Cyber Defense Management

Part 1: General

Introduction

1. The continuous technological progress and innovation have a far-reaching impact on how banking corporations conduct their business, ultimately transforming the ways they engage with customers, suppliers, and partners.

2. Several trends are cultivating material weaknesses that threaten every aspect of a banking corporation's cyber defense and expose it to significant cyber risks: The rapid change in technology infrastructure, consistent innovation in the delivery of banking services, their ubiquitous and omnipresent ("anytime, anywhere") availability, the growing connectivity of legacy information systems to modern and "open" computing infrastructure, and a growing dependency on third-party computing and communications services.

3. With the development of the trends above, cyber threats have intensified significantly in scope, volume, and threat-actors involved, as well as the attack tools' sophistication and availability.

4. The materialization of cyber risk may disrupt a banking corporation's ability to operate properly and securely, and could result in denial of services from customers, exposure of private information, deletion of or tampering with customers' and banks' records, decline in public trust, and damage to the banking corporation's reputation and its ability to adequately manage both its own and its customers' assets. In a worst case scenario, cyber risk materialization could jeopardize the banking corporation's stability.

5. Therefore, banking corporations must pay special attention to cyber risks and take the necessary measures for effective cyber defense management. In particular, the banking corporations must expand and deepen their existing information security capabilities in a manner that shall enable them to confront cyber threats.

6. Cyber risk management constitutes a part of the overall risk management process within the banking corporation. This directive is intended to complement and supplement the directives detailed in Paragraph 8 below in all matters concerning the adequate management of cyber risks.

Underlying Principles of Cyber Defense Management

7. A banking corporation's cyber defense management shall be based on the underlying principles detailed in this directive. These principles constitute guidelines that confer the flexibility that is required, in light of the rapid pace of change in the cyber domain, and in recognition that each banking corporation has a unique risk profile, which requires adaptation of the cyber defense program to the individual characteristics of the activity and unique business requirements of each corporation.

8. A banking corporation shall manage cyber risks from an integrated corporate-wide perspective in accordance with the risk management and control rules set in the Proper Conduct of Banking Business Directives ("PCBBD"), specifically in the following:

   (i) Directive No. 310 - "Risk Management";
   (ii) Directive No. 350 - "Operational Risk Management";
   (iii) Directive No. 355 - "Business Continuity Management";
   (iv) Directive No. 357 - "Information Technology Management".

9. As part of the operational risk management process, in accordance with PCBBD No. 350, a banking corporation shall take into account and document the relevant cyber risks.

10. In all matters concerning business continuity management, in accordance with PCBBD No. 355, the banking corporation shall also address cyber incident scenarios that could potentially affect the corporation's business activity, its suppliers and service providers, the availability of supporting infrastructures, etc. This is in order to enhance the corporation's resilience during the occurrence of operational disruptions due to materialization of cyber risks, and to reduce the impact such disruptions may have to the continuity of business activity within the corporation, and throughout the national economy at large.

11. Adequate management of cyber risks requires augmentation and adjustment of the banking corporation's existing information technology (IT) risk management framework, from the perspectives of threat landscape perception and the required defense capabilities, as detailed in this directive.

Applicability

12. This directive shall apply to:

   (i) A banking corporation, as defined in the Banking (Licensing) Law, 5741-1981 (hereinafter: the Banking (Licensing) Law);
   (ii) A corporation as defined in Sections 11(a)(3a), 11(a)(3b) and 11(b) of the Banking (Licensing) Law, which is under the direct or indirect control of a banking corporation, as if it was a banking corporation;
   (iii) The Supervisor may issue directives, in addition to those detailed here, which shall apply to certain banking corporations.

Definitions

13. In this directive, the following terms shall have the following specific meanings:

"**Cyber Threat**"- A threat of occurrence of a cyber incident.

"**Cyber Incident**" - An event during which computer systems and/or computer-embedded systems are attacked by, or on behalf of, adversaries (external or internal to the banking corporation), which could lead to the materialization of cyber risk. It should be noted that this definition includes an *attempt* to carry out such an attack even if no actual damage is caused.

"**Defense Control Assessment**" - Activities intended to examine the adequacy of actual implementation of defense controls (administration, operational and technical), their regular operation, and their effectiveness vis-à-vis applicable defense requirements.

