CYBERATTACKS ARE AT THE TOP IN THE MOST FEARED BUSINESS RISKS' LIST IN EUROPE AS IN ITALY

SERGIO GUIDA

Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: Technological risks - cyberattacks - NIS Directive

Category: Technical Area

From the Regional Risks for Doing Business Report 2019 issued by the World Economic Forum in collaboration with the international insurance giants Zurich and Marsh, it emerges how cyber risk is the first perceived concern both of European and Italian companies.

"The world in 2019 is more intertwined and more complex than ever. But while the interconnections have brought a certain degree of stability in recent decades, through reliable commercial relationships, actually tightly wound systems are becoming more vulnerable." For this reason, since 2018 the World Economic Forum has developed the annual Regional Risks for Doing Business Report in collaboration with Marsh & McLennan Companies (MMC) and the Zurich Insurance Group, asking 13,000 business leaders in 130 countries worldwide to classify the main fears related to the performance of their activity in the next 10 years.

In the World Economic Forum surveys, respectively on the Executive Opinion and on the Global Risks Perception, five risk categories are drawn: economic, environmental, geopolitical, social and technological. "Technological risks is the only category classified in the five most urgent concerns by both sets of respondents. "Cyberattacks" and "fraud or data theft" are the second and seventh global risks that are likely to increase within the next 10 years in the world private sector vision and have been perceived as the fourth and fifth largest risk by the largest multi-stakeholder network interviewed for the Global Risks Report 2019. The fact that cyber threats worry the business community as much as the academic world, civil society, governments and other thought leaders show how disruptive this risk could be for all aspects of life."

According to the annual cybercrime cost study conducted by the Ponemon Institute in collaboration with Accenture, cybercrimes have cost companies an average of 12% more between 2017 and 2018 and are changing due to:

- Evolving goals: information theft is the most expensive and fastest growing consequence of cybercrime. But data is not the only goal. Basic systems, such as industrial controls, are violated in a dangerous tendency to interrupt and/or destroy.
- Evolving impact: while data remains an objective, theft is not always the result. A new wave of cyberattacks sees data no longer simply being copied but destroyed, or even modified in an attempt to generate distrust. Attacking data integrity is the next frontier.
- Evolving techniques: cyber criminals are adapting their attack methods. They are targeting the human level - the weakest link in cyber defence - through increased ransomware and phishing attacks and social engineering as an access route. It may even happen that some nation-state 'associated' attack groups use this type of technique to attack commercial enterprises. An attempt is made to classify attacks from these sources as "acts of war" by insurance companies as to limit compensation in cases of computer security breaches.

So, according to the WEF, “concerns about "cyberattacks" are at the top among the leaders of the four major economies of the European Union (EU): Germany, France, Italy and the United Kingdom; and in first place in six other countries across the continent. At the end of 2018 and throughout 2019, European countries suffered from cyberattacks and data theft attacks on state agencies and large corporations: Germany saw attacks on parliamentary, military and various embassy email accounts in November 2018 , while in the culminating phase of the European elections in May, various types of harmful activities were found. Similar attacks occurred before the Finnish elections in April and against public institutions in Croatia and the Czech Republic in April and August, respectively. Furthermore, since 2018 the number of IT incidents aimed at the European business sector has increased: 61% of companies reported cyber incidents compared to 45% in the previous year.”

To mitigate these threats, companies and authorities are responding with specifically designated computer training centers. At the regulatory level, in March 2019 the EU adopted the Law Enforcement Emergency Response Protocol, a cybersecurity emergency response protocol designed to combat large-scale attacks and in May 2019 implemented a new sanctioning framework for the purpose to use more effective tools to discourage attackers.

In Italy cyber risk occupies the first place in the ranking, too. Although the European NIS Directive on Cybersecurity has defined the necessary measures to achieve a high level of security of networks and information systems and the national implementing decree applies to Essential Services Operators (OSE) and Digital Service Providers (FSD), a widespread action to assess cyber risk is even more necessary in Countries- like ours- where the economic-corporate system sees a strong

prevalence of small and medium-sized enterprises, that is to say subjects more exposed in terms of both understanding the risk and capacity to face it.

Source: https://www.weforum.org/reports/regional-risks-for-doing-business-2019.

Link: http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2019.pdf