this could help in putting counter measures in place. At an operational level, before or after an attack, information sharing with privileged stakeholders, such as law enforcement agencies, banks etc., could increase the resilience of the system to mitigate the damages it might incur.

From the analysis conducted in international reports, information collected regarding the cybercrime phenomenon, norms issued at the European and Italian level regarding cyber security, and, more importantly, from the investigation conducted through interviews of institutional players, law enforcement agencies tasked with opposing cybercrime and the companies in the Province of Lucca; it became clear that the only real effective weapon against cybercrime is awareness. The problem is not just technical, but it is mostly cultural.

The measures put in place to oppose this phenomenon have to be geared, as much as possible, towards informing the user and promoting information sharing. These two objectives can be reached through the implementation of two projects.

The first project, which has the objective of increasing knowledge and information sharing in this sector on two corporate levels, could include the organization of seminars, workshops and differentiated training courses geared towards non-technical decision makers, in other words Boards of Directors and company owners, and technical staff, such as IT personnel. This differentiation allows us to structure the seminar in a way to best cater to the background and needs of the participants and their functions within the company. Organizing very technical seminars for those who have to make decisions for the whole company, or being too generic for those who have a very technical background, may make the seminars unappealing and may not train the participants adequately. The differentiated courses have the advantage that they can provide the company managers with all the basic knowledge necessary to understand the various aspects of this phenomenon to be able to make informed and responsible decisions. For the IT personnel, the more technical and specialized courses can update them on the new threats, especially the emerging or the sophisticated ones, while maintaining their level training which is usually left to their own initiatives. These two training paths can be reorganized and differentiated

by commodity sector, or be based on the size of the company. This methodology, beyond the training, is designed to promote sharing between companies and give birth to a network for sharing experiences and information. It is advisable for these courses to be conducted with the support of trade associations and not private companies, to prevent participating companies from thinking that they are taking part only to see sponsored products. Beyond the theoretical aspects, it would be very important to also include practical simulations that demonstrate to participants the ease with which a cyber-criminal conducts an attack that can compromise the security of company data.

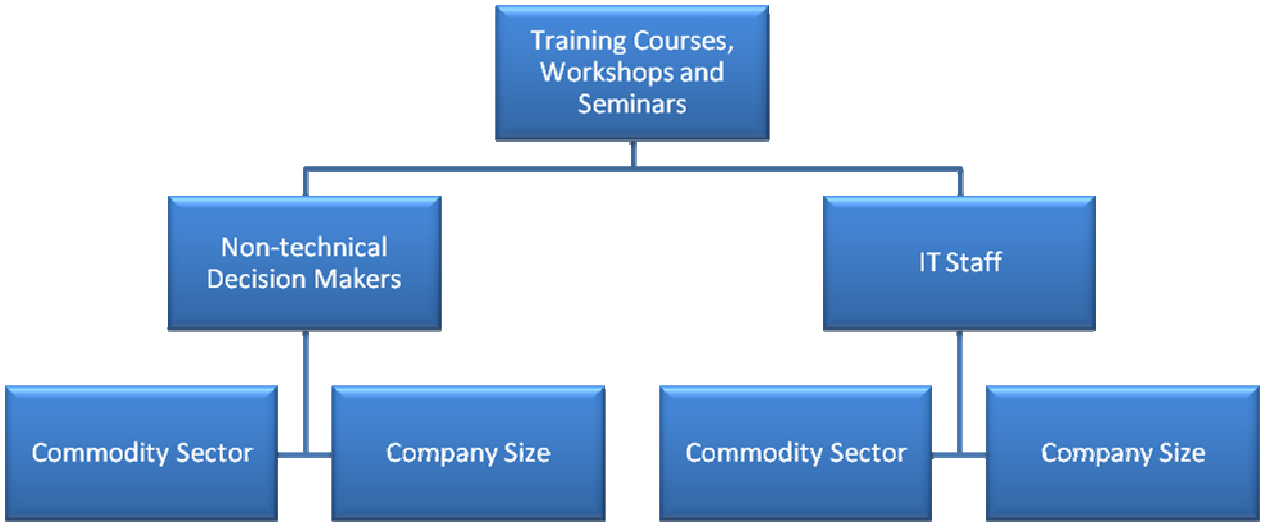


Figure 28 - Differentiated Training Courses Project

A second project, complementary to the first one, includes the organization of round tables for specific players such as representatives of SMEs per commodity sector, trade associations, Universities, the Prosecutor's Office (*Procura della Repubblica)*, law enforcement agencies and legal experts. The objective of this project is not just to share information on the emerging risks related to cyber space, but also to identify contact persons for each sector of the SMEs, and especially to allow for the foundation, over time, of a sort of community of practice that will drive the engine of knowledge in this sector and become a shining example of cybercrime prevention. By way of strengthening this project, in time, the large companies of Central Italy could also be involved in the process.

Figure 29 - Project to Establish Periodic Round Tables

Through the implementation of these two projects, it is possible to provide the conducive environment for the creation of an community of practice, which will not only promote a true security culture, but will also have the advantage of never becoming obsolete, compared with simple best practices, and can adapt to any type of evolution of the cybercrime phenomenon, taking note of changes and adapting to them.

INDEX OF FIGURES

INDEX OF TABLES

METHODOLOGY

The subject of the study, and its objectives, have made it necessary to conduct the study in two stages.

In the first stage, we analyzed the most recent reports concerning the cybercrime phenomenon. These reports were published by major information technology companies (CISCO, Kaspersky, McAfee, Ponemon, TrendMicro, Clusit, etc.) and accredited independent entities (UNIDOC, ENISA, World Economic Forum, etc.). All reports are readily available on-line. The scope of this analysis is to highlight the facts regarding cybercrime that are common to the majority of the reports so as to obtain a better picture of the phenomenon, with particular emphasis on its relevance to SMEs. Furthermore, in the first phase, we examined the existing legislation at both the national and European levels and the entities that combat this type of crime. The scope of this study is to summarize the current legislative situation, and within it, the response capacity of Italy and other states in combating cybercrime. Through a targeted OSInt activity and by monitoring major international news publications, we identified and examined major cases of international cyber-attacks, and how some states are fighting this kind of crime. During this stage, the need emerged to produce a panoramic view of the types of attacks, attackers, vulnerabilities and current risks. The above was produced in an effort to understand the evolution of this phenomenon to date and the risks it constitutes for SMEs. This section can be considered as a sort of guide to cybercrime for SMEs, illustrating the risks and vulnerabilities that are of concern to companies.