"**Cyber Incident Alert"** - A notification that refers to an imminent cyber incident, or to an incident that has already occurred, or is still occurring, but has not yet been identified by the entity under attack.

"**Adversary**" - With respect to this directive: an individual, group, organization, or political entities that intend to inflict damage on the banking corporation.

"**Cyber Incident Management**" - A structured process that refers to following stages:

(1) **Detection** – initial inquiry concerning the occurrence of a cyber incident and the rapid formulation, as soon as possible, of the mode of operation required for next steps.

(2) **Analysis** – a comprehensive and in-depth inquiry regarding the cyber incident to enable operative decision making, formulation of possible counter measures to thwart the attack, and a recommendation for the primary mode of operation for the containment stage.

(3) **Containment** – achieving initial control of the incident to prevent escalation. Conducting a process of neutralizing the attack vectors within the banking corporation, and preventing damage escalation.

(4) **Eradication** – neutralizing the attack elements located in the banking corporation's systems, while striving to remedy or mitigate the damage that has already been inflicted.

(5) **Recovery** – resume normal operation and complete activity at the targeted banking corporation whose operation was shut down, limited or disrupted.

Each stage includes reporting to the relevant internal and external entities.

"**Damage**" - An adverse outcome, including disruption/disturbance/shut down of activity; theft of an asset; gathering of intelligence; harm to reputation/ public trust.

"**Post-incident activity**" - A structured process that refers to following stages:

(1) **Investigation and lessons learned** – a process of inquiry and methodological analysis of the response to and management of the entire cyber incident, from beginning to end, from the perspectives of people, processes and technology. The investigation is carried out, as soon as

possible, upon concluding the operative management of the incident in order to provide insights and lessons that will improve and expedite a more efficient response to future cyber incidents.

(2) **Monitoring the implementation of lessons and insights** – a process intended to ascertain that all recommendations and insights raised during the incident are implemented.

"**Cyber Risk**"- The potential for damage resulting from an occurrence of a cyber incident, taking into account its probability and its impact.

Part 2 – Corporate Governance

Board of Directors and Senior Management

14. The banking corporation shall manage cyber risks in accordance with the principles stated in PCBBD No. 350. The Board of Directors and the Senior Management of a banking corporation shall create an effective cyber risk management framework.

15. The Board of Directors of the banking corporation shall be responsible for the following activities:

    (i) Set and approve a corporate-wide cyber defense strategy;
    (ii) Approve a cyber risk management framework and a corporate-wide cyber defense policy;
    (iii) Determine the manner in which it oversees senior management with regard to implementation of the cyber risk management framework;
    (iv) Receive reports on significant cyber incidents.

16. The Senior Management of the banking corporation shall be responsible for the following activities:

    (i) Create of an overall cyber risk management framework and adequately oversee its implementation;
    (ii) Formulate a corporate-wide cyber defense policy;
    (iii) Implement and consistently maintain an integrated, corporate-wide, cyber risk management framework, including sufficient resource allocation;
    (iv) Monitor the effectiveness of the cyber defense array and coordinate cyber defense activities with internal and external risk management entities, as stated in this directive;
    (v) Receive periodic reports on the current situation with respect to cyber threats and cyber risk treatment, in accordance with the results of the risk assessment, as stated in this directive;
    (vi) Receive periodic reports on relevant cyber incidents (internal and external) and analysis of their implications on the corporation;
    (vii) Discuss the cross-organizational operative implications of cyber risks. Guidance and control over implementation of required changes or adjustments in the defense array and/or in business activity, as necessary.

Chief Cyber Defense Officer

17. The banking corporation shall appoint a senior executive with suitable qualifications and experience as a Chief Cyber Defense Officer and shall define his authorities and responsibilities.

    (i) The Chief Cyber Defense Officer shall report to a senior executive of the banking corporation, and shall officially be given the authority to influence any decisions that affect the banking corporation's exposure to cyber risks.

(ii) The organizational hierarchy of the Chief Cyber Defense Officer's role shall be set in a manner which minimizes conflicts of interest.

(iii) The Chief Cyber Defense Officer shall not hold any other responsibilities that could interfere with the role's daily responsibilities.

(iv) The required working interfaces and reporting channels between the Chief Cyber Defense Officer and the relevant functions within the organization shall be determined and approved by senior management.

