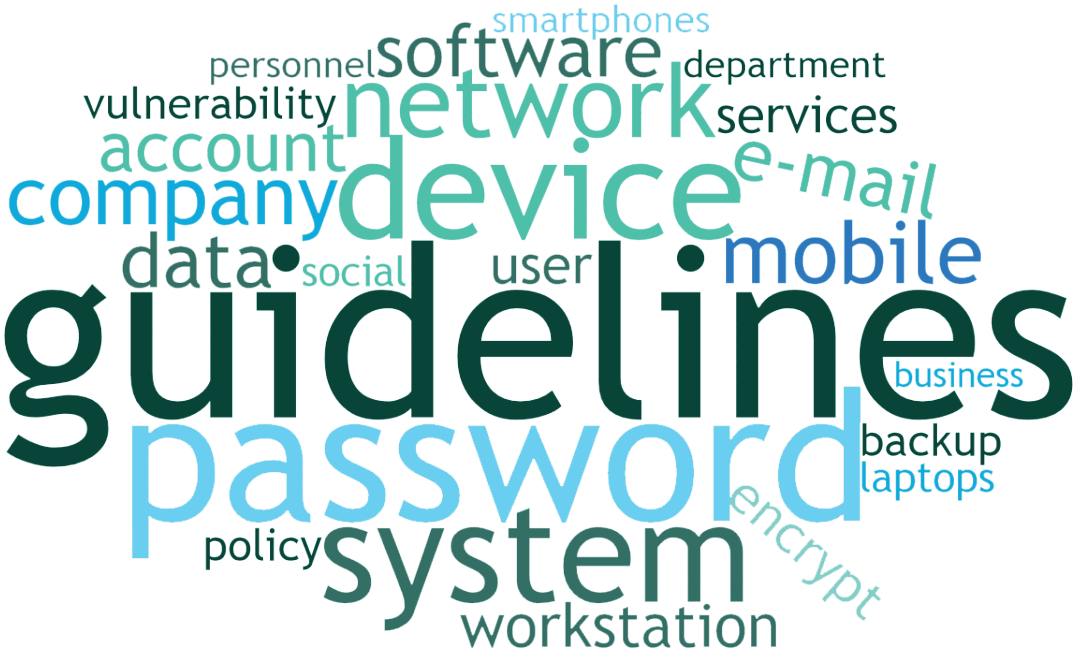
GUIDELINES FOR IT SECURITY
IN SMEs



unicri
United Nations
Interregional Crime and Justice
Research Institute

Fondazione
Cassa di Risparmio
di Lucca

United Nations
Interregional Crime and Justice
Research Institute

Guidelines for IT Security in SMEs

This study was conducted by Dr. Flavia Zappa Leccisotti.

Disclaimer

The views expressed are those of the authors and do not necessarily reflect the views and positions of the United Nations. Authors are not responsible for the use that might be made of the information contained in this publication.
Contents of the publication may be quoted or reproduced, provided that the source of information is acknowledged.
The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI, concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.
The mention of specific institutions, companies or of certain manufacturers' products does not imply that they are endorsed or recommended by the Secretariat of the United Nations or UNICRI in preference to others of a similar nature that are not mentioned.

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

Table of Contents

Acknowledgements

We would like to thank all of the people who contributed to this research study by providing valuable material and interviews, which has led the insights and observations obtained. In particular, we thank Judge, and Professor of Computer Science at the University of Rome La Sapienza, Giuseppe Corasaniti, Deputy Prosecutor Vito Sandro Destito from the Prosecutor's Office of Turin and Marco Tullio Giordano, Associate Criminal Lawyer at R&P Legal, for their willingness to clarify legal rules and procedures within this field.

Many thanks to all the companies, and their respective representatives, who have validated the guidelines drawn up for SMEs. These include: Dr. Davide Del vecchio of Fastweb, Dr. Pier Luigi Rotondo of IBM, Dr. Giuseppe Vinucci of Kaspersky, Dr. Andrea Piazza and Dr. Carlo Mauceli of Microsoft, Dr. Alessandro Burresi of Lucart, Luca Landucci of Lucense, and Matteo Fava and Dr. Santo Natale of Tagetik.

In addition, we would also like to thank Dr. Marilina Labia of Si.Camera, Dr. Monica Pellegrino of ABI Lab, Dr. Tocci of Unindistria and Rossano Rogani for the information provided and for their cooperation.

Executive Summary

IT security for small and medium enterprises (SMEs) represents one of the most important challenges for both the Italian and European economies. It is therefore necessary that a series of proactive measures are put into place with the aim of increasing awareness in this field.

This set of guidelines constitutes the first update following the release of the study entitled "*Cybercrime and the risks for the economy and enterprises at the European Union and Italian levels*", which was published in December 2014 by UNICRI. Within the study, the current situation concerning SMEs and computer related crime was thoroughly investigated.

SMEs make up 99.8% of European and 99.9% of Italian enterprises, respectively. In the European Union (EU), 86.8 million people are employed within this sector making SMEs the backbone of the Italian and European economies. While at the same time, they also represent a major point of weakness in terms of security.. As seen in the previous research study, the whole economy of a country is at risk if SMEs are attacked - considering that many national economic systems are largely based on the viability of this type of company.

The investigation carried out in 2014 underlines that the level of perception and knowledge regarding this threat, in Italy is still too low, as are the countermeasures being implemented by SMEs. A section of the previous study was dedicated to the different types of cyber threats and cyber attacks faced by enterprises. Various interviews were conducted with institutional bodies such as Public Prosecutors *(Procure)*, the Postal Police *(Polizia Postale)*, and a large number of SMEs with the aim of investigating their needs in order to understand what was lacking in their IT security.

This update will focus on data and trends regarding cyber crime for the first half of 2015. Italian case studies are analyzed in this report, and guidelines for SME's IT security have been drawn up. We believe that these guidelines can help SMEs to fill in the gaps which were identified during the previous study. The need to provide assistance to SMEs in identifying and defining suitable guidelines comes from the analysis of qualitative interviews conducted with companies during the previous research.

Accordingly a set of guidelines was drafted and has been submitted to, and validated by, IT security experts from leading companies, such as Fastweb, IBM, Kaspersky and Microsoft. Additionally, the guidelines were also reviewed by three IT managers from three

different enterprises who were interviewed within the previous study on SMEs (Lucart, Lucense and Tagetik). Cyber crime poses a severe risk to all types of enterprises present throughout Italy. Preventing these risks requires implementing initiatives based on both education and awareness. Action in this field is not only required on behalf of SMEs, but also needs to be taken into account at the national level. For this reason, we have also included within this report opinions relating to IT security from institutional bodies.

List of Acronyms

AIPSI	*Associazione Italiana Professionisti Sicurezza Informatica*
APT	Advanced Persistent Threat
BIS	Department for Business and Innovation Skills
BYOD	Bring your own device
C&C	Command and Control
CMS	Content Management System
DDL	*Disegno Di Legge*
DDoS	Distributed Denial of Service
EBA	European Bank Authority
EC3	European Cybercrime Centre
ENISA	European Union Agency for Network and Information Security
EU	European Union
IoT	Internet of Things
IT	Information Technology
MaaS	Malware-as-a-Service
POS	Point of Sale
PwC	PricewaterhouseCoopers
SME	Small and Medium Enterprise
UNICRI	United Nations Interregional Crime and Justice Research Institute
WEF	World Economic Forum

CHAPTER 1

Overview of the trends and impact of cyber crime in Italy: First half of 2015

Cyber crime is a growing phenomenon worldwide, representing a threat to citizens and the global economy. Cyber crime provides a huge source of income for criminal organizations and is a key priority for the European Agenda on Security, alongside terrorism and organized crime[1]. The latest World Economic Forum (WEF) report[2] on global risks confirms that cyber attacks remain among the major risks - both in terms of impact and likelihood of occurrence.

Even though the budgets allocated by large companies to combating cyber crime is increasing significantly every year, for small and medium enterprises (SMEs), it is still very hard to perceive cyber crime as a real threat to their businesses and survival in the market. Gartner data[3] has shown that by 2018 40% of large companies will have adopted appropriate security systems in order to defend themselves against cyber attacks. However, SMEs represent "easy" targets because they are less protected, unaware of risks, and are often not even able to detect the extent of theft which has taken place in the cyber setting. Moreover, SMEs that collaborate with major corporations, producing individual parts or who

1 Communication from the EU Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, European Commission, Strasbourg, 28-04-2015, available at: <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf> (retrieved 09-06-2015)

2 The Global Risks 2015 10th Edition, World Economic Forum, available at: <http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf> (retrieved 06-05-2015)

3 Cybersecurity: il 40% delle grandi aziende pronte ad attacchi cyber nel 2018, by Lorenzo Sorbini, Key4biz, 24-02-2015, available at: <http://www.key4biz.it/cybersecurity-40-delle-grandi-aziende-pronte-ad-attacchi-cyber-nel-2018/> (retrieved 21-05-2015)

play a role in complex projects, are easy targets for cyber criminals that wish to enter the systems of large corporations via backdoors.

Considering the growing trend regarding this type of threat, it is more necessary than ever to develop efficient preventative security systems. At the corporate level, damage is not only caused via a simple, one-off or indiscriminate attack. Instead, many attacks have long-term consequences. We are now witnessing an increase in targeted attacks that have the aim of appropriating sensitive data, deleting data altogether, or stealing copyrighted material This type of attack can interrupt the activity of a company for several days or months, damage its reputation, or even jeopardize its existence. With the increase in the use of IT tools within SMEs there is more of a chance of a company being attacked - from many different directions.

Alarm regarding this phenomenon also comes from authoritative sources such as the director of the European Cybercrime Centre (EC3), Troels Oerting[4]. Oerting has said that all companies need to take the risk of cyber crime seriously because they are all potential victims. Cyber crime is of a stronger nature and more widespread than one might imagine. In fact, most cyber attacks are still not being detected and/or reported. Losses due to cyber crime for an individual company can reach up to several million euros. Only companies that invest in the appropriate processes, procedures and technology will have long-term benefits in terms of security, reputation and profit.

It is a fact that SMEs are a very attractive target for cyber criminals; yet, SMEs unfortunately still underestimate this threat. A recent study by the UK government found that more than two-thirds of SMEs have never thought that they could become a victim of cyber crime[5]. However, the reality seems to be different. A report published by the UK's Department for Business and Innovation Skills (BIS) and PricewaterhouseCoopers (PwC)[6] shows that 60% of the SMEs involved had had their computers violated. SMEs are a very attractive target for cyber criminals; nevertheless, decision makers working in these enterprises still often underestimate the threat posed by cybercrime. No matter the nature of an SME's business, every company is seen as a lucrative target. Various types of information, be it intellectual property, commercial data and contact lists, personal data, account credentials, and more can be sold on the black market to individuals intent on committing fraud, spreading malware and facilitating other crimes.

