Gross Orad Schlimoff & Co.
Incorporated Law Firm

7 Menachem Begin Rd.
Ramat-Gan 5268102, Israel
Tel: 972-3-6122233
Fax: 972-3-6123322
Web Site: www.goslaw.co.il

LEGAL REVIEW JUNE 2022

Cyber Insurance
Update Regarding Developments in Israel

New Circular: Reporting of Cyber and Technological Failure Incidents by Institutional Organizations

On 23rd May 2022, the Capital Market, Insurance and Savings Authority **(the Authority)** published the "Circular for Institutional Organizations 2022-9-15: Reporting of Cyber and Technological Failure Incidents" **(the Circular)**, which constitutes another step in promoting expected cyber risk management standards for Israeli institutional organizations (namely – insurers and management companies of provident funds, pension funds, study funds etc.).

The Circular is supplementary to the "Circular for Institutional Organizations 2016-09-14: "Cyber Risk Management in Institutional Organizations", which stated that an institutional organization shall report to its board of directors and the Authority, as soon as possible, regarding any significant cyber incident, as a result of which (directly or indirectly): (i) Production systems containing sensitive information have been damaged or shut down for more than three hours; (ii) There are indications according to which sensitive information of an institutional organization's clients or employees has been exposed or leaked.

Pursuant to the new Circular's Explanatory Notes, the increase in the scope and complexity of cyber incidents on various organizations in Israel, including institutional organizations, necessitates certain clarifications in respect of the reporting requirements which apply to institutional organizations.

The Circular includes instructions in respect of the following issues: (i) a requirement to report an incident; (ii) the manner in which a report should be made; (iii) a requirement to update the Authority regarding developments during an incident; (iv) a requirement to report to the Authority regarding the incident's outcome.

In essence, an institutional organization is required to report to the Authority regarding any "material incident". The Circular states that an incident shall be defined as "material" based on an institutional organization's internal procedures. Having said that, the Authority provides certain criteria when an incident shall be considered "material" and thus a report shall be mandatory. These include an incident which caused a material disturbance in the organization's activity and which lasted over 3 hours, an incident which the organization considers to be of material impact on the rights of its members/ insureds and the existence of indications that sensitive data of insureds, members or employees had been exposed, leaked, corrupted or deleted.

According to the Circular, preliminary reporting shall be made via telephone and email to the Authority, as soon as possible following the time on which an institutional organization identified that a material incident occurred, however no later than **two hours from the time of discovery.**

An institutional organization shall also issue a supplementary report to the Authority, through a designated form, no later than 12 hours after the preliminary report was made. In addition, an institutional organization is required to submit written updates to the Authority, at least once a day (through the aforementioned form), regarding developments in respect of a reported incident.

The Authority instructs that an institutional organization shall make a report regarding the outcome of the incident - according to the Circular, an institutional organization shall carry out the following reports by phone: (i) a preliminary report up to 2 hours after the incident was concluded; (ii) a supplementary report (on the designated form) up to 6 hours after the incident was concluded. A conclusion regarding the incident's termination shall be made by an institutional organization in accordance with its internal procedures and based on estimations, according to which there is no concern regarding any escalation or reoccurrence of the incident.

GOS Cyber Department handles cyber claims for insurers and reinsurers in the framework of Cyber Policies issued to various organizations. From our experience, institutional organizations are considered as targets of threat actors, as they have substantial economic impact in the Israeli economy. In many cases, cyber claims concern issues related to mandatory reporting to relevant authorities. The Circular and other regulatory guidelines contribute to better understanding the reporting duties which appear to become more extensive, similarly to global trends.

Contact persons:
Sigal Schlimoff Rechtman, Adv. – Sigal@goslaw.co.il
Omer Shalev, Adv. – Omer@goslaw.co.il
Maya Salomon, Adv. – maya@goslaw.co.il

Gross Orad Schlimoff & Co.
7 Menachem Begin Rd.
Ramat-Gan 5268102, Israel
Tel: 972-3-6122233
Fax: 972-3-6123322
Web Site: www.goslaw.co.il