During the second stage of the study, qualitative semi-structured interviews were conducted with the scope of defining and illustrating the actual state of the phenomenon at the local level and, more specifically, in the Province of Lucca, which is the focus of the last chapter of this study. These interviews were conducted following the identification of key interlocutors. We also attempted to find participants for the research through a generic e-mail request, but as often happen in these cases, without great success. The project was presented to the Director of *Assindustria* of Lucca, who sent a circular (annex A), to the associated companies, in which he announced the start of this research and requested the availability to being contacted and providing information of use to the study. Following this, only one company replied asking for information, and later agreed to an interview. Personally contacting known strategic players proved more fruitful. Members of law enforcement agencies and Magistrates had a positive reaction to the cooperation request. Specifically, the interview with the Deputy Commissioner *of the Postal Police of Florence (Questore Aggiunto Polizia Postale di Firenze)*, Dr. Pierazzi, is presented in this section (annex B), because it was possible to record the conversation. The Prosecutor's Offices of Florence and Turin *(Le Procure della Repubblica di Firenze e Torino),* respectively, have provided statistical data and a case study to be included in the research paper.

Companies in the Lucca area that are representatives of the various commodity sectors, *Assindustria*, *ABI Lab*, *Consorzio Bancomat* and IBM, agreed to being interviewed. The analysis of

all the conducted interviews led to the identification of key factors necessary for the implementation of steps designed to fight cybercrime.

Annex A

27/2014/V/1 - Indagine sulla criminalità informatica

Riferimenti Internet:			
Numero	Data	Settore Merceologico	Argomento
27/2014	08/07/2014	Tutte le Aziende	Internet – Siti vari

UNICRI(1) sta svolgendo una Ricerca sulla criminalità informatica e i rischi per l'economia e le imprese a livello internazionale, europeo ed italiano, con un focus specifico sulla Provincia di Lucca. I risultati saranno presentati durante una conferenza e utilizzati per la progettazione di programmi di formazione.
Gli scopi della ricerca sono:

- identificare e analizzare i principali problemi legati alla criminalità informatica e sicurezza informatica a livello internazionale;
- identificare e analizzare i principali problemi legati alla criminalità informatica e sicurezza informatica e rischi per l'economia e le imprese a livello dell'UE e le relative contromisure;
- identificare e analizzare i principali problemi legati alla criminalità informatica e sicurezza informatica e rischi per l'economia e le imprese a livello italiano, con un focus sulle PMI;
- focus sulla provincia di Lucca e le sue piccole medie aziende, attraverso indagini sul campo."

Le aziende interessate a partecipare possono contattare direttamente:
Flavia Zappa

Referente:
Daniele Chersi

(1) UNICRI-*United Nations Interregional Crime and Justice Research Institute* di Torino.

Annex B

Interview with Deputy Commissioner Dr. Stefania Pierazzi

Q: *First and foremost I would like to thank you for accepting to be interviewed. Polizia Postale has a critical role in opposing all cybercrimes and according to the Law 48 of 2008 all cybercrimes are handled at a district level. So do you receive the cases of the whole of the Tuscany Region*?

A: Yes, if we are the ones receiving the complaint, as Postal Police (*Polizia Postale)*, we send it to the Prosecutor's Office *(Procura),* which usually delegates this office, but it does happen for other offices to handle these cases. The total number of crimes committed can be retrieved at the Prosecutor's Office (*Procura),* which has all the data for the Region. We at the district level have all the data of the provinces, except Massa, which is under Genova's jurisdiction.

Q: *You have been working on this phenomenon for 15 years so you had the chance to see it evolve. What can you tell us about it*?

A: Yes, in the beginning it was subdued, in fact, there was embarrassment when it came to pressing charges for this type of crime, and banks, if they were victims of an attack, tended not to disclose it to the outside. They might have even returned money to their clients, who lost it, but they never declared the phenomenon, over time it became a common crime and they realized that being a victim doesn't diminish one's image and doesn't affect a person's credibility or that of a company. Then the victims have begun to report more and today even large companies press charges against these types of crimes, for sure more now than used to happen in the past. First it was very difficult, we would come to know about it indirectly, perhaps there was a related act and then we would come to hear about it…. For example, there was an e-mail bombing against Google in 2002-2003, several Florentine companies suffered the attack, and functioned as an entry point for this attack on Google. In reality, we received the complaint from a small company in Prato and then we were able to ascertain that the phenomenon touched Florence and its Province. The case was of various individuals around the world who agreed to flood Google's e-mail; some of these individuals were in Bologna and were engineering students who managed to breach several companies in Prato and Florence in order to perform this attack. But the Florentine companies did not file a complaint, instead it came from a small company and from there we were able to reconstruct everything. Today it is no longer like that, they press charges with ease, even large companies do so. Even large companies and big brands, here in Florence there are many which might have been attacked or attempted attacks or attempted fraudulent acquisitions, and they lodged complaints even when they only had the suspicion of being a victim.

Q: *When did you start noticing this shift in tendency*?

A: I would say 4-5 years ago definitely. In fact, the more it is talked about the more people can understand that this is a phenomenon which affects everybody as such we can talk about it. Then the privacy law gave us more duties on managing personal data and as a result of this we can communicate it with more ease.

Q: *What trends have surfaced in relation to cybercrime in these recent years within your jurisdiction*?

A: that cybercrime is steadily increasing; registering a real escalation, especially in the last 3 or 4 years. Phishing and spear phishing have now reached their highest peaks ever. These however, are not considered crimes by themselves, but only if combined with an unauthorized access to an IT system with the objective of stealing data and bank credentials of an individual or a company of any size and use them to conduct transactions. This trend doesn't show any signs of decreasing; it continues to develop in a constant manner over time

Q: *In the Lucca area the paper mill district is the largest and most SMEs belong to it, can you confirm that? And is there a particular type of company more predisposed to becoming a victim of this phenomenon*?

A: Yes, in the Lucca area the paper mill district is very large. The cyber phenomenon is crosscutting, and through our empirical data based on the charges pressed and other complaints, I would say that there isn't one type of company. It is a non-discriminating phenomenon, we get visits from the small enterprises as well as large companies contacted by their bank because they flagged an unusual transfer of perhaps a considerable figure such as 70,000 euro sent to X and the company in reality never authorized a transfer. So we usually encounter cases of medium to large enterprises with considerable amounts of money stolen and smaller companies with smaller stolen amounts.

Q: *What is the monetary value of this type of attack*?

A: It is easier to have several attacks with non-exorbitant figures and in line with the victim's size of monetary capabilities. For example, a large company can suffer an attack for 35 or 40 thousand euro. A small company can suffer an attack for 1,500 – 2,000 euro, obviously more than once and repeated over times they can have the same impact. This way companies don't even notice that they suffered an attack. Using for example false orders, false invoices, and giving invoices a different address instead of the actual recipient's, you can get sums of money which are not necessarily high, but it is a common practice.

Q: *Is it difficult to identify the person responsible for the attack*?

A: Yes, because the criminals are very prepared and they use systems that allow them not to be identified. All they have to do is use a proxy and they immediately make themselves untraceable,

or at least the transaction will seem like it happened through a server abroad. At that point I wouldn't say that the activity would stop, but almost.

Q: *So it is difficult even to find out the nationality of the attacker*?

A: Yes, exactly, in some cases we were able to locate the subjects and we actually ascertained that the money came back to Italy. But it is not always the case. And usually they can make their traces disappear in no time. For example, if I use a proxy that makes it seem that the activity originated in any country in Oceania, we are back to square one.

Q: *What is the level of trans-nationality of the recorded crimes in your area of competence? Does the nature of cybercrime make it hard to conduct investigations*?

A: Absolutely. The problem is bigger because the attacks usually come from countries which are not in the European Community, so they are not connected through Europol which is a tool that we use. So in these cases, the attack which is coming from a country with which we have no reciprocity, exchanges or data acquisition, we can ask for an international rogatory letter. But the Prosecutor's Office (*Procura)* will engage in a cost benefit analysis, for a 300 euro fraud we would not activate a 5000 euro International rogatory letter, that is understandable, that is common sense. Assuming it is activated, the timeline is so long that due to the volatility of the data necessary to conduct an investigation, by the time you get to the location the data will be gone. So, transnational crimes are really among the most difficult to manage.

Q: *Is there collaboration on investigation at an international level*?

A: In this case we can go one of two ways. Either through our service of Postal Police (*Polizia Postale)* which has its HQ in Rome, which is the same as the International cooperation service, Interpol, both belong to the Ministry, both are at the same level and they talk to each other, sometimes when there is something urgent we contact them directly, and there is effective collaboration, as much as possible in terms of data acquisition. They can provide collaboration by providing me with some information, such as in identification for example. Then there are some types of information which need to be retrieved through specific procedures. Otherwise they have no relevance in court. So we have to activate an international rogatory letter etc. For example, if I am monitoring a subject in a foreign country and I want to know his identity, through the collaboration with the local police I can obtain the identification useful for my investigation. What I can then use in court is different, in that case I need to activate standard operating procedures, in other words the international rogatory letter with formal acquisition, and in that case the timeline will become considerable longer as such it is understandable how this is not always possible to do. In the case of pure investigation the timeline is more rapid, also because we can sometimes call the colleague functioning as liaison officer in the State X and get the information necessary to proceed in the investigation, then you can create a dossier and then follow other more complex procedures.

Q: *So the difference is mainly in the type of attack*?

A: Yes, it always depends on the Prosecutor's Office (*Procura)*, I understand that for a citizen who makes 100, 10 is a lot, but for the Prosecutor's Office (*Procura)* [it] has certain costs that it has to consider, it does an actual cost benefit analysis, sometimes the stolen sum is not high enough but the perpetrator has done it multiple times so the Prosecutor's Office (*Procura)* has to make a move. But in other cases where the stolen sum is low the Prosecutor's Office (*Procura)* might opt not to proceed as the process might be so long and expensive that not always Italian justice can afford it.

Q: *Are there groups of Italians which operate on the territory*?

A: We have not encountered international criminal organizations operating from Italy; there could have been small groups which put together an activity. But I am also engaged in a different activity, perhaps the colleagues in the Antimafia or DIA have a vision of this phenomenon which goes beyond, maybe International organized crime which operates in this way. We happened to identify groups of subjects, in reality common criminals, not of certain level, perhaps slick, and able, but still common criminals. They do tremendous economic damage because they have the competence, but their profile is quite low.

Q: *Regarding the type of damage that they suffer, in your experience, do SMEs in Tuscany suffer only economic losses or have you recorded instances of loss of intellectual property*?

A: There is a bit of everything, but I have to say that purely economic damages are usually perpetrated by individuals from outside the company. More often than not, the theft of data and related damages which are usually quantified at a later date, such as the theft of patents, client lists, billing data alteration, etc., are perpetrated by untrustworthy employees, disgruntled ex-employees, which have created their own company or simply are poisoned against the company from which they came out, and having knowledge of access etc., use this information to create damage, spread patents, produce them in turn, prevent the company from having contact, do mediation; this has happened more than once "look at this company, I'll sell the same product, but the price is lower." Because SMEs base their business on patents, excellence, specific business contacts, and on the exclusive use of a brand rather than another. In this case most of the time, I would not say 100%, but we are there, are former employees…rarely is it competing companies.

Q: *Are there cases of theft of know-how and intellectual property abroad*?

A: It can happen. Something like that can happen for example in China somebody hooks a subject who is in Italy and makes him an offer. Or an ex-employee starts his own activity and uses the know-how and data he took from his previous employment.

Q: *So it is difficult to quantify in the short run*.

A: Yes, surely, I unfortunately miss the civil part, I know the penal aspect. I know that Tizio caused damage to Caio. Then we investigate and find proof. But I miss the activity that happens after that. Sometimes we hear something from an acquaintance. But most times we don't hear anything.

Q: *And companies, how do they usually react to this type of attack*?

A: If I have to be honest, most of the time they wait for the damage to happen and then run for cover, because for them their cyber security represents a big investment, especially for SMEs. It is expensive to put in place a policy of prevention and 360 degrees of total coverage. IT also grows at an exponential rate, what we know today is obsolete tomorrow, so updating is both hard and expensive. Even if a company has planned well and established a good system, the need to update I so frequent that everybody manages to stay up to date.

Q: *So a sort of cost benefit analysis then*.

A: Yes, exactly. Sometimes there are some very simple things that can be done, such as changing passwords. For example if an employee which used to manage administration leaves, the least you can do is to immediately change the password and deactivate his account. But what usually happens is they do nothing for months. Sometimes there are things that don't cost anything; it would be enough to employ somebody to take care of these things.

Q: *In this regard, in the conversation with inspector Bozzi it surfaced that there are banks that have lower protections than their WI-FI network*.

A: Yes, it is possible in a very short time to take an incredible amount of data. Not only that, we have often knowledge of attacks on banks from the claims of account holders, normal citizens through whom we noticed a trend. For example within 15 days they are coming to file claims regarding cloning, fraudulent transfers, all within the same bank which leads us to believe that the bank is under attack or the system they use is under attack.

Q: *Regarding large companies, many of them have specific departments and they invest in this sector, but they still suffer attacks. I imagine that it must be more difficult for SMEs to protect themselves*.

A: Yes, because they usually have few employees and perhaps one employee has several functions and this is one of them. And they surely suffer for this more and when the damage happens then they try to remedy the situation.

Q: *Is there a good level of trust towards law enforcement agencies by the companies*?

A: Yes, I have to say that they rely on us a lot. Often a company comes to leave a statement regarding an attack they suffered, such as in cases of theft of the client list, and they ask as to

conduct some verification as they would feel better if we did it. This is a very positive aspect, I rarely found reluctance to cooperate with us, and they accept advice and provide their details willingly. There is good collaboration from this point of view

Q: *Given the peculiarity of this type of crime, do you think that current norms are adequate*?

A: Yes, I understand that it is difficult for a legislator to think of all aspects. Let's say that so far we have managed quite well to manage all the phenomena we had to deal with. If the legislator was to insert within economic systems even IT systems, then he gives us the possibility to apply it to those types of crimes, with this addition which has been made for various types of crimes. From fraud, which has become cyber fraud, and including the acquisition of mail, where it is written that e-mail is equated to regular mail that gives me the possibility to engage in investigative activities.

Q: *And has this integration been made for every type of offense*?

A: Yes, there are crimes from 615 cp forward which deal with cyber systems. And then the modifications are made.

Q: *The latest European Directive, which has not yet been recognized, does it deal only with the providers of critical infrastructure? Does this limit you somehow*?

A: Yes, it has not yet been recognized. I have to say that we base ourselves on the collaboration with the provider, which for us is crucial. The handicap is that they are often abroad, but we still manage to obtain the data we need because they have legal offices here in Italy or they provide the information anyway. For example, Google, which is not Italian, collaborates through Google Italia and accepts the requests made by the Italian Police. Although the companies are foreign we can still cooperate.

Q: *Is this valid only for substantial sized thefts or is it valid even for small violations*?

A: No, In this case it depends only on the provider company. It requires a decree from the Italian Authority because it is sensitive data and the moment you have the decree they consider it as if it came from their authority. In so doing they recognize it and give us the possibility to collaborate.

Q: *What is the level of digitization of the SMEs in your jurisdiction*?

A: Quite high. Yes, even the small ones have completely digitized all the economic aspects. They also digitized their contacts and their internal network, but now the IT system is a reality for all companies. Obviously with different levels of proficiency.

Q: *You were telling me that they often wait for an attack and then eventually fix the damages, for economic reasons, what is their perception of the risk of cybercrime*?

A: Sometimes I don't think they have the perception of how vulnerable their systems really are. Perhaps we are dealing with the old school, old entrepreneurs with few employees who don't have a good rapport with cyber tools. Sometimes they are a little more aware, but they still wait for an attack to happen before they put any measures in place.

Q: *Are there examples of small enterprises, satellites of larger ones attacked to attack the larger ones*?

A: From what I remember it has never happened at least not on a cyber-level, it is possible that this happened at an economic level. But this is not a sector I work with; perhaps the *Guardia di Finanza* can answer that question.

Q: *Are you aware of any activities or initiatives by SMEs or any other Institutions to increase awareness of the risks of cybercrime*?

A: Some years ago the National Confederation of Italian Traders (*ConfCommercio)* organized one regarding the use of POS [Point-of-Sale systems]. They did some seminars to alert about the risks and a world opened up to me, because I had the opportunity to speak directly to Florentine business owners, which were already not happy about the imposition of using a POS. When I explained all the risks they could go up against such as using them incorrectly, or allowing others to use them without authorization, perhaps by a person pretending to be a technician… There I noticed that they were unaware of any of those risks and I realized that small business owners were not exactly informed and were extremely vulnerable. For sure larger companies or newly established companies, have more awareness and knowledge of this problem. Sometimes we have an article published in order to increase awareness. Or, for example, we use the arrival of summer vacation as an excuse to start initiatives geared at informing. Years ago, the Prefect of Pisa (*Prefetto di Pisa)* held events to increase awareness among elders about the risks of ATMs and how to use them properly.

Q: *Have these initiatives had a good impact? Has there been an evolution over the years in the awareness of SMEs regarding cyber risks*?

A: Often, yes. Sometimes, however, these initiatives start out of a request or specific needs. After an attack happens, we try to understand what the problem was. These meetings are often done post attack and are done by sector. It is probably more efficient if these meetings are conducted on a sector-by-sector basis. In so doing we are investing more on quality than quantity. Obviously, often there is also the non-answer, or people that underestimate the phenomenon, and believe it to be far from their activities and feel sufficiently safe and don't worry about those risks.

Q: *What sector initiative are you referring to*?

A: Yes, the National Confederation of Italian Traders (*ConfCommercio)* organized meetings of this kind, sometimes even with other associations, but sporadically. There was a Prosecutor (*Questore)* in Florence who years ago organized frequent meetings with all the trade associations and the Police and discussed risk at 360 degrees. The colleague would present the risk of fraud, while we would present cyber risks.

Q: *What degree of sharing is there between companies about cyber risks within the categories of the sector*?

A: I don't think they do. Nobody from the companies ever came to me and told me I had the same problem as so and so. I never had the impression that there was dialogue between them, on the contrary. Perhaps concerning the strictly economic aspects of a sector, such as banking; banking associations do encourage information sharing.

Q: *The Characteristic of Italian enterprises is the made in Italy. Have you had cases regarding this aspect of SMEs*?

A: More than a theft of patents we had episodes of theft of image in the tourism sector regarding tourism companies in the area. Property of some tourism companies, such as pictures, certificates, which were published on their website, were stolen and used by others. The theft of patents happened some time ago to a pharmaceutical company. A group of ex-employees established a new a company and started producing a drug which was patented by their former company, to this you have to add theft of data and of course clients, a considerable amount of damage.

