by Adv. Sigal Schlimoff Senior partner at Gross Orad Schlimoff & Co. and Lloyd's representative in Israel and Adv. Maya Salomon, partner at Gross Orad Schlimoff &Co.

CYBER INSURANCE IN ISRAEL - PAST, PRESENT & FUTURE

Although Israel is considered a "Start Up Nation", with a highly developed technological scene, the penetration rate of cyber insurance in the Israeli market has been very low in recent years and until this day. The increased awareness of cyber risks, combined with recent legal developments, may change this trend.

In recent years, data security has been reported as the most significant risk facing modern corporations.

Cyber threats, information security and privacy remain critical issues for organizations to address. This is common to all territories. Yet, penetration rates of cyber insurance in many countries varies dramatically.

The penetration rate of cyber insurance in the United States is by far the highest in the world, mainly due to mandatory legislation regulating cyber security and notification duties to individuals who may be affected by a data breach in case of a cyber security event.

U.S. legislation imposes specific duties to notify such individuals and dictates very restricted time frames for such notifications, as well as the form and method of notifications.

The notification costs may be very significant, and this factor, together with other first party and third party losses associated with cyber-attacks, is the main growth engine in US cyber insurance market.

In Europe, cyber related legislation has been, until recently, very limited. However, the European Council has passed regulations regarding data protection and security, which will be brought into effect in May 2018.

The new Network and Information Security (NIS) Directive and General Data Protection Regulation (GDPR), will require all organizations that are in, or do business with, countries in the European Union, to incorporate 'state of the art' practices into their cyber security.

The new legislation requires companies to consider and ensure that their cyber security processes are adequate and robust. This includes clear notification procedures and incident response plans.

These regulations are expected to increase the purchase of cyber insurance policies by EU companies and by companies doing business with EU domiciled companies.

The Situation in Israel

The penetration rate of cyber policies in general and in particular to SMEs is very low and estimated to be in the region of about 1%. In the last year, there has been a sense of gradual awareness and interest about this important insurance, but it is far from being part of the basic basket, which management of any company, association, or business entity, deems essential.

The low penetration is in opposite correlation to the risk of cyber-attacks, especially in Israel and the potential damage involved in such attacks.

The main reason for this is without doubt the absence of specific legal duties imposed by the regulator.

In Israel, legal cyber related regulation has not kept pace with the rapid technological developments and associated risks involved.

In principle, with certain exclusions detailed below, there are no specific regulations obliging an Israeli entity to report about a cyber event to the regulator or to parties who may be affected, including clients, whose personal information may have been leaked as a result of a cyber attack or other cyber risk.

The Israeli Law, Information and Technology Authority (ILITA), was established by the Ministry of Justice of Israel in September 2006, with the purpose of becoming the national data protection authority, which regulates personal data protection issues and increases the enforcement of privacy and IT-related offences.

However, since 2006, practically no specific cyber regulations have been enacted by the Israeli legislator.

In August 2016, the Commissioner of the Capital Markets and Insurance and Savings (the Commissioner) issued a circular directed solely to financial institutions, regarding the main principles of proper cyber risk management and the duties of such financial institutions to manage such risks. The circular deals with corporate governance principles which any financial institution must adopt in respect of cyber risk management. It specifically refers to the duties of the board of directors and of the CEO, which include the duty to appoint a special steering committee to manage cyber risks, to allocate sufficient financial resources for handling cyber risks, the duty to establish reporting procedures within the organization regarding cyber threats and the duty to discuss and approve a cyber risk policy by the board of directors on an annual basis.

The most interesting duty which this circular includes is, for the first time, a reporting duty imposed upon the financial institution to the Commissioner, as well as to the board of directors, regarding any significant cyber attack resulting in disrupted IT systems for over three hours, as well as, in case an indication exists that data relating to clients, members or employees was leaked.

In March 2017, the Legislation Committee of the Israeli parliament approved new Regulations for the Protection of Privacy (Information Security) – 2017.

The Regulations establish, for the first time in Israel, a specific updated and comprehensive arrangement regarding protection of databases. They present new duties regarding the management of databases, including the establishment of written information security procedures (similar to WISP in the U.S.).

One of the most significant duties, according to the draft Regulations, refers to the duty to report any "severe data breach" to the Database Registrar and to parties whose personal data was compromised.

The Regulations will enter into force in March 2018, and will become the first step to be initiated by ILITA to impose specific cyber related duties on Israeli entities, and specifically notification duties. Israeli entities are expected to adopt inter organizational procedures and risk management enhancement steps in implementing the Regulations.

These specific new duties presented by the latest legislation may encourage a significant change in the manner in which Israeli companies handle cyber risks in the future.

There can be no doubt that the management of any corporation will be required to discuss the major cyber risks faced by the organization in the near future, and implement procedures to manage such risks.

The existence of an insurance policy that has been adapted to the Israeli market's needs and legislation is definitely something that should be considered as one of the main means to manage cyber risks in a corporation.

The failure to seriously examine whether the corporation should acquire a cyber policy may be a source of imposition of personal liability on a corporation's directors and officers, or anyone who advises those corporations on risk management issues, including its insurance consultant, insurance agent and broker.

It is now the duty of all stakeholders in the insurance industry to make an effort to explain to the management of any company, association or business entity, whether large, medium or small, the importance of purchasing a cyber policy, the potential resulting damage and the personal liability which may be imposed on any manager or officer who fails to seriously discuss the need to purchase cyber insurance or any reasonable alternative that contains this growing risk.

For further information, you are welcome to contact the cyber team at Gross Orad Schlimoff & Co.: Adv. Sigal Schlimoff, Adv. Maya Salomon and Adv. Laurie Shachar