March 2019

GORNITZKY
80 Years of Excellence

Israel Securities Authority Publishes Findings from Cyber-Security Survey Among Portfolio Managers

The Israeli Securities Authority ("ISA") published a memo summarizing its findings and recommendations from a recent cyber-security survey it had conducted among portfolio managers (the "Memo").

The Memo emphasizes the need to treat cyber-security not only as a technological issue, but also as a strategic business issue that requires establishing effective controls and combining organization-wide human, technological and policy efforts.

The ISA further noted the Privacy Protection Regulations (Data Security), 2017 (the "Regulations"), that apply to any entity in Israel that owns or processes a database containing personal data. The ISA stressed that it may consider companies that failed to comply with the Regulations as incompliant with the special requirements applicable to entities regulated under the Regulation of Investment Advice, Investment Marketing and Investment Portfolio Management Law, 1995.

The ISA's recommendations address, among others, the following issues:

1. **Risk Management** – prioritize treatment of cyber-security risks and adopt a business continuity plan to address such risks;
2. **Protocols and Documentation** – keep a comprehensive and up-to-date inventory of data systems, data infrastructure and other data assets of the business; ensure that the company's internal information security procedure is compliant with the requirements of the Regulations;
3. **Risks Emanating from the Human Factor** – increase employee awareness to cyber-security risks, including by providing timely updates on new risks; restrict the use of computers and other company tech equipment solely to business matters;

4. **Technological Tools** – install software updates on a regular basis; implement website and content filtering applications and measures for preventing unauthorized access to the company's internal network (e.g., firewall, IPS); secure remote access to the company's internal network, among others, by using strong authentication mechanisms, encrypted communication channels and by enforcing preconditions on the remote computer (e.g., require that the remote computer have an up-to-date anti-virus);
5. **Physical Access Control** – restrict physical access of unauthorized personnel to the company's facilities, systems and internal network;
6. **Transferring Data Out of the Company** – restrict the use of portable devices; restrict the use of email for transferring sensitive data; secure channels for accessing customer data (e.g., encryption or use of a secure website);
7. **User Accounts** – avoid using one user account for multiple users; restrict user access permissions to what is necessary for the relevant user's tasks; automatically lock inactive user accounts; enforce strong access password requirements; log user activity in the company's systems;
8. **Supply Chain** – take appropriate measures for reducing supply chain cyber-security risks; supervise cyber-security measures implemented by third-party cloud vendors;
9. **Recommendations for Large Portfolio Management Companies** – such companies should conduct timely board discussions on cyber-security, appoint a cyber-security officer, implement effective screening measures when recruiting personnel; and conduct cyber-security risk surveys and audits.

The Memo provides another example of how Israeli regulators view the responsibility of regulated entities with respect to cyber-security. The Memo notes the ISA's intention to continue promoting awareness of portfolio managers to cyber-security risks (and the handling of such risks) including, among others, by addressing cyber-security issues in audits conducted by ISA staff.

Although the Memo is addressed to portfolio managers, its recommendations are essentially relevant to any company that processes personal data in Israel.

To read the Memo (Hebrew) click here.

For further information please contact:

Sharon Werker-Sagy, Partner
sagy@gornitzky.com

Yair Shiloni, Partner
shiloni@gornitzky.com

Assaf Harel, Partner
assafh@gornitzky.com

This client update was prepared with the assistance of Ms. Yael Heiman.