4 Top 10 cyber crime stories of 2014, by Warwick Ashford, *Computer Weekly*, 31-12-2014, available at: <http://www.computerweekly.com/news/2240236215/Top-10-cyber-crime-stories-of-2014> (retrieved 28-04-2015)

5 Misunderstanding cyber threats puts a third of SME revenue at risk, by Neil Ford, 27-02-2015, available at: <http://www.itgovernance.co.uk/blog/misunderstanding-cyber-threats-puts-a-third-of-sme-revenue-at-risk/> (retrieved 30-04-2015)

6 2014 Information Security Breaches Survey, Department for Business, Innovation and Skills Cabinet Office, available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307297/bis-14-766-information-security-breaches-survey-2014-executive-summary-revision1.pdf> (retrieved 30-04-2015)

Due to large-scale cyber attacks in 2014, approximately one billion records[7] were compromised – affecting, on average, one in every three Internet users. Many of these records were totally unencrypted, and thus easy to exploit. Automated attacks are now cheap and easy to conduct, and being indiscriminate, are not aimed at a particular company or site, but instead have the objective of hitting the largest number of victims as possible through the exploitation of known vulnerabilities.

The time in which a cyber criminal is able to exploit a new vulnerability and it being patched is very short. In October 2014, for example, Drupal announced that users who had not patched their Content Management System (CMS) platform within seven hours after the discovery of a bug had to consider their website violated. The response speed is a high risk factor for SMEs, as they often lack the resources to tackle these automated attacks and to implement policies regarding patching and updating software as fast as large companies that are able to depend on prepared IT departments and conduct actions such as penetration tests and vulnerability assessments.

In recent research conducted by the UK government through the Cyber Streetwise campaign, it emerged that by underestimating the dangerousness of cyber crime English SMEs put a third of their revenue at risk, be it via susceptibility to data loss, financial loss or reputational damage. The SMEs interviewed in the study believed that security measures are too expensive, and these SMEs often do not know where to start with respect to implementation. It is clear that SMEs require support in order to try and mitigate the damage caused by cyber crime, build awareness, and increase security assets.

A recent report by HP[8] reveals that 44% of the violations that occurred in 2014 exploited known vulnerabilities dating back to 2-4 years prior. Moreover, according to this study, the main flaw exploited by cyber criminals was misconfiguration, which had unnecessarily exposed companies to attack. This not only shows that knowledge in this area is still low, but it also demonstrates the level of superficiality that still exists in the maintenance of IT equipment within companies.

Websense Security Labs has recently released its *Threat Report 2015,* which shows that more and more criminals are creating increasingly sophisticated threats by adopting cutting-edge tools already in existence (in other words, tools which are not being developed from scratch). In the cyber crime world, codes and programs (which are the basis of new threats) are in fact exchanged, leased and sold. The exchange network of these instruments is increasing rapidly, thus allowing even unskilled individuals to commit cyber criminal acts (Malware-as-a-Service, MaaS). For example, in 2014, 99.3% of Command and Control (C&C) used for malware had already been used before, and, in 98.2% of cases, had already been

7 Why SMEs are an attractive target for cyber criminals and what they can do about it, by Neil Ford, 02-03-2015, available at: <http://www.itgovernance.co.uk/blog/why-smes-are-an-attractive-target-for-cyber-criminals-and-what-they-can-do-about-it/> (retrieved 21-05-2015)

8 HP Cyber Risk Report 2015, HP, available at: <http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/> (retrieved 01-05-2015)

used more than 5 times. The same study found that 81% of the e-mails scanned by Websense were considered malicious.[9]

According to *The Guardian*[10], cyber threats that will generally have the greatest trend increase in 2015 will be the Advanced Persistent Threat (APT) and increasingly sophisticated spam. In regards to spam, the most interesting aspect is that its volume is decreasing in absolute measure, but at the same time it is becoming increasingly more sophisticated - making it even more difficult for anti-spam software to filter messages. The result is that users receive more spam e-mails in their inboxes. This finding is also confirmed in the latest *Symantec Internet Security Threat Report*[11].

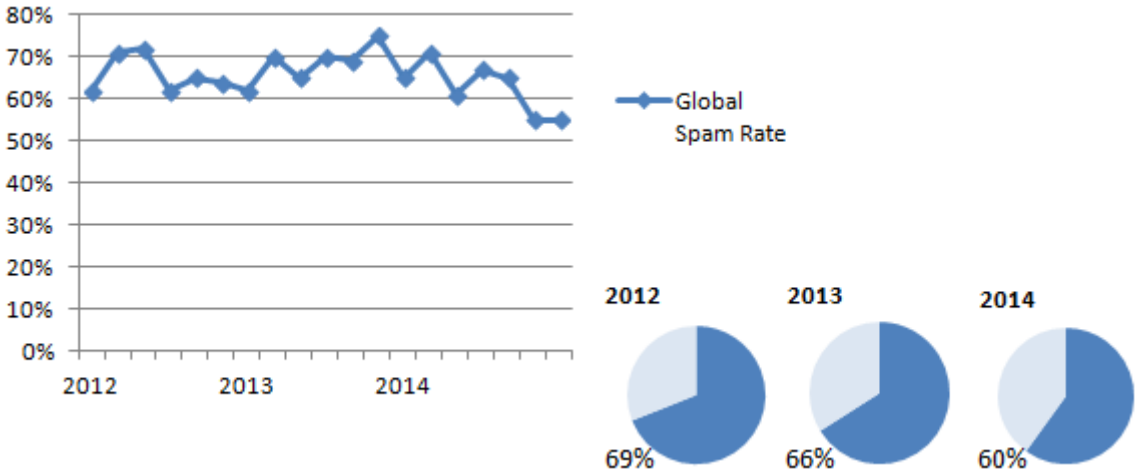


Figure 1 – Global Spam Rate, 2012-2014
Source: Internet Security Threat Report, Symantec, 2015

Furthermore, ransomware is not showing any signs of decreasing in activity. The number of this type of attack more than doubled in 2014 – rising from an estimated 4.1 million attacks in 2013, to 8.8 million in 2014. From a psychological point of view, ransomware represents a very profitable form of attack because if a victim has not performed regular backups of their data, they are normally willing to pay the ransom in order to be allowed to retrieve it.

9 Websense Threat Report 2015, fare cybercrime è sempre più facile, Websense Security Labs, 13-04-2015, available at: <http://www.techfromthenet.it/201504101252/News-analisi/websense-threat-report-2015-fare-cybercrime-e-sempre-piu-facile.html> (retrieved 22-04-2015)

10 How you could become a victim of cybercrime in 2015, The Guardian, 24-12-2014, available at: <http://www.theguardian.com/technology/2014/dec/24/cybercrime-2015-cybersecurity-ransomware-cyberwar> (retrieved 10-04-2015)

11 Internet Security Threat Report, Symantec, April 2015, available at: <https://know.elq.symantec.com/LP=1542> (retrieved 22-06-2015)

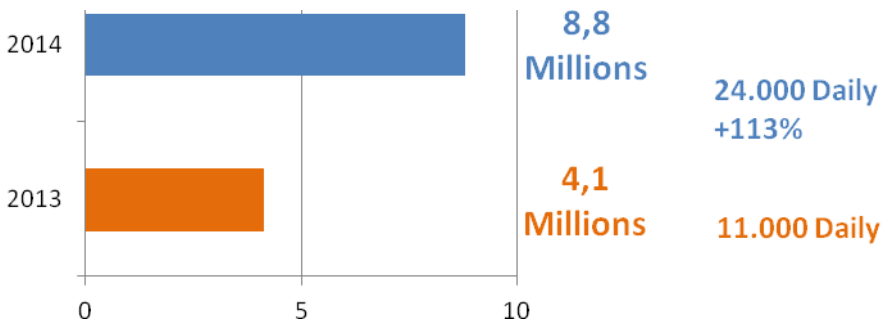


Figure 2 – Ransomware Total
Source: Internet Security Threat Report, Symantec, 2015

Another interesting topic in 2015, from the perspective of cyber criminals, is the increased widespread use of on-line economic transactions - also being carried out via mobile devices. With reference to mobile devices, 2015 may be the year that sees the myth of the iPhone's inviolability with regard to cyber attacks erased; however, the Android platform will remain the preferred target for cyber criminals. According to BitDefender[12], which published a list of the ten biggest scams on Facebook in 2014, in 2015 this kind of fraudulent activity will tend to increase because of the growing user base of social networks - obviously of great interest to criminals. In 2014, we saw a strong turnaround regarding the dissemination of social network scams, recording a dramatic increase in the exchange of malicious video and messages between real users.

The Clusit 2015 Report also confirms that cyber crime is a growing phenomenon and that it is the main cause behind computer attacks. According to the Fastweb analysis included within the report, 93% of attacks [13] are in fact due to cyber crime.

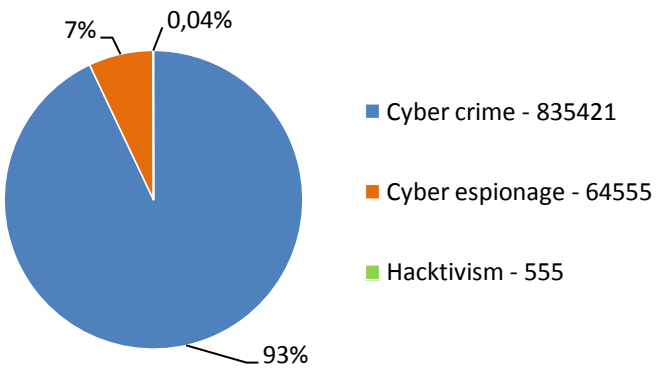


Figure 3 – Fastweb data on the motivations of attackers
Source: Clusit, 2015

12 It's been a great year! Thanks to these Facebook scams for being a part of it..., *The Guardian*, 24-12-2014, available at: <http://www.theguardian.com/technology/2014/dec/24/facebook-scams-malware-naked-videos> (retrieved 10-04-2015)
13 Data from about 6 million IPv4 addresses (including both customers and Fastweb networks), belonging to Fastweb SpA AS, collected and analyzed by the Security Operations Center

The main problem is that the risks related to a low IT security prevention level are growing faster than the ability to protect against cyber attacks. While investment in information security has increased in recent years, the number of attacks and their severity level continue to rise. The report also estimates that two-thirds of incidents are not even reported by the victims due to lack of skills and appropriate tools.

