International Journal of Academic Research in Accounting, Finance and Management Sciences
Vol. 9, No.3, July 2019, pp. 185–191
E-ISSN: 2225-8329, P-ISSN: 2308-0337
© 2019 HRMARS
www.hrmars.com

To cite this article: De Marco, E., Dibari, P., Scalera, F. (2019). *Cyber Risks and Costs for the Company,* International Journal of Academic Research in Accounting, Finance and Management Sciences 9 (3): 185-191

http://dx.doi.org/10.6007/IJARAFMS/v9-i3/6357 (DOI: 10.6007/IJARAFMS/v9-i3/6357)

www.hrmars.com
ISSN: 2225-8329

Cyber Risks and Costs for the Company

Eusebio De Marco[1], Patrizia Dibari[2], Francesco Scalera[3]

[1]Accountant in Bari, Italy , D. Alighieri Street 228 - 70122, Bari, Italy, [1]E-mail: eusebiodemarco@iol.it
[2]Lawyer in Bari, Italy, D. Alighieri Street 228 - 70122, Bari, Italy, [2]E-mail: patriziadibari@iol.it
[3]Department of Economics and Finance - University of Bari "Aldo Moro", Italy , P. Amedeo Street 160 - 70122, Bari, Italy, [3]E-mail: roby_sca@virgilio.it (Corresponding Author)

Abstract

The interest in the security of IT systems has grown in recent years, proportionally to their diffusion and to the role they play in the community. With the spread of computerization of society and services (public and private) the risk of cyber-attacks and accidents has increased. From the results of the analysis of the present study it is noted that only in Europe, more than 4 thousand computer attacks per day have occurred and also in Italy the phenomenon has recorded increasingly heavy consequences to the detriment of businesses. From the analyzes reported in the present study, the causes of the problem are multiple but in particular they are due to the scarce training of the personnel, which does not allow to notice in time of possible threats and intrusions in the control systems, to a cultural problem and to the inadequacy of the investments to face the problem, in fact, despite, a general concern of the companies about the risks of cyber security. The present study examines the main sector reports, including those in the international context of the World Economic Forum, Kaspersky, McAfee, Norton Cybercrime Report and at a European level, the recent Euro barometer research to investigate the risks of company and identify the tools that allow to improve the degree of knowledge of the real threats, to know the business costs in order to activate a series of measures able to guarantee the security of company data.

Key words

Cyber Security, Computerization, Cyber-Attacks, Productive Sector, Company Costs, Data Security.

Received: 10 Sep 2019
Revised: 18 Sep 2019
Accepted: 22 Sep 2019
Published Online: 06 Oct 2019

© The Authors 2019

Published by Human Resource Management Academic Research Society (www.hrmars.com)

This article is published under the Creative Commons Attribution (CC BY 4.0) license. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this license may be seen at: http://creativecommons.org/licences/by/4.0/legalcode

1. Introduction

In recent years, computer crimes have assumed vast proportions, at the international level, in Europe and in Italy with heavy repercussions in numerous productive sectors in which the problem is registered; in particular, the manufacturing, energy, transport and car sectors are most affected (Apostol and Bălăceanu, 2011). For crime, computer crimes represent a very profitable and low-risk activity. The authors state that "One of the major challenges, when discussing about Cyber Age and Cyber Revolution, revolves around the greater issue of security, both personal and national" (Apetroe, 2019). And It is pointed out that "Cyber Risk means any risk of financial loss, disruption or damage to the reputation of an organization or a person from some sort of failure of its information or control systems" (Darlington, 2017). It should also be noted that "Cyber security also referred to as IT security or computer security is the safeguarding of information systems from damage, theft, and disruption, as well as misdirection of services offered. It involves restriction of physical access, as well as protection against dangers posed through code and data injections, illegal network access, and malpractices. The field is of considerable importance because of the growing

rate of computer usage around the globe" (College of Computer Science and Information Technology, 2015; Zappa, 2014).

Private computer security companies and state Institutions have carried out interviews and analyzes in which they identify the multiple risks of SMEs affected by computer crimes, starting with the loss of intellectual property and exposure of sensitive data, the loss of competitiveness and jobs, without considering the costs related to the destruction of services and the damage to the corporate image and reputation. Analysis shows that: "At the global level, in 2015 the cyber security industry came close to a turnover of over 75 billion dollars and by 2020 it is expected to double. The investments in cyber security are inevitably destined to grow, on pain of blocking the activities of the companies, the national security of the countries and, consequently, the geopolitical balances" (Teti, 2016). All the reports referred to in this study, underline how the risk of being attacked cyber-attacks should convince SMEs, civil society and governments to take this threat more seriously and work together to limit the damage (Schmidt, 2014). The present study on the basis of the reported analyzes examines the tools that allow to improve the degree of knowledge of the real threats and the business costs to be sustained to guarantee the safety of the corporate data.

2. Cybercrime: International Threat

The main sector reports, including those of the World Economic Forum report, drawn up on the basis of interviews with 250 experts in the sector and company executives, they show that, in the coming years, cyber-attacks could generate economic losses of up to 3 trillion dollars. It is noted that: "Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cyber security breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Another growing trend is the use of cyber-attacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning" (World Economic Forum, 2018).

According to Kaspersky (2019), the most fearsome attacks remain those towards critical infrastructures and there is concern with the significant increase in crimes against companies such as fraud or data theft. "The ECI directive, EC. (2008, December 23) n. 2008/114/EC of the Council (GUUE 23 December 2008, n. L 345) is one of the pillars of the European program for critical infrastructure protection (EPCIP), concerning the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. It defines 'critical infrastructure' as an element, system or part of it located in the Member States and essential to maintaining the vital functions of society, health, safety and economic and social well-being of citizens, whose damage or damage to destruction would have a significant impact. It establishes a procedure for identifying and designating critical European infrastructure (ECI) and a common approach to assessing the need to improve their protection."

McAfee points out that company tend to underestimate the severity of cyber risk and its speed of growth. This problem is more evident in SMEs, where the budget dedicated to defense instruments is lower than that of a large company and compared to what would be needed to implement at least acceptable safety policies. "CSIS and McAfee explore the growth of cybercrime from an economic impact perspective. It's estimated that cybercrime may now cost the world almost $600 billion, or 0.8% of the global GDP" McAfee (2014). The Norton Cybercrime Report (2018), which has carried out one of the most extensive studies on the impact of cybercrime on users, estimate that every year on average cybercrime directly affects over 500 million victims, among which, the most industrialized states, due to their greater computerization, suffer most of the losses but less developed countries are also involved, as their computerization increases.

3. Cybercrime: in Europe

At European level, the recent Eurobarometer research (Aazami, 2015) confirms that European citizens consider computer security as a topic that raises enormous concerns. The data show that 89% of the sample declares to be worried about the security of their personal information accessible online; 74% think that the risk of being a victim of cybercrime has increased compared to the previous year; 10% of

European users surveyed are assured that they have been online frauds and the 6% claims to have been the victim of identity theft. In Addition, 50% of the sample admits that it has not changed any passwords of its online services in the last year and 52% feels little or misinformed about the threats of cybercrime, while the 12% have been blocked in Internet access, the 12% have been hacked into their social network account and finally the 7% have suffered credit card theft. Only half of Europeans put in place acceptable protection measures to tackle this type of crime.

4. The Causes of the Problem

The researches mentioned in this study trace the causes of cybercrime:

1) the scarce training of personnel that does not allow to detect in advance any threats and intrusions into the control systems;

2) to a cultural problem because companies do not continually share official information about the spread of the phenomenon; in this way, the cyber-attack is discovered after months or years;

3) inadequate investments to deal with the problem; in fact, despite a widespread concern among companies about cyber security risks, only 9% increase the cyber security budget by 25%;

4) to the low risk index for hackers in the face of enormous gains. Industry studies estimate that the internet generates a volume of business for the global economy that varies between 2,000 and 3,000 billion dollars a year and that, given the high growth of computerization, constitutes a constantly growing market;

5) to the increase of technology and digitalization of every aspect of daily and economic life and to the exponential increase of internet users.

5. The Consequences of the Problem

Based on the analyzes reported in the present study, the consequences of cyber-attacks fall on the companies that suffer unpredictable economic and productivity losses and that bear the costs for cyber security, malware cleaning, investigation and post-accident management, risking:

1) loss of credibility and market positioning;

2) the loss of data and or the theft of trade secrets with the consequent effect on customer relations, compensation to be paid or contractual penalties, costs for recovering image damage, countermeasures to mitigate losses, disaster recovery plans and insurance, reputational damage and in terms of competitiveness;

3) loss of business and jobs. Intellectual property theft losses are difficult to estimate in the short term, but they represent a huge cost for companies especially in the long term.

Cybercrime has a serious impact in terms of employment within a country. All this acts as a brake on the growth of the company, and of the country as a whole, preventing the growth of national and global economies.

6. The Risks in the National Security Strategy

The Cyber threat has been identified as one of the main risks in the national security Strategy (Teti, 2016). To this end in Canberra, the new Cyber security Centre (CSC) was established in 2014; it relies on the expertise of the Nation's best IT security experts and will increase the Nation's ability to defend itself against cyber-attacks. The Center will analyse the nature and extent of cyber-threats, and will guide the Government's response to cyber incidents. The work is carried out in close contact with the sectors of critical infrastructures and companies in the Country, to protect national networks and systems, creating a sort of epistemic community, with the aim of dealing with this type of threat. The Centre also provides advice and support for the development of prevention strategies to combat cyber-threats.

Canada has adopted directives on the safety and security of government systems and critical infrastructures, planning to collaborate outside the Federal Government on vital IT systems; in addition, it supports the programming of actions to strengthen education and awareness of the Canadian population about cyber threats and the correct use of the web. In the United States, the relevance of the cyber threat from Nations, terrorist organizations, criminals and other subjects has grown to lead to the formulation of one of the earliest strategies in the field of informatics. It envisages collaboration between local, federal and international agencies to combat cybercrime, which has as its peculiar characteristic that it has no

boundaries and territoriality (Teti, 2016). In the last few years, several States have begun to develop IT security policies, including through support for innovative SMES directly engaged in this sector (Teti, 2016). Among these, France and the United Kingdom promote opportunities for SMEs that deal with innovative IT products and allow them to play an active role in making cyber space a safer place (Teti, 2016).

7. The Definition of Cyber Crime

Cybercrime is defined as the set of illegal operations that take place on the Internet (Zappa, 2014; Darlington, 2017; Kaspersky, 2019). Initially, cyber threats were mainly viruses, worms and Trojans. Subsequently, techniques related to social engineering have been added, such as targeted phishing aimed at employees who have access to databases containing confidential business information, and others such as pharming, credit card fraud, DDoS attacks, identity theft and theft of data. Offenses against mobile devices, smartphones and tablets are on the rise; the crimes perpetrated through social media, on which many companies have a public profile; attacks through internet banking services, attacks against multinational companies by hacktivists, which exploit the enormous echo that the web guarantees for these demonstrative actions all over the world.

8. Types of Threats

The Cyber Crime universe is quite extensive and includes different types of attack, attackers, risks and threats (Zappa, 2014; Darlington, 2017; Kaspersky, 2019).

A) Fraud

The fraud consists in accessing, without permission, computer systems with the aim of obtaining, free of charge, and therefore unlawfully, the services provided by the victim company. There are mainly two ways in which the attacker can access these services, the first, by coming into possession through different techniques (phishing, social engineering) of credentials of an administrator or an employee of the company, the second, coming into possession of the credentials of a legitimate user. This fraud can also be perpetrated as an intermediate step to reach a more demanding goal. This type of illicit action may also have as an objective to intercept or divert data passing through the POS to steal credit card data or divert payments to a bank account controlled by the attacker.

B) Identity Theft

Identity theft, even in computer science, is a scam with the purpose of stealing the identity of another person (or a company) in order to obtain unlawfully resourced resources, information or authorizations. In the corporate sphere, this threat materializes in two different ways, the first, more traditional, in which an attacker steals the identity of a person inside the company (employee, manager) in order to obtain valuable information directly from a Unsuspecting colleague; In this case, instead in the second and more dangerous way, the attacker steals the identity of the entire company (logo, production projects, catalog) to use these resources in an illicit way in a foreign Country (China and example) producing the same goods marketed By the victim company, and placing them in the market as counterfeit merchandise. Theft of sensitive and confidential material is one of the biggest risks for the world of Small and Medium-sized Enterprises.

The theft of sensitive data concerns both the internal data of the company, (production of the goods, novelty, employee staff, financial information, etc.) and the data of the customers and the suppliers (personal identities, credit card numbers or bank accounts, credentials of access to the service offered by the victim company, email accounts, passwords etc.). This kind of attack has a very strong impact on the company business, in case of theft of internal data in fact there could be a block or a drop in the production, in case of theft of external data, for example of customers, there could be a drop in sales due to The loss of customer confidence in the company, as well as potential legal damages for negligence in the preservation of sensitive data. This certainly represents the most serious threat to an SME, especially in Italy, where the loss of the brand or the production catalogue represents a damage which is difficult to repair.

C) Espionage

Industrial espionage is an activity that has as its main objective that of obtaining in an illicit way business and commercial information. The methodologies through which this kind of attacks take place generally involve a direct attack, through social engineering activities and/or the installation on the systems of the company malware victim which allow the attacker to Check. This kind of attack mainly has as a sender a competitor company that has the objective of recovering a production or market gap, but of course it is necessary to involve a computer expert or an unfaithful employee.

D) Sabotage

Sabotage is that action that aims to slow down or block the victim's activities through the obstruction of normal operations such as material destruction or important instrumentation to the business. Also in this case there are different technological and social methodologies, and the figures involved and the objectives are the same as the espionage.

E) Demonstration Attacks

This type of attack is mainly caused by individuals or groups of people as a protest against the victim company, accused of misbehaving against end users or private citizens. Mainly through attacks of defacement or DDoS, they aim to interfere with the normal working activities of the company and to make propaganda to their idea and their anger.

F) Extortion

Computer extortion is a criminal act, perpetrated through the illegal installation by the criminal, a ransomware-type malware, on the victim's computer, without its authorization. Through This software the criminal blocks, remotely, the victim's computer or encrypts the company data making it impossible to use. The victim is required to pay a sum of money in order to unlock the PC or decrypt the data taken hostage.

9. Types of Attack

The different types of cyber-attack that can be perpetrated by attackers to the detriment of companies, for the purposes specified, can divide into different typologies:-Attacks on-line (most of the attacks, either by number or by Different types, such as spam and phishing) and offline attacks (often caused by the improper behavior of employees, both voluntarily, to create damage to the company in case of internal problems; both unconsciously, through improper use Of company machines for personal use).-Targeted Attacks (in which the attacker strikes a well-defined company, selected for its specific characteristics, such as the product category or the geographic area) and untargeted attacks (in which the attacker strikes one or more companies that they were vulnerable to the threat put in place by the attacker).

A) Hacking

Hacking is the act of illegally accessing a system to obtain a high degree of knowledge and a large number of information about the system itself, both on its functioning and on the data it contains, in order to adapt it to its own needs. The term hacking has acquired many nuances during the period in which the computer systems have developed, acquiring connotations both negative and positive. The use of techniques and methods of hacking, with the aim of obtaining a gain, be it material and direct, or indirect, stealing information to resell or with the purpose of damaging the company victim of the attack is properly called cracking. The figure of the solitary and curious hacker who acts behind the thrust of the challenge and the personal interests, leaves more and more the place to groups of organized criminals who, through actions of hacking, pursue economic and profit purposes.

B) Spam

Spam is the term that indicates the sending of unwanted messages, generally commercial type, usually through e-mail. The main goal of spam is the advertising and sale of illegal, fake and/or illicit material, until you get to real attempts to scam.

C) Phishing

Phishing is an attempt to scam via the Internet through which the attacker tries to mislead the victim of deception to provide sensitive personal data, often through the sending of e-mails that simulate the graphics of postal or banking sites, by requesting access credentials or credit card number to avoid possible problems or penalties. The term phishing comes from fishing ("fish" in English), and alludes to the attempt to "fish" personal data, financial and password of a user.

10. Conclusions

The risks that cyber space hides for businesses can involve different aspects of business life, not only those closely related to computer tools, but also and especially on business and on the most important corporate assets: data, people and Services. Therefore, being able to know the right strategy for defending against cybercrime at international, national (in Italy) and local level through studies and research is a good starting point to promote the security culture at various levels and moving from understanding to initiative, from knowledge to action.

References

1. Aazami, S. (2015). “Crimini informatici nella UE aumenta la percezione di insicurezza”. Retrieved February 10, 2015 from file:///C:/Users/Francesco/Downloads/Crimini%20informatici,%20in%20Ue%20aumenta%20la%20percezione%20di%20insicurezza%20(2).pdf

2. Apetroe, A. C. (2019). ”The Role of Governments in Ensuring Global Security in the Cyber Age: Cyber-crimes, Cyberterrorism and Cryptocurrencies”. Cluj-Napoca: CA Publishing.

3. Apostol, D. M. and Bălăceanu, C. (2011). Growth and Technology: The New Economy in the 2000’S CEE countries and Romania, International Journal of Academic Research in Accounting, Finance and Management Sciences, Vol. 1, Issue 2.

4. College of Computer Science and Information Technology. (2015). “Cyber security”. CIS 313 - Technical Reports, University of Dammam.

5. Darlington, P. (2017). “Cyber Security in Action”, Institute of Railway Signal Engineers (IRSE) - CEng MIET FIRSE. Retrieved May 14, 2017 from https://www.linkedin.com/pulse/cyber-security-paul-darlington?articleId=6269507341453008896#comments-6269507341453008896&trk=public_profile_article_view

6. EC. (2008). Directive n. 2008/114/EC of the Council (GUUE 23 December 2008, n. L 345) concerning the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Retrieved December 23, 2008 from https://publications.europa.eu/it/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/

7. Kaspersky Lab. (2019). “Cybercrimine”. In Enciclopedia “Kaspersky”. Retrieved from https://encyclopedia.kaspersky.it/knowledge/cybercrimine/

8. McAfee. (2014). “The Economic Impact of Cybercrime: No Slowing Down”. Report by the Center for Strategic and International Studies (CSIS) and McAfee. Retrieved February 21, 2014 from https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

9. Norton, L. (2018). Cyber Safety insights (2018). Report – Global results. Retrieved from https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_Global_Media_Deck.pdf

10. Schmidt, N. (2014). “Cyber Security”. In Ondrejcsák, R. (Ed.), Introduction to Security Studies. Bratislava: Centre for European and North Atlantic Affairs (CENAA).

11. Teti, A. (2016). “Cyber security e investimenti. Quali scenari?”. Rivista italiana di intelligence – GNOSIS, 2/2016. http://gnosis.aisi.gov.it/gnosis/Rivista47.nsf/ServNavig/47-24.pdf/$File/47-24.pdf?OpenElement

12. World Economic Forum. (2018). The Global Risks Report 2018 13th Edition. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

13. Zappa, F. (2014). “La Criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo - United Nations Interregional Crime and Justice Research Institute (UNICRI). Retrieved from http://www.unicri.it/in_focus/files/Criminalita_informatica_def.pdf