Preparation for and Response to a Ransomware Attack in the Organization

Cybersecurity Best Practices

B.07

Volume B:
A technical approach

IDB

INCD
Israel National
Cyber Directorate

This document was originally published by the Israel National Cyber Directorate (INCD) in Hebrew. Its translation into English was carried out by the cybersecurity team of the Innovation in Citizen Services (IFD/ICS) division of the Inter-American Development Bank (IDB), and it is included as a chapter of the "Cybersecurity Best Practices" collection.

The reader should keep in mind that cybersecurity is a rapidly evolving field. Although these documents reflect established principles, they may be periodically updated as necessary to reflect developments in this field. Additionally, while every effort has been made to present the recommendations and resources in a way that is universally applicable to organizations around the world, the reader may find references that are specific to Israel's cyberecosystem and context (such as the amounts indicated in New Israeli Shekels [NIS], or references to Israeli law or government agencies).

The original document is available at: **https://www.gov.il/he/pages/rasomware_org**. Please note that it includes the following disclaimer:

"This document has been prepared by the National Cyber Directorate in order to promote cybersecurity in the Israeli economy. All rights reserved to the State of Israel - National Cyber Directorate. The document has been prepared for the benefit of the public. Duplication of the document or its incorporation in other documents will be subject to the following conditions: the acknowledgment of authorship of the National Cyber Directorate in the format that appears below; the use of the latest version of the document; not making changes to the document. The document contains information of a professional nature, the implementation of which will require knowledge of the systems and adaptation to their characteristics by a professional in the field of cybersecurity. Any comments or references can be sent by email to: tora@cyber.gov.il."

Contents

Foreword

Digital Transformation and the Challenges of Cybersecurity

As digital transformation continues to expand throughout the world, governments, organizations, individuals, and even objects are increasingly connected to the internet. Although digitalization offers undeniable benefits, such as efficient public service delivery, economic growth, and essential connectivity, it also contributes to our growing collective exposure to cybersecurity risks. Recently, the global COVID-19 pandemic has been an important driver of this phenomenon. As a result of widespread social distancing policies, the number of e-commerce transactions and online personal communications grew sharply in a short period of time, along with the number of employees who began teleworking for the first time. In this unprecedented situation, many internet users undertook novel online interactions without enough awareness of the security risks involved. Organizations had to quickly adapt to these challenges by setting up fully remote workflows, often without all of the necessary security measures in place or appropriate guidance to employees.

Cybercriminals are quick to exploit the uncertainty and vulnerability of unsuspecting individuals. Phishing and other social engineering scams proliferated, taking advantage of the global need for information related to the pandemic and the massive use of videoconference applications. In April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 in only a week. Hackers posing as the World Health Organization sent phishing emails and massively spread malicious links to fake videoconference meetings and attachments containing malware. According to the Check Point Research 2021 Security Report, in the first few months of 2020, almost a million attack attempts against Remote Desktop Protocol (RDP) connections, widely used among organizations for employees' remote connections, were observed every day. In fact, RDP attacks were the most popular form of cyberattack, surpassing even phishing emails. In the second half of the year, as more organizations strengthened the security of their remote platforms, hackers focused their efforts on exploiting vulnerabilities in employees' private assets and remote access devices to penetrate their organizations. Although such threats were maximized by this global context, they are not novel and will not go away; we continue to live in an environment of heightened risk, which is particularly serious in regions of the world where cybersecurity policies and technology are less developed and where citizen education and awareness around this issue are lacking. In other words, although the shifts due to the COVID-19 pandemic may revert to what they were before the pandemic, they have brought to light the urgent need to strengthen individual and collective protections against cyberrisks.

Strengthening cybersecurity is essential to safeguard citizens' rights to privacy and property in the digital sphere, promote citizens' trust in digital technologies, and support economic growth through safe digital transformation. In particular, citizens must be assured that the digital systems they use for their personal or professional activities, as well as those that involve their personal data, possess adequate security measures to guarantee the integrity, confidentiality, and availability of their information and the services that they need. Moreover, security breaches have a significant negative economic impact. A recent report by McAfee estimated that cybercrime costs the world economy around US$6 trillion annually, or 0.8 percent of global GDP.

Israel: A Global Leader in Cybersecurity

Israel's innovation and entrepreneurship ecosystem is globally recognized as one of the most vibrant in the world, earning it the name Startup Nation. According to the March 2021 OECD Science and Technology Indicators, Israel is the country that invests the highest percentage of its GDP (4.9 percent) in research and development (R&D). The country is host to more than 300 research and development and innovation (R&D&I) centers of multinational companies. Of these, dozens are dedicated to cybersecurity.

