# Supply Chain Cyber Risk Management

## A. Background

### Introduction

1. Financial organizations around the world and in Israel have been experiencing a growing number of cyber incidents in recent years. Most of the cyber incidents are characterized, among other things, by massive damage and sophisticated and innovative methods of attack, sometimes originating in external parties that provide various services to the banking corporations . These entities are included in the banking corporations' supply chain.

2. Proper Conduct of Banking Business Directive 361, "Cyber Defense Management," expresses the need to have in place an effective process for risk detection and assessment, *inter alia* with regard to banking corporations' external activity environments and their work with external service providers. The directive also states that supply-chain management and dependency on external entities processes, shall be included in the cyber defense array. In addition, the directive requires a banking corporation to have necessary processes in place with which to ascertain that external entities are taking the necessary measures to mitigate the banking corporation's exposure to cyber risks.

3. It should be emphasized that some external entities that belong to a banking corporation's supply chain (such as companies that support capital-market trading services) are material to its activity and/or expose it to potentially high cyber and information-security risks that, when they eventuate, make it possible to attack the banking corporation or impair its activity (hereinafter: material service providers).

4. The purpose of this directive is to clarify the banking corporation's responsibility for maintaining a secure working environment vis-à-vis material service providers and

it's obligation to manage the cyber-risks appropriately in regard to these service providers' activity on their own premises, on the banking corporation's premises, and in material providers' interfaces with the corporation.

5. Notwithstanding the contents of Section 3 *supra,* when the material service provider is a corporate member of the banking group, the requirements in this directive shall be implemented in accordance with the banking corporation's risk assessment. For the purposes of this section, a "banking group" is a banking corporation, a banking corporation that controls it, and corporations controlled by either of them.

6. The Banking Supervision Department is drafting a far-reaching directive on the topic of outsourcing. In the future, this directive will be inserted into it.

**Incidence**

7. (a) This Directive shall apply to banking corporations as defined in the Banking (Licensing) Law, 5741-1981 (hereinafter in this Directive: "banking corporation"):

(1) a banking corporation;

(2) a banking corporation as set forth in Sections 11(a)(3a) and (3b);

(3) a banking corporation as set forth in Section 11(b).

(4) an acquirer as defined in Section 36i.

## B. General Remarks

8. Banking corporation shall lay down principles for the obligations of material service providers toward it in respect of cyber risk management.

9. In its contract with a material service provider, a banking corporation shall define specific reference to the management of cyber risks (see Chapter C below) and shall ensure that the provider abide by the principles that the banking corporation has established (Section 8 *supra*).

10. A banking corporation shall conduct the following on a periodic basis:

    (a) mapping of its material service providers; examination of the contract with them; compliance with their contractual undertakings; with reference to the need to make necessary changes on the supplier's part pursuant to developments and technological changes and changes in services rendered.

    (b) a risk assessement derived from the services provided by the material service providers, also based on the examination referenced in Section 10(a) *supra* and the results of the overviews specified in Section 12(c) below.

11. In the event that relevant players in the banking corporation reach the conclusion, after the examination referenced in Section 10 *supra,* that a material service provider does not meet its obligations in a manner that exposes the banking corporation to significant events, they shall report this to the corporation's management, describing said risks and their implications on the corporation and its customers. In this case, management shall consider and make a decision on continuing to contract with the provider.

## C. Contracting

12. When it contracts with a material service provider, a banking corporation shall take into account the need to include the following in the contract, in accordance with the risk assessment:

(a) hardening systems of the material service provider that are installed on the banking corporation's network in accordance with the banking corporation's information-security and risk-management procedures.

(b) transferring log files from the service provider's systems, at the banking corporation's request.

(c) producing an overview of a Vulnerabilities Survey and controlled Penetration Tests on a periodic basis, at the request of the banking corporation, including the test scenarios, and in accordance with risk management.

(d) dealing with findings detected in the Survey and the Penetration Tests within a reasonable time after their discovery.

(e) subjecting employees of the material service provider who are associated with service given to the banking corporation to reliability checks.

(f) appointing an information-security and cyber trustee with the material service provider and defining his/her powers and duties.

(g) providing a list of third-party (secondary) service providers who support the services that the material service provider gives to the banking corporation, on a periodic basis that the banking corporation shall determine.

(h) making arrangements for the deletion of banking-corporation data that are stored on the service provider's premises after the end of the contractual relationship and/or at the request of the banking corporation.

(i) creating a separation of working environments (development, production, etc.) on the material service provider's premises.

(j) reporting to the banking corporation about cyber incidents that occur at the material service provider or its third-party providers.

## D. Support and Maintenance

13. Banking corporations shall specify activities, in accordance with the risk assessment, for which the material service provider shall have to use strong authentication (2FA) in matters such as remote access to the banking corporation's systems, maintenance of the corporation's systems, and so on.

14. Banking corporations shall establish remote-access security and control mechanisms vis-à-vis the material service provider, in accordance with the risk assessment, such as denying access except with the corporation's approval; secured access from an activity environment separate from the material service provider's other working environments; operating a timeout mechanism after an interval in which the material service provider conducts no activity; recording and monitoring of maintenance activity; and so on. In addition, access to the banking corporation's production environment should not be allowed unless the corporation approves it.

**Updates**

| Circular no. | Version | Details | Date |
|---|---|---|---|
| 2560 | 1 | Original circular | April 24, 2018 |
| 2669 | 2 | Update | September 30, 3021 |