Box 1.1
A Standard-Scenario Cyber Stress Test for the Banking System

- Cyber attacks against organizations around the world, including those in financial services, have been growing in number and sophistication in recent years, causing more and more concern about a cyber attack in Israel generally and against its banking system particularly.
- Cyber risk has unique characteristics, including the nature of cyber attacks as malicious and sometimes deliberate, focused, and sophisticated events that flow from lengthy planning. For these reasons, cyber attacks may have unexpected implications, making the intensity of their expected damage hard to estimate.
- To reinforce the banking system's management of cyber risk and improve the Banking Supervision Department's understanding of this risk and its repercussions on banking system stability, in 2019 the Department conducted a stress test for the banking system based on a cyber event. Apart from being the first of its kind at the Department, the stress scenario in this format is, to the Department's best knowledge, the first conducted by a financial supervision entity anywhere. Importantly, the test was not a forecast but rather an approximation of an extreme scenario that probed a bank's ability to cope with a risk of this kind.
- The test was based on the scenario of a serious cyber event, in which the current-account and deposit data of all private customers of a bank are corrupted. The attack has technological and financial effects on the bank and its customers. Therefore, its span includes numerous fields such as cyber risk, operational risk, compliance risk, legal risk, and reputation risk, along with the synergy that exists among these risks, and it challenges the way the bank manages its business continuity.
- Testing this scenario made it possible to examine focal points of risk that emerge when a grave cyber event occurs. Also examined were the direct and indirect effects of the event on banking activity and how the bank copes with it, including its activity vis-à-vis customers, the impact on its information systems, and the financial implications of the scenario in both the near and long terms.
- The test helped the banks to identify discrepancies that have to be narrowed in order to cope with a scenario on such a scale. It is expected to be helpful in drafting contingency plans for future events of this kind and in reinforcing communication among the bank's various units in order to optimize its comportment in the case of such an event. The test also helped to enhance the Banking Supervision Department's and the banking system's existing knowledge about such an event and its implications, including the possibility of microprudential damage, and it will be helpful for drawing supervisory conclusions and determining continuing activities in this context.
- The coronavirus crisis has intensified various risks, including cyber risk; thus, it pointedly demonstrates the importance of the banking system's ongoing preparedness to cope with the risks that it faces, including by means of stress tests, among them the kind that is based on a cyber scenario.

Background

- The Banking Supervision Department has been subjecting the banking system to standard-scenario stress tests since 2012, in order to get a better understanding of focal points of risk to which the system and each bank are exposed. In 2019, it was decided that the test would probe focal points of risk that would rise to the surface if a stress event of cyber nature were to occur. A cyber stress test, due to its essence, reveals effects beyond the direct damage that a serious cyber event causes. The process is expected to help reinforce and improve the Israeli banking system's cyber-risk management and augment what the Banking Supervision Department and the banking system already know about such events and their implications. The test is a continuation of previous activity by the Department vis-à-vis the banking system in 2017–18 in regard to

cyber-stress scenarios, in which the Department reviewed the banks' internal cyber stress tests. In the review year, it was decided to set up a standard scenario for the entire system.

Cyber risk in the banking system

Cyber attacks against organizations worldwide, including those in financial services[76], have been escalating in recent years in both number and sophistication. The trend evokes concern about a major cyber event in Israel generally and against its banking system particularly. In a survey of risks that the Banking Supervision Department carried out among senior officials of the banking system in February 2019 and February 2020, it was found that cyber risk is the most troubling risk of all[77] and that many of these senior officials consider it one of the three most significant risks that the banking system faces.

Cyber risk has characteristics that distinguish it from the other risks to banking systems. A financial shock, for example, originates in an exogenous event (to which the markets' response, together with the contagion effect, may cause much harm); a cyber attack, in contrast, is undertaken at someone's initiative and is sometimes deliberate, focused, sophisticated, and carried out after lengthy planning.[78] In sophisticated attacks such as these, perpetrators invade systems weeks or even months in advance in order to map them and thereby determine the best way to damage them. It is true that such an assailant needs ample resources and advance planning to put the attack into effect; however, he carries out the attack at the time of his choosing and in a manner that will make it hard to detect. Thus, by the time the attack is discovered, the target has most likely sustained considerable damage. The probability of success in such an attack is strong and major effects are possible. In addition, the cyber field is highly complex and the systems at risk are networked, interconnected, and interdependent. Therefore, the corruption of one system may unexpectedly trigger disruptions elsewhere, making it hard to determine how the corruption of one system can bring down others. This sets cyber risk apart from financial risks, in which different effects on sundry fields and linkages among fields have been researched and estimated by means of models based on past events. Consequently, the effects of financial risks on the banking system are more clearly understood than are those of a cyber attack, and the tools with which these risks can be mitigated are also more apparent (Healey et al., 2018).

If a cyber event in the banking system comes to pass, its implications may be significant at both the microprudential and the macroprudential levels. One of the main concerns in such an event at a bank is that the event will touch off a "cyber run," i.e., massive withdrawals of deposits due to fear of impairment to deposits in view of the cyber attack and due to serious harm to the bank's reputation. The large-scale withdrawal of deposits may degrade the bank's ability to remain liquid and meet its payment liabilities on time. In addition, a liquidity crisis at a given bank may have major repercussions for the real economy long after the bank recovers and access to deposits is restored. because the delay in payments, coupled with uncertainty, may project onto other financial institutions, particularly if the latter do not receive payments that they are expecting (Duffie and Younger, 2019).

In view of these risks, many regulators around the world, as well as the Banking Supervision Department,[79] have been expressing the importance of managing cyber risk by means of regulation and in other ways. Kashyap and Wetherilt of the Bank of England, in an article titled "Some Principles for Regulating Cyber Risk," set forth several major regulatory tenets that should inform

[76] For a review of cyber attacks against the financial-services sector in various countries in 2016–2018, see Box 1.3 in *Israel's Banking System* for 2018.

[77] For elaboration, see the section on risks in *Israel's Banking System* for 2018 and the section on risks in this report.

[78] These attacks, known as advanced persistent threats (APT), are among the paramount risks in the cyber field. The perpetrators are skilled and advanced elements that target specific organizations.

[79] In Proper Conduct of Banking Business Directive 361, "Cyber Defense Management, "Proper Conduct of Banking Business Directive 363, "Supply Chain Cyber Risk Management," and elsewhere.

action to strengthen cyber-risk management throughout the financial-services system, including the banks. Among them:

- Require banking corporations to operate under the assumption that total prevention of a successful and highly damaging attack is impossible.[80] Similarly, banking corporations are expected to continue operating despite disruptions to their systems. This requirement induces corporations to produce a profile of critical services that they must continue delivering even in the case of a cyber attack.
- Require banking corporations "to make plans for prolonged and system-wide disruption, with particular attention to resourcing for response and recovery," which may be constrained. This principle encourages banking corporations "to plan for a wide range of scenarios and go beyond their pure idiosyncratic concerns."
- "Aim for a two-way dialogue between firms and supervisors as part of a wider collaborative approach to recovery objectives," allowing stakeholders to learn and develop tools for cyber-risk assessment and management.

Also, as Kashyap and Wetherilt note, regulators worldwide are enunciating the need for cyber-related stress tests. Although banks have been performing internal stress tests of this type, no central bank or regulator to date, to our knowledge, has conducted a standard-scenario cyber stress test for an entire banking system. One possible reason for this is difficulty in estimating cyber risk by means of models, unlike a macroeconomic stress test, as noted.

A cyber-scenario-based stress test

The stress test that the Banking Supervision Department conducted in 2019 was meant to examine the way a bank would cope with a significant and grave cyber attack and its immediate and long-term implications. The test scenario was a serious but reasonable cyber event consisting mainly of data corruption that has technological, operational, and financial effects on the bank and its customers. The banks were instructed to test the totality of these effects, both direct and indirect, on their activity, including customers' activity, the impact on the bank's information systems, and the financial repercussions. Unlike actual economic scenarios, this stress test required every bank to analyze the scenario under the assumption that it is the only victim and that the rest of the banking system is unscathed. The idea here was to amplify the possible harm to the individual bank and test how it copes with a blow to its reputation and, particularly, its implications. The bank had to make assumptions about actions and measures that its management would take upon the realization of this scenario and to granulate them in its analysis of the scenario. Importantly, a stress scenario is not a forecast but an approximation of an extreme scenario that proposes to test how the bank would cope with such a risk.

The banks were instructed to analyze, separately, the implications of the cyber attack in the immediate term—from discovery of the attack to the detection of its origin and nature[81]; the short-to-medium term—from the time the damage is understood to the conclusion of technological recovery; and the long-term—from technological recovery to the end of the period in which experience all implications of the attack: reputational, legal, and so on. After all, as can be seen from major cyber events abroad, the additional implications of cyber attacks may be long-lasting and their treatment may be time-consuming. The banks were instructed to explain, at length, the actions they took throughout the scenario, including management decisions in each stage, the implications of the attack, and how they coped with it in the full range of fields—technology and cyber, activity vis-à-vis customers, and financial repercussions.

[80] Reiterated in Section 26 of Proper Conduct of Banking Business Directive 361, "Cyber Defense Management."

[81] To amplify the damage in this scenario, the length of such a period for the bank [] was defined irrespective of the bank's technological ability to trace the source and nature of the attack. The goal here was to challenge the bank's ability to continue doing business at a time of business and technological uncertainty.

Purposes of the scenario

The stress test was performed for several purposes. For the banks, the goal was to help strengthen and improve processes of managing cyber risk and its implications. The scenario covered the entire field of cyber risk—operational risk, compliance risk, legal risk, and reputation risk—and challenged the bank's ability to manage its business continuity. Therefore, in responding to the scenario, all divisions of the bank had to examine the impact of the scenario on their purviews and respond collaboratively.[82] This level of work was meant to yield a better understanding of holes in bank's ability to cope with such a scenario, draft contingency plans for future events, and strengthen communication among its units to assure the viability of conduct if such an event comes to pass.