Q: *What about in the fashion sector*?

A: Yes, It happened a while ago to a well-known fashion company of our area, but it being well structured, it had a department dedicated to this and has its internal investigators which perform widespread checks whenever they perceive there has been a violation pertaining more to the penal code than the civil one. In reality, the theft of a patent, unless it is done in such a way to require proceeding against it through the penal code, usually has civil code implications. As such, these types of cases do not usually come to us. It is easier to find this information through the Chamber of Commerce (*Camera di Commercio)*. The Chamber of Commerce (*Camera di Commercio)* may know of actions that have been activated and so on. They come to me if the patent was seized through unauthorized access, but it rarely happens, for patents of a high caliber, which are kept open to all, or are computerized.

Q: *Have you recorded cases of Hacktivism*?

A: No, we haven't encountered those. But Anonymous did attack us on some occasions or the Ministry of the Interior, and then disseminated the information they stole. We also experienced the defacement of the front page in Arabic, episodes like these without other types of damage.

Q: *Can you tell about a case which left an impression on you in recent years*?

A: I remember very well the case of a company in Florence which was a victim of targeted phishing, and lost large sums of money. We were able to locate the Romanian suspects in collaboration with the Romanian police. Obviously, the problem was that the company noticed the theft late, the bank doesn't always alert you, or when they do, the economic damage is already done. The suspects were able to steal, through their access to the database of the bank, the credentials of the company and took control of the bank accounts and started making random transactions. The sums of money were considerable and it was possible to block some of them. The bank doesn't always ask you about your money movements if they do not seem suspicious. So some time might pass, even 15 days in these cases are valuable because that information can no longer be recovered. In that case we located the Romanian individuals and Romania being in the European Community, we were able to move quite quickly, but this is a quite rare case. Rarely do companies notice, and by the time they do, it is too late for the investigations to yield real results. Speed is of the essence in these cases, if we move in time we can do something, otherwise no.

Q: *According to your experience, what do think are the necessary tools to oppose this phenomenon*?

A: Awareness, absolutely, also because a lot is based on social engineering. Man versus man. Pierazzi states concerning what is more useful for SMEs to defend themselves is quite representative: "Knowledge. Absolutely... also because a lot is based on social engineering. Man versus man. It is true that there is a machine in between, but there is a man in front of that machine. I think that the preparedness of the user, the client, the employee, is crucial. First and foremost it is important to be aware of the risks, so as to prepare even the last of the employees to face said risks, and not make stupid mistakes, such as accessing malicious sites which can infect the system. There is a need for awareness about and training on cyber tools, because there is a presumption that this tool is easily manageable. It is deceiving because it gives you the opportunity to do everything immediately. IT is amazing, really, it allows you to do some amazing things, I believe that it is truly amazing, but you have to approach it with a bit of slyness and don't rely on it with your eyes closed.

Q: *The use of social networks can be strategic in this case*.

A: Yes, in fact we do a lot of activities in schools because kids have no perception of the risks of posting information like "Today we are going on vacation and nobody will be home," or "This is my telephone number and I live here," and then find somebody with bad intentions at your home, because this is what happens. The same thing also happens to companies.

BIBLIOGRAPHY

Ablon L., (2014) "*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*", available at: <http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf> (retrieved 6-11-2014)

AIDiM, ANVED, eCircle (2012), *Quanto è "Social" la tua Azienda?*, available at: <www.slideshare.net/kornfeind/quanto-social-la-tua-azienda> (retrieved 7-11-2014)

Audiweb (2014), *Audiweb pubblica i dati dell'audiencemobile e della total digital audience del mese di agosto 2014*, available at: <http://www.audiweb.it/wp-content/uploads/2014/08/Audiweb_CS_TotalDigitalAudience_07082014.pdf> (retrieved 7-11-2014)

Biondi A. (2014), *Agcom: bene 3 Italia e Fastweb. Ed è boom per Lycamobile*, in "Il Sole 24 Ore" October 7, 2014, available at: <http://www.ilsole24ore.com/art/impresa-e-territori/2014-10-07/dati-agcom-bene-3-italia-e-fastweb-ed-e-boom-lycamobile-173237.shtml?uuid=ABdmQx0B> (retrieved 8-11-2014)

Bodnar C. (2014), *Kaspersky Mobile Malware Evolution: 2013,* February 24, available at: <https://blog.kaspersky.com/mobile-malware-evolution-2013/> (retrieved 6-11-2014)

Cabinet Office and The Rt Hon Francis Maude MP (2013), *Government launches information sharing partnership on cyber security*, March 27, Keeping the UK safe in cyber space and National security, available at: <https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security> (retrieved 6-11-2014)

Cencetti C., (2014), *Cybersecurity: Unione Europea e Italia Prospettive a confronto,* Quaderni IAI, Edizioni Nuova Cultura

Cheslow D. (2012), *Interpol Ups The War Against Cyber Crime*, in "Huffingtonpost", August 5, available at: <http://www.huffingtonpost.com/2012/05/08/Interpol-cyber-crime_n_1499734.html> (retrieved 6-11-2014)

CISCO (2014), *Annual 2014 Security Report*, page 10, available at: <http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf> (retrieved 6-11-2014)

CloudEntr (2014), *2015 State of SMB Cybersecurity*, available at: <https://app.box.com/s/2mf328i6a7j0z2tbdv07?src=undefined> (retrieved 15-11-2014)

COPASIR (2010), *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, July 7, 2010, available at: <http://www.senato.it/service/PDF/PDFServer/BGT/525461.pdf> (retrieved 9-11-2014)

CSES (2012), *Evaluation of the SME Definition September 2012, Final Report Framework*, Center for Strategy & Evaluation Services, available at: <http://ec.europa.eu/enterprise/policies/sme/files/studies/evaluation-sme-definition_en.pdf> (retrieved 6-11-2014)

CSIS (2014), *2014 McAfee Report on the Global Cost of Cybercrime*, June, available at: <http://csis.org/event/2014-mcafee-report-global-cost-cybercrime> (retrieved 6-11-2014)

Decreto convertito in legge 134 del 7 agosto 2012, *Conversione in legge, con modificazioni, del Decreto-legge 22 giugno 2012, n. 83, recante misure urgenti per la crescita del Paese*. (GU n. 187 del 11-8-2012)

Decreto del *Ministero dell'Interno* del 9 gennaio 2008 in attuazione della legge 31 luglio 2005 n° 155. *Individuazione delle infrastrutture critiche informatiche di interesse nazionale*

Decreto legislativo n° 61 11 aprile 2011, del Presidente della Repubblica. *Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione*. (GU n. 102 del 4-5-2011)

Decreto legislativo 28 maggio 2012, n. 70 *Modifiche al Decreto legislativo 1° agosto 2003, n. 259* (GU Serie Generale n.126 del 31-5-2012)

Decreto legge 179 del 18 ottobre 2012, *Ulteriori misure urgenti per la crescita del Paese*. (GU n.245 del 19-10-2012 - Suppl. Ordinario n. 194)

Department for Business, Innovation & Skills Cabinet Office (2014), *Cyber essentials scheme*: *overview*, available at: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> (retrieved 6-11-2014)

Di Corinto A. (2014), *Tutti i segreti del deep web,* in "Repubblica.it", April 20, available at: <http://www.repubblica.it/tecnologia/2014/04/20/news/tutti_i_segreti_del_deep_web-84053410/> (retrieved 11-11-2014)

Digital Agenda for Europe (2014), *A Europe 2020 Initiative*, available at: <http://ec.europa.eu/digital-agenda/digital-agenda-europe> (retrieved 6-11-2014)

Directive 2013/40/EU Of The European Parliament And Of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040> (retrieved 6-11-2014)

Dunn J.E. (2013), *Ransomware criminals attack SMEs using strong file encryption, ESET warns Summer surge in complex attacks*, in "Techworld", September 24, available at: <http://news.techworld.com/security/3470388/ransomware-criminals-attack-smes-using-strong-file-encryption-eset-warns/> (retrieved 1-11-2014)

EC3 (2014), *The Internet Organised Crime Threat Assessment (iOCTA) 2014*, available at: <https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf> (retrieved 6-11-2014)

EISAS (2007), *European Information Sharing and Alert System A Feasibility Study 2006/2007*, available at: <http://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/files/EISAS_finalreport.pdf> (retrieved 1-11-2014)

EISAS (2011), *Basic Toolset 1.0 Feasibility Study of Home Users' IT Security*, available at: <http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas-basic-toolset/at_download/fullReport> (retrieved 6-11-2014)

EMC (2013), *The Year in Phishing*, January, available at: <http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf> (retrieved 6-11-2014)

ENISA (2007) *Deliverable: Information Package for SMEs*, February, available at: <http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/information-package-for-smes/at_download/fullReport> (retrieved 6-11-2014)

ENISA (2013), Threat *Landscape 2013 Overview of current and emerging cyber-threats,* December 11, available at: <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport> (retrieved 6-11-2014)

ENISA (2014), *Annual Incident Reports 2013 Analysis of Article 13a annual incident reports September 2014*, available at: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013/at_download/fullReport> (retrieved 6-11-2014)

ENISA (2014), *Biggest ever cyber security exercise in Europe today*, available at: <http://www.enisa.europa.eu/media/press-releases/biggest-ever-cyber-security-exercise-in-europe-today> (retrieved 6-11-2014)

European Commission (2003), *Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [Official Journal L 124 of 20.05.2003]*, available at: <http://europa.eu/legislation_summaries/enterprise/business_environment/n26026_en.htm> (retrieved 1-11-2014)

European Commission (2006), *The new SME definition User guide and model declaration. Enterprice and Industry Publications*, available at: <http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_en.pdf > (retrieved 1-11-2014)

European Commission (2009), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 30 March 2009 on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [COM(2009) 149 final- Not published in the Official Journal]*, March 30, 2009, available at: <http://europa.eu/legislation_summaries/information_society/internet/si0010_en.htm> (retrieved 20-11-2014)

European Commission (2010), *Communication From The Commission To The European Parliament And The Council. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe* Brussels 22 November, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF> (retrieved 6-11-2014)

European Commission (2011), Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security", March 31, 2011, available at: <http://ec.europa.eu/transparency/regdoc/rep/1/2011/EN/1-2011-163-EN-F1-1.Pdf> (retrieved 20-11-2014)

European Commission (2012), *Cyber security strengthened at EU institutions following successful pilot scheme*, *Brussels, 12 September 2012*, available at: <http://europa.eu/rapid/press-release_IP-12-949_en.htm> (retrieved 6-11-2014)

European Commission (2013), *A recovery on the horizon? Annual Report on European SMEs 2012/2013,* available at: <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/supporting-documents/2013/annual-report-smes-2013_en.pdf> (retrieved 11-11-2014)

European Commission (2013), Cyber Security Report Special Eurobarometer 404, available at: <*http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf > (retrieved 6-11-2014)*

European Commission (2013), *Enterprise and Industry 2013 SBA Fact Sheet ITALY*, available at: <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/performance-review/files/countries-sheets/2013/italy_en.pdf> (retrieved 6-11-2014)

European Commission (2013), *Eurobarometer Special Surveys, Cyber security Report*, available at: <http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_it_en.pdf> (retrieved 7-11-2014)

European Commission (2013), *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* February 7, available at: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf> (retrieved 6-11-2014)

European Commission (2013), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union*, February 7, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF> (retrieved 20-11-2014)

European Commission (2014), *Implementation of the Digital Agenda for Europe. Actions under the responsibility of Member States. Dashboard,* available at: <http://daeimplementation.eu/dashboard2.php> (retrieved 9-11-2014)

European Council (2001), *Convention on Cybercrime,* Budapest, 23.XI.2001, available at: <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm> (retrieved 6-11-2014)> (retrieved 6-11-2014)

European Council (2003), *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No.: 189*, January 28, available at: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&CM=8&NT=189> (retrieved 6-11-2014)

European Council (2008), *"Think Small First" A "Small Business Act" for Europe*, June 25, available at: <http://europa.eu/rapid/press-release_IP-08-1003_en.htm> (retrieved 6-11-2014)

EUROPOL (2011), *Threat Assessment on Internet Facilitated Organised Crime (iOCTA) 2014*, January 7, available at: <https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf> (retrieved 6-11-2014)

Federal Ministry of Education and Research (2014)*, Cybersecurity research to boost Germany's competitiveness*, available at: <http://www.bmbf.de/en/73.php> (retrieved 6-11-2014)

