CYBER RISK & BUSINESS VALUATION

Valuation professionals and lawyers practicing in the area of New York, USA, are now strongly concerned about cyber risk and data breach issues. The importance of these issues arises in various cases involving business valuation such as in due diligence projects and also in cases presented in a court of law. Cyber security has become indeed a very hot thing after the numerous corporate data breaches and cyber attacks that have occurred in the past. These concerns have also triggered actions on behalf of regulatory authorities. In Europe for example, there is the General Data Protection Regulation established in order to strengthen and unify data protection within the European Union.

One can easily observe that over the past couple of years, several and well publicized data breaches took place worldwide. Look for example at the cases of Equifax, Deloitte, Yahoo (two massive data breaches in 2016) and Tesco Bank. In such a high-risk environment, it is even more critical for corporations and companies alike to protect their internal IT infrastructure and databases which are greatly exposed due to the operation of various networks, and the use of the Internet as well as other IT platforms. This "new" high-risk environment comes of course with no surprise as we live in a world of increased use of "big data" by everybody (corporations, companies and individuals), from everywhere and every time.

Certainly no company enjoys to be hacked. However reality can be even more complex: According to sources claiming very good knowledge of the cyber security industry, most of the US companies have been hacked in some way, but they don't know it yet. Moreover, former Cisco CEO John T. Chambers has reiterated the above view noting that "There are two types of companies: those who have been hacked and those who don't yet know they have been hacked".

According to valuation practitioners in the US market, cyber risk consideration is more than ever important in business valuation of both large corporations and smaller companies. Cyber risk is affecting the subject company's specific risk and particularly the risk associated with its business. For example if it is to value a cloud computing business, then cyber risk should be a source of major assessment. The same would stand in the valuation of an on-line store or a fin-tech company. In the case of smaller companies the risk may imply even larger potential damage given that smaller companies might not possess adequate resources to tackle cyber attacks or to handle such incidents one they have occurred. Therefore every company, no matter how big or small it is, has to follow the rules and abide by regulations in order to protect itself from data breach accidents. In any case, a huge liability or damage might emerge and the risk of it has to be identified, quantified and included in the valuation exercise.

In this context, when applying the present value approach, practitioners are required to consider the risk of cyber attack and data breach, measure it and add it to the discount rate they use in order to bring the future cash flows into present values. Though, what is the precise percentage one must add to the discount rate? Is it around 1%-2% or more? Nobody really knows or can tell for sure. On the other hand if you have to present a valuation report in a court of law or to utilize a valuation outcome along a due diligence project, you have to come up with a justified assessment of that risk and be able to defend it.

It is not secret that cyber risk management is now becoming among the top priorities of large corporations globally caring for sustainable and highly protected business and IT operations. In this context, every entity has to carefully measure the value of the assets which must be safeguarded and justify any expenditure required to apply this safeguard policy. Furthermore in order to estimate the potential damage due to cyber attacks a company must also value the assets that are subject to such an attack.

As a conclusion, given that corporations and companies understand now, and better than in the past, the need for effective cyber risk management, valuation practitioners and lawyers dealing with cases involving business valuation will sooner or later face the challenge of adjusting the subject company's specific risk to reflect this new environment that lies ahead.

VRS (Valuation & Research Specialists)