NEW PRODUCT: CYBER RISKS

THE FUTURE IS NOW

Looking back, we would have probably once thought that we were talking about pure science fiction when considering many of the acts that are now part of everyday lives, or our daily routine. Asking the car to call home, unlocking your cell phone by using your fingerprint or saving all files in a digital cloud are some of the hundreds of examples that now seem normal and "not so long ago" we would have thought were part of a Men in Black script.

New technologies are advancing at breakneck speed, and the world with them. They affect everyone, individuals, governments, small businesses and large corporations, and have completely changed the way we relate to each other. From instant messaging applications to submitting official documents electronically to social networks or platforms. Does anyone remember the planes flying over beaches dragging ads behind them?

As a general rule, all technological advances have a principle or common denominator: they are created to make many of the tasks of humans, animals and nature easier, faster and (often) better.

This statement, generally positive, also leads to another thought away from ethical discussions: New scenarios, new risks.

The asset situation of businesses has changed significantly. Intangible goods increasingly have greater weight and relevance compared with tangible goods. This change required a rethinking about the role of traditional insurance, which focused on providing solutions mainly in the transfer of tangible property risks, leaving a significant gap in terms of intangible assets.

The speed with which changes in situations occur has led to the perception of new risks, those which we could call "cyber risks", moving away from the real scope of such risks.

We can now say that in the area of large multinationals, this distance begins to shorten. In the last survey by the World Economic Forum on the major risks to the economy, cyber attacks are among the five biggest concerns.

In articles published recently in specialized circles, a more mature discourse is perceived by the main European Risk Managers. In this respect, there is a need to raise full awareness by the company in which senior management is actively involved. Furthermore, tailored solutions are required from the insurance industry that are adapted to the complexity of the new risks. We cannot and should not now speak of an emerging risk or a problem that is only limited to the IT areas in companies. We are in a phase in which Brokers, as well as insurance companies and Risk Managers, are beginning to coordinate and are required to understand each other.

The growing number of cyber attacks (Spain is the third most affected country in the world after the USA and the UK), which generate annual losses for companies of over 14 billion euros, a significant increase in average cost per incident, which increased from 0.5 million euros in 2012 to 0.8 million euros in 2013, with an average annual cost per company of almost 9 million euros, are making investments in technology one of the priority items on the agenda of companies, although there is still a long way to go with regard to small and medium enterprises.

In this regard, the Cost of Cyber Crime Study, published by the Ponemon Institute in 2014, shows the high return on investment in key security technologies, such as encryption systems (18 percent), security intelligence systems (21 percent) or advanced firewall control perimeters (15 percent).

Most high-intensity incidents derive from the American market (Target, Anthem and Home Depot) and mainly from security breaches affecting large personal databases.

Notably, the U.S. market has been a pioneer in terms of coverage of cyber risks in response to the special features of local regulations governing compensation linked to the protection of this data.

The case of Target, one of the largest supermarket chains in the United States, where cyber criminals stole financial and personal data on 110 million clients by sneaking into company systems through a small cooling service provider, revealed the need to not only have your own security measures, but also the need to control the fact that external providers who have access to sensitive information must take the same measures.

Notwithstanding the foregoing, and apart from the special characteristics of the U.S. market, within the consequences of cyber threats, the impact generated by business disruption in companies is increasingly important.

The vast majority of companies mainly depend on their computer systems to operate. An attack or failure of these can cause real internal chaos with the possible implications of contagion in the markets. In this way, all security measures must not only be targeted at protecting sensitive information, but also protecting and ensuring business continuity.

The variety of actors within the box of cyber threats (cyber spies, cyber criminals, hacktivists, terrorists or even a company's own staff) and the growing sophistication of the tools and methods they use to attack (including phishing, malware and) exploits mean that nobody is safe. Just a few days ago it was released that hackers"assaulted" the databases of the U.S. Government Staff Agency and stole a large amount of personal data on federal employees.

Against this backdrop, and despite being at a stage in which progress is being made from a legislative standpoint to adapt to these new scenarios, the key word to emphasize is "prevention".

As mentioned above, the development of the role

of the insurance industry in preventing these risks represents a new business opportunity in which companies that know how to listen and better adapt to client needs will have a competitive advantage.