Cybercriminals: The Great Threat

MARÍA ÁNGELES CABALLERO VELASCO
Assistant Director General of Security and Environment MAPFRE

Technology has taken giant steps since the first personal computers were born in the 1980's, such as the *Spectrum*, to the most sophisticated systems available today, from mobile devices which allow us to be connected in any part of the world to the "Internet of Things," objects of everyday life interconnected to each other through the net. The proliferation of social networks, the increase in the consumption of web services and the cloud revolution have further boosted the new era of interconnected devices.

This new scenario has led users, companies and governments to change their behavior, their way of interacting with people. Today companies are totally dependent on Information Technologies (IT). It is impossible to image a company that is not supported by technology for its proper operation, and IT equipment and their security are key in organizations. Can you imagine a cyber-catastrophe that could affect several sectors and multiple companies in the style of "Die Hard 4.0"? This would cause the disruption of their activities and theft or damage to their computer systems, which in some cases could have direct effects on the state of well-being of a country (nuclear power plants, energy companies, etc.). It has been estimated that if companies' activities come to a standstill for a week, this could have an economic impact of up to 10 trillion dollars[1].

The rise of technology that we have been experiencing in the last few decades has been associated with an increase in technological risk, especially in recent years, mainly due to the fact that a new world of fraud has been made available to cybercriminals, with the consequent creation of new ways of committing crime through technology. This situation has caused growing concern leading to the creation of specialized teams dedicated exclusively to the control and supervision of these risks (*blue-teams*), having even engaged in responses to possible security incidents.

To understand this situation, the concept of **risk** will be explained briefly from a corporate perspective, measured as the product of threats, vulnerabilities and their impact on business. Risk can be understood as possible scenarios that may compromise the whole or part of a company's resources, jeopardizing its viability. As a counterweight to this risk, companies must establish proper measures to mitigate, prevent, transfer or accept these risks. The **threats** that stalk us on the internet will be explained, and later the **countermeasures** to mitigate and manage these threats.

CYBERTHREATS, FRAUD AND CRIME ON THE INTERNET

Each year, the "bad guys" reinvent new ways of committing telematic crime, but it is also true that there are some constants that have been repeated over the years and that some of them have been decreasing. For example, *spam* has decreased 50 percent in a decade according to the latest *Intelligence* Report from Symantec.

The most common attacks target corporate servers as well as end-user devices. Physical attacks are starting to be less common but social attacks have increased in recent years. The **main cyberthreats**[2] which companies faced last year can be described using nine patterns: attacks to webpages (35 percent), cyber spying (22 percent), intrusion at client points of sale (14 percent), illegal copying of credit cards (9 percent), misuse of systems by internal employees (8 percent), malware (4 percent), miscellaneous errors (2 percent), theft or physical loss (<1 percent) and denial-of-service attacks (<1 percent). It is calculated for this year, 2015, that the economic losses that European companies will undergo exceed the €14 billion[3] due to cyberattacks. These attacks are not only of an economic nature, but also of a reputational nature. It is noteworthy that Spain is the third country with the most cyberattacks worldwide, after the United States and the United Kingdom. Each of these attacks consists of the following.

[CYBER SPYING AND CYBERWARFARE]

Cyber spying not only affects governments and public administrations, but private companies as well. These targeted attacks or APTs (*Advanced Persistent Threats*) are specifically designed for a particular company and one of their main goals is to obtain confidential information from companies, with a monetary purpose or for industrial and/or political espionage.

In 2012, Saudi Aramco, the largest oil company in the world, suffered one of the worst[4] industrial cyber spying **attacks** in the history of cybersecurity. Around 30,000 computers and about 2000 servers were inaccessible in a matter of hours. The attack started through an email which contained a link that downloaded malware, which expanded silently through the rest of the network to simultaneously attack during Ramadan, when most of the company's employees were on vacation. Saudi Aramco had to enter the world of paper and fax again and was not able to monitor the purchase/sale of oil for months, deciding after a time to give it away so as to not stop production, which resulted in millions in losses. The attack was self-attributed to the group *"Cutting Sword of Justice"* which mentioned Saudi Aramco's support to the political regime of the royal family of Saudi Arabia.

In the case of cybernetic war or **cyberwarfare**, which goes beyond mere industrial espionage, we have the example of "Stuxnet." In 2010, Stuxnet came out, known at the time as the most intelligent *malware* ever created, and which was developed for SCADA type industrial systems. It was devised to attack nuclear power plants in Iran, slowing down the manufacture of enriched uranium in these power plants by 10 years. Due to evidence found in the source code, it is believed that it was developed jointly by the U.S. and Israel over more than a year's time by a team of experts. It was not some toy created by a mere amateur.

[MALWARE]

In the case of *malware*, or malicious software, we can distinguish between the variants that attempt to pass for a "legitimate" program by forging the identity of an entity and the variants that restrict access to certain parts of the operating system by encoding their files and asking for ransom in exchange. The latter are technically known as *ransomware*.

One example of identity forging *malware* is known as "the police virus," which will be addressed later in the section on social engineering. Regarding the second variant: who has not suffered from or does not know someone whose device has been infected with a virus that encoded all of their files and would not let them perform any actions on their system? *Cryptolocker* ***malware*** is one of the worst headaches for security and customer support teams at companies. Operations teams must study the entire infection cycle, from when the *malware* is received (usually by email) to its detection, and after the systems have been infected, quarantined and corrected through the recovery of system *backups,* since some of these viruses are practically impossible to eliminate and the system has to be restored to a previous state. Another option for eliminating it is to pay the "bad guys," but then we would be collaborating directly with cybercrime.

This type of fraud is known as **crimeware**, which compromises user systems or servers through malicious software and includes *phishing*. The "bad guys" look for user data, passwords, payment information, etc., through seemingly trustworthy websites. Their objective is to forge the identity of an organization (usually banking *sites*) with the aim of obtaining an economic reward. On occasion, the attacks are highly sophisticated, but sometimes they are easy to detect.

For example, there is a variant of this kind of *phishing*, where the user is asked for all of his or her bank card numbers and, depending on the victim's naiveté, he or she may or may not take the bait.

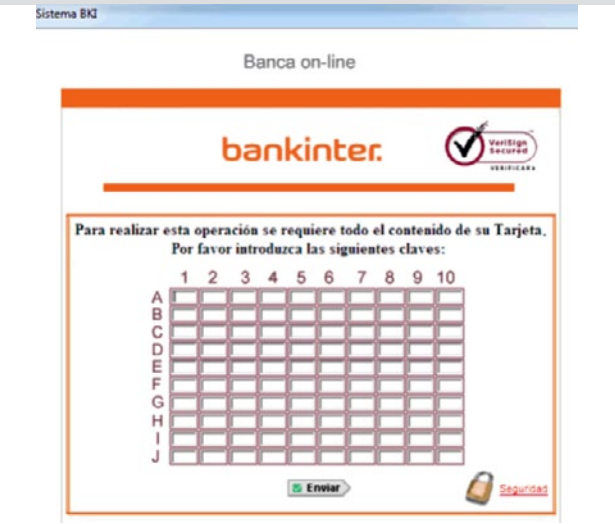


Image 1. Example of Bank *Phishing*

[POS AND CREDIT CARD COPIES]

When we talk about attacks on **Points of Sale (PoS)**, the attackers try to compromise the servers or the devices of the PoS with the aim of obtaining payment information. The companies that suffer from this kind of attack the most are those that sell to the common consumer, such as companies in the hotel industry. Another related threat is the installation of skimmers in automated teller machines (ATMs) to steal credit card information, which mainly affects banking entities. To prevent this type of fraud, Visa and MasterCard designed a mandatory standard (PCI-DSS) with the aim of increasing the security of data and operations conducted with credit cards. This affects all companies (and shops) that process, transmit and/or store these data.

[WEBPAGES]

Attacks on webpages is based primarily on jeopardizing user credentials by brute force or theft and/or exploiting vulnerabilities in the software or infrastructure that supports the web application, such as content managers or e-commerce platforms Most companies provide their clients and their employees with web platforms that are necessary for business, but which could put the company's information at risk.

[DENIAL OF SERVICE]

In recent years, companies have suffered numerous **distributed denial of service attacks** (DDoS). On the news, you may have heard mention of attacks by *hacktivist* organizations, such as Anonymous or LulzSec, which have disconnected or disable company websites. Ordinarily, this is done through DDoS attacks and with the aim of causing damage to the company's reputation. This kind of attack is undertaken by infecting a large number of computers that are connected to the internet in order to obtain sufficient resources and achieve a successful attack. This is how they form what is called a botnet or a network of infected computers or bots. At the time of the attack, all of the infected machines are used to generate an immense number of simultaneous connections to a specific target, the webpage of the company in question.

[INFORMATION LEAKS]

Information leaks are a critical threat to an organization. The **misuse** of the organization's systems and its data, the **loss of devices** or printed information, a lack of control over access in the facilities or **miscellaneous errors** (such as the disclosure of private information over a public network or sending emails to the wrong recipient) could compromise the organization's information. Without proper management of these threats, we could incur serious fines in the case of high-level security data in the face of data protection regulations, such as personal or health data, for example.

SOCIAL ENGINEERING

One of the greatest challenges faced by the information security teams at companies is social engineering. **Social engineering** techniques manipulate the user through psychology and the attacker's social skills in order to obtain information from the victim, ranging from finding out their username and password, seeking to obtain access to restricted areas, to making money in exchange for something that will never arrive. Social engineering techniques are increasingly more sophisticated and more difficult to detect. Cybercriminals no longer need to develop complex applications. Instead, they focus on the person, which is the weakest link in the chain from a security standpoint. Cybercriminals rely on psychological manipulation in order to persuade their victim to do things that they would normally not do, obtaining truly valuable information from them.

Many of the aforementioned attacks such as the *cryptolocker* and bank *phishing* are examples of *malware* that use social engineering techniques. One example of this that has become popular is the "police virus". This type of virus tries to scare its victims, making them believe that they have broken the law (intellectual property theft, pornography, pedophilia, *copyright infringement,* etc.) and kindly puts easy and simple payment methods at the disposal of the victim in order to solve the crime that "they committed."

Image 2. Police virus

These attacks are very difficult to resolve since they involve people directly. The best **countermeasure** in this regard is dissemination, awareness and training of users so that they recognize the existence of this type of technology and are able to protect themselves against it.

THE "BAD BUYS" AND THEIR VICTIMS

Who are these "**bad guys**?" They are the new thieves of the internet, organized mafias from all over the world, whose malware essentially originates in Eastern European and Asian countries dedicated to the creation of this type of software for the purposes of illegally obtaining information or money. The work of security forces and bodies of the state has become very complicated in order to capture these "bad guys" that essentially use two factors: **distance/borders and the anonymity of the internet.** They sometimes operate through "mules," who are nothing more than mere intermediaries doing the "dirty work." These organized mafias hire people through job offers, leading them to believe that they are going to cooperate on strategic multinational plans and that they can earn money easily and quickly. Their work turns out to be transporting merchandise or money from one location to another, and this way traceability is lost and the search for the "bad guys" becomes complicated.

Not all attackers are organized mafias; many attacks are caused by **internal personnel**, known as insiders, who are familiar with and dominate the scene, which is why their attacks can be much more damaging than with external actors. Furthermore, we also have the profile of the **hacktivist**, which was previously mentioned, motivated by a specific ideology, and who undertake attacks with a determined goal. Lastly, there is another type of profile that exists within cyberwarfare, which are known as **states** on one hand and **terrorists** on the other.

The **victims** of these attacks could be one of us. All industries and businesses are at risk. Even though we think that the risk of an external attack is not high, there will always be a risk of an internal attack or a risk that one of the users does not use the systems correctly, leaking sensitive information to the public. The fact is that the target audience has changed from large companies to SMEs, small and medium sized enterprises, which is exponentially raising the number of cyber attacks. Attacks are seen everywhere from companies and public administrations to the pharmaceutical, hotel and retail sectors.

The number of cybercriminals reached over than 70,000 last year, causing losses, as was previously mentioned in this article, of more than 14 billion euros in 2015. We can confirm that cybercrime is moving more money than drug trafficking[5] in recent years.

So why are do we call them "bad guys" when they are commonly known as "hackers?" It is worth mentioning that the word *hacker* has lost value over time. In the 80's it was known as people skilled with computers who were able perform any type of operation for fun, but today they are associated with "information pirates," a term the Royal Spanish Academy (RAE) added in October 2014. Back then, this meaning prompted strong criticism from the group of security experts for not also associating it with its original meaning. The name *cracker* or *cybercriminal* would be more accurate.

WHAT CAN I DO TO MANAGE RISK IN MY COMPANY?

Fighting the main cyberthreats to which we are exposed over time and in due form can involve a differential and definitive element in the continuity and sustainability of our business. It is necessary to define a proactive strategy, instead of just taking action when accidents occur. Sooner or later our company is going to be attacked.

The risk cannot be eliminated, due to its very nature, but we can develop countermeasures in order to reduce it on the legal and organizational levels, as well as with more technical measures. The success of the risk reduction to which we are exposed revolves around two **pillars: technological governance and security**, on one hand we have the guidelines framework, legal and juridical, to establish appropriate safety policies and good practices in the companies, and on the other hand we have technological security. The goal that these basic pillars strives for is the protection of company assets, emphasizing people as the most important asset.

With respect to **security governance,** several factors must be considered. Firstly, it is essential be familiar with the risk appetite of the company and to put it in context with the legal and juridical framework of the country: regulations associated with the protection of information, regulations related to cyberterrorism, health and finance regulations and regulations of our sector of activity. Along this same line, we must establish appropriate company and security policies within our company, as well as develop a code of conduct and invest in dissemination and awareness so that all company users are familiar with these regulations. A study from *Enterprise Management Associates* reported that only 56 percent of employees have received any type of training on security, protocols or policies.

Within the scope of **technological security,** we differentiate between logical or information security and physical security. We must work on key aspects within our company, such as managing a proper security infrastructure, establishing an appropriate incident response team and implementing suitable physical security controls in our company's facilities. Incident response teams provide service through Security Operations Centers and are created as CERTs *(Computer Emergency Response Team)* as part of the global network of CSIRTs *(Computer Security Incident Response Team)*. Some of the most renowned at the national level are the CCN-CERT of the National Cryptologic Center of Spain or the Security and Industry CERT operated by INCIBE (National Cybersecurity Institute of Spain), which work to protect critical national infrastructure and to fight against cybercrime and cyberterrorism, among other things. These kinds of institutions at the government level (existing in other countries) focus their work essentially on safeguarding the country's well-being. In Spain specifically, the activities undertaken by these centers are part of the **National Cybersecurity Strategy.**

As a final recommendation, we would stress that being up-to-date on security is imperative, not only for the expert teams, but for all employees of a company. The users of the organization must be familiar with the risks to which they are exposed and the capacity to manage these risks in some way. One of the products that is spreading among companies is **cybersecurity insurance,** which attempts to respond to cybernetic and reputational disasters. Once the risks have been minimized, the residual risk, which remains latent, is transferred via specific cyber risk policies. We should highlight the famous SONY case of 2011, in which more than 25 million accounts were stolen, containing nearly 18,000 credit cards and bank accounts, through the *Play Station Network*.

It is definitely necessary to design a continuous, persistent and sustainable security strategy, to implement updated systems and infrastructure and to invest consistently in cybersecurity to ensure company infrastructure and to guarantee the success and continuity of our company.

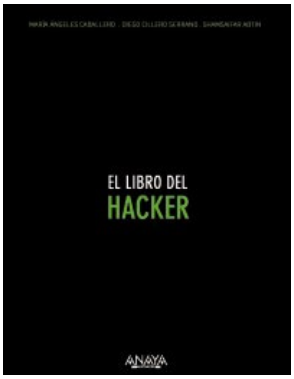
MAPFRE AND ITS CONTRIBUTION TO THE WORLD OF INFORMATION SECURITY

MAPFRE, as a company that is committed to the society, works continuously and actively to protect the interests of its clients, employees, shareholders and providers, through the prevention and detection of security incidents.

This ongoing work is undertaken by its team of cybersecurity experts from the **Corporate Security and Environment Division** and its **Information Security Incident Response Team** known as the **CCG-CERT.** MAPFRE's incident response team has a sophisticated laboratory and a group of highly qualified professionals who are committed to preventing, responding to and minimizing the impact of any security incidents. In MAPFRE's global and multinational context, the work of the CCG-CERT is not just internal; it collaborates actively with other companies and institutions both at the national and international levels.

RECOMMENDED READING: "EL LIBRO DEL HACKER" FROM ANAYA

If you want to delve into the world of information security or learn about the subject of the article further, we recommend **El Libro del Hacker** from ANAYA publishing house. The book addresses questions of security, from the introductory chapters to information insecurity to the most sophisticated attack techniques, from the first phases (*footprinting/fingerprinting*) to the more advanced stages (*exploiting*) to deleting the evidence. We can also find other emerging issues, such as security on social media, *cloud computing*, identity management, cyberthreats, etc.



This book can help people who are interested in entering the world of information security, as well as somewhat more advanced experts. Consult the file on the webpage of the publishing house for more information: http://www.anayamultimedia.es/libro.php?id=3608921

[1] "Cyber Catastrophe" *working paper, University of Cambridge Judge Business School*

[2] "Verizon Data Breach Investigation Report" (DBIR) – 2014

[3] "España, a la cabeza del cibercrimen" Diario ABC – 2015

[4] "Arabia Saudí dice que el ataque informático contra Aramco fue lanzado desde el exterior" El País http://economia.elpais.com/economia/2012/12/09/agencias/1355069609_526898.html

[5] La ciberdelincuencia mueve más dinero que el narcotráfico en el mundo http://www.abc.es/espana/20141207/abci-ciberdelincuencia-dinero-201412062106.html