ieee.es
Instituto Español de Estudios Estratégicos

Analysis
Report

45/2013 6th August 2013

Mª José Caro Bejarano

MORE ON CYBER THREAT

This document has been translated by a Translation and Interpreting Degree student doing work experience, IGNACIO CUEVAS MARTÍNEZ, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.

MORE ON CYBER THREAT

Abstract:

The technological development in the field of Information and Communication Technology, ICT and CIS in Spanish, have changed and continue changing our society in the so-called global world. This technological activity raises many dilemmas, as the result of the different sides. Thus, besides the remarkable progress for the humanity, we face the consequences of misuse of these technologies, intentional or not, at all levels, government, business, citizenship, etc

Keywords:

Information and Communication Technology, ICT, cyber threat, cyber-attack, cyber security, critical infrastructures.

MORE ON CYBER THREAT

As reflected in the sixth edition of the Annual Report "Society on-line 2012 (2013 edition)" by the National Observatory on Telecommunications and Information Society (ONTSI)[1], from the Secretary of State of Telecommunications and Information Society presented at the beginning of July 2013:

- The number of internet users globally in 2012 is estimated in 2,493 millions, with an annual growth rate of 10.7%
- The mobile broadband has grown as an Internet access technology, with 1,529 lines, producing a growth of 33.5% in 2012.
- The fixed broadband at home is used in 72% of European households.
- The recorded expenditures on landline, mobile telephone, Internet and pay television in Spanish households in the fourth quarter of 2012 reached 3.155 million euros, which adds up to a total of 13,308 millions the whole year.
- In 2011, the ICT and Content sector reached a business turnover of more than 100 billion Euros in Spain.

The information on this report at a European level, contrasted and brought to line in an international context, enables us to retain comparative data with our neighbor countries. This data allows us to measure the level of implementation and dissemination of ICT's in a European and Spanish context, as an example of what is taking place worldwide.

CYBER CONCERN IN BUSINESSES

According to a Lloyd's and Ipsos report, Risk Index 2013[2], developed together with a number of international institutes, cyber attacks have turned into one of the five biggest concerns of big companies all around the world. Only two years ago, the impact of cyber attacks was underrated. The list given by this report exposes the five biggest risks pointed up by these companies:

[1] See the report at: http://www.ontsi.red.es/ontsi/
[2] See the report at: http://www.lloyds.com/news-and-insight/risk-insight/lloyds-risk-index

- High taxation, from number 13 in 2011, reaches the top one
- Loss of customers and cancellation of orders, the number one risk in 2011, today is in second position
- Feasible cyber attacks rose to third position in 2013, up from 12th place in 2011
- Cost of materials, and
- Excessively strict legislation

In the case of the United States, cyber attacks are the second biggest concern for companies, right behind taxation, while in Europe, cyber attacks are only in sixth position.

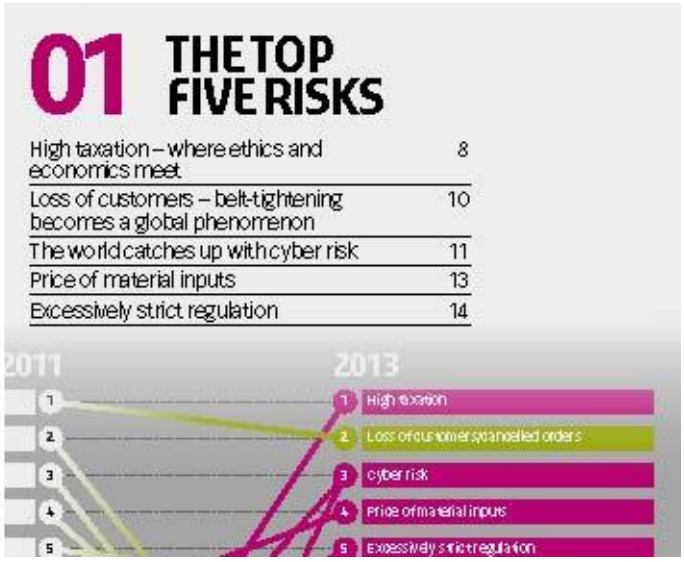

Figure1. The five major risks. Lloyd's Risk Index 2013.

The shifting in the assessment of cyber attacks can be justified by the evolution of perception in the motivation of cyber attacks, from financial crime to political and ideological attacks. 2012 has witnessed attacks against Interpol, CIA, and companies like Boeing websites, massive passwords thefts in the professional network Linkedin, the interruption of websites of the six major banks in the US etc.

Also, the number of incidents attributed to acts of piracy promoted by states and revenge attacks by hacktivists networks are increasing. Likewise, the cost of cybernetic infringement

is rising. In a 2012 study, the Ponemon Institute[3] found out that the average annual cost of 56 organizations in the US, taken as a reference, was 8.9 millions a year, in 2011, the cost was 8.4 million dollars, ranging from 1.4 millions to the astonishing amount of 46 million dollars by year and company. The most expensive cyber crimes involved malware, denial-of-services and attack on the web databases.

Neelie Kroes, the European Commissioner for Digital Agenda, claims that "Cyber security is too important to be left to chance and the companies good will", and "many governments have made a significant progress in this matter during the last few years".

In may 2013, democrat and republican senators held a meeting in order to create an act[4] to stop the theft of valuable commercial information from American companies by foreign companies and governments. The European Commission on its behalf is considering the imposition of sanctions to guarantee that companies that store information on the Internet communicate the loss or theft of personal information.

According to a report published by the Insurance Information Institute[5] in April 2013, 39% of data breaches are due to employee negligence, 24% to malfunction of the system and 37% due to attacks. This information shows that almost two thirds of these events are caused by business management related issues.

As in 2011, the right question to make would be if the increase in costs on cyber security is translating into an adequate placement of investment by the companies. The experts in cyber insurance are offering better-integrated cyber-products, even those that provide packs of coverage for data breach costs, forensic analysis and public relations crisis. Although these products are highly efficient in case of emergency, the previous investment in risks management –and the certainty that recommendations will be followed at a company level- still have a long run before they can prevent a cybernetic disaster before it occurs.

[3] See the report at Ponemos Institute: 2012 Cost of Cyber Crime Study. www.ponemon.org/library/2012-cost-of-cyber-crime-study

[4] See H.R. 2281: Cyber Economic Espionage Accountability Act y S. 1111: Cyber Economic Espionage Accountability Act June 6, 2013.

[5] See the report Insurance Information Institute: Cyber Risks: The Growing Threat, April 8 2013. www.iii.org/assets/docs/pdf/paper_CyberRisk_2013.pdf

CYBER ATTACKS POINT TO THE STOCK MARKETS

The global stock markets are ICT users, therefore they also are a cyber attack target. Almost half of the stock markets around the world suffered cyber attacks last year, according to a survey carried out on 46 of them, that appeared in a Reuters agency article.

The increased frequency of the attacks and the interconnectedness of markets creates potential for a considerable impact, according to the document from the investigation department of the International Organizations for Securities Commissions (IOSCO[6]) and the office of the World Federation of Exchanges (WFE[7]).

According to the author of the report: "Some systemic impacts may happen (...) from cyber attacks in the securities markets, especially considering that our financial system is increasingly dependent on technology infrastructure."

Among the stock markets surveyed, 53% said they experienced a cyber attack last year. The most common form was Denial of Service (DDos), which seeks to close websites and other computer systems by overloading the networks of the targeted organization with excessive traffic and even viruses. Other forms of cybercrime included laptops theft, modification of websites, data theft and insider theft. None of the stock markets reported financial theft as part of the attacks.

"Cybercrime also seems to be increasing in sophistication and complexity, expanding its infiltration and damage potential at a large scale", claims the report, adding that a major attack could create public distrust and a withdrawal from the markets. In the UK, fears about cyber attacks outperformed the euro zone crisis as the main risk to the country's banks, according to a senior official of the Bank of England. In the U.S., Nasdaq OMX Group and BATS Global Markets traders reported they suffered denial of service DDos attacks in February last year.

In October 2011, the New York Stock Exchange NYSE Euronext website remained inaccessible for 30 minutes, according to an Internet monitoring company, but the stock market reported no interruption of service. In 2010, hackers who infiltrated Nasdaq's computer systems installed malicious software that allowed them to spy the CEO's of companies listed on the stock markets, as reported by Reuters.

We have limited data regarding the costs involved in cybercrime to the stock exchanges, but the report says that several studies have estimated the cost to society in genera oscillates

[6] See http://www.iosco.org/
[7] See http://www.world-exchanges.org/

between 388,000 million and one billion dollars. The markets that participated in the survey said that the direct and indirect costs of cyber attacks accounted for less than 1 million dollars last year.