18. The Chief Cyber Defense Officer shall head the corporate cyber defense array and shall be responsible, *inter alia*, for the following activities:

(i) Overall integration of cyber defense management aspects within the banking corporation;
(ii) Advise senior management on cyber defense management;
(iii) Assist management in formulation and implementation of cyber defense policy;
(iv) Establish a corporate methodology for cyber risk management;
(v) Develop, oversee implementation, and monitor a comprehensive and in-depth cyber risk management program as detailed in this directive;
(vi) Define detailed policies and working procedures for the implementation of cyber defense controls;
(vii) Promote cyber threats awareness and provide training on mitigation processes across the banking corporation including employees, suppliers, partners and customers;
(viii) Work with the relevant functions (technological and business) within the banking corporation in order to analyze and assess the levels of inherent risk, the respective controls required, and the levels of residual risk and exposure to cyber threats;
(ix) Determine the reporting mechanisms which the Chief Cyber Defense Officer receives from different functions at the banking corporation;
(x) Coordinate and liaison with external entities on cyber defense matters;
(xi) Develop relevant metrics and measurements, prepare and disseminate status reports and provisioning of continuous reports as stated in this directive;
(xii) Integrate and monitor cyber incident response management within the banking corporation;
(xiii) Initiate and execute cyber exercises;
(xiv) Lead and coordinate cyber defense management processes ;
(xv) Cyber defense control assessment;
(xvi) Analyze significant cyber incidents in Israel and worldwide, analyze and implement lessons learned with respect to the banking corporation.

19. The Supervisor of Banks is entitled to permit the Chief Cyber Defense Officer at a banking corporation to serve also as Chief Cyber Defense Officer at banking corporations that are controlled by the same banking corporation or at corporations as detailed in Sections 11(a)(3a), 11(a)(3b) and 11(b) of the Banking (Licensing) Law.

Internal Audit

20. The management of cyber defense and the manner in which it is applied shall be periodically audited by the internal audit.

Interfacing Management, Coordination, and Control Systems

21. As part of corporate-wide cyber risk management, the cyber defense array shall operate in coordination with internal and external interfacing management, coordination, and control systems.

22. The reciprocal relationships and information flows among the functions within the banking corporation shall be formally defined and documented. Interfacing management, coordination, and control systems within the banking corporation include, *inter alia*: information security, physical security, information technology (IT) governance, IT operations, risk management, fraud detection, human resource, business continuity, customer relations management, spokesmen and legal department.

23. In particular, the Chief Cyber Defense Officer shall collaborate with the Chief Risk Officer and the Internal Audit, in accordance with the relevant PCBBDs.

24. The reciprocal relationships and information flow among the internal functions and external entities shall be formally defined and documented. External entities to the banking corporation include, *inter alia*: regulatory entities, investigative and enforcement entities, the National Cyber Bureau, peer cyber risk management entities within the financial sector, risk management functions of suppliers and counterparties, and cyber-information-sharing bodies.

Part 3: Defense Strategy and Cyber Risk Management Framework

Cyber Defense Concept

25. The banking corporation shall expand and deepen traditional information security's countermeasure capabilities (that is: Prevention, Detection, Response) to enable it to withstand cyber threats. In particular, the banking corporation shall develop and expand its capabilities in the following areas: Prediction, Detection and Deception, and Resilience.

26. The banking corporation shall maintain an effective and efficient cyber defense array, which shall be operated from a process-oriented perspective and shall apply inter alia the following principles:

    (i) An overall perception of the operational environment—the cyber defense array shall take into account the banking corporation's location in the overall supply chain of banking services, the use of external infrastructures and services (such as social networks) and the risks deriving from interacting with different counterparties in Israel and overseas, including, subsidiaries suppliers, contractors and customers;
    (ii) Cooperation with all the relevant functions within the banking corporation in creating and implementing the cyber defense strategy and policy;
    (iii) Proactiveness—intelligence capabilities, continuous monitoring and real-time response to threats, and sharing actionable cyber information and intelligence.
    (iv) Enhancing the ability to confront targeted cyber threats by creating a cyber defense array that integrates organizational and human infrastructures, procedures and processes, and technologies (people, processes, technologies) in a "defense in-depth" structure in order to minimize the exposure to cyber threats and their impact;
    (v) Integrating advanced capabilities in the defense array, including: attacker's deception and delay, deployment of honeypots, and detection of suspicious patterns and anomalies both at the technology infrastructures level and at the business activity level (for example: fraud detection);
    (vi) Placing an emphasis on detection, investigation, forensics and response mechanism, in recognition of the complexity of the threat and adversaries' capabilities, based on the assumption that completely mitigating the cyber risk is impossible, also taking into account low-probability, high-impact scenarios;
    (vii) Resilience—mapping and analysis of the environment, prediction and analysis of threats, a mission-oriented cyber defense array that enables the banking corporation to withstand a significant (direct or indirect) operational disruption resulting from a cyber-incident, while maintaining continuous business operations and banking services delivery;
    (viii) Placing an emphasis on the protection of the privacy of the banking corporation's customers' data and assets, while maintaining high levels of reliability, adequacy and availability of the services supplied by the banking corporation.