It is no surprise that 40 percent of all private investment in cybersecurity worldwide takes place in Israel, which also has one of the world's largest private ecosystems in this area, second only to that of the United States. According to 2021 data, in that year US$8.8 billion were invested in around 131 Israeli companies from this sector, and more than 40 were acquired for a total of US$3.5 billion. Israel has more than 500 cybersecurity startups, and by 2021, 33 percent of the world's "unicorns" were Israeli. Overall, Israel's export of cybersecurity products was estimated in 2020 at US$6.85 billion.

The Israel National Cyber Directorate (INCD) is responsible for securing Israel's national cyberspace and for establishing and advancing its cyberresilience. The INCD operates at the national level to constantly raise the level of security of organizations and citizens, to prevent and manage cyberattacks, and to strengthen cyberemergency response capabilities. Its positioning as part of the Prime Minister's Office clearly demonstrates the centrality and importance of its responsibilities. Its goals include to prepare and enable the Israeli private sector and general public to protect themselves from cyberthreats by adopting cybersecure technologies, publishing best practices, training personnel, and raising awareness. Furthermore, it aims to establish and strengthen the cyberscience and -technology base by developing highly qualified human capital, supporting advanced academic research, engaging in deep technological R&D, and fostering the cyberindustry. The INCD strives to maintain a protected, safe, and open cyberspace for all of the State of Israel's population and businesses and to facilitate the country's growth and its scientific and industrial base.

The State of Cybersecurity in the Latin American and Caribbean Region

The Inter-American Development Bank (IDB) carries out periodic assessments to capture the evolving capacities of its member states to defend themselves against the growing threats in cyberspace. The 2020 Cybersecurity Report, "Risks, Progress, and the Way Forward in Latin America and the Caribbean," developed in partnership with the Organization of American States (OAS), showed that countries were at varying stages of development in their preparedness to face cybersecurity challenges, but generally still had ample room for improvement.

While in 2016, the year of the report's first edition, 80 percent of the countries in the region did not have a national cybersecurity strategy in place, this number had only fallen to 60 percent by 2020. Furthermore, only a few countries manage the exposure of their critical infrastructure, such as their energy, healthcare, telecommunications, transportation, water supply, and financial sectors, to cyberattacks. As revealed by the 2020 report, only 7 countries of the 32 assessed had a critical infrastructure protection plan in place. This is one of the most worrisome findings of all, considering the catastrophic impact that attacks on these sectors could have not only on national economies, but on the lives of all their citizens.

In terms of countries' capacity to manage and respond to cybersecurity incidents, the same study found that 63 percent of countries had security incident response teams in place, such as computer emergency response teams (CERTs) or cybersecurity incident response teams (CSIRTs). However, of the 20 countries that did, only 3 had reached advanced maturity in their ability to coordinate such responses. In fact, 23 out of the 32 countries were still in an initial stage of maturity in this respect. This finding underscored the general need for countries to strengthen the capacity of their teams to effectively coordinate their responses to cyberincidents. Moreover, the report examined the availability of educational and training opportunities in cybersecurity and found that fewer than half of the countries in the region offered formal education in cybersecurity, such as postgraduate, master's, or technical degrees. Needless to say, having sufficient trained professionals is essential to design and implement the cybersecurity policies and measures that are necessary to ensure a country's resilience in the face of increasingly sophisticated and complex cyberattacks.

The Inter-American Development Bank's Support to Strengthen Cybersecurity Capacity in the Region

For the past few years, the IDB has actively supported the region in the development of cybersecurity capacity, the design and implementation of national-level cybersecurity policies, and the strengthening of cybersecurity capabilities in the sectors it helps develop. This support takes a number of forms. The IDB has provided financial assistance amounting to tens of millions of dollars to develop national cybersecurity capabilities through more than 15 public sector investment loan operations, as well as significant additional funding to ensure the cybersecurity of digital transformation investment projects.

It also provides technical guidance and conducts cybersecurity projects across the region through consultancies, assessments, and tailor-made cybersecurity-strengthening projects on topics that include critical infrastructure protection, cybercrime and forensic analysis, design and strengthening of CSIRTs and security operations centers (SOCs), and national and sectoral cybersecurity strategies. In addition, the IDB has made substantial efforts to provide opportunities for Latin American and Caribbean professionals to strengthen and update their skills in this field by regularly offering workshops and training opportunities. These have included two-week cybersecurity executive courses, offered jointly with the Hