Bufetes –Article. Michael DeMarco

“A cyber attack implies a huge legal risk for companies.”

U.S. attorney Michael DeMarco, a partner at the international law firm K & L Gates LLP, specialist in international disputes and criminal defense in the financial field, currently ranked among the best lawyers in the United States.

In this interview Michael DeMarco addresses diverse topics including anti-corruption laws, cyber security for businesses; and also highlights the work done by himself and his partners aimed at protecting their clients in such matters. K & L Gates LLP is a law firm composed of 2000 lawyers with 47 offices fully integrated and located in five continents, representing world leading companies, growing businesses and middle market companies, entities involved in capital markets, industrial groups, public sector entities, educational institutions, philanthropic organizations and individuals. The firm provides its clients full services worldwide.

From a legal perspective, what are the critical issues that should be of concern to international business today?

In my opinion, business globalization has created new risks for businesses, risks that did not exist for previous generations of executives. Among them, the ones that stand out are cyber attacks, such as those suffered by US and Japanese companies, specifically Target and Sony, and also risks dealing with the impact of anti-corruption laws in countries and cultures where this practice has now become present.

Undoubtedly, the attacks against Target and Sony have served to remind many businesses executives that today's world is not the same as twenty years ago. What should employers today do to protect customers and businesses from these new risks?

Companies and Officers themselves can perform a series of actions in order to mitigate these risks. Today it is critical for an international company to have advanced technological equipment and qualified experts for the prevention and resolution of problems. However, the preparation may not be enough, as often happens with a cyber attack. A cyber attack involves enormous legal risks for companies ranging from unauthorized dissemination of confidential customer information to outright theft of money or intellectual property. One strategy I advise and which is being used by different companies, is hiring an insurance policy to cover these risks. As you can imagine, the insurance companies don’t always want to pay what they owe under the terms of these policies. Long ago, our firm decided to represent our corporate clients in the negotiation of these insurance policies and possible disputes with insurance companies. We analyze and negotiate insurance policies for our corporate clients and advise our clients during the term of the policy how to secure the defense of their rights under the respective policy. In some cases, this defense has brought lawsuits against the insurance companies, but our duty is

to do everything possible to protect our client. In fact, we are world leaders in this specialized legal area called "Insurance Coverage."

What other action can companies perform to address such problems?

My advice is that each company should add to its Management Board a member with knowledge in "transfer of technology management" and security. In addition, companies should create a professional figure in charge of the enforcement of existing legislation on computer security, which would be responsible for taking the necessary methods to prevent cyber attacks.

Here in Spain we have many companies operating in regions such as Latin America and Africa. Some countries in these regions of the world have complicated histories with issues of bribery, corruption and money laundering. As you just explained the subject of cyber attacks, what can international companies do to limit the business risks incurred with respect to issues of bribery, corruption and money laundering?

These are hard and real in today's world issues and present risks for companies. For example, there are several international laws criminalizing acts of corruption abroad, such as the Foreign Corrupt Practices Act of the United States of America ("FCPA"), the Bribery Act 2010 of the United Kingdom, or Article 445 of the Penal Code in Spain, introduced in 2004. In general, these laws do not pardon ignorance. That is, its the legal responsibility of each company to understand the laws and comply with them. In the last twenty years or so, no case under the FCPA arose in the US, but recently the US government has shown its maximum rigor regarding corruption and bribery. An interesting aspect of that US regulation (FCPA) is that it has application worldwide; ie, the US government can punish a company that violates the FCPA anywhere in the world. Penalties for breach of the FCPA, as well as other laws cited can be catastrophic for some companies, including financial penalties of up to millions of US dollars. Consequently, international companies operating in some regions of the world where these practices are common need to invest in specialized legal advice to establish internal security practices globally to comply with these laws. In addition, investing time is required on behalf of the executives and internal legal counsel, as well as the financial investment required to perform such practices.

In cases of corruption it is often necessary to initiate an internal investigation to determine the legal risk of the company and report the incident to the competent authority. I and other partners in Europe and the USA are specialists in directing these internal investigations and advising client companies on how to limit this legal risk and prevent such incidents from recurring in the future.

Do issues such as terrorism and drug trafficking affect international companies and the mitigation of their legal risk?

Absolutely yes. No legitimate company intends to hire terrorists or transact with drug traffickers, however it needs to know and understand the international laws that apply in every situation. For example, the US Treasury Department has a division called Office of Foreign Assets Control or "OFAC" for its acronym in English. OFAC is an organization of financial intelligence and enforcement of the US government which is responsible for planning and executing economic and commercial sanctions as support for the objectives of national security and foreign policy. OFAC focuses its attention primarily on problematic states, organizations and individuals. It publishes a list of these entities and individuals, and as you can imagine, the list includes names of individuals, companies or groups that, at some point, have supported terrorism or drug trafficking. That is, if a company is not negotiating directly with a terrorist or drug dealer, it may still incur a legal risk by doing business with a third party who has had direct contact. One of the things we do to protect American companies in international transactions is to check the list of OFAC before authorizing a transaction. The world is already very small and business globalization is unstoppable, but we have to reconcile this reality with the need to comply with international laws and standards governing the conduct of companies around the world