In terms of risk prediction for 2015, the report identifies social networks as one of the biggest critical points because of their expansion - not only as a network between users, but also as a showcase for SMEs and large corporations. It makes social networks an attractive platform for the spread of malware and for the purpose of committing fraud. Among other trends in 2015, the Clusit report highlights the fragility of Point of Sale (POS) systems. Cyber criminals are increasingly hitting these systems because of the ease with which they can exploit ad-hoc cheap malware used for financial fraud. Another critical point will be mobile devices, due to their increased use for making purchases - so-called "m-commerce". Finally, the continued spread of ransomware, such as Cryptolocker, is also a threat to this field.

A study conducted by SecuRe Pay, the European forum on the security of retail payments, claims that for the years for which it had data (2011 and 2012), there was an increase in fraudulent e-commerce transactions of 21.2%. In fact, 94 million euros were stolen from users that had made on-line purchases with credit cards[14] - a figure so worrying that it pushed the European Bank Authority (EBA) to publish guidelines regarding e-commerce that will be in place by next August. The guidelines will include information on the verification of clients' identity before proceeding with the on-line transaction, and providing clients with customer service information and assistance regarding the issue of on-line payment security. According to the EBA, "card not present" fraud constitutes 60% of the 1.33 billion euros stolen in 2012[15]. We must also consider that almost half of the users who were victimized from a scam as a result of on-line purchases were not able to recover their money[16].

With the rapid spread of smartphones and tablets, 2014 has seen even more criminals exploiting these new points of attack. In a report published at the end of 2014, Alcatel-Lucent's Motive Security Labs[17] has estimated that more than 16 million mobile devices around the world have been infected with malware for the purpose of carrying out industrial and personnel espionage, to steal information and to attack companies, private,

14 Ecommerce: le frodi costano 794 milioni l'anno, by Marco Boscolo, Wired Italia, 30-12-2014, available at: <http://www.wired.it/economia/business/2014/12/30/pagamenti-online-frodi-valgono-794-milioni-lanno/?utm_content=buffer4be2c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> (retrieved 05-03-2015)

15 New report on card fraud shows online fraud increased in 2012, European Central Bank, Press Release 25-02-2014, available at: <https://www.ecb.europa.eu/press/pr/date/2014/html/pr140225.en.html> (retrieved 05-03-2015)

16 Acquisti online e frodi: il 44% degli utenti non recupera il denaro, La Stampa tecnologia, 24-12-2014, available at: <http://www.lastampa.it/2014/12/24/tecnologia/acquisti-online-e-frodi-il-degli-utenti-non-recupera-il-denaro-Ft9RDDFyPpYTbyoJi1J96J/pagina.html?utm_content> (retrieved 20-03-2015)

17 Motive Security Labs malware report – H2 2014, Alcatel-Lucent's Motive Security Labs, available at: <https://resources.alcatel-lucent.com/asset/184652> (retrieved 23-03-2015)

banks and government. In 2014 alone, mobile device infections increased by 25% (an increase of 5% compared to 2013).

The continued growth of mobile malware is mainly due to the use of devices without employing the necessary security precautions, especially in the workplace where the device is used in the same way as it is for personal use. Six of the 20 most common types of malware are spyware: applications used by criminals to spy on the owner of the phone - tracing it, monitoring incoming and outgoing calls and reading text messages. Among the other top 20 malware there are scareware applications: used to extort money by claiming to have encrypted a phone's data; applications that steal personal information from a device; and then there are the web proxy applications that allow hackers to browse the web anonymously at the owner's expense through an infected device. This data is alarming if we consider that the level of user awareness regarding mobile device use is still very low. A recent study by Kaspersky Lab and B2B International[18] shows that nearly 30% of users do not even know what malware is.

In this environment, the very low level of attention and awareness of users who often download applications and visit unsafe sites is evident. The aforementioned Symantec report states that 17% of all Android applications (almost one million) contain malware.

The human factor in cyber crime is always the most decisive, even in the processes related to the use of mobile devices - and this factor undoubtedly represents the weakest link. Research conducted by Carnegie Mellon University in Pittsburgh[19] found that the average user's already low level of mistrust towards unsecure software is completely ignored if the file for download is also linked to a financial incentive - even if the financial incentive is paltry. Researchers at Carnegie Mellon University shared a program within its network that offered a small cash credit in exchange for a download, whilst at the same time issuing a warning of the potential risks related to the download of uncertified software. The result was that 22% of the users who downloaded the file did so for only one US cent, 36% for 50 cents, and 42% for 1 US dollar. The result of this research confirms that the spread of cyber crime is undoubtedly facilitated by human behavior. The lack of awareness about the dangerousness of the web allows for user behavior that aids the spread of viruses and allows for the creation of fraud or other types of attacks - behavior on which cyber criminals rely.

18 Kaspersky Lab Survey: un utente su quattro non comprende i rischi delle minacce informatiche mobile, Kaspersky Lab, 27-02-2015, available at: <http://www.kaspersky.com/it/about/news/virus/2015/Indagine_Kaspersky_Lab_un_utente_su_quattro_non_comprende_i_rischi_delle_minacce_informatiche_mobile> (retrieved 28-03-2015)

19 It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice, by Nicolas Christin, Serge Egelman, Timothy Vidas and Jens Grossklags, INI/CyLab, Carnegie Mellon University, National Institute of Standards and Technology, ECE/CyLab, Carnegie Mellon University, IST, Pennsylvania State University, available at: <https://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf> (retrieved 07-05-2015)

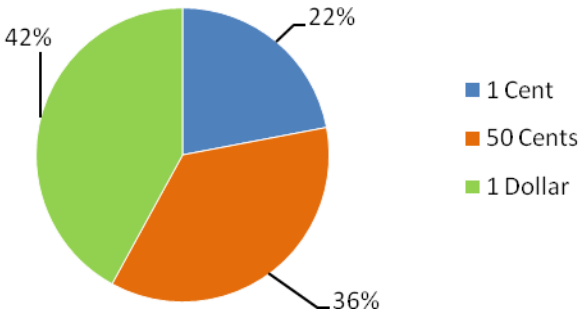


Figure 4 – Software download distribution, related to an economic incentive
Source: Carnegie Mellon University, Pittsburgh

A study by Kaspersky Lab shows that more than a quarter of mobile device users also ignore basic security practices, not taking into consideration the sensitivity of the data stored in the device (addresses, e-mail or social network passwords, banking information, and other data such as personal photos, videos, and SMSs). The study also confirms low-level use of antivirus software and basic protection like passwords or PINs, and that Android devices are the most vulnerable - especially for the least competent users.

The critical nature of the human element also emerges in a study conducted by the Ntt[20], which found that in the days following a weekend or public holidays there was a 75% increase in the number of infected machines - highlighting just how much the user constitutes a real danger for a company's infrastructure due to the undifferentiated use between work and private devices.

A Kaspersky Lab survey regarding Bring Your Own Device (BYOD)[21] policies shows that 62% of employers and employees regularly use private devices for work purposes, often without effective protective measures. In fact, 92% of respondents store sensitive corporate data on smartphones and tablets used for both work and private life, and 60% of employees think the activation of security systems is the responsibility of the company they work for. For SMEs, the percentage of workers and business owners who consider cyber threats a real and dangerous risk is still very low, while, conversely, nearly 60% of large companies are seriously alarmed by the phenomenon of cyber crime.

Phishing is still one of the most common methods of attack. Despite possibly being the most well-known cyber-attack technique, the percentage of users who click on phishing e-mails is still very high, even today. The 80,000 security incidents analyzed in the *Verizon*

20 Cybersecurity, così Intelligence e imprese possono collaborare, by Michele Pierri, 16-03-2015, available at: <http://www.formiche.net/2015/03/16/cybersecurity-minniti-ruffinoni/> (retrieved 20-03-2015)
21 Consumer Security Risk Survey 2014: Multi-device threats in a multi device world, Kaspersky Lab, July 2014, available at: <http://media.kaspersky.com/en/Kaspersky_Lab_Consumer_Security_Risks_Survey_2014_ENG.pdf> (retrieved 28-05-2015)

Data Breach Investigation Report[22] have led to economic damage and data loss of more than $400 million for the companies involved. Phishing is confirmed as being one of the most commonly used attacks, even though it is a longstanding social engineering technique. However, there is still not enough attention paid to it, especially with regard to the human factor. Despite years of experience people cannot resist the temptation to click on malicious links. Verizon data confirms that this trend is growing. The percentage of users who click on a phishing e-mail has risen from 10% last year to 23% this year. The data shows that 11% of users also open attachments in e-mails that contain malware, which is even more disheartening. The Verizon study therefore shows how highly profitable it is for a cyber criminal to use phishing techniques. Based on the data analyzed, for every ten phishing emails sent out, there was a more than 90% chance that at least one user would fall victim to an attack. The experiment conducted by Verizon's researchers estimated that almost 5% of users click on a phishing e-mail during the first hour of it being sent. This data suggests that with adequate user training, the human factor can be a more effective censor in detecting phishing e-mails than any technological tool. Data taken from an Intel Security survey of 19.000 users in 144 countries revealed that only 3% had succeeded in recognizing all phishing e-mails, and 80% failed to identify even one[23].

22 2015 Data Breach Investigations Report, Verizon, available at: <http://www.verizonenterprise.com/DBIR/2015/> (retrieved 25-05-2015)

23 Il 97% di chi naviga su Internet non sa riconoscere il phishing, Il secolo XIX Tech, 23-05-2015, available at: <http://www.ilsecoloxix.it/p/magazine/2015/05/23/AR7IpzXE-phishing_internet_riconoscere.shtml> (retrieved 05-05-2015)

CHAPTER 2

Empirical survey on the impact of cyber crime in Italy: Interviews and Case Study

IT security is a topic that requires a sound knowledge of all aspects involving cyber crime. The lack of official national studies and statistics regarding this phenomenon was one of the factors that encouraged the development of an empirical approach for carrying out our previous research. To give continuity to the original study, it was decided that interviews should be conducted at the national level in order to address other strategic aspects in this area. This decision was made in order to study the characteristics of the phenomenon of cyber crime, which can provide qualitative information that is useful in understanding the evolution of threats, the actions to be put in place to prevent damage, and the general level of awareness about this phenomenon.

ABI Lab data

One of the most sensitive sectors with respect to cyber crime is the banking sector. For this reason, the 2015 Observatory Computer Fraud and Security Report: "*Security and Computer Frauds in Banks. How to Prevent and Combat Fraud on the Internet and Mobile Banking*,"[24], (provided for this research by Dr. Monica Pellegrino from ABI Lab) was analyzed.

