d+i developing ideas
LLORENTE & CUENCA

» Cyber-risk and the new reputational paradigm

Madrid » 05 » 2017

“Spain is the country with the fifth-highest number of systems controlling Internet-connected installations and industrial processes, most of them with no protection.” Such is the view of Merce Molist, a journalist specializing in cyberthreats. Last year, according to data provided by Molist, cyberattacks increased by 357 percent in Spain. Even if this figure might seem exaggerated, those provided by the Spanish National Cybersecurity Institute (INCIBE) show that attacks rose from 50,000 to more than 120,000 last year alone. Are companies ready to respond to the challenge of protecting their reputation? For some, the answer will be yes; however, the regulatory changes implemented by the NIS Directive and new European General Data Protection Regulation (GDPR) may may corner others. Let us try to clarify all this below.

It is nothing new that companies now face a remarkably high level of digital vulnerability. We need only mention three examples. Mere days ago, the WannaCry worm affected over 150 countries. Last year's denial of service (DoS) attack on the Dym servers in the United States affected one billion customers of companies such as Twitter, Amazon, Whatsapp or The New York Times. And lastly, it is interesting to remember how cyber-criminals remotely attacked ATMs, forcing them to spit out cash in more than a dozen countries across Europe. But this was only the beginning.

In order to try to limit the damage, promote a culture of risk management and ensure incidents are always reported, a new Directive for Security of Networks and Information Systems (NIS) and a new European Regulation on Data Protection have been adopted, both of which will enter into force by 2018. These regulations, which are now being transposed into the Spanish legal system, represent a significant change in company cultures regarding the privacy, rights and obligations in the secure digital processing of personal data and provision of services.

Such regulation sets out that, by May 2018, it will be compulsory to report any kind of security gap arising from either computer attacks or an internal incident to the CERN (or final designated body), as well as affected parties, in less than 72 hours. If the organization is not aware of which customers' personal data was compromised, it must also report this situation publicly.

> – Excuse me? If I do that, I will be letting everyone know that my customers' data have been compromised, and soon after dozens of journalists will be out there asking for an explanation.

And that is correct. This is the idea.

Just to clarify, let us use an example: If a bank whose clients' data have been seized, and it is not able to determine how many of them were affected by the attack, it must inform all of them. It makes no difference

[1] *La ciberseguridad de la industria española es un sainete, y los ataques se están disparando* Mercè Molist 2017 http://www.elconfidencial.com/tecnologia/2017-03-20/ciberseguridad-industria-espanola-infraestructuras-criticas_1350398/

whether it has been made public or not. From that moment on, social media will do the rest. A few minutes later, that information will be online and the media will be aware of it. Undoubtedly, the reputation and value of your stock (if your company is listed) will be affected.

> "According to the new European Regulation on Data Protection, in addition to being hacked, financial penalties may be as high as millions of euros or 4 percent of the annual general turnover"

FINANCIAL PENALTIES

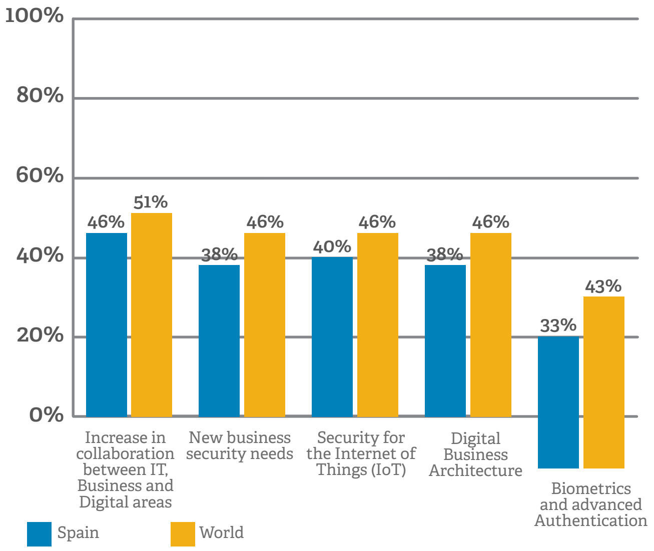
– Oh! There's more?

– Indeed. A regulation without a penalty system is not worthy of the name. According to the new European Regulation on Data Protection, in addition to being hacked, financial penalties may be as high as millions of euros or 4 percent of the annual general turnover.

Some Chief Information Security Officers (CISOs) have publicly described this law as true regulatory blackmail, which may wipe many companies off the map and will further benefit the formation of oligopolies.

– But hold on, you will still have to pay a little bit more; you have not heard about the Data Protection Officer yet, have you? All companies will be required to have someone representing them in this area, either inside or outside their organizations. This will be the sole spokesperson for all these matters, in charge of reporting all attacks suffered or any kind of data disclosure–IP addresses are now considered personal data—to the relevant organizations and authorities. That is to say, new, specific procedures for cyber-attack prevention, data protection and management must be made available. This implies specific documentation, reporting and communication mechanisms. Some big companies, which suffer dozens of attacks every day, will have to create specific units whose main task will be reporting the attacks suffered to the relevant authorities and, occasionally, customers.

Figure 1. Where will companies intervene, in matters of cyber-security, in the following twelve months?



Source: PwC, *The Global State of Information Security Survey 2017.*

A NEW SECURITY PARADIGM

At this stage, it is important to be aware of the **new communication paradigm we are living with; it is characterized by synchronized digital information–online, fluid and living in a hyper-transparent framework.**

Nowadays, not only are we potential communication channels thanks to our mobile devices, but we have also become, for the same reason, a potential risk for every organization we become part of. For ourselves and for others, we are a true risk vector. And our PCs are not exactly the most critical point. Most likely, our workstation is under the strong vigilance of the IT team. But what about our mobile phones or tablets?

The security paradigm has not adapted to the new dynamic of social digital behavior, mobility, clouds and Big Data. We have spent the last few years discussing digital transformation processes across organizations, but at the same time, we have not addressed the risks attached to such changes. The high complexity of the four elements mentioned above will change the whole precautionary approach, since the area to be protected is now larger. It is, in fact, a global perimeter; Our connections are global, and just as we are capable of making information go viral in real time, a threat can be spread across the world within a few seconds of an attack.

Therefore, it is normal that, when such a vulnerability occurs, governments take action to protect the system, organizations and companies, defining the trajectory of the data. However, the implementation of controls around these circumstances will place strong limits on rights and liberties, and it is just a matter of time before we start suffering even stricter controls. As we have seen recently, after the Berlin attacks, German authorities were asking for access to WhatsApp's data to fight terrorists. Cyberattacks will be no exception, but rather a new motivation. What is at stake is the security of critical infrastructures, of the financial system and, of course, a country's citizens.

In light of this, it will not be long before we see different levels of access to data, which will involve defining new cyber-social castes. Different access, services and fee profiles, depending on the data interactions; this will end up creating social castes that reflect our level of vulnerability.

> "According to information published by PR Newswire, in 2016, 90 percent of cyberattacks originated in information stolen from employees after their systems were hacked"

THE NEW SOCIAL LICENSE REQUIRED TO OPERATE

Keeping a social license to operate will not solely rely on the need to keep our reputations safe anymore. Since they are constantly under the supervision of regulators, companies will be required to constantly prove they can protect customer data in an efficient way and keep their systems operational. This implies a change in company culture, moving toward proactive responsibility.
The regulator's continuous scrutiny and constant notifications to customers will make companies modify their DNA, making themselves especially transparent and collaborative. In fact, only those companies that manage to adapt to this new scenario will be able to continue operating in their markets.

THE MOST VULNERABLE ELEMENT – THE EMPLOYEE.

According to data collected by IBM in 2016, two-thirds of company attacks were carried out by internal agents[2]. According to information published by ***PR Newswire,*** in 2016, 90 percent of cyberattacks originated in information stolen from employees after their systems were hacked. It is therefore not surprising that, according to the Allianz barometer of Risks for 2017[3], reputational damage was the main cause of losses for 69 percent of companies following an attack.