Cyber Defense Strategy

27. Corporate-wide cyber defense strategy shall be defined and documented, including, *inter alia*:
    (i) The position and importance of cyber defense at the banking corporation;
    (ii) The cyber-threat concept and the challenges facing the banking corporation;
    (iii) The banking corporation's approach to cyber risk management, definition and oversight the level of exposure to cyber threats;
    (iv) Key elements of cyber defense strategy: objectives, principles of operation and implementation.

28. The strategy shall be revised as necessary and in any case, at least once every three years.

Cyber Risk Management Framework

29. The cyber risk management framework shall be defined and documented, including *inter alia*:
    (i) Identification of the corporate governance elements for cyber risk management, including areas of responsibility and reporting lines.
    (ii) Detailed definition of tools and methodologies for the evaluation of risks and the manner in which they are implemented;
    (iii) Detailed definition of main defense processes and measures and the manner of their control and assessment.

Cyber Defense Policy

30. The banking corporation shall define a corporate-wide cyber defense policy, which shall refer to the entire array of controls, and the means to achieve the cyber defense objectives in accordance with the defined cyber defense strategy.
    The policy shall be reviewed annually and shall be revised as necessary.

31. The policy shall refer *inter alia* to the following subjects: cyber defense objectives; definition of areas of responsibility, involved positions and functions (including work interfaces); organizational structures; structure and governance of the cyber risk management process at the banking corporation; the internal procedural framework of the banking corporation; details of the controls required and the framework for their implementation; monitoring and response; training and awareness; information gathering, research, and sharing; process maturity and effectiveness metrics and indexes; evaluation, control and reporting.

32. Based on the cyber defense policy, the banking corporation shall define detailed policies for the implemented defense controls. The detailed policy documents shall be revised as necessary.

Work Plan

33. Based on the cyber defense strategy and policy, and as derived from cyber risks and exposures analysis, the banking corporation shall formulate a perennial work plan which shall outline and prioritize the ways of implementing controls to mitigate cyber risks. The work plan shall be approved by the banking corporation's management, which shall allocate suitable resources to achieve the program's targets.

Part 4: Cyber Risk Management

Cyber Risk Management: Identification and Assessment of Risks

34. An effective identification and assessment process of cyber risks encompasses, in addition to Section 26 of PCBBD No. 350, the various cyber threat actors, the diverse corporation's operating environments (internal and external) and the different scenarios, Including reference to risks deriving from cybercrime, and dependency on supporting infrastructures and external suppliers.

35. At least once a year, the banking corporation shall conduct an assessment of cyber risks and controls, which identifies the inherent risk, the effectiveness of the control environment, and the residual risk.

36. The cyber risk identification and assessment process shall be ongoing and carried out in accordance with internal and external factors, including business, organizational and technological changes.

37. The banking corporation shall ensure that the assessment of cyber risks and their control infrastructure are revised in accordance with the changes and trends in the threats landscape and in accordance with the pace of growth or changes in products, activities, processes, and systems.

38. For the purpose of analyzing and assessing cyber threats, the banking corporation shall take into account the factors detailed in Section 28 of PCBBD No. 350, with emphasis and changes as detailed below:

    (i) Surveys and audit findings, and all current information that could be indicative of weaknesses in the relevant controls;
    (ii) Collection and analysis of external data that could be indicative of potential vulnerabilities or lead to the detection of risk exposures that were not identified in the past;
    (iii) Collection and analysis of data regarding cyber incidents within the corporation;
    (iv) Mapping of business processes for the purpose of exposing specific risks, interdependencies between risks, and areas of weakness in controls or risk management;
    (v) Use of metrics for the purpose of quantifying the exposure to cyber risks, use of qualitative and/or quantitative assessment indexes, in a manner that shall make it possible to monitor changes in these values from time to time.