The financial and banking sector is undoubtedly one of the most attractive sectors for cyber criminals, not only for financial theft but also for the theft of information assets

24 The report contains results of the survey conducted by ABI Lab on Internet and mobile banking fraud. In this edition, 45 banks and 4 outsourcer and specialized companies have participated

managed by banks. In the digital age the value of information and data is becoming increasingly important. An analysis carried out by ABI Lab shows that in 2014 80% of banks studied cases of identity-related crime affecting their own retail customers, and 66.7% studied crimes affecting their corporate customers. The statistics that correspond with the case studies will be analyzed later in this chapter, which will provide an in depth view concerning the type of fraudulent transactions committed by cyber criminals. Among the various types of fraud in existence, fraud via wire transfer is the most commonly used method for making unauthorized transactions, as experienced by retail clients. The report also shows an increase in the use of prepaid cards by defrauders; however, for corporate customers the wire transfer is the only mode used to transfer large amounts of money especially to foreign banks accounts[25]. A relevant fact is that even if fraud affecting retail customers is greater in comparison to corporate clients, the largest loss, in terms of economic value, associated with unauthorized transactions concerns corporate customers - as much as 72.3% of the total. As far as attack vectors are concerned, the report states that crimeware continues to be the most commonly used method of committing fraud, especially against companies - which suffer more targeted attacks. Specifically, there was an increase in fraudulent transactions made during legitimate client sessions (Man-in-the-Browser) corresponding with 60% of the attacks that affected companies, as well as cases of phishing and attacks in which a combination of techniques were used.

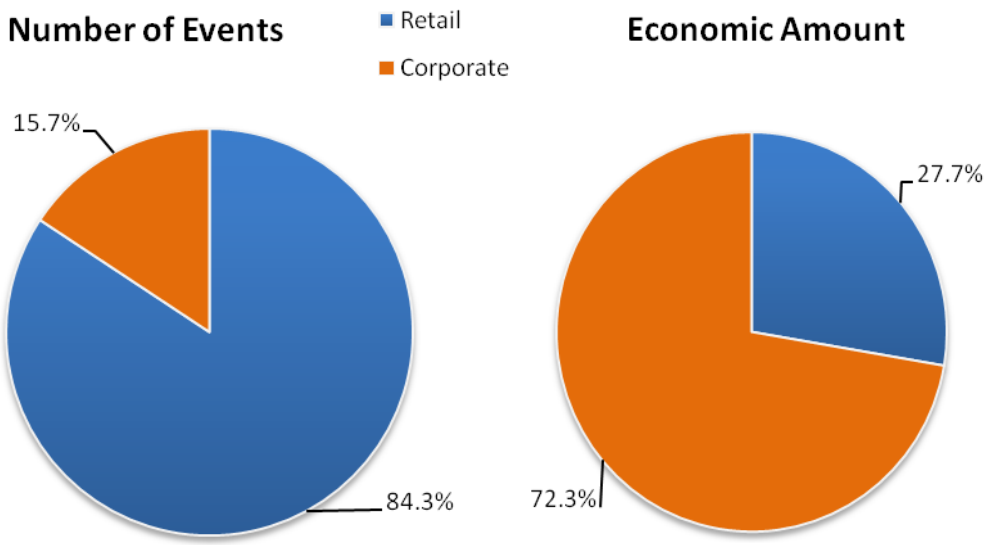


Figure 5 - The total effective transactions, divided by segments
Source: Sicurezza e Frodi Informatiche in Banca, ABI Lab, June 2015

25 Proof of how criminal organizations increasingly maintain extra-national coordination and networks. At the same time, the criminals are aware of the main difficulties faced by banks in blocking actions addressed to foreign recipients in a timely fashion

Si.Camera and Unindustria: compared experiences

The chamber system and trade associations are the institutions that have the most direct contact with companies. For this reason we involved Dr. Labia of Si.Camera and Dr. Tocci of Unindustria with the aim of investigating the situation regarding SMEs and cyber security at the national level.

In recent years, a lot has been done to combat cyber crime. For SMEs the priorities are strongly related to prevention and educational activities, but the widespread distribution of organized and coordinated national training and support activities regarding cyber crime for SMEs is still lacking. This is confirmed by both Dr. Labia, who is the Head of The Intellectual Property and Anti-Counterfeiting department and Head of the Supply Chain Development of territories at Si.Camera, and Dr. Tocci, working in Affairs and Official Contracts for Unindustria Rome. The initiatives that have been carried out until now are in fact only local. According to Dr. Labia, the level of knowledge about cyber crime is still very low, as is the level of attention given to this problem by companies. *"The level of information and awareness has certainly grown in recent years but it is still quite low. Companies operating within the 'Made in Italy' sector appear more sensitive. We are facing an important and urgent matter that impacts on business life and competitiveness of enterprises as a whole. It's a corporate culture matter. The actions to be put in place are awareness, training and one on one support. It is mandatory to raise the professionalism of operations within companies starting with the administrators, involving them in individual coaching but also in the networking process."*

Dr. Tocci agrees and notes that the level of attention changes according to the size of the company, with bigger companies being very careful and smaller companies less so. In addition, Dr. Tocci thinks that Italy is still lacking *"a culture of company data as a strategic asset and is therefore ill-equipped with tools in order to prevent cyber crime events which undermine know-how and business."* This is in fact more crucial than ever in the implementation of a security culture. The use of the computer as a tool is increasingly critical in the context of theft and counterfeiting of products, patents and trademarks.

The opinions of two Italian IT companies

The aim of cyber criminals is not only to create immediate damage, but also to gain control of the victim's systems in order to conduct more sophisticated attacks. An interview with a company called Certego regarding these new attack scenarios was therefore carried out. Certego, founded in 2013, is an innovative organization with headquarters in Modena. Certego specializes in fighting cyber crime and managing IT security services. Certego has actually developed a platform capable of identifying the presence of anomalies within network traffic and in the execution of internal application processes within a system, analyzing and identifying the presence of possible cyber attacks.

Through analysis of the data provided to us by Certego, which was collected through their Breach Detection, Investigation & Response service[26] within the networks monitored by the company,[27] the following is evident: in the first five months of 2015 alone, 278 "true positive" attacks were detected. These attacks got through the defense barriers imposed by main IT security technologies (firewalls, antivirus software, intrusion prevention systems, etc.). In addition, an important fact to be considered is that as many as one-third of the detected attacks were classified as critical, meaning that there was a considerable risk to the business or operations of a company and required immediate action.

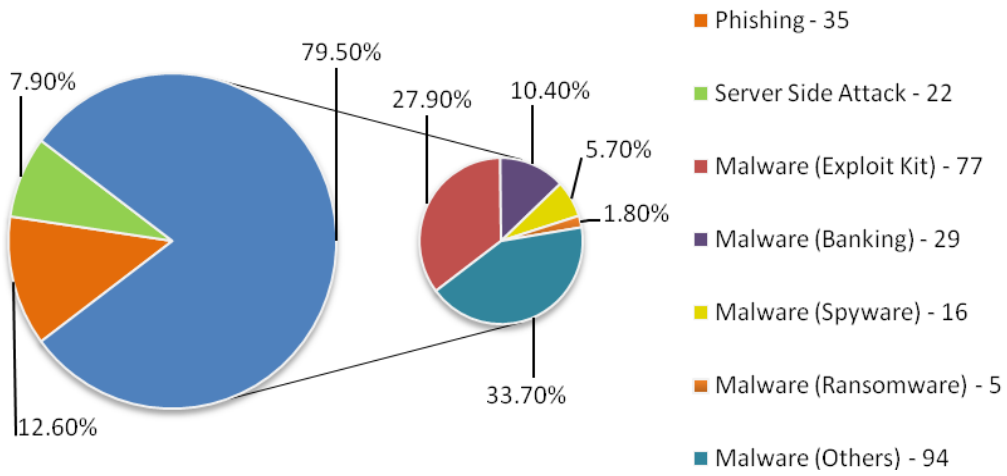


Figure 6 – Distribution of the attacks within the networks monitored by Certego
Source: Certego, 2015

As shown in the graph, 12.5% of all successful attacks are represented by phishing, namely e-mails that have passed the technical barriers of spam filters and are able to deceive recipients. 79.5% of detected threats include all types of malware, for example ransomware, spyware, and exploit kits of programs such as Adobe Reader, Java Runtime and Adobe Flash. These attacks also passed antivirus software protection and were installed by users. The remaining 8% are related to server-side attacks that targeted the resources of a server or an application.

An important observation of Dr. Roberto Tanara, Lead Consultant of Certego, is that *"for macro categories the distribution of threats we have observed against SMEs does not differ a lot from that of large companies, which confirms that cyber crime is opportunistic in nature with large scale operations, with no distinction between small companies and large organizations."* Dr. Bernardino Grignaffini, CEO of Certego, adds that *"For this reason, even the small ones should have the same concerns as larger ones, albeit with fewer available resources."*

26 With the average number of monitored systems daily being approximately of 15,000, divided among clients, servers and mobiles
27 Relating to SME customers in the north-central area of Italy

As far as the timing of remediation is concerned, not all companies are so careful even after reporting an incident. Certego still records cases where sensibility and responsiveness after an attack are very low.

Given the lack of complete and comprehensive statistics in Italy regarding the extent of cyber crime, Dr. Tanara and Dr. Grignaffini underline the importance of the promotion of a data culture, for example, by establishing a platform for anonymous data sharing that would therefore depict a situation closer to reality.

The low level of attention maintained by Italian SMEs regarding the dangers of cyber crime is a common aspect in all regions. Rossano Rogani, a member of the *Associazione Italiana Professionisti Sicurezza Informatica* (AIPSI) admits that when speaking about SMEs, the level of computerization and awareness about cyber crime is still very low in his territory. *"In some cases we even find the same shortcomings in large companies."* Rogani also notes that recently in his area there has been an increasing trend of ransomware cases (especially Cryptolocker) and attacks on websites. Regarding this aspect, he points out that the culture of information security is still very low, even among web agencies who make web sites without paying significant attention to security. This behavior leads web sites to become easy targets for cyber criminals. In the past two months, Rogani has assisted more than 20 SMEs that were victims of ransomware. In his opinion, this is a very serious phenomenon and the first step to address it is to educate and train staff in the correct use of computer systems. But, unfortunately, in his region there are not any training initiatives in place yet at the institutional level.

Legal field: compared experiences and opinions

In order to better understand what an SME faces after suffering an attack, we asked the opinion of Marco Tullio Giordano, lawyer and expert in the field of criminal law of new technologies at the law firm of R&P in Milan. A trend that Giordano has recorded in recent months is that there has been a significant increase in cases related to Man-in-the-Middle attacks and industrial espionage. The Man-in-the-Middle attack is a type of silent attack in which the attacker infiltrates the victim's systems (or the victim's partner's system). In this case, the attacker studies the cyber habits of two victims for a long period of time, reading and modifying communications between the two parties whilst keeping his presence hidden.