Garante PMI (2014), *Relazione al Presidente del Consiglio articolo 17, comma 1, legge 11-11-2011 n. 180 "Norme per la tutela della libertà d'impresa. Statuto delle Imprese"*, Rome, February 6, available at: <http://www.governo.it/backoffice/allegati/75045-9261.pdf> (retrieved 7-11-2014)

Gartner (2012), *Gartner Says Worldwide Mobile Payment Transaction Value to Surpass $171.5 Billion,* May 29, available at: <https://www.gartner.com/newsroom/id/2028315> (retrieved 6-11-2014)

GCHQ (2012), *10 Steps to Cyber Security Executive Companion CESG The Information Security Arm of GCHQ*, available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf> (retrieved 6-11-2014)

Global Cybersecurity Center (2013), *On-line Fraud Cyber Centre and Experts Network (OF2CEN)*, available at: <http://www.gcsec.org/activity/research/online-fraud-cyber-centre-and-experts-network-of2cen> (retrieved 10-11-2014)

Gori Umberto (2012) "*Riflessioni propedeutiche alla cyber intelligence"* in "*Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale"* edited by Umberto Gori and Luigi Sergio Germani, Franco Angeli Editore.

Guardia di Finanza (2014), *Intervento Comandante Reda Nucleo Speciale Frodi Tecnologiche*, available at: <http://www.aracneeditrice.it/scaricabili/interventoreda.pdf> (retrieved 7-11-2014)

Iacono N. (2014), *Sicurezza delle reti in Europa: il punto sui ritardi,* in "Agenda Digitale", March 13, available at: <http://www.agendadigitale.eu/infrastrutture/718_sicurezza-delle-reti-in-europa-il-punto-sui-ritardi.htm> (retrieved 6-11-2014)

IC3 (2013), *2013 Internet Crime Report*, available at: <https://www.ic3.gov/media/annualreport/2013_ic3report.pdf> (retrieved 6-11-2014)

IDC (2014), *Worldwide Quarterly Mobile Phone Tracker,* January, available at: <http://www.idc.com/tracker/showproductinfo.jsp?prod_id=37> (retrieved 6-11-2014)

Italian Parliament (1998), *Legge 3 agosto 1998, n. 269, Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù*, *GU* n. 185 del 10 agosto 1998, available at: <http://www.camera.it/parlam/leggi/98269l.htm> (retrieved 9-11-2014)

Italian Parliament (2008), Legge n° 48 del 18 marzo 2008 "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*" (GU n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79), available at: <http://www.camera.it/parlam/leggi/08048l.htm> (retrieved 1-11-2014)

INTERPOL (2012), *Speech Opening remarks by INTERPOL President Khoo Boon Hui at the 41ST European Regional Conference. Israele, Tel Aviv*, May 8, available at: <http://www.Interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (retrieved 6-11-2014)

ITsecurity (2014), *Europol, FBI, NCA and others disrupt the Gameover Zeus botnet — claim a 2 week window for users to get clean,* available at: <http://itsecurity.co.uk/2014/06/774/> (retrieved 6-11-2014)

Kaspersky Lab (2014), *IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats*, available at: <http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf> (retrieved 6-11-2014).

Kaspersky Lab (2014), *Security Network Report: Windows usage & vulnerabilities Version 1.0*, August, available at: <https://securelist.com/files/2014/08/Kaspersky_Lab_KSN_report_windows_usage_eng.pdf> (retrieved 6-11-2014)

Kaspersky Security Network (2014), *16.37% Users Still Run Windows XP, Kaspersky Lab Statistics Say*, August 19 , available at: <http://www.kaspersky.com/about/news/virus/2014/16-37-per-cent-Users-Still-Run-Windows-XP-Kaspersky-Lab-Statistics-Say> (retrieved 6-11-2014)
Kroes N.(2014), *A secure on-line network for Europe Cyber security conference*, Brussels February 28, available at: <http://europa.eu/rapid/press-release_SPEECH-14-167_en.htm> (retrieved 6-11-2014)

McAfee (2014), *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies,* June, available at: <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (retrieved 6-11-2014)

McDonald E. (2013), *On-line fraud costs global economy 'many times more than $100bn'*, in "The Guardian", October 30, available at: <http://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars> (retrieved 6-11-2014)

Mick J*., Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit*, "Daily Tech" April 4 2011, available at: <http://www.daiytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm> (retrieved 6-11-2014)

MISE (2003), *Decreto interministeriale 14 gennaio 2003 - Istituzione Osservatorio permanente per la sicurezza e la tutela delle reti e delle telecomunicazioni*, available at: <http://www.mise.gov.it/index.php/it/?option=com_content&view=article&idmenu=1620&idarea1=0&idarea2=0&idarea3=0&andor=AND&sectionid=0&andorcat=AND&MvediT=1&cattitle1=Decreti%20interministeriali&partebassaType=0&showMenu=1&showCat=1&idarea4=0&idareaCalendario1=0&page=15&id=2017545&viewType=0> (retrieved 9-11-2014)

OPMI (2014), *Empowering the knowledge of small and medium enterprises management,* Divisione ricerche Claudio Demattè Osservatorio sulla competitività delle PMI, 10 Luglio 2014, SDA Bocconi, available at: <http://www.sdabocconi.it/sites/default/files/upload/pdf/report_PMI_10_luglio_2014.pdf> (retrieved 7-11-2014)

Paganini P. (2013), *Cost of cybercrime for UK Small Businesses*, in "Security Affairs", May 23, 2013, available at: <http://securityaffairs.co/wordpress/14628/cyber-crime/cost-of-cybercrime-for-uk-small-businesses.html> (retrieved 6-11-2014)

Perlroth N. (2014), *Home Depot Says Hackers Also Stole Email Addresses*, in "The New York Times", November 6, available at: <http://bits.blogs.nytimes.com/2014/11/06/home-depot-says-hackers-also-stole-email-addresses/?_r=0> (retrieved 7-11-2014)

Polizia di Stato (2014), *Relazione annuale 2014 della Polizia Postale e delle Comunicazioni*, provided to this research project by Vice*Questore* of Florence, Dr. Stefania Pierazzi.