(vi) Use of process maturity indexes, Key Risk Indicators (KRIs) and Key Process Indicators (KPIs), in order to provide insights on the status of control mechanisms and the cyber defense program

(vii) Analysis of scenarios, in cooperation with business line managers and risk managers in order to detect potential incidence of risk materialization, to assess their potential impact, and to enhance the ability to detect and respond to those incidents;

(viii) A comparative analysis of the results of various assessment tools in order to provide a comprehensive view of the banking corporation's cyber risk profile.

39. Cyber risk identification, measurement and assessment methodologies at the banking corporation shall be documented and approved by the senior management.

Cyber Defense Control Assessment

40. The Chief Cyber Defense Officer shall ensure that management, operational, and technical mechanisms are in place for the monitoring and assessment of cyber defense controls and shall initiate operation of such mechanisms as necessary.

41. The architecture of cyber defense control assessment shall be derived from a holistic perception of the entire cyber threat landscape facing the banking corporation, taking into account the types of risks, cyber threat scenarios, the probability of their materialization and the results of previous surveys.

42. Mechanisms for cyber defense control assessment shall be coordinated and integrated with the current assessment mechanisms at the corporation, *inter alia* in vulnerability assessments and resilience tests/controlled penetration tests in accordance with PCBBD No. 357, internal audit processes in accordance with PCBBD No. 307, and regulatory compliance processes.

43. The cyber risks assessment indexes and metrics shall be updated from time to time in accordance with the results of the cyber defense control assessment.

44. Cyber defense control assessment shall include an analysis of the controls' current status vis-a-vis relevant cyber threats, weaknesses and risks across the different activity segments, including: physical access; administration and organization; information system lifecycle in various operational environments; technology management, including critical supporting systems; interaction with customers, including devices used by customers; remote access; messaging and communication; identity and access management; business partners and suppliers, including information and data exchange channels; organizational culture and awareness; online presence, including direct and online banking and use of social networks, and business continuity.

45. Material findings identified during cyber defense control assessments, shall be reported to the senior management and the board of directors, with lessons learned and a remediation work plan, in accordance with this directive.

Risk Reporting

46. The regular reports submitted to the senior management and the board of directors concerning operational risks, as detailed in PCBBD No. 350, shall include specific reference to cyber risks.

47. Cyber risk reports shall include:

(i) An updated and cogent status report of current cyber risk indexes and metrics;
(ii) Detailed report of significant risk/damage incidents within the corporation:
(iii) Relevant external incidents and data that could have a potential impact on the banking corporation.

Part 5: Control Objectives and Cyber Defense Controls

General

48. As part of its cyber defense management, the banking corporation shall establish an effective controls array for reducing the level of cyber risks.

49. The array of controls shall be based on a corporate-wide integration of technologies, processes, procedures and people, which shall enable the banking corporation to reduce the exposure to cyber threats to the acceptable level.

50. The banking corporation shall take the necessary measures for achieving the control objectives and implementation of controls as detailed in this section.

Security of the Operational Environment

51. The banking corporation shall map the operational environment in which it operates, shall identify the cyber risks involved in its activities, and shall define policies for treating these risks, according to the level of the risk and the nature of the connections with other entities.

52. In this respect, the banking corporation shall examine the entire scope of business and operational services, including: suppliers, related corporations, customers, counterparties, technology suppliers, outsourcing, other service providers (for example: lawyers, accountants, PR and marketing agencies and printing house) and overseas entities.

53. The banking corporation shall determine suitable mechanisms for the protection of its online presence and in particular, protection against the threats involved with its activity in social networks.

54. The banking corporation shall define the required actions for ensuring, to the highest possible extent, that the relevant entities, including external entities, take the necessary measures for mitigating its exposure to cyber risks. The banking corporation shall examine and monitor the compliance of the entities that have been identified as material for its adequate business activity and services delivery.