Specifically, Giordano presented us with a case study concerning a manufacturing company in northern Italy with a low-level presence on the Internet due to its product not being directed at the end user, but to other very specific business clientele. This company received an e-mail from an Asian supplier in which it was asked to make all ensuing payments into a new bank account, which had been opened at a British bank in order to facilitate its European customers. Over the next three months this Italian company made transfers totaling 600,000 euro. As an added measure of security, when the CFO of the

company made the payments to the bank account he wrote the name of the Asian supplier as the beneficiary. The criminals tried to profit further from this by asking for the transfers to be made again, claiming that the payments were unsuccessful due the transfer not being made out to the name of account holder. At this point the Italian company realized that something was wrong. After investigating further, the company became aware of the scam and enlisted a law firm specializing in these cases to deal with the situation. Initially, the firm focused on the anomalies taking place at the moment the account was opened with the British bank, but the bank refused to give information about the account holder due to privacy regulations. After verification was obtained through a request from the Asian supplier, it was discovered that the invoice was made by a third party. *"The European laws that protect payments made to anyone other than the account holder is a real fallacy of the system"*[28] Giordano declared, and he went on to say that *"Unfortunately there is nothing that can be done. Intervention at European level is what is required."* The obligation to activate an alert when the bank receives an economic transaction for large amounts with the beneficiary stated as something different from that of the actual account holder is lacking. Following a complaint and a request by the Italian law firm, the British bank returned to the victim the amount which was remaining in the account and closed it, admitting the alleged wrongdoing, but without providing additional details relevant to the investigation. Giordano's office has made various attempts to redress the issue, even consulting a law firm in London, but given the nature of the law, the chance of recovering the lost amount in full is almost nil.

In this case, the criminals had infiltrated the communications between the two companies for a long period of time. They monitored and blocked e-mails from the authentic Asian supplier, sending fake but extremely well made e-mails in their place.

The damage caused in this scenario was the equivalent to one year's earnings for this Italian company, and it had to close its research and development department as a consequence. The feedback given by Giordano's clients reflects feelings of abandonment and frustration due to never having been alerted to the dangers of cyber crime by any trade association in which they are enrolled. *"The low rate of prosecution involves another critical aspect. What can happen is that the police do not receive complaints or close them after a very short time causing the victim feel completely abandoned by the institutions. This is a message that must not continue."* Although the rate of prosecution for this type of crime is very low due to of the trans-nationality of the phenomenon, we should not allow victims to feel abandoned by institutions. Above all, we should aim for more education and training for the law enforcement officials who deal with the victims of cyber crime.

The level of knowledge relating to cyber crime is so low, as reflected in the cases referred to us by Giordano, that there are actually companies who initially thought they had been cheated by the supplier - totally oblivious to the existence of this type of cyber crime.

28 For more details, see: Art. 74 of Payment Service Regulation 2009 (PSR) United Kingdom and Art. 24 of L. 11/2010, c.d. Testo Unico Bancario and to: Attuazione del Titolo II del Decreto legislativo n. 11 of 27 January 2010 relativo ai servizi di pagamento (Diritti ed obblighi delle parti), Banca d'Italia, Eurosistema

"Trade associations should promote more widespread training events on this topic. Even just trade associations or banking institutions sending out newsletters would at least limit cases like this and would raise the level of attention." From what was said by Giordano, one can conclude that cyber criminals are studying the banks which have minimum diligence and a lack of additional control parameters in order to commit fraudulent activities. *"We need the information before these cases occur and an international institutional connection after the event in order to centralize the investigation."* The time frame for dealing with these cases is currently too long. On average, an incident is discovered after a few months, and then more months pass before the affected companies understand what they must do. In these cases, the amounts taken from the companies are high and often undermine their survival.

Giordano additionally mentioned that: *"Another trend that we register concerns industrial espionage cases."* Often these cases involve employees who either go out on their own or change company, and steal data and know-how from the company they have left by leveraging their access levels or forcing IT systems open. A recent case handled by Giordano involved an ex-employee from an Italian company accused of transferring know-how and a customer database to their new (foreign) company. The new company subsequently contacted customers to offer the same products at a quarter of the price. As a result the Italian company had to lay off some employees. *"With these cases however it is possible to do something more."*

The Deputy Prosecutor of the Prosecutor's Office of Turin (*Sostituto Procuratore della Procura della Repubblica di Torino*), Dr. Vito Destito, is of the same opinion, *"Better results were obtained in cases involving a corporate insider compared with other types of cyber crime, at least in regards to the investigation, identification of the person responsible and the prosecution. It is characterized by a manager, designer or other person who is connected by employment to a particular company who then breaks the relationship in order to undertake a new one (become employed by another organization or become self-employed) and steals corporate data from the previous workplace. This phenomenon is related to cyber crime because the access for their own purposes is incompatible with those of the institution that allowed them the access in the first place which constitutes illegal access to computer system even if the person who is logging was equipped with the credentials."*

In one case reported to us by Dr. Destito, a designer from a manufacturing company in Piedmont stole and transferred all his employer's projects to the German company in which he was going to start working, stealing the entire collection of the Piemontese company's know-how.

In a second case, also provided to us by Dr. Destito, a marketing employee of a manufacturing company stole some project data related to sheet metal machinery. These project data were then sold to a British company that has since opened a subsidiary in Italy. In this case the employee *"should not have had access to projects (in this case the offense is being contested under Article 621 c.p., that is, information which is to be kept a secret of which the subject has come to possess illegally and not of that of the next Article relating to*

communication of information of which the person obtained legitimately). Meaning, this was made possible by 'badly' distributed access to corporate data. The employee should not have had access to the company's project data. This happened due to a low level of internal security that did not provide a subdivision of levels of access relating to the data that the individual could and could not access in relation to the undertaken role."

As reported to us by Dr. Destito, often in cases such as these the plaintiff company begins the investigation in a definitive manner, assisted by IT and business consultants and even private investigators. The enquiries carried out by the Prosecutor of Turin start with an examination of the cyber documentation that proves the suspicion of the crime as described by the victim. Following this, a computer requisition is performed at the company in which the insider has started his new role (and this is also done at the insider's home), designed to collect computer data used. Next, a comparative examination of data, projects and databases (e.g. customer lists) is carried out. This task is assigned to a consultant who reconstructs how, and how frequently, the stolen data has been used. Very often such action requires both technical-mechanical engineering skills and computer skills.

In the opinion of both Giordano and his colleague, Attorney Giuseppe Vaciago, *"The drafting of appropriate behavior policies and the adoption of regulations regarding the use of corporate information technology would be highly recommended. It would be very useful both in preventing this kind of incident and in order to have a documental basis from which to carry out an internal investigation using digital forensics techniques in the case of illegal conduct."*[29]

In recent years, the focus on cyber crime has increased, including within the legal field; however, while a lot has been done there is still much more to do. One of the first Magistrates to deal with this phenomenon, and one of the few to have achieved important investigative results at the Prosecutor of Rome's Office (*Procura della Repubblica di Roma*), is Magistrate Giuseppe Corasaniti[30]. Since 2012, he has been working with the General Prosecutor of the Supreme Court (*Procura Generale della Corte di Cassazione*) in trying to settle the differences between Public Prosecutors (*Pubblici Ministeri*) in this matter. Corasaniti notes that *"Unfortunately cyber crime as a trend has been increasing steadily since the '90s and this is due to the availability of tools on the Internet and its relative ease of use. At the same time international cooperation has also improved as has broadening of the countries belonging to the Budapest Convention of 2001,"*. He also added that, *"We are working on updating the Convention of the Council of Europe, which has remained the same since 2001. On-line tracking should be implemented and above all a research system for the cloud due to it becoming the rule not the exception."* Obviously the transnational nature of

29 La sicurezza informatica, un asset aziendale strategico, by Giuseppe Vaciago and Marco Tullio Giordano, Rivista 231 (02-2015) pag. 273

30 General Deputy Prosecutor of the General Prosecutor of the Republic in the Supreme Court. He is among the most experienced researchers dealing with legal matters concerning communication and information technology and IT Law. Member of 24/24 group, for the Council of Europe, that provides assistance to requests from foreign judges

this type of crime creates many problems for criminal prosecution. This fact has also emerged in the data of the previous report published by UNICRI[31]. Much more can still be done to address this issue such as "*improving the international cooperation instruments that already exist and that are defined by the Convention of 2001, for example by defining the rules of jurisdiction more precisely. Recently the Italian Supreme Court (Corte di Cassazione) ruled that when settling a conflict between courts in Italy, the competent court is where the attacker is. It is specific criteria that could be extended to international level. We must not forget that the very notion of the 'information system' as it is recognized today in the Convention as a unitary notion comes from a previous position of the Italian Supreme Court in 1999*." And concerning the regulations such as all the legal requirements, *"This also must be adapted to the evolution of technology but the model is starting to show positive effects. We must overcome the mistrust and trust a model of cooperation between the public and private sectors in the interest of collectivity."*

We also asked Magistrate Corasaniti what he thought about the formation of assistance, support and information networks for SMEs relating to cyber crime, including issuing guidelines that will help all types of SMEs to be more aware of what they can do to defend themselves from this type of crime. He stated that *"It is an essential tool. SMEs are a central point of the economic system in the EU and are also involved as potentially the biggest victims of cyber crime. Until now there has been a certain underestimation, but I think for some time now things have been changing and the interests of SMEs in terms of the problems of cyber crime are increasing. This issue also involves them when considering the aspect of liability of legal people, provided for in the Convention of 2001 and in Italy by Decree-Law 231/2001. An appropriate and effective organizational model is in fact essential in the prevention of cyber crime."*

Information sharing between companies on this subject is still very low, almost non-existent (as per the information which emerged during the interviews conducted in the previous study). The opinion of the Magistrate is that this can be improved by *"Planning more organic on-line cooperation, sector by sector, distinguishing between fraud, identity theft and the attacks on systems. A security policy is built by sharing information."*

In addition to trying to mitigate this phenomenon, Corasaniti said that *"Preparing, like in the US, information and assistance portals for victims and making on-line complaints possible with special links and assistance in the case of malware infections"* would be useful, and a *"larger international awareness, and here I emphasize the role of the United Nations. At internal level, with the creation of a Conference of Cooperation which is also active at the international level - where the public and private sectors conduct their observations and develop their proposals, and above all to share their experiences, both negative and positive."*

31 Cybercrime and the risks for the economy and enterprises at the European Union and Italian levels, UNICRI, 2014, in <http://www.unicri.it/in_focus/files/Criminalita_informatica_def.pdf> (retrieved 04-07-2015)

CHAPTER 3

Guidelines for SMEs in the field of IT security

Within the research study, *"Cybercrime and the risks for the economy and enterprises at the European Union and Italian levels"*, numerous interviews were conducted at the local level. Law enforcement, institutions and companies from the province of Lucca were interviewed. These interviews revealed not only the biggest risks faced by companies every day, along with the frequency of the attacks they experienced, but also: the level of knowledge and preparation regarding these threats. The weak points (or gaps) in this regard concern what people would do in the event of an attack, and what people think they need in order to prevent these risks.