Ponemon Institute (2013), *2013 Cost of Cyber Crime Study: United States*, available at: <http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf> (retrieved 6-11-2014)

Ponemon Institute (2014), *Exposing the Cybersecurity Cracks:A Global PerspectivePart IWebsense*, April, available at: <https://www.websense.com/assets/reports/report-ponemon-2014-exposing-cybersecurity-cracks-en.pdf> (retrieved 7-11-2014)

Presidency of the Council of Ministers of the Italian Republic, Dipartimento per l'Innovazione e le Tecnologie (2002) , *DIRETTIVA 16 gennaio 2002. Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni,* GU Serie Generale n.69 del 22-3-2002, available at: <http://www.gazzettaufficiale.it/eli/id/2002/03/22/02A03219/sg%20;jsessionid=nBvFj9k-8FcOCREFNlFaag__.ntc-as1-guri2a> (retrieved 9-11-2014)

Presidency of the Council of Ministers of the Italian Republic (2013), *Quadro Strategico Nazionale per la Sicurezza dello spazio cibernetico*, December 2013, available at: <http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf> (retrieved 9-11-2014)

PR Web (2014), *SMEs face increased risk of cyber attack*, September 8, available at: **<**http://www.prweb.com/releases/2014/09/prweb12147240.htm> (retrieved 6-11-2014)

PwC (2013), *Information Security Breaches Survey Technical Report,* available at: <https://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf> (retrieved 6-11-2014)

PwC (2014), *Global Economic Crime Survey. Le frodi economico-finanziariein Italia: una minaccia per il business Settima edizione,* available at: <http://www.pwc.com/it/it/services/forensic/assets/docs/gecs-2014.pdf> (retrieved 7-11-2014)

Quadrio Curzio A. e Fortis M. (2002), *Complessità e Distretti Industriali. Dinamiche, Modelli, Casi reali*, edited by Curzio and Fortis, Il Mulino, Bologna

Reynolds K. (2013)*, CryptoLocker Virus. Best Practices to Ensure 100% Immunity***,** 25-10-2013, in Comodo available at: <https://blogs.comodo.com/it-security/cryptolocker-virus-best-practices-to-ensure-100-immunity/> (retrieved 6-11-2014)

Ricciardi A. (2010), *Le Pmi localizzate nei distretti industriali: vantaggi competitivi, evoluzione organizzativa, prospettive future*, in Quaderni di ricerca sull'artigianato N°54 Rivista di Economia, Cultura e Ricerca sociale dell'Associazione Artigiani e Piccole Imprese Mestre CGIA Edited by Centro Studi Sintesi, available at: <http://www.quaderniartigianato.com/wp-content/uploads/2011/05/Quaderni-N%C2%B054.pdf> (retrieved 11-11-2014)

Robinson N. (2013), *The European Cyber Security Strategy: Too Big to Fail?*, available at: <http://www.rand.org/blog/2013/02/the-european-cyber-security-strategy-too-big-to-fail.html> (retrieved 6-11-2014)

Stempel J. (2014)*, Goldman says client data leaked, wants Google to delete email*, in "Reuters" July 2, available at:
<http://www.reuters.com/article/2014/07/02/us-google-goldman-leak-idUSKBN0F729I20140702>
(retrieved 6-11-2014)

Street Insider (2014), *The Home Depot Reports Findings in Payment Data Breach Investigation*, PRNewswire November 6, available at: <http://www.streetinsider.com/Press+Releases/The+Home+Depot+Reports+Findings+in+Payment+Data+Breach+Investigation/9986431.html> (retrieved 7-11-2014)

Symantec (2009), *National Small Business Study*, National Cyber Security Alliance e Symantec, available at: <http://eagleintelligence.com/wp-content/uploads/2009/12/NCSA-SB-Study-Factsheet.pdf> (retrieved 6-11-2014)

Symantec (2014), *Internet Security Threat Report 2014 Volume 19*, April, available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf> (retrieved 6-11-2014)

TimesLive (2012), *India training half a million cyber security experts*, October 16, available at: <http://www.timeslive.co.za/scitech/2012/10/16/india-training-half-a-million-cyber-security-experts>
(retrieved 6-11-2014)

TrendMicro (2013), *Guadagnare sulle informazioni digitali*. *Verifica di sicurezza annuale*, TrendLabs, available at: <http://www.trendmicro.it/informazioni-sulla-sicurezza/ricerca/trendlabs-2013-annual-security-roundup/index.html> (retrieved 7-11-2014)

UNODC (2013) *Comprehensive Study on Cybercrime,* February, available at: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> (retrieved 15-11-2014)

Vanson Bourne (2014), *Emc Global Data Protection Index*, available at: <http://www.emc.com/microsites/emc-global-data-protection-index/index.htm#infographic-italy>
(retrieved 8-12-2014)

Verga M. (Edited by), *L'obbligatorietà dell'azione penale come un mito? Appunti sul caso italiano*, Centro Universitario per le Ricerche sulla Sociologia del Diritto, dell'Informazione e delle Istituzioni Giuridiche (CIRSDIG), in "Quaderno dei lavori 2007, Terzo Seminario Nazionale di Sociologia del Diritto, A.I.S. – Sezione di Sociologia del Diritto", Working Paper n. 25, 2007, pp. 121-136, available at: <http://www.cirsdig.it/Pubblicazioni/capraia.pdf> (retrieved 11-11-2014)

Verizon (2014), *2014 Data Breach Investigation Report,* available at: <http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf>
(retrieved 15-11-2014)

Wagaman A. (2012), *Europe tests cyber security capabilities in simulation*, in "NewEurope" October 4, 2012, available at: <http://www.neurope.eu/article/europe-tests-cyber-security-capabilities-simulation-today> (retrieved 6-11-2014)

Wagner K. (2013), *More Than 70% of Email Is Spam*, Kaspersky Lab, available at: <http://usa.kaspersky.com/about-us/press-center/in-the-news/more-70-email-spam> (retrieved 6-11-2014)

WEF (2012), *Risk and Responsibility in a Hyperconnected World. Pathways to Global Cyber Resilience*, available at: <http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf> (retrieved 6-11-2014)

WEF (2014), *Global risks 2014 Ninth edition*, available at: <http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf> (retrieved 6-11-2014)

Zanier M. (2009), *Tra il dire e il fare. Obbligatorietà dell'azione penale e comportamenti degli attori giuridici*, EUM Edizioni, Macerata University Press

Zetter K. (2013), *Feds Arrest Alleged 'Dread Pirate Roberts,' the Brain Behind the Silk Road Drug Site* in "Wired" February 10, 2013, available at: <http://www.wired.com/2013/10/silk-road-raided/> (retrieved 6-11-2014)