Report of the State Comptroller of Israel – Cyber and Information Systems | November 2024

Government Defense Industries

Cyber Security: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.

Cyber Security: Aspects of Regulation and Protection of the Information and Computer Systems at Rafael Advanced Defense Systems Ltd.

Background

According to the government's resolution in August 2011[1], the Israeli civil cyberspace encompasses all state and private entities within the State of Israel, excluding special entities[2]. Consequently, the Israeli cyberspace integrates civil, governmental, and Military Cyberspace domains. The increasing activity within the Cyberspace domains facilitates technological innovation and advancements beneficial to individuals and their environments. However, a significant challenge has emerged alongside the advantages of computerized systems in cyberspace: the cyber threat. A cyber incident is defined as an occurrence suggesting potential harm to the regular operation of a computer system. Rafael Advanced Defense Systems Ltd. (Rafael) enhances the nation's military strength and resilience. The company is subordinated, among others, to the provisions of the Government Companies Law, 1975, and the Regulation of Security in Public Bodies Law, 1998. The Director of Security of the Defense System (MALMAB) supervises enterprises within the defense system[3] and those manufacturing products for this sector. The Government Companies Authority disseminates circulars to government companies and subsidiaries on various matters under its authority under the Government Companies Law, 1975, encompassing corporate risk management.

In 2022, the National Cyber Directorate (NCD) received reports of 9,108 cyber incidents from all entities nationwide, with about 31% of these incidents attributed to phishing attacks[4].

[1] Government Resolution 3611 (august 7th, 2011).

[2] Government Resolution 3611 (august 7th, 2011) defined special entities as follows: the IDF, the Israel Police, the Israel Security Agency (ISA), the Mossad Institute for Intelligence and Special Operations (Mossad), and the defense establishment through the Director of Security of the Defense Establishment (MALMAB). Additionally, the defense establishment was defined as follows: the bodies directed by MALMAB by virtue of the Regulation of Security in Public Bodies Law, 1998, as well as suppliers and enterprises developing or manufacturing defense equipment for them.

[3] The Defense Establishment – the IDF and the Ministry of Defense (MOD), including its auxiliary units.

[4] Phishing – A cyber-attack in which the attacker poses as a trustworthy entity in order to deceive people and make them reveal sensitive information.

Key Figures

10%

in 2022: the budget for the Technology Security and Cyber Defense Department at Rafael out of the computing budget of the Information Technology and Processes administration at Rafael

12 years

the NCD and the Director of Security of the Defense System did not implement the government's resolution on promoting national capability in cyberspace regarding the establishment of special arrangements for promoting cyberspace defense

31%

the phishing cyber rate incidents reported to the NCD in 2022 out of all cyber incidents

Audit Actions

From November 2022 to July 2023, the State Comptroller's Office audited the cyber Security regulating and protecting information systems at Rafael. The audit focused on the following issues: the regulation of the working relations between the National Cyber Directorate and the Director of Security of the Defense System; The directive and supervisory powers of the Director of Security of the Defense System; The concept of cyber defense at the Director of Security of the Defense System; Rafael's information security policy; Corporate risk management at Rafael; Rafael's cyber defense work plans and budget; The protection of specific computer networks and information systems at Rafael and the information security controls implemented therein; And the safeguarding of specific infrastructures at Rafael. The audit was conducted at the Director of Security of the Defense System and Rafael. Completion examinations were performed at Israel Aerospace Industries Ltd. (IAI), Israel Electric Company Ltd., and the National Cyber Directorate (NCD).

The Knesset State Audit Committee sub-committee decided not to submit data from this chapter before the Knesset to protect the state's security and its international trade relations under Section 17 of the State Comptroller’s Law, 1958 [Consolidated Version].

Key Findings

- **Regulating the Working Relations Between the National Cyber Directorate and the Director of Security of the Defense System –** even though 12 years have passed since the government's resolution in August 2011 enhancing national capacity in cyberspace, the NCD and the Director of Security of the Defense System have not implemented specific arrangements regarding the protection of cyberspace and the promotion of research and development, as mandated by the government resolution.

- **The Director of Security of the Defense System's Directive and Supervisory Powers –** the Regulation of Security in Public Bodies Law from 1998 did not confer apparent authority to the Director of Security of the Defense System (MALMAB) concerning operational, technological activities, nor did it empower MALMAB to offer professional guidance on specific networks.