It was revealed through the initial report that often when a company falls victim to a cyber attack, managers were unprepared and were not sure who to contact. This was the case when companies were faced the consequences of an attack, but, above all, when trying to understand the actions required in order to prevent future attacks. Some companies call law enforcement agencies, such as the Postal Police (*Polizia Postale*), while many others only contact external (often local) consultants with whom they entrust the management of their IT system.

Often companies do not realize when their systems have been violated. Enterprises that suffer any kind of cyber attack, or that have at least a minimum level of awareness of the risks they face, often do not know what can be done in order to protect themselves from cyber threats and erroneously believe that defensive actions are expensive and only technical. A framework for assistance in the implementation of IT security systems is generally lacking for the SMEs of Italy. Technical elements, such as antivirus software and firewalls, etc. are not lacking, but a system of policy needs to be taken into account in order

to build a base which can be adapted and re-implemented over the years according to the evolution of cyber threats.

In response to this environment and the analysis of the existing gaps, a suggested plan of action has been the creation of a framework of comprehensive, identifiable guidelines that are adaptable to various types of SMEs, particularly those in Italy. The guidelines should be distributed based on particular areas of business so each company knows which guidelines can be adopted according to the presence, or lack thereof, of certain aspects within their particular structure.

Within individual areas, guidelines were listed in order of urgency. Proactive action, both technical and behavioral, to be taken into account were included with a simple and cost-efficient policy that could mitigate one of the most critical issues for companies: human behavior. Due to the huge differences between SMEs, a top down approach is useless and uncongenial in achieving the required results. Companies do not have to adapt to the guidelines; instead, the guidelines must be adaptable to the companies. After a thorough self-assessment, the company itself will adapt the guidelines to to fit its own profile.

IT security should not be seen as a state to be achieved, but rather as a process that involves constant action. It must become an integral part of business processes and must be implemented, developed, and changed over time - according to the developments of the threats. The corporate culture of security will improve only if the individual employee culture regarding security improves as well.

In order to create a comprehensive and communal document, we submitted these guidelines for validation to experts from leading companies in IT sector: Davide Del Vecchio, Security Operations Center Manager at Fastweb; Pier Luigi Rotondo, IT Security Architect at IBM; Gianfranco Vinucci, Head of Support & Services/Technical Manager at Kaspersky Lab Italy; Carlo Mauceli, Chief Technology Officer and Andrea Piazza, National Security Advisor at Microsoft; and IT managers of the companies involved in our previous research, Lucart, Lucense and Tagetik. These experts contributed their expertise in order to make the document more complete. Moreover, Fastweb, IBM, Kaspersky and Microsoft have also released, through their security experts, opinions on the main aspects concerning the current situation relating to SMEs and the IT field.

Interviews with security experts

Fastweb, IBM, Kaspersky and Microsoft were asked what about the biggest problems related to the fight against cyber crime. Everyone agrees that the lack of sensibility and awareness about the subject is the main stumbling block. Specifically, Dr. Piazza believes that one of the main problems is *“the imbalance of knowledge between attackers and defenders. This applies to both large companies and to SMEs. The level of sophistication of the attacks nowadays is so high that even companies with an extremely high budget and dedicated security team have suffered really large-scale attacks that have been difficult to*

detect. This involves very serious potential economic impact ranging from reputation damage and theft of intellectual property to the damage claims made by customers." Additionally, Dr. Mauceli specified that, *"the overall attack surface exposed by our digital civilization is growing faster than our ability to protect it."* And, Dr. Vinucci added that, *"we are facing professional organized groups that aim to obtain valuable information and who target high level victims including governments. Unfortunately, often within companies there is a lack of strong ability and skills required to counter this type of targeted campaign and they are unable to keep up with cyber criminals. The consequences of this are considerable for victims, primarily for the loss of sensitive information such as intellectual property that can compromise corporate networks, disrupt business processes and for the loss data."*

SMEs, with respect to cyber security, represent a different reality from personal users and large companies. This difference obviously leads to the development of peculiar advantages and disadvantages in combating cyber crime. Dr. Del Vecchio is very clear about this. He thinks the low budget and lack of awareness regarding the subject are undoubtedly the main disadvantages for SMEs, but at the same time, however, he believes they can count on having greater flexibility than large companies thanks to *"less bureaucracy and the possibility of taking direct action in order to correct problems."* Whatever the size of a company there are some best practices that should be observed as simple daily practices for the purpose of protecting corporate assets. This is the opinion of Dr. Rotondo. Accordingly, he has stated that *"just like we periodically check the safety of our cars - the efficiency of the brake system and the wear of the tires, we should do the same for our IT tools. An SME undoubtedly pays the costs of access to technologically advanced solutions in cyber security."* Unfortunately, SMEs underestimate the cyber threat, which is extremely dangerous. Dr. Rotondo expanded upon this notion, declaring that: *"Many SMEs think that their size does not make them attractive in the eyes of criminals and that they have no data interesting enough to be targeted. In reality this is absolutely untrue. In fact entrepreneurs should consider that when they make payments by credit card, store client information, or develop plans for the creation of new products they are in possession of invaluable information for cyber criminals. An SME without protection is an easy target and although the gain that a cyber criminal is able to obtain from each victim is less than that which they would get by attacking a large corporation it requires minimal effort and it is this that encourages criminals to attack many SMEs. Large companies generally have the resources to deal with the losses experienced from a cyber attack, which may also amount to millions of dollars depending on the type of attack. These costs are related to the loss of customer data, time spent offline and the expenses necessary to restore infrastructure. For small businesses however, this type of attack and the resulting economic damages may be enough to cause the business to close."*

Industrial and development plans, the know-how of companies, and the economic system of Italy are at risk due to the threat of cyber crime, not just company budgets.

Owners of SMEs should ask themselves the following questions: How much do I really know about cyber crime? What am I doing to protect my business, my data and my company's vital assets? The priority here is to increase the level of knowledge and awareness about cyber crime, which is extremely low. Addressing these issues, Dr. Rotondo told us that *"The starting point is to build awareness of those who use IT tools. Ways of recognizing and avoiding risky behavior must be explained to them: whether or not to open an attachment from an unexpected e-mail; whether or not to download software when you are not able to assess with certainty the authenticity and source; the use of the same password on social and business systems; to ignore messages on our IT system informing us that there are software updates available; and to store a backup disk in the same bag that we keep our computer in. These risks are all behavioral and not all people are aware of them. We are talking about really basic practices for which there are absolutely no excuses not to follow. SMEs should be informed that they stand to lose information, which is vital to business continuity, forever - with direct effects on the ability to stay in business. A company will no longer be able to recover after a well-aimed cyber attack."* Dr. Vinucci from Kaspersky also emphasized the importance of greater investment in educational campaigns regarding information security that highlight threats against SMEs, and underline the measures they can take to reduce the risks related to this type of crime: *"The problem is that most businesses (like people in general) tend to heed warnings and recommendations only after being hit by a disaster. Often the reality is the most effective teacher. Companies gain greater knowledge and awareness of computer crimes only when they get hacked or if another famous company is struck and the news has spread. Attacks on large companies make headlines and small businesses often think that they are not attractive targets for cyber criminals."* According to Dr. Piazza, in addition to awareness campaigns, the adoption of specific measures are also required, such as *"duties of reporting a compromise, staff training, adopting specific security measures, and the preparation of a team in charge of IT security."*

Even Dr. Del Vecchio from Fastweb agreed on the need to promote the sharing of information between companies and institutions relating to cyber risks via legal obligations. Dr. Vinucci stressed that, *"cyber criminals operate in an environment without borders so we need to fight them by creating open relations and by working between the public and private sectors, as well as between nations. Collaboration and information sharing are two of the most powerful weapons we have in this struggle, then the encouragement of confidence and transparency in the sector is of paramount importance."*

A substantial risk when dealing with an issue such as cyber crime is not being able to keep up with the rapid evolution of the phenomenon. For this reason, planned and targeted preventative actions are necessary. The experts interviewed were asked to delineate what the most urgent actions are in this respect. According to Kaspersky, *"first of all, small and medium-sized enterprises need to realize that the threat of cyber crime is real. The government has a fundamental responsibility to ensure that all companies understand this.*

In terms of specific measures for SMEs, I would say that the starting point for any company is to assess the risks: What are the business' assets? (intellectual property, customer data, etc.), Who would want to attack the company? Which tools could they use? After evaluating these aspects the company needs to chart a strategy in order to reduce the risks. Technology is important (anti-malware, firewall, encryption, etc.), but it is not enough. The company must also establish policies and procedures that reduce the risk of exposure, for example the segmentation of the network in order to make the spread of an attack more difficult. In addition, raising awareness amongst employees is essential. In fact many attacks today start simply because of a careless employee who unwittingly endangers the security of the company so in order to prevent possible damage caused by people it is therefore important, and at the same time protects digital assets of the company. Seeing security as a process is very important." Microsoft added a fundamental concept regarding this, calling for the development of *"school courses and an educational program, computer science and specializations related to cyber security in order to provide strong partnerships between the private and the academic world. Putting a greater number of experts in this field who have practical experience in the market is required."* Education of future generations plays a key role in balancing the current gap between the skills of the attacker and those responsible for protecting IT systems.

