Bank of Israel
Banking Supervision Department
Bank-Customer Division
Policy and Regulation Unit

March 16, 2015

Circular 2457-06-H

To the banking corporations and credit card companies

Re: Cyber Defense Management

(Proper Conduct of Banking Business Directive No. 361)

1. Cyber threats, to which financial institutions in Israel and worldwide are exposed, have increased recently. These threats are characterized *inter alia* by the growing sophistication of cyber attacks, by the growing extent of the potential damage, by the increasing difficulty of identifying such attacks, and by the advanced capabilities of the adversaries involved. Since Israel—and especially the financial sector—is a preferred target of attack by various adversaries, the banking corporations in Israel are even more exposed to cyber threats. In recognition of the centrality of cyber threats in the threat landscape facing the banking corporation, the need has arisen to issue a specific directive regarding cyber defense management.

2. Issuing a dedicated directive regarding cyber defense management is intended to emphasize the Banking Supervision Department's view, that cyber risk treatment is a corporate-wide concern, which requires the active involvement of the senior officials at the banking corporation. Despite the fact that cyber risk is derived from the use of technology, it is rather a strategic-business issue and not merely a technological matter.

3. The directive contains regulatory provisions of the Banking Supervision Department's requirements and expectations regarding the management of cyber defense. The directive prescribes a structured but flexible framework for cyber risk management, while allowing the banking corporation to exercise discretion in its implementation. This form of regulatory approach is intended to enable the banking corporation to adapt its defense system in a dynamic manner to the changing cyber threat landscape.

4. Therefore the directive defines principles for cyber defense, rather than specifying a strict "list of controls". The expectation is that the banking corporation shall adopt these principles while establishing a cyber-defense array in accordance with the scope and the nature of its business activity, and its risk profile. Appendices to the directive will be published, as necessary, and will include detailed guidelines in relevant subjects, such as the matter of a sectorial cyber defense center, when established. In addition, it is recommended that reference be made to acceptable standards in the area of cyber defense.

5. Following the publication of this directive, the Banking Supervision Department intends to publish a dedicated directive regarding information security. In this respect, the appropriate adjustments between the directives will be made as necessary.

6. After consulting with the Advisory Committee on Matters Concerning Banking Activity and with the approval of the Governor, I have prescribed the following Proper Conduct of Banking Business Directive as detailed below.

Structure of the Directive

7. The directive contains five parts:

   (i) **Part 1: General**– Includes introduction to the directive, detailed underlying principles of cyber defense management, applicability and definitions.
   (ii) **Part 2: Corporate Governance—**specifies the functions and responsibilities of the board of directors and of senior management, describes the roles of the Chief Cyber Defense Officer and the interfacing management coordination and control systems necessary for maintaining effective cyber defense.
   (iii) **Part 3: Defense Strategy and Cyber Risk Management Framework—**depicts cyber defense concept, definition of cyber defense strategy, determination of cyber risk management framework, definition of cyber defense policy and formulation of a work program.
   (iv) **Part 4: Cyber risk Management—**specifies the requirement for maintaining an orderly cyber risk management process, including identification and assessment of risks, cyber defense control assessment, and reporting on risks.
   (v) **Part 5: Control Objectives and Cyber Defense Controls—**concerns control objectives which the banking corporation must institute in order to reduce the exposure to cyber threats, including: security of the operational environment, proactive cyber defense, reducing the attack surface, defense in-depth, process view, the human factor, information and intelligence sharing, monitoring, control and identification of cyber incidents, response and cyber incident management, exercises , and cyber incident reporting.

Introduction (Sections 1–6 of the directive)

8. The directive stipulates that the banking corporations shall place a special emphasis, and employ the necessary measures, for effectively managing cyber defense. In particular, banking corporations shall expand and deepen the existing capabilities of the information security system in a manner that will enable them to withstand cyber threats.

9. The directive regards the cyber risk management as a part of the overall risk management process within the banking corporation. As such, the directive is integrated with the existing Proper Conduct of Banking Business Directives, adding more details and elaborated

information regarding aspects of cyber risk management. The directive does not replace other directives, particularly Proper Conduct of Banking Business Directive–"Information Technology Management"–No. 357 (hereinafter: Directive 357).
In this respect, it is emphasized that apart from operational risk, cyber risk also constitutes a strategic and systemic risk for the banking corporation.

Underlying Principles of Cyber Defense Management (Sections 7–11 of the directive)

10. The cyber defense management of a banking corporation shall be based on the principles specified in Part 3 of the directive.

11. Cyber risk management shall be conducted within a process framework, in accordance with the relevant risk management principles for all risk management processes as detailed in the relevant Proper Conduct of Banking Business Directives. The directive identifies the relevant provisions and the emphasis and context for their implementation.

12. Proper management of cyber risks requires extension and adaptation of the current IT risk management framework at the banking corporation from the perspectives of threat landscape perception and the corresponding defense capabilities. Directive 357 refers to information security controls and technical controls for IT risk management. The Cyber Defense Management Directive is focused on the mechanisms and processes required for cyber risk management, on cyber defense objectives, on the required expansions of defense capabilities, and finally, on the required designated controls for the purpose of achieving defense objectives.

Applicability (Sections 12 of the directive)

13. The applicability of the Cyber Defense Management Directive matches the applicability of Directive 357.

Definitions (Sections 13 of the directive)

14. The definitions are intended to create a uniform taxonomy for the purpose of this directive, while focusing on definitions that have a practical significance for the purpose of implementing the directive.

15. With respect to the definition of "Cyber Incident Management", the directive refers to 5 stages in this process. However, the banking corporation may combine these stages, as long as activity continuum is maintained throughout the stages.

16. Considering the characteristics of cyber threats and the attack scenarios, an operational malfunction could subsequently prove to be a cyber incident. Accordingly, the expectation is

that when an operational malfunction in the IT system occurs, Chief Cyber Defense Officer will be involved as required.

Corporate Governance (Sections 14–24 of the directive)

Board of Directors and Senior Management

17. The directive specifies the areas of responsibility of the board of directors and the senior management. The involvement of these bodies constitutes a key factor in the banking corporation's ability to manage cyber defense effectively. Therefore, it is expected that the banking corporation will create the control and necessary reporting mechanisms for this purpose.

18. With respect to receiving a periodic report, as stated in Paragraph 16 (f), it is clarified that the reporting required under this paragraph can be integrated with the reporting required under Sections 33–34 of Proper Conduct of Banking Business Directive No. 350.

Chief Cyber Defense Officer

19. In order to provide effective defense from a corporate-wide perspective, a new designated integrated function is required. This position integrates all functions relevant to cyber, including those that are not associated with IT management, such as: fraud detection, business continuity, physical protection, personnel and compliance.

20. Accordingly, the directive stipulates that the banking corporation shall appoint a senior employee with suitable expertise and experience Chief Cyber Defense Officer. The directive does not dictate an organizational structure and apportionment of authorities in the area of cyber defense. However, the banking corporation must ensure that the organizational position and the authorities of the Chief Cyber Defense Officer support his roles as a guiding, overseeing and integrating function for the relevant activities and processes, including at the business - strategic level from an integrated corporate-wide perspective, and not only IT management.

21. The effectiveness of the Chief Cyber Defense Officer is reflected by his ability to influence the decision-making within the corporation. In this respect the Chief Cyber Defense Officer is expected to express his opinion independently vis-a-vis the managers responsible for the business lines and IT management. In addition, his positions will be considered to a material extent in the decisions making.

22. The Chief Cyber Defense Officer may also serve as Information Security Manager, as long as no conflicts of interests arise between the different functions.

Interfacing Management, Coordination, and Control Systems

23. Integration of the cyber risk aspects at the banking corporation reflects a holistic concept of cyber risk management, which is applied *inter alia* by reporting lines and professional and organizational subordination to the relevant bodies, as detailed in the directive.

Defense Strategy and Cyber Risk Management Framework (Sections 25–33 of the directive)

24. The directive outlines a structured framework for cyber risk management which is based on the cyber defense concept as detailed in the directive. The list of principles for maintenance an effective and efficient cyber defense array, as detailed in the directive, is not a closed list. The list is intended to provide guidelines regarding operational best practices and the strategic objectives of the cyber defense array. The means and mechanisms for implementing them are detailed in the fifth part of this directive.

25. Cyber defense strategy constitutes a fundamental document outlined by the board of directors of the banking corporation. The strategy is focused on high-level goals and cyber defense objectives. The directive details the subjects that are to be included in the strategy document. The expectation is that the strategy document will be reviewed, as necessary, in accordance with the development of cyber threats and anyhow will be reviewed at least once every three years.

26. The banking corporation shall determine and document the cyber risk management framework. The framework defines the manner in which the banking corporation will implement the cyber risk management process, including organizational mechanisms, tools and methodologies, and processes as specified in the directive.