- **The Concept of Cyber Defense Within the MALMAB –** the cyber defense doctrine as outlined by the Theory and System Defense Division in the MALMAB's technology does not incorporate a standard for an organization's monitoring center, even though such a center is a critical component of organizational defense. Furthermore, the Theory and Defense Division has not issued directives for the guided entities concerning preparedness required for managing cyber incidents or for incident management itself, which should encompass monitoring processes, incident identification, response strategies, recovery efforts, investigations, lessons learned, cyber incident simulations, internal participation in managing a cyber incident and the interfaces between them, and necessary activities of the guided entity vis-à-vis external factors.

- **Corporate Risk Management at Rafael –** in May 2023, during the audit, the corporate risk management committee approved a risk strategy document and risk management policy, about three and a half years after the Government Companies Authority's circular on corporate risk management was published in January 2020. However, these documents were not approved by Rafael's board of directors. As of July 2023, the risk management policy lacked provisions for reporting mechanisms to external parties. Additionally, Rafael has not reported as required to the Government Companies Authority, contravening the circular's corporate risk management stipulations.

- **Physical Protection for Certain Infrastructures –** gaps have emerged in this field.

- **Cyber Incidents Insurance –** as of July 2023, during the audit, Israel Electric Company Ltd. held two insurance policies for property damage and third-party claims related to cyber incidents. Israel Aerospace Industries Ltd. (IAI) and Rafael[5] lacked such

[5] Except for Rafael's IT equipment and computer systems that are insured against a cyber incident originating from an error or omission.

policies. Rafael did not purchase insurance against cyber incidents mainly for the following reasons: Rafael's level of cyber protection is high, purchasing insurance is economically inefficient, it is unlikely that compensation will be granted by the insurance company for damage to production or sales turnover, classified information cannot be disclosed to the insurance company following damage due to a cyber incident, complicating the claims process, and insurance coverage is limited to a maximum of ten million dollars, an amount that is not material to Rafael's operations.

- **Reporting Gaps at Rafael –** Rafael failed to disclose several cyber incidents to its board of directors during meetings as required.
- **Investigating Cyber Incidents –** Rafael's management failed to investigate cyber incidents that occurred between 2020 and 2022 concerning certain aspects critical to Rafael's operational integrity.
- **Comprehensive Plan for the Management of Information Security Incidents –** the Detailed, Information, and Process Administration Order from February 2023 does not delineate the recovery process for specific cyber incidents, nor does it reference a defined plan or include pertinent documentation.
- **Deriving Lessons from Certain Cyber Incidents –** several incident investigation documents did not sufficiently address the lessons derived therefrom.
- **Surveys and Penetration Tests –** Rafael has not set the frequency for conducting mandated surveys and penetration tests, resulting in inconsistencies in this area.

Key Recommendations

- The NCD and the Director of Security of the Defense System should adhere to the government's resolutions concerning the regulation of their cooperation through the established mechanisms.
- The MALMAB should regulate the powers required to fulfill its mission effectively.
- It is recommended that the technological unit of the MALMAB finalize the cyber defense doctrine, including the standards for the monitoring center and the necessary guidelines for managing cyber incidents and occurrences, conducting investigations, and deriving lessons learned.
- Rafael's management should provide the board of directors with required updates related to cyber incidents.

- Rafael's management Should annually assess the budget needed for cyber defense concerning potential damage, annual sales turnover, and annual operating profit.
- Rafael's management should investigate cyber incident management as mandated. Rafael should complete the guidelines for technology security incident management and cyber protection in computer systems.
- Rafael is recommended to address the deficiencies identified in surveys and penetration tests.
- Rafael should rectify the deficiencies highlighted in this report.

Summary

Rafael is a significant component in enhancing the country's military strength and resilience. The audit raised deficiencies related to, among other issues, the lack of regulation in the working relations between the National Cyber Directorate (NCD) and the Director of Security of the Defense System (MALMAB) and safeguarding information and computer systems at Rafael. Rafael's management and board of directors should address these deficiencies and ensure, in collaboration with the MALMAB, that Rafael adheres to the directives of the MALMAB as required.