Trying to predict what future developments might be in order to deal with such a quickly evolving threat might also be important. The experts were asked about what the expectations concerning security in SMEs actually are. According to Microsoft, *"2014 was the worst year in terms of attacks and 2015 is showing further aggravation of the situation. We cannot assume a turnaround right now. The number of attacks is growing. The impact will be heavier and larger sectors of the population that are less familiar with IT tools will be hit. I think we should expect an expansion of attacks on mobile tools and Internet of Things (IoT) related instruments."* Dr. Rotondo from IBM added that *"more and more, we will see targeted attacks commissioned by competitors or new companies, also located geographically far away, who intend to enter the market also using cyber crime techniques. The automation of attacks allow for a large number of objectives and potential victims to be targeted. With the 'watering-hole' technique for example, websites or other resources shared by a particular group of users can be compromised with specifically configured malware - for a specific attack on the group. After credentials are captured the new malware is able to reuse them automatically in order to continue the attack. The year that has just ended was marked by Advanced Persistent Threat (APT) attacks based on already known malware that was re-used according to an articulate scheme of attack targeted at specific entities or organizations. APT attacks involve the use of sophisticated tools and malware and a long persistence over time. They base their success on careful previous study of the target, which often continues during the attack. Using techniques of obscuring and evasion they are able to remain undetected within systems and can continue to increase their impact as much as possible."* Dr. Del Vecchio noted that the spreading of *"blackmail acting in exchange for the*

release of all business operations" is a prospect that could pose a huge danger for a company. Finally, Dr. Vinucci from Kaspersky cites as a possible developing trend, the increase of ransomware and Distributed Denial of Service (DDoS) attacks. Also, specifically for SMEs, he said that *"'stepping stone' attacks will continue to emerge as a serious threat - those in which a supplier is being targeted. The attacked enterprise*[32] *is used as a means to gain access to information that can open doors to a larger or more important goal. The threat landscape is made up of random attacks (those that we face as individuals) and targeted attacks against companies or groups of companies (operating in a particular sector of the market). Unfortunately SMEs are victims of both types of attack. Compared to a large company, in-house skills are lacking and the key objectives of SMEs are sensitive to social engineering 'tricks'. So criminals are able to steal their identities and access bank accounts and confidential data. In other words, the same modus operandi used to deceive people is used but for an SME the consequences are more serious. Training is an essential part of a corporate security strategy for this reason."*

Starting with the first study commissioned by UNICRI on the impact of cyber crime on the economy and SMEs, the importance of supporting companies through an assistance framework and providing specific information to them concerning cyber crime has been evident. In regard to this issue, all respondents agree on the need and importance of this type of project. On this topic, Dr. Rotondo from IBM stated, *"I totally agree, both with plans of staff training and with regular updates on an extremely changeable phenomena such as cyber crim.,"* He went on to say that, *"The cyber crime activities we have observed in recent months were unimaginable only few years ago. From an architectural point of view we had security mechanisms that we considered a guarantee of security. Some of these mechanisms have been overturned and become obsolete. At the same time I am sure that in a few years we will be faced with attack patterns that we cannot even imagine now. Any type of assistance, support and information framework for SMEs must take all of this into account. This framework must periodically review the proposed solutions and raise awareness among SMEs that cyber crime changes to adapt itself to the defense mechanisms that organizations adopt."*

Kaspersky added that *"It is an extremely positive idea." "We know that SMEs often have limited IT budgets and thus don't have the ability to rely on dedicated security consultants. We also know that SMEs are increasingly a target of cyber criminals who hinder or harm their business. Although they are not the ultimate goal, small and medium-sized enterprises are increasingly being targeted by cyber criminals as links in a chain - a weak link in order to gain access to on-stream systems of a partner. Cyber crime is an important issue*

32 We have already seen some examples of this type of attack. For example, in 2011, some criminals infiltrated the IT networks of several companies operating at the Port of Antwerp. This attack allowed them to control the movements of containers and smuggle drugs into Europe. For more details, see: "Police warning after drug traffickers' cyber-attack", by Tom Bateman, 16-10-2013, available at: <http://www.bbc.com/news/world-europe-24539417> (retrieved 22-06-2015)

that continues unabated. Rather in reality, in recent years it has gotten worse. Giving enterprises of all sizes support, training and information to improve their defenses, but in particular small and medium-sized enterprises which make up such a large part of the total companies, is vital."

Guidelines for SMEs

Below is a summary of the guidelines[33], which have specifically been drawn up with the needs of SMEs in mind. These needs emerged from the interviews conducted in the previous empirical study. These guidelines address the need to provide a complete and useful guide for SMEs in understanding what they can do for the security of their data, their businesses, their know-how and their company infrastructure. The guidelines have been developed, keeping in mind the main areas present within a company. After a short self-analysis test, each SME can adopt guidelines based on the presence or absence of a particular area within its facility. For example, a small enterprise such as a professional studio does not have a manufacturing area and therefore does not follow the guidelines relating to manufacturing and must instead refer only to the guidelines relating to policies about sensitive data protection relevant for administrative and commercial areas. In addition, if an SME does not have an IT department of their own, the help of an external consultant is required in order to implement relevant and mandatory actions within the IT area. Technical aspects within the IT area , such as maintaining backup plans, are very important in protecting the company against threats such as Criptolocker. Having these policies in place are important, for example, for the situation of an accounting firm during the delivery period of tax documentation to its customers, or a firm of architects where it is crucial that the plans for tenders are stored in secure areas of the corporate network, preferably not connected to the Internet. Obviously, there are common policies that should be employed within several business areas, such as the secure management of passwords and training in detecting fraudulent e-mails, like phishing and spear-phishing e-mails, which are on the increase and becoming more sophisticated. Staff must be constantly informed and updated on the necessary regulations in order to recognize fraudulent e-mails. Simple steps such as passing the mouse cursor over the name of the sender in order to check that the e-mail address matches the one displayed, and that it is not a counterfeit with the purpose of misleading the user, is a simple precaution that can help users from contracting malware on their devices. An example of this is shown in the next figure.

33 The full text of the guidelines for SMEs will be provided upon request to UNICRI

Figure 7 - Example of how to recognize a phishing e-mail

As we can see in the example in Figure 7, the scam e-mail was sent from an "@infas.it" address not belonging to Wind. In addition there are many other clues, such as punctuation mistakes and the request to download an .html file. All of these clues allow the user to understand that the e-mail is not authentic, so that they can then mark it as spam and delete it. The objective of this kind of e-mail can be twofold. First of all, it can be to gain credit card data, and, secondly, to infect the PC, making it part of a botnet or to encrypt data in order to ask for a ransom.

As can be seen from the summary diagram of the guidelines, six main business areas have been identified:

- Administration area
- Marketing area
- Research and development area
- Logistics area
- Manufacturing area
- IT area

Guidelines for SMEs by area[34]

Administration area

- Manage user accounts of administrative personnel
  - Password security management
  - Use of certified e-mail services
- Human resources
- Sensitive data protection of all personnel data
- Company's mobile device use (e.g. smartphones and laptops)
- Social network management
- Manage physical accesses of company personnel

Marketing area

- Manage user accounts of marketing personnel
  - Password security management
- Customers and suppliers database management
  - Sensitive data protection of customers' and suppliers' data
- Security management in relations with suppliers
- Invoicing
  - Protection of invoicing data
- Company's mobile device use (e.g. smartphones and laptops)

R&D area

- Manage user accounts of research and development personnel
  - Password security management
- Know-how, intellectual property and corporate assets protection (e.g. patents, projects, catalogs)
  - Schedule continuous backup and devise disaster recovery plans
  - Use data encryption systems on all workstations, laptops, mobile devices and external devices (e.g. HD and USB sticks)
- Company's mobile device use (e.g. smartphones and laptops)

34 Guidelines have been realized thanks to the advice of Dr. Daniele De Nicolò and were validated by Fastweb, IBM, Kaspersky, Microsoft and IT Manager by Lucart, Lucense and Tagetik

Logistics area

- Manage user accounts of logistics personnel
  - Password security management
- Warehouses, materials and products handling
- Company's mobile device use (e.g. smartphones and laptops)

Manufacturing area

- Manage user accounts of manufacturing personnel
  - Password security management
- Protection of IT systems of automated production lines
- Company's mobile device use (e.g. smartphones and laptops)

IT area

- Analysis of the IT environment of the whole company
- IT systems management
  - Workstations management
  - Network security
  - User accounts management
  - Schedule continuous backup and devise disaster recovery plans
  - Securely erase all data from devices no longer in use (e.g. HD, backup DVDs/tapes, USB sticks) even if marked for disposal
  - Data encryption policy
  - Social network management
  - Public sites and e-commerce management (if any)
  - What to do in case you have been attacked

Figure 8 - Guidelines for IT Security of SMEs

Through analysis of these areas, each SME can find the most suitable position and then adapt the appropriate guidelines for its particular structure. For each area, the most important corporate assets have been identified. The best practices that will help to better manage and mitigate potential risks were highlighted for each area, while simultaneously ranking them in order of urgency.

Among these policies we can see sensitive data protection regarding both company personnel (names, personal information, banking etc.) and data related to customers and suppliers (names, VAT, IBAN, historical invoices, etc.). Even cloud management has been considered. The cloud is a tool that is becoming more interesting for enterprises due to the benefits that it can provide, especially for SMEs. These include the lowering of management and maintenance costs related to computer equipment. In order to help companies be more aware in terms of cloud usage, the European Union Agency for Network and Information Security (ENISA) has recently published *ENISA's Security Guide and Online Tool for SMEs when going Cloud*[35]. Within this report, eleven of the biggest opportunities offered by cloud services are discussed, in conjunction with eleven of the biggest risks in this field. Additionally, the report outlines twelve questions that SMEs should ask themselves when choosing to adopt cloud solutions for their business.

Note: When drafting the guidelines we gave special attention not only to technical, but also to behavioral aspects, being that the majority of threats rely on human error for achieving their success, and can be conveyed through seemingly innocuous images attached to e-mails.[36]

35 Cloud Security Guide for SMEs. Cloud computing security risks and opportunities for SMEs, ENISA, April 2015, available at: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes> (retrieved 24-06-2015)

36 How to hack a computer using just a image, The Hacker News, by Swati Khandelwal, June 2015, available at: <http://thehackernews.com/2015/06/Stegosploit-malware.html> (retrieved 2-6-2015)

Conclusions

The impact of cyber crime on the economy is an issue that is becoming increasingly worrisome. One of the main difficulties in dealing with this type of crime is that the tools and knowledge held by cyber criminals, as compared to those who are responsible for combating it, are disproportionate. Moreover, the trend of rapidly deploying cheap, malicious tools on-line has served to bolster cyber criminals' capabilities. These tools have an ease of use that allows even those without high technical expertise to take part in cyber crime. A further security threat for SMEs is the ever-increasing use of legitimate software, in place of malware, in order to gain access to corporate systems. This fact implies two main risk factors for SMEs. Firstly, recognizing these programs as a threat is very difficult for antivirus software. Secondly, the high speed at which attackers can exploit this software makes it difficult for SMEs to combat this issue in real time. Nowadays, cyber criminals don't have to create malware from scratch, so they already have a base from which to develop their attacks, allowing them to develop new techniques at a rapid pace.