CRITICAL INFRASTRUCTURE CONTROL SYSTEMS ON THE SPOTLIGHT

The latest document of the U.S. industrial CERT (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT) reports more than 200 security incidents in all sectors of critical infrastructure in the first half of 2013. 53% of these attacks have been aimed at the energy sector.

As an example, ICS-CERT points out an attack in February against a gas compression station. The attackers reportedly tried to access the company process control network with the launching of brute-force attacks. After receiving notification of the attack, ICS-CERT issued 10 IP addresses in the US-CERT website to warn other resource managers of critical infrastructures. Soon after, other operators of critical infrastructure began to report similar incidents and identified a total of 39 new malicious IP addresses.

None of the attempts were successful, but the incident emphasized the need for constant vigilance, ICS-CERT warned.

The cyber security of critical infrastructures is a hot topic today, cyber threats could reach foreign countries and cause loss of human lives in identical ways to a conventional attack, governments face a silent and unpredictable threat that could be performed by hackers sponsored by states or cybercriminals for different purposes such as sabotage or cyber espionage.

The Computer Emergency Response Team (CERT) of all countries are approaching the problem, work is being done to complete a census of infrastructures that examines their security level, these groups are also working on awareness and exchange of information programs, key activities to palliate risks.

ICS-CERT recently released a report warning about the growing number of attacks on U.S. critical infrastructures between 2009 and 2011, recording an impressive growth in the number of incidents. This report also provides a guide with the following recommendations:

- Conduct detailed surveys of the structures and classification of risk assessments to identify key vulnerabilities and cyber threats that could take advantage of them

- To define, disseminate and adopt the best practices to protect critical infrastructures.
- To deal with phishing companies, a security-training program must be developed to prepare employees for attacks to potential vectors and against major social engineering techniques.

In this scenario, it is expected that the number of attacks also increase in the coming years, however, the increased level of awareness and interest in the subject could avoid serious consequences.

JOINING FORCES AGAINST THE COMMON CYBER ENEMY

Taking into account that all states, companies, administration and citizens are target of cyber attacks, different proposals call for sharing the information regarding the characteristics of the attacks in order to protect against them. The different CERTs or Computer Emergency Response Center exchange information in this regard.

In other cases there are government-business partnerships to enhance cyber security, this is the case of the U.S. and lately the UK too. This country has established an alliance with defense and telecommunications firms to improve their cyber security.

In particular, nine of the largest arms manufacturers in the world and some telecom providers are partnering with Britain to improve cyber security in the country towards addressing the growing threat posed by hackers and other similar.

Cyber security became a priority for Britain's national defense in 2010, citing the growing threat of cyber attacks by criminals and foreign groups with state support. Companies such as BAE Systems, Rolls-Royce, Lockheed Martin and Hewlett Packard are among the companies that will partner to share information and address cyber threats, according to the British Ministry of Defence.

Government and industry networks suffer 70 sophisticated cyber attacks a month, and 15% are against the defense sector, according to GCHQ[8], the government's intelligence center than also participates in this partnership.

The partnership comes as contractors like BAE increase their cyber deals ahead of the growing demand from governments and businesses, at a time when the demand for

[8] See http://www.gchq.gov.uk/Pages/homepage.aspx

equipment suffers from budget cuts in defense. The so-called Association of Cyber Defense Protection will also try to apply controls and share threat intelligence to enhance the security of the defense supply chain. "It is a clear demonstration that the government and industry can work together: to share information, experiences and knowledge," said Minister for Defence, Support and Technology, Philip Dunne.

Other companies involved are Selex, a unit of Finmeccanica, Cassidian, a division of EADS, Thales, CGI Group and BT Group[9].

CONCLUSION

As it can be seen with these series of examples that affect companies, the financial world, the critical infrastructures, all of them as well as governments and citizens are in the spotlight of cyber-attacks. The strategic companies that are subjects of attack, and the ones related to cyber-security with the knowledge and capacity to prevent and relieve these attacks, have begun to collaborate with governments so to exchange information related to cyber-attacks that will make it possible to exercise a common and compact defense against a threat that has arrived to stay and has evolved in an exponential pace in both complexity and number of targets, as well as in impact of the attacks.

Mª José Caro Bejarano
Senior Analyst IEEE (Spanish Institute for Strategic Studies)

[9] See the news ítem at Europa Press 8/7/2013