State Comptroller's Report – Cyber and Information Systems | May 2023

The National Insurance Institute

Regulation of Cyber Security at the National Insurance Institute

Regulation of Cyber Security at the National Insurance Institute

Background

In 2021, more than 22 billion records were leaked worldwide due to cyber-attacks[1]. People's names and social security numbers (including SSN[2]) are the two data types that were leaked more than any other data. As of November 2022, about 2.9 million cyber-attacks are carried out daily against the National Insurance Institute (NII), of which about 66,000 attacks have the potential for damage.

The NII provides various services to residents of the State of Israel from birth to death. Therefore, the NII's databases are susceptible, both due to their enormous volume and because the databases interface with parties outside of the NII. Hereby are the normative regulations of cyber and information security: The Protection of Privacy Law, 1981, which defines the duties of the Database Owner, the Database Possessor or Database Manager as defined in the law, to secure the information therein; The Protection of Privacy (Data Security) Regulations 2017; And the Regulation of Security in Public Bodies Law, 1998 (the Regulation of Security Law), which establishes powers and responsibilities for physical security, information security and the security of vital computer systems of various public bodies, both of government entities and privately owned entities.

1 2021 Year End Report – Data Breach Quick View, Risk Based Security & Flashpoint (p. 3)

2 Social Security Number (it should be noted that in several countries such as the USA, the SSN number is equal to an ID number in Israel).

Key Figures

22 billion records
were leaked worldwide in 2021 due to cyber attacks

about 2.9 million
the daily average of cyber-attacks on the NII

hundreds of terabytes (TB)
the size of the NII's database, which includes the personal data of about 9.5 million insured in Israel

20 employees
at the NII (of which 6 are students) supervise the information security in its computerized systems. Compare to the IDF, which is also self-supervised, has a Computer and IT Directorate (network environment) under the command of an officer with the rank of colonel

Audit Actions

From October to December 2022, the State Comptroller's Office examined cyber protection regulations in the NII. The examination included mapping the bodies that currently regulate the NII, the possible damage from the lack of a fixed regulatory body, and the need to change the regulatory bodies. The audit was conducted in the NII, the National Cyber Directorate, the Israel Security Agency, and the Privacy Protection Authority in the Ministry of Justice.

The Knesset State Audit Committee sub-committee decided not to bring this report in its entirety before the Knesset but to publish only parts thereof to protect the state's security under Section 17 of the State Comptroller's Law, 1958 [Consolidated Version].

Key Findings

The Regulation of the Privacy Protection Authority vis-à-vis the National Insurance Institute – the audit raised that since the establishment of the Privacy Protection Authority in 2006 and until the audit completion (more than 16 years), the

Privacy Protection Authority has carried out six administrative procedures regarding information security in the NII. As for transversal supervision, only in August 2022 did the Privacy Protection Authority begin to conduct it in the NII.

- **The Regulation of the Israel Security Agency and the Interface of the National Cyber Directorate vis-à-vis the National Insurance Institute –** the Second Schedule to the Regulation of Security Law lists the bodies required to receive guidance regarding issues classified as top secret. These bodies carry out self-supervision and have dedicated units to protect cyberspace. The Fifth Schedule to the Regulation of Security Law lists entities with critical cyber infrastructure (CCI). These entities are guided by the National Cyber Directorate (NCD). It was raised that the NII is indeed listed in the Second Schedule but is not defined in the Fifth Schedule to the Regulation of Security Law, even though it is a body that maintains a database of information on the residents of the State of Israel. Therefore, the NII receives directives from the Israel Security Agency regarding classified issues only but is not required to receive regular instructions from the NCD.

- **The "Voluntary Instruction" Process of the National Cyber Directorate –** as of 2016, the NCD began instructing the NII under "voluntary instruction." I.e., the NCD instructs the NII similarly to the CCI bodies, but the NII has no obligation to implement these instructions. From the audit team's conversations with the NII, it became clear that the NCD's level of involvement over the years has decreased: from 2016 to 2020, the "voluntary instruction" was tight and included ongoing consultation daily. From the end of 2020, three supervisors have come and gone, and instruction has been sparse and sporadic. At the audit completion, there is no supervisor on behalf of the NCD, and contact is carried out through the NCD call center (CERT), which handles all cyber incidents in Israel. Therefore, the NII does not have a regular and systematic response for handling all information security incidents.