Proactive Cyber Defense

55. The banking corporation shall establish a dynamic cyber defense array with proactive capabilities *inter alia* by:

    (i) Mapping the environment—ongoing mapping and analysis of the internal and external operational environment, in order to identify critical entities, systems and processes, and their vulnerabilities, weaknesses and/or mutual interdependencies.
    (ii) Prediction and threat research—ongoing information gathering, identification and analysis of attack methods and vectors, intentions and activities of threat actors within the

cyber domain, and information sharing with other relevant entities for the purpose of gaining operative information, scenario analysis and "out of the box" thinking, which shall help to strengthen the cyber defense array and the operational environment against potential attacks;

(iii) Situational awareness—perception of the corporation's current state of cyber defense vis-à-vis threats. Comprehensive monitoring of the banking corporation's internal and external environment for the purpose of detecting weaknesses and/or threats and/or security incidents and/or indicators (IOAs, IOCs) of their existence, using detection capabilities such as: pattern recognition, anomaly detection, and big data analysis. Prioritization of incidents considering their level of risk and the potential damage, as a basis for operative decisions making;

(iv) Responsiveness—development of rapid and effective response capability to cyber incident and its management, regarding all its aspects and throughout all of its stages as defined in this directive, in order to mitigate to the possible extent, the materialization of damage to the banking corporation;

(v) Deception, diversion and delay—the use of dedicated techniques and technologies (such as honeypots , diverting communication) in order to deceive and delay the attacker, and in order to facilitate detection and analysis of tactics, techniques and procedures employed by the attacker;

(vi) Cyber resilience and recovery—the ability to withstand the ramifications of a significant operational disruption resulting from a cyber incident, while continuing the operation of essential processes and services, and rapid recovery of business activities to an acceptable level;

(vii) Investigation and prosecution—the ability to retain evidence and conduct in-depth analysis and forensics of cyber incidents for the purpose of gathering evidence, assessing the damage, identifying attack sources and entities, conducting an investigation, lesson learning and preserving knowledge. All the above, while employing legal mechanisms and cooperating with law enforcement entities, as necessary, for the purpose of prosecuting the perpetrators.

Reducing the Attack Surface

56. The banking corporation shall act on an ongoing basis to reduce the exposure to cyber threats. For this purpose, the banking corporation shall *inter alia* take the following actions: system and infrastructure hardening; secured development life cycle; allocation of authorizations on the basis of "need to know" and "least privileged" principles; control and limitation of mobile devices usage; file filtering; blocking address ranges and/or networks used as a source of attacks.

Defense In-Depth

57. Defense In-Depth is characterized by the use of different controls at various points, so that weakness in one control is compensated by strength in another control. Implementing Defense In-Depth, by applying multi-layer defenses, can significantly strengthen the overall security of business processes, information systems, banking products and services. Defense In-Depth can

be effective in protecting customers' privacy, preventing identity theft and preventing losses resulting from unauthorized usage.

58. When deploying Defense In-Depth, the banking corporation shall take into account the cyber risk analysis, the status of controls and the exposure to threats.

Process View

59. The banking corporation shall map the cyber defense processes, shall determine performance metrics and indicators, shall assess the maturity level of the processes at the banking corporation, shall identify the required improvements, and shall implement the necessary changes according to the work plan.

60. Cyber defense processes are also relevant to corporate-wide processes, including: cyber risk management; system lifecycle management; asset management, configuration and patch management; identity management; monitoring and control; information sharing and reporting; incident and response management; supply chain management and dependence on external entities; training and awareness; cyber defense program management.

61. The banking corporation shall review the assessment of process maturity at least once a year.

The Human Factor

62. Recognizing the central role of the human factor in the cyber defense array, the banking corporation shall define the necessary controls regarding recruitment and hiring of personnel (including employees and suppliers), clearance, identity and access management, segregation of duties, mobility, transfer and leave.

63. The banking corporation shall define and implement a comprehensive training and awareness program for cyber defense. The program shall encompass the entire range of target audiences, including employees, managers, developers, system and infrastructure administrators, external entities, suppliers and customers. The program shall be reviewed periodically according to the threat landscape and current risk assessment,

Information and Intelligence Sharing

64. The banking corporation shall gather and analyze relevant information from internal and external sources, for the purpose of creating a comprehensive and current perception of the cyber threat landscape and the banking corporation's exposure to it. This information shall be used as a basis for a knowledgeable decision making, prioritizing modes of operation, and maintaining real time effective defense.