27. Corporate-wide cyber defense policy defines the controls and modes of operation for cyber threats mitigation. The directive details the subjects that should be included in the policy document. The expectation is that the policy document shall be assessed at least once a year.

28. The documents of the detailed defense policies shall include principles concerning each of the control types that are implemented by the banking corporation.

29. The directive determines that on the basis of cyber risks analysis, the banking corporation will formulate and approve work plans. The banking corporation is expected to allocate sufficient resources, and to monitor and ensure the implementation of the work plans in accordance with the determined.

30. A banking corporation is entitled to integrate the requirements of Sections 27–32 above in the strategy and policy documents that are required in other directives of the Supervisor of Banks.

Cyber Risk Management (Sections 34–47 of the directive)

31. The directive details the requirements regarding the maintenance of an effective process for cyber risk identification and assessment. Taking into account the dynamic nature of the cyber domain, the banking corporation is expected to conduct identification and assessment of cyber threats and risks, on an ongoing basis.

32. As part of the cyber defense control assessment, the banking corporation is required to carry out an ongoing examination of the effectiveness level of the defense controls that have been implemented to mitigate cyber risks. The Chief Cyber Defense Officer will collate the relevant information in the various segments of the corporation's activities. It is expected that the mechanisms of the cyber defense control assessment shall be adapted and integrated within the current assessment mechanisms. For example: vulnerability assessments and resilience tests/controlled penetration tests (as specified in Directive 357). Notwithstanding, the Chief Cyber Defense Officer shall initiate the performance of assessment and control mechanisms (such as vulnerability assessments and resilience tests/controlled penetration tests) where necessary.

33. The directive emphasizes that cyber defense control assessment should be assessed in different segments of the corporation's activities and processes, and its relations with external entities, such as customers and suppliers.

34. Regular reports on the current status of cyber risks will be delivered to the senior management and to the board of directors. It is emphasized that reporting on cyber incidents is covered in Paragraphs 81–82 of the directive.

Control Objectives and Cyber Defense Controls (Sections 48–82 of the directive)

35. The establishment of an effective control array against cyber risks requires a cross-organizational integration of people, technologies, processes and procedures. This part of the directive is based on the fundamental principles and concepts that have been presented in the directive, mainly in Part 3, and includes guidelines for an effective cyber defense array implementation. This part places an emphasis *inter alia* on activities that characterize cyber defense controls, including those aimed to implement and base proactive defense, multi-layer defense, information and intelligence sharing, monitoring, and cyber incident management and exercising.

36. The directive emphasizes the need for maintaining proactive cyber defense that *inter alia* includes:

    (i) Mapping the operational environments in which the banking corporation operates, including the external environment in which its control and oversight capabilities are weaker compared to the internal environment (See Section 37 below). The external environment includes customers' activity, suppliers, service providers and other entities in the supply chain, and social media.

(ii) Information Gathering and information and intelligence sharing with relevant external entities that are exposed to similar cyber threats. This will aid the banking corporation's to conduct early preparedness activities to threats and various attack scenarios. In addition, this will aid the banking corporation to strengthen, as necessary, the cyber defense array, including the ability to act in real time.

(iii) Ability to respond rapidly and effectively to various types of threats. The ability to know which functions within the banking corporation should be involved in handling with a particular cyber incident. The reference is not only to technological personnel but also for example, to business functions and spokespersons. The key factor in response is speed. The importance of speed is in the ability to detect an incident as soon as possible after its occurrence in order to mitigate the potential damage.

(iv) On-going and comprehensive monitoring of the banking corporation's operational environments in order to identify anomalies and suspicious incidents. The scenarios and tools employed in monitoring activities must be examined on an ongoing basis and be reviewed as necessary, in order to check the extent to which these activities are effective.

37. It is not enough for the banking corporation to implement internal mechanisms to mitigate cyber risks. A banking corporation can be exposed to a cyber threat materialization via weakness exploitation of an external entity that has connections with the corporation. Therefore, the directive presents the importance of actions which the banking corporation shall take in order to ensure that the relevant external entities also implement mechanisms to mitigate the corporation's exposure to cyber risks. The reference is mainly to material entities in the corporation's supply chain.

Commencement

38. Commencement of the said in this circular is as from September 1, 2015.

Update of the File

39. Enclosed are update pages for the Proper Conduct of Banking Business Directive file. The update regulations are set out below:

Remove page	**Insert page**
-----	(3/15) [1[361-1-19

Sincerely yours,

David Zaken

Supervisor of Banks