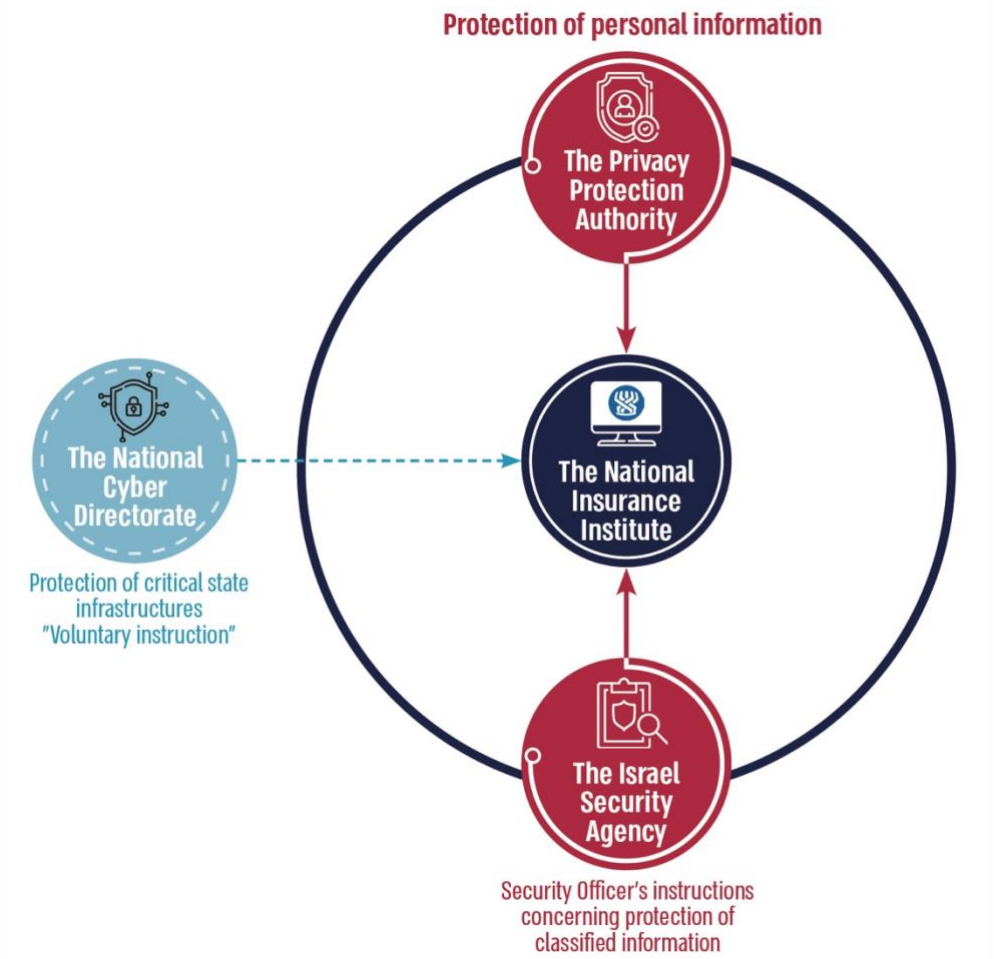
- **The Attempt to Define the NII as a Critical Cyber Infrastructure (CCI) –** Government Resolution B/84 from 2002 established a top steering committee[3] to examine which bodies are critical and, therefore, need cyber protection. It was found that as of the audit completion – about two years after a hearing in the Steering Committee for the Protection of Critical Computerized Systems resulted in a decision to examine the NII as a CCI body, the NCD did not begin the examination procedure. An inquiry by the audit team at the NCD raised that the NCD intends to start examining the NII as a CCI body in the first quarter of 2023. I.e., at the audit completion, the NII, which manages a database, does not receive ongoing and binding professional instruction, which raises a concern for risk.

3 The Chairman of the Steering Committee is the head of the NCD and its members include representatives from the Ministry of Defense, the Ministry of Justice – the Head of the Privacy Protection Authority, the National Security Council, the IDF and the Israel Security Agency.

Key Recommendations

- It is recommended that the Steering Committee for the Protection of Critical Computerized Systems promote the examination of the NII as a CCI body, given the extent of the information stored therein and the risks of its leakage.
- It is recommended that until the end of the Steering Committee examination, for the Protection of Critical Computerized Systems, a professional interface will be established between the NCD and the NII to provide a direct response, forwarding reports, monitoring the correction of deficiencies, etc.
- It is recommended that the Steering Committee for the Protection of Critical Computerized Systems examine whether there are other entities with databases of a similar scope to the NII whose definition as CCI bodies should be considered, thus improving the protection of the State of Israel's critical infrastructures.

Regulatory Bodies in the NII Information Security



Summary

Like other countries, Israel is exposed to cyber-attacks for ransom and information theft. Apart from that, given the complex security geopolitical climate, Israel is an extensive target for a potential cyber attacker wishing to harm its resilience and national security. A body such as the NII requires a satisfactory regulatory response formulated, including guidance from the National Cyber Directorate and the Privacy Protection Authority and coordination between the two to ensure optimal protection. Given the volume of information kept at the NII and the risks of its leakage, it is recommended that the Steering Committee promote the examination of the NII as a CCI body. It is recommended that until the end of the examination, a professional interface between the NCD and the NII will be arranged to provide a direct response, forward reports, monitor the correction of deficiencies, etc. It is also recommended that the Steering Committee examine whether there are other entities with databases of a similar scope to the NII whose definition as CCI bodies should be discussed, thus improving the protection of the State of Israel's critical infrastructures.