65. The threat and vulnerability landscape shall be derived *inter alia* from the following information: mapping of relevant threat factors, with respect to motivation and capabilities; techniques, tactics, scenarios and attack tools; weaknesses, system configurations and/or vulnerabilities that could be exploited for attacks; attacks that occurred in the past (at the banking corporation and/or in its

operational environment); response actions taken in the past, means and indicators for detecting and identifying attacks and handling them.

66. The banking corporation shall share information that may help other banking corporations in handling cyber threats.

67. Information shall be gathered and shared in accordance with the directives of the Supervisor of Banks, and the applicable law.

Monitoring, Control and Identification of Cyber Incidents

68. The banking corporation shall maintain an effective control and monitoring array, which shall be staffed continuously (24 x 7 x 365), shall receive data in real time from the various systems, including operational and business systems, shall identify indicators of cyber incidents, and shall initiate reporting and response activities as necessary.

69. Notwithstanding paragraph 68 above, the Supervisor of Banks may permit, in exceptional cases, non-continuous staffing, provided that the monitoring and control system shall operate in a manner that supports functional continuity.

70. For the purpose of detecting cyber incidents, the banking corporation shall also use means for identifying anomalies, both at the technological level (systems' activity) and at the business activity level.

71. The banking corporation shall determine the period of time necessary for retaining the information required for detecting cyber incidents, including "low-and-slow" attacks, in order to facilitate incident investigations.

72. The monitoring systems shall be integrated with other systems at the banking corporation in order to enable an effective cyber incident detection and response, including: detection of indicators of abnormal activity, information retrieval and enrichment, investigation and documentation, knowledge management and decision making, generation and management of alerts and reports, communication with relevant entities, and real time change management.

73. The banking corporation shall periodically examine cyber incident scenarios for the purpose of assessing its ability to detect them and respond, and shall update the monitoring and detection systems accordingly.

Cyber Incident Management

74. In the course of cyber incident management, the banking corporation shall identify the current stage of the incident (see Paragraph 13 above), and shall handle it according to its characteristics. A cyber incident shall be regarded as concluded only after it has been handled throughout its lifecycle.

75. The banking corporation shall define procedures for cyber incident alert, and for cyber incident management, including alerting, reporting, handling, responding and concluding, in accordance to its severity and stages.

76. For the purpose of managing a cyber incident, the banking corporation shall operate a situation room, and shall define from an integrative corporate-wide perspective, its staff, its authorities and responsibilities, internal and external reporting lines, communication channels, tools and detailed working procedures.

77. The banking corporation shall record and document in an orderly manner incidents that have been handled and the actions that were taken by the relevant functions. In particular, the corporation shall maintain an "incidents log" in which all the notifications, decisions and actions taken, in relation to cyber incidents, are documented, as close as possible to the time of their occurrence.

78. The banking corporation shall define a pool of response activities (such as configuration change, restriction and/or diversion of communications, and deployment of software) in accordance with the different scenarios. In addition, the corporation shall define the conditions in which these response activities shall be employed; their specific implementation; the authority for their activation; the communication channels; the required approvals; and assessment of their effectiveness, in the context of a given incident.

79. The banking corporation shall define a scale of alert levels, and the required activities in accordance with various alerts and scenarios, such as: prediction of an organized attack; the volume and severity of detected attacks within the banking corporation, the banking sector or the nation; detection of a material weakness or identification of attack tools that constitute a direct threat to the banking corporation.

Exercises

80. The banking corporation shall define a program for exercising the various response arrays, taking into account the various types of exercises (such as attack simulations, "war games" and "table top" exercises) and with reference to the relevant stakeholders (for example: technical staff, crisis management team, decision-makers, and spokespersons).

Cyber Incident Reporting

81. The banking corporation shall maintain an adequate internal reporting system as part of its cyber risk and cyber incident management. In this respect, a detailed reporting policy shall be defined, which shall determine *inter alia* the internal and external entities to which reports shall be provided, the reports format and frequency.

82. The banking corporation shall report to the Supervisor of Banks on a cyber incident or on a suspected cyber incident, in accordance with Proper Conduct of Banking Business Directive no. 366 on “Reporting of Technological Failures and Cyber Events”.

UPDATES

Circular 06 no.	Version	Details	Date
2457	1	Original directive	March 16, 2015
2643	2	Update	December 29, 2020