To successfully counter a transnational threat such as cyber crime, a global response which maintains shared regulation is required. The strengthening of European and international cooperation is also essential in this domain. This can be done through the use of collaborative tools, law enforcement mechanisms, and legislative action to combat cyber crime. Case studies are fundamental for achieving widespread comprehension of this phenomenon, and they must be both highlighted among stakeholders and shared. The use of case studies and information sharing are beneficial in understanding what has to be done with respect to addressing cyber crime, how it has to be done, and in facilitating the study of new measures to combat and prevent this phenomenon. Security must be considered a common goal of everyone - both public and private - in which collaborative, coordinated and effective logic must prevail.

Providing support to SMEs in this area is vital for the economies of states, particularly Italy. The awareness of this threat is slowly increasing through the diffusion of reports, studies, and articles on this topic; however, knowledge pertaining to what SMEs should be doing in order to defend themselves is still scarce. Start-up companies,, for example, are very vulnerable entities in this environment. These are young companies who, for the most part, belong to the IT industry, or have a strong information technology component; yet they often have limited resources and budgets. These companies, who should be supported and considered a driving force for the economy, usually consider security as a secondary aspect. Small businesses often make the dangerous mistake of thinking that they do not attract the interest of cyber criminals due to their being too small and insignificant compared with large companies. In reality, the presence of money or data which can be stolen, and the ease with

which violating a target can take place, are the main factors that cyber criminals consider when carrying out their activities. Unfortunately, SMEs meet both these requirements. Nowadays, digital information security and proper use of the web and computer tools must be considered a priority by each individual citizen, and especially by companies. Companies need a methodical approach to knowledge and assessment of risks in order to create a constantly updating security management system.

The guidelines presented in this report are intended to provide more adequate knowledge to SMEs concerning the risks they face from cyber space on a daily basis. SME owners should ask themselves what they really know about cyber crime, what is being done to protect their business and its data, and how they can improve the current level of security in this domain. The aim of UNICRI's project is to share and explain these guidelines in training projects for SMEs. Each guideline will be expounded upon and justified to companies, explaining what they can do individually and what they can do with the help of specialized companies. A risk associated with simply distributing the guidelines is that SMEs may view these instructions as too abstract and not within their reach; therefore, an explanation regarding the correspondence that exists between cyber crime and physical crime is very important. Through examples taken from everyday life, we can try to counter the low perception of risk held by SMEs concerning this phenomenon. The goal is to make these risks, which are still considered abstract and far from everyday reality, more concrete and tangible.

The problem in fighting cyber crime is primarily cultural. The first step is to educate the user as much as possible and to provide a framework for managing their activities, while keeping security in mind. It is important that users overcome the belief that security constitutes a cost that is too high. In fact, many solutions that significantly raise the security of a company can be implemented with minimal investment. Another false myth that must be dispelled is that IT security is a wasted investment. Investing in IT security can in fact actually achieve significant returns economically, and with respect to reputation, reliability and competitiveness. The real price to be paid is not that of the cost of security, but of the cost that can be incurred in its absence – which can be more expensive than the initial investment required – as has been shown through the case studies examined in this report.

Index of Figures

Methodology

The subject matter of this report, along with its objectives, has made it necessary to conduct the research in three stages.

In the first stage, we analyzed the most recent reports concerning cyber crime. These reports were published in 2015 by major information technology companies (Kaspersky, Verizon, Symantec, Clusit, etc.) and accredited independent entities (ENISA, WEF, etc.). All of these reports are readily available on-line. The scope of this analysis served to highlight the facts regarding trends in cyber crime in 2015, with particular emphasis paid to the issues facing to SMEs.

During the second stage of research, qualitative, semi-structured interviews were conducted with the aim of defining and illustrating the actual state of cybercrime with respect to SMEs at the national level, with additional insights being gained through the interviewees' depictions of case studies. These interviews were conducted following the identification of key interlocutors.

The third phase of the project consisted of drafting the guidelines for SMEs. The guidelines were developed according to the results of the interviews conducted in the first UNICRI report on cyber crime and risks to the economy and SMEs. These guidelines were submitted to, and validated by, companies such as Fastweb, IBM, Kaspersky and Microsoft. These companies have always been involved in developing solutions to support SMEs and to mitigate this type of threat.

Bibliography

Alcatel-Lucent's Motive Security Labs (2014), *Motive Security Labs malware report – H2 2014*, available at: <https://resources.alcatel-lucent.com/asset/184652> (retrieved 23-03-2015)

Ashford W. (2014), *Top 10 cyber crime stories of 2014*, Computer Weekly, 31-12-2014, available at: <http://www.computerweekly.com/news/2240236215/Top-10-cyber-crime-stories-of-2014> (retrieved 28-04-2015)

Bateman T. (2015), *Police warning after drug traffickers' cyber-attack*, 16-10-2013, available at: <http://www.bbc.com/news/world-europe-24539417> (retrieved 22-06-2015)

Boscolo M. (2015), *Ecommerce: le frodi costano 794 milioni l'anno*, Wired Italia, 30-12-2014, available at: <http://www.wired.it/economia/business/2014/12/30/pagamenti-online-frodi-valgono-794-milioni-lanno> (retrieved 05-03-2015)

Christin N. (2015), *It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice*, by Nicolas Christin, Serge Egelman, Timothy Vidas and Jens Grossklags, INI/CyLab, Carnegie Mellon University, National Institute of Standards and Technology, ECE/CyLab, Carnegie Mellon University, IST, Pennsylvania State University, available at: <https://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf> (retrieved 07-05-2015)

Clusit (2015), *Rapporto 2015 sulla sicurezza ICT in Italia*, available for request at: https://clusit.it/rapportoclusit/ (accessed 15-07-2015)

Department for Business, Innovation and Skills Cabinet Office (2014), *2014 Information Security Breaches Survey,* available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307297/bis-14-766-information-security-breaches-survey-2014-executive-summary-revision1.pdf> (retrieved 30-04-2015)

ENISA (2015), *Cloud Security Guide for SMEs. Cloud computing security risks and opportunities for SMEs,* April 2015, available at: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes> (retrieved 24-06-2015)

European Central Bank (2014), *New report on card fraud shows online fraud increased in 2012*, Press Release 25-02-2014, available at: <https://www.ecb.europa.eu/press/pr/date/2014/html/pr140225.en.html> (retrieved 05-03-2015)

European Commission (2015), *Communication from the commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security*, Strasbourg, 08-04-2015, available at: <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf> (retrieved 09-06-2015)

Ford N. (2015), *Misunderstanding cyber threats puts a third of SME revenue at risk*, 27-02-2015, available at: <http://www.itgovernance.co.uk/blog/misunderstanding-cyber-threats-puts-a-third-of-sme-revenue-at-risk/> (retrieved 30-04-2015)

Ford N. (2015), *Why SMEs are an attractive target for cyber criminals and what they can do about it*, 02-03-2015, available at: <http://www.itgovernance.co.uk/blog/why-smes-are-an-attractive-target-for-cyber-criminals-and-what-they-can-do-about-it/> (retrieved 21-05-2015)

Giordano M. and Vaciago G. (2015), *La sicurezza informatica, un asset aziendale strategico*, in Journal 231 (02-2015) pg. 273.

HP (2015), *Cyber Risk Report 2015,* available at: <http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/> (retrieved 01-05-2015)

Il secolo XIX Tech (2015), *Il 97% di chi naviga su Internet non sa riconoscere il phishing*, 23-05-2015, available at: <http://www.ilsecoloxix.it/p/magazine/2015/05/23/AR7IpzXE-phishing_internet_riconoscere.shtml> (retrieved 05-05-2015)

Kaspersky Lab (2014), *Consumer Security Risk Survey 2014: Multi-device threats in a multi device world*, July 2014, available at: <http://media.kaspersky.com/en/Kaspersky_Lab_Consumer_Security_Risks_Survey_2014_ENG.pdf> (retrieved 28-05-2015)

Kaspersky Lab (2015), *Kaspersky Lab Survey: un utente su quattro non comprende i rischi delle minacce informatiche mobile*, 27-02-2015, available at: <http://www.kaspersky.com/it/about/news/virus/2015/Indagine_Kaspersky_Lab_un_utente_su_quattro_non_comprende_i_rischi_delle_minacce_informatiche_mobile> (retrieved 10-05-2015)

Khandelwal S. (2015), *How to hack a computer using just a image*, The Hacker News, June 2015, available at: <http://thehackernews.com/2015/06/Stegosploit-malware.html> (retrieved 02-06-2015)

La Stampa tecnologia (2014), *Acquisti online e frodi: il 44% degli utenti non recupera il denaro*, 24-12-2014, available at: <http://www.lastampa.it/2014/12/24/tecnologia/acquisti-online-e-frodi-il-degli-utenti-non-recupera-il-denaro-Ft9RDDFyPpYTbyoJi1J96J/pagina.html> (retrieved 20-03-2015)

Pierri M. (2015), *Cybersecurity, così Intelligence e imprese possono collaborare*, 16-03-2015, available at: <http://www.formiche.net/2015/03/16/cybersecurity-minniti-ruffinoni/> (retrieved 20-03-2015)

Sorbini L. (2015), *Cybersecurity: il 40% delle grandi aziende pronte ad attacchi cyber nel 2018*, Key4biz, 24-02-2015, available at: <http://www.key4biz.it/cybersecurity-40-delle-grandi-aziende-pronte-ad-attacchi-cyber-nel-2018/> (retrieved 21-05-2015)

Symantec (2015), *Internet Security Threat Report*, April 2015, available at: <https://know.elq.symantec.com/LP=1542> (retrieved 22-06-2015)

The Guardian (2014), *It's been a great year! Thanks to these Facebook scams for being a part of it...*, 24-12-2014, available at: <http://www.theguardian.com/technology/2014/dec/24/facebook-scams-malware-naked-videos> (retrieved 10-04-2015)

The Guardian (2014), *How you could become a victim of cybercrime in 2015*, 24-12-2014, available at: <http://www.theguardian.com/technology/2014/dec/24/cybercrime-2015-cybersecurity-ransomware-cyberwar> (retrieved 10-04-2015)

Verizon (2015), *2015 Data Breach Investigations Report*, available at: <http://www.verizonenterprise.com/DBIR/2015/> (retrieved 25-05-2015)

Websense Security Labs (2015), *Websense Threat Report 2015, fare cybercrime è sempre più facile,* 13-04-2015, available at: <http://www.techfromthenet.it/201504101252/News-analisi/websense-threat-report-2015-fare-cybercrime-e-sempre-piu-facile.html> (retrieved 22-04-2015)

World Economic Forum (2015), *The Global Risks 2015 10th Edition*, available at: <http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf> (retrieved 06-05-2015)