From the supervisory standpoint, the analysis of the scenario revealed the bank's potential vulnerabilities and focal points of risk in the event of a serious cyber attack. Tested in addition to the bank's financial resilience to such an event were the effects of the scenario on the bank's level of customer service, its existing controls for the detection of a cyber attack, the way it attains technological and operational recovery, and measures taken by management and by the bank to contend with the challenges that the test brought to light. The banks' responses will be helpful in assessing the adequacy of these aspects of the risk-management process and will be integrated into the Supervisory Review and Evaluation Process (SREP). In addition to all these, the test will help to enhance the Banking Supervision Department's knowledge about a material cyber event and its implications by giving it quantitative and qualitative information in various domains, including the possibility of microprudential damage in view of this kind of event.

The background story of the stress test

A corporation that belongs to the bank's supply chain has experienced a cyber attack by a malefactor at an unknown time and without its knowledge. The attack enabled the perpetrator to contact the bank regularly, posing as being the company in question. In one of these contacts, the perpetrator planted unfamiliar malware in the bank's system that circumvents the bank's security mechanisms, evolves surreptitiously in the bank's system, and successfully impairs the bank's core systems. This malware causes random corruption of current-account balance data (credit and debit) and deposit balances of retail customers for five months, in all the backup systems of the bank's databases, all without the knowledge of the bank and its customers. At the end of the five months, the malware is activated in the production environment as well, with immediate manifestations in all channels of customer service, including direct and digital. The devastation immediately impacts bank customers' activity in various fields.[83]

Results of the test

The analysis of the stress test prompted the banks to examine the tools, processes, and systems that they can use to cope with cyber attacks. To carry out the test, as stated, all units of the bank had to be involved, strengthening cyber management capabilities in each field individually and risk management in systemic terms. By undergoing this process, the banks detected various gaps among themselves and some have already learned the lessons thoroughly and integrated them into their work plans, including schedules for implementation.

The banks' responses broadened the Banking Supervision Department's knowledge of the environment of controls, architecture, and backups in which a bank operates. The test also shed

[82] See also Circular E-2457-06 (cyber defense management), section two –issuing a special directive on cyber defense management, as stated, is meant to emphasize the approach of the Banking Supervision Department that coping with cyber risks is a cross-organizational matter that entails the active involvement of the highest echelons of the banking corporation. Even though cyber risks originate in the use of technologies, they are not a mere technological issue but rather a business-strategy issue.

[83] The corruption of current-account data mangles a wide variety of customer operations, such as instructions to credit an account, transfer funds, and so on.

further light on the importance of certain processes that a bank uses to keep its systems functioning soundly. The banks' replies also revealed discrepancies between the way a supervisor would expect banks to behave in the course of such an event and the decisions that a bank actually makes in reference to business continuity and bank-customer relations, among other things, and in understanding and internalizing the challenge of decision-making under the conditions of uncertainty that typify the way an entity copes with a cyber attack that it has experienced. These outcomes will help the Department to draw conclusions and determine its next activities in this matter. For one thing, it will consider issuing regulatory updates in order to lay down clear procedures that it will expect the banks to follow when they face business-continuity events generally and cyber events particularly.

The cyber scenario in view of the global coronavirus crisis

The outcomes of the coronavirus crisis include growing reliance on direct and digital channels for banking services among member of the public, some of whom are unaccustomed to their use. The pandemic has forced the banking system to make quick and much more extensive use of remote work (both in the number of employees who connect remotely and in the remoteness of the way they connect). Furthermore, the crisis has made it more probable that banks will face shortages of trained personnel to deal with cyber attacks (due to restrictions on travel and assembly or due to illness). These changes have placed various risks on a higher level and made the banking system more exposed to hazards such as embezzlement, fraud, data corruption, data breaches, and cyber attacks generally. They are also relevant for entities in the banking system's supply chain in that the escalation of risks among them, including cyber risk, also affects the risks that the banking system faces.

Furthermore, it is feared in Israel and abroad that the current sensitivity of the economy and the widespread transition to remote work will be exploited for more attempts at cyber attack. Indeed, according to the National Cyber Directorate, since the World Health Organization declared a state of emergency due to the spread of the coronavirus, reports about cyber attacks that take advantage of public fear began to arrive from various countries.

Cyber-based stress testing is one of many tools that the Banking Supervision Department has employed in recent years to strengthen the management of the growing cyber risk. These developments in the coronavirus crisis, which magnified risks generally and cyber risk particularly, accent the importance of the banking system's ongoing preparedness to cope with the risks that it faces, including stress testing of various kinds. The Banking Supervision Department will continue to track and monitor the full set of risks that the banking system has to confront, including cyber risk.

Sources

Darrell Duffie and Joshua Younger, "Cyber Runs: How a Cyber Attack Could Affect U.S. Financial Institutions." Hutchins Center on Fiscal & Monetary Policy at Brookings, Working Paper n.51. June 2019.

Jason Healey et al., "The Future of Financial Stability and Cyber Risk." The Brookings Institution Cybersecurity Project, October 2018.

Anil K. Kashyap and Anne Wetherilt, "Some Principles for Regulating Cyber Risk." AEA Papers and Proceedings. Vol. 109, 2019.