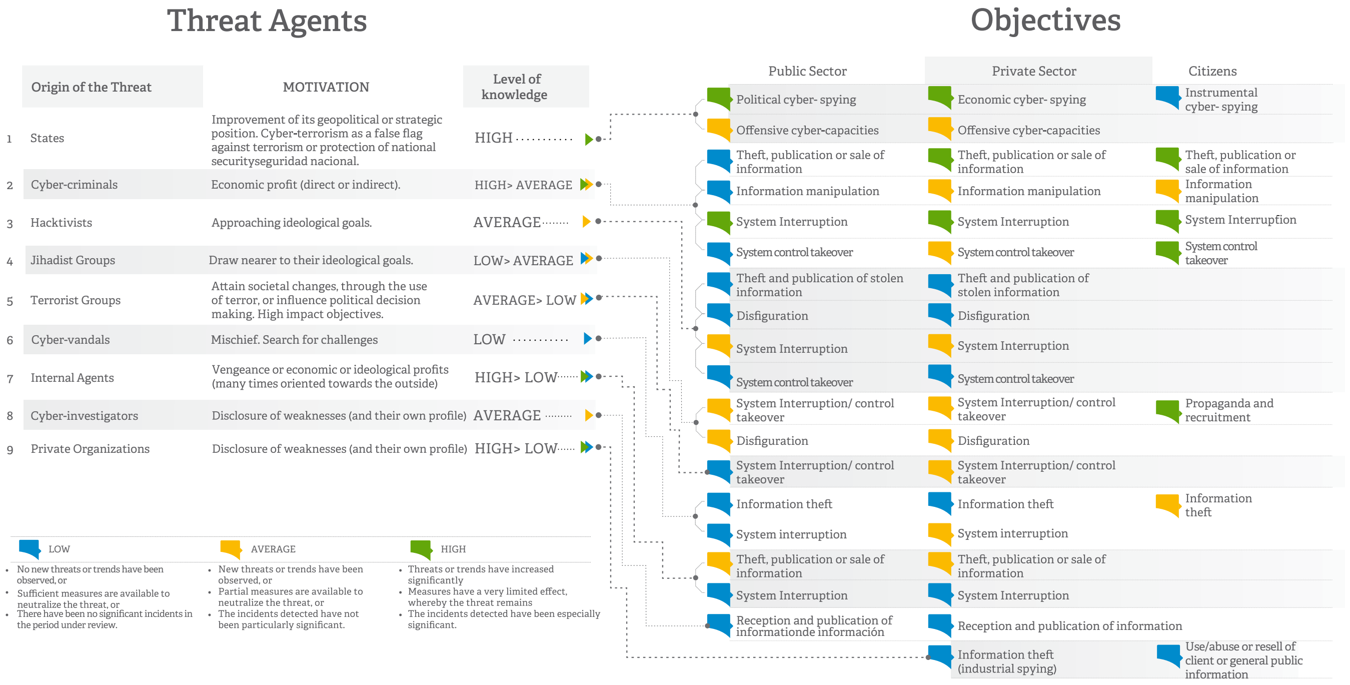
Therefore, in our opinion, the new reputational risk paradigm leads to the conclusion that individuals with access to company data can rewrite them, which also involves rewriting the company's reputation. In light of the above, the proper protection of company data will be a necessary condition to preserving its reputation.

Once they are aware of these risks, CEOs and companies will have no choice but to focus on digital security; this will be a transversal theme for the whole organization, since complying with regulations and protecting reputation is not only a matter for the IT

[2] According to IBM, data compromised by the cyber-attacks rose by 566% in 2016 Telam 2017 http://www.telam.com.ar/notas/201704/185558-ciberataques-seguridad-crecimiento-2016-informe-ibm-sector-financiero.html

[3] *Allianz Risk Barometer 2017,* Allianz 2017 http://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2017/

Figura 2. Threat Agents.



Threat Agents

	Origin of the Threat	MOTIVATION	Level of knowledge
1	States	Improvement of its geopolitical or strategic position. Cyber-terrorism as a false flag against terrorism or protection of national securityseguridad nacional.	HIGH
2	Cyber-criminals	Economic profit (direct or indirect).	HIGH> AVERAGE
3	Hacktivists	Approaching ideological goals.	AVERAGE
4	Jihadist Groups	Draw nearer to their ideological goals.	LOW> AVERAGE
5	Terrorist Groups	Attain societal changes, through the use of terror, or influence political decision making. High impact objectives.	AVERAGE> LOW
6	Cyber-vandals	Mischief. Search for challenges	LOW
7	Internal Agents	Vengeance or economic or ideological profits (many times oriented towards the outside)	HIGH> LOW
8	Cyber-investigators	Disclosure of weaknesses (and their own profile)	AVERAGE
9	Private Organizations	Disclosure of weaknesses (and their own profile)	HIGH> LOW

Objectives

Public Sector	Private Sector	Citizens
🟩 Political cyber- spying	🟩 Economic cyber- spying	🟦 Instrumental cyber- spying
🟨 Offensive cyber-capacities	🟨 Offensive cyber-capacities	
🟦 Theft, publication or sale of information	🟩 Theft, publication or sale of information	🟩 Theft, publication or sale of information
🟦 Information manipulation	🟨 Information manipulation	🟨 Information manipulation
🟩 System Interruption	🟩 System Interruption	🟩 System Interruption
🟦 System control takeover	🟨 System control takeover	🟩 System control takeover
🟦 Theft and publication of stolen information	🟦 Theft and publication of stolen information	
🟦 Disfiguration	🟦 Disfiguration	
🟨 System Interruption	🟨 System Interruption	
🟦 System control takeover	🟦 System control takeover	
🟨 System Interruption/ control takeover	🟨 System Interruption/ control takeover	🟩 Propaganda and recruitment
🟨 Disfiguration	🟨 Disfiguration	
🟦 System Interruption/ control takeover	🟨 System Interruption/ control takeover	
🟦 Information theft	🟦 Information theft	🟨 Information theft
🟦 System interruption	🟨 System interruption	
🟨 Theft, publication or sale of information	🟨 Theft, publication or sale of information	
🟦 System Interruption	🟦 System Interruption	
🟦 Reception and publication of informatiode información	🟦 Reception and publication of information	
	🟦 Information theft (industrial spying)	🟦 Use/abuse or resell of client or general public information

🟦 LOW
- No new threats or trends have been observed, or
- Sufficient measures are available to neutralize the threat, or
- There have been no significant incidents in the period under review.

🟨 AVERAGE
- New threats or trends have been observed, or
- Partial measures are available to neutralize the threat, or
- The incidents detected have not been particularly significant.

🟩 HIGH
- Threats or trends have increased significantly
- Measures have a very limited effect, whereby the threat remains
- The incidents detected have been especially significant.

Source: CN-Cert, Centro criptológico nacional department to be concerned with. In fact, corporate reliability will divide companies into those which are ready to face cyberthreats and those which are not.

> "Corporate reliability will divide companies into those which are ready to face cyber-threats and those which are not"

THE SYMPTOMS OF REPUTATIONAL CYBER-STRESS

The new paradigm of cyber-risk will cause higher levels of stress in organizations due to:

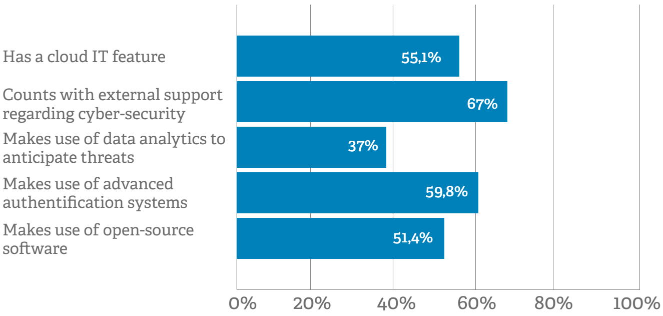
- The increase in regulatory pressure and the ensuing technical and organizational adaptations to these new legal measures.
- The increase in organizational stress within companies due to the need to protect the endpoint, understanding that every employee represents a risk both at their workstation and their mobile devices.
- Increasing pressure on corporate management due to their hypervulnerability, to the detriment of organizational value.
- The absence of a solid reputational shield that can ensure identification of potential risks and offer ad hoc preventive and management operational procedures for each cyberthreat from the point of view of both IT and communications management.

REPUTATIONAL RISKS IN THE NEW CYBER-RISK PARADIGM

As a result of this new scenario, the reputational risks traditionally affecting companies will only increase, focused on two main themes:

- Ongoing communications and notifications from companies regarding all attacks suffered, as well as the difficulties they face in ensuring data protection, will involve an exponential increase in lack of trust due to clear company vulnerability. Users will require more guarantees regarding data protection and will move toward large companies that can offer more guarantees.

Figure 3. Five trends in security matters in Spanish companies.



Source: PwC, *The Global State of Information Security Survey 2017.*

- Companies will have to develop new communication procedures with their customers, using all channels available to keep them informed in real time and prevent media from focusing on their vulnerabilities. This will require stronger communication teams and a continuous information stream. Online criticism can occur at any time and must be neutralized as soon as possible. Public exposure is increasing, so one must be ready at any moment, any time.

HOW TO FACE THIS NEW REPUTATIONAL CYBER RISK SCENARIO?

After analyzing the new reputational risk scenario companies will soon have to face, it is obvious the only solution is multidisciplinary preparation to help reduce risks. With this in mind, some measures to deal with the topics discussed include:

- **Data protection**: invest in IT experts, increase investments in protective technology and, overall, create a corporate culture of prevention.
- **Protect evidence in case of an attack:** have multidisciplinary teams comprised of IT, Legal and Financial experts, improving all internal training processes to promote a culture of protection among the employees. To do this, it will be paramount to test the protection tools available for subsequent analysis.
- **Big data and artificial intelligence:** implement the best technology available to analyze large volumes data to help prepare risk and suffered damage reports.
- **Regulatory pressure**: have compliance and data protection experts and improve relationships with regulatory and oversight institutions.
- **Stress within the organization**: focus on modifying internal management processes within the organization. Involving Human Resources, create a Crisis Committee whose members are trained in the cyberthreat field and improve internal precautionary training for employees, setting strict requirements.

- **Corporate pressure**: strengthen all information channels that help neutralize the perception of company investment risk by presenting reports that demonstrate how data security, tests and reputation are increased and guaranteed.

- **Reputational risk and a protective shield**: create communication teams trained in specific prevention procedures to completely manage cyber-risk. It will be necessary to use digital monitoring and management tools to substantially reduce the distance between human time and machine time when managing alerts, establishing a strategy and implementing crisis management tactics.

- **Time reduction**: cyber-security management will require combining new, specific digital tools with the perspective provided by expert data analysts with legal, financial and reputational communication backgrounds.

In short, large companies face major challenges regarding cyber-security. They must make great efforts to adapt their materials, procedures and methodologies to the new regulatory requirements without ignoring the fact that managing cyberattacks will be a major element of managing company reputation to avoid destroying trust. Therefore, the security paradigm will be linked to a company's holistic digital transformation, to the organizational adaptability, to new communication and digital social behavior dynamics.

Luis Serrano is the Director of the Crisis Area at LLORENTE & CUENCA. Luis holds a degree in Journalism and is one of the leading experts in Spain in the field of management of communication of emergencies and catastrophes, and the development of action plans for crisis in social networks. He has been press officer of the 112 Emergency Centre of Madrid for 17 years, where he actively participated in the management of critical situations, such as the 11M attacks in Madrid. He has intervened in more than 100 industrial accidents, accidents with multiple victims, accidents in leisure areas, health crisis, etc. His book *11 M and other catastrophes. Managing communication in emergencies* is the result of all these experiences. He also has vast teaching experience in the field of emergencies and crisis management. He is a lecturer at the Master's Program in Emergencies of CEU-TASSICA, as well as the Master's Programme in Fire of the University of Lleida. Master's Programme in Political Communication of the Camilo José Cela University, Master's Programme in Security and Emergencies of the Ortega y Gasset Foundation and the Rey Juan Carlos University, Master's Programme in Emergencies of the Murcial-Alebat University. He also worked as lecturer for 12 years in the National Civil Protection School of Spain. As a journalist, he spent seven years working for the information services of Onda Cero.

lserrano@llorenteycuenca.com

Natalia Sara is Manager of the Crisis Area of LLORENTE & CUENCA. Natalia holds a degree in Information Science from the University of Navarra, as well as a master's degree in Human Resources Management and Leadership and master's in Marketing, Internet and New Technologies from ESIC Business & Marketing School. She has 25 years of experience in the field of communication, of which the last 15 working as a corporate public affairs and crisis consultant, and initially as a journalist for national leading media, such as Expansión o Actualidad Económica. She is specialized in crisis communication and reputation, and has vast experience in the design of protocols, crisis manuals and strategic performance to prevent potential risks, and to manage adverse situations for brand, persons and organizations. She trains managers and professionals in communication and management of digital reputation, and is a lecturer of the School of Journalism and Communication Unidad Editorial, in Digital Corporate Communication and Online Crisis Management, as well as in Foro Europeo Business School. She is the author of the section on crisis management of the book *Political Consultancy*, published by the Centro Internacional de Gobierno y Marketing Político (CIGMAP) of the Camilo José Cela University (UCJC).

nsara@llorenteycuenca.com

d+i developing ideas
LLORENTE & CUENCA

Developing Ideas by LLORENTE & CUENCA is a hub for ideas, analysis and trends. It is a product of the changing macroeconomic and social environment we live in, in which communication keeps moving forward at a fast pace.

Developing Ideas is a combination of global partnerships and knowledge exchange that identifies, defines and communicates new information paradigms from an independent perspective. **Developing Ideas** is a constant flow of ideas, foreseeing new times for information and management.

Because reality is neither black nor white, **Developing Ideas** exists.

www.developing-ideas.com
www.uno-magazine.com

amo

AMO is the leading global partnership of corporate and financial communications consultancies.

Our best-in-class approach brings together local-market leaders with unrivalled knowledge of stakeholder perceptions, financial markets and cross-border transactions in the key financial centers of Europe, Asia and the Americas.

Providing sophisticated communications counsel for reputation management, M&A and capital market transactions, media relations, investor relations and corporate crises, our partner firms have established relationships with many S&P 500, FTSE 100, SMI, CAC 40, IBEX 35 and DAX 30 companies.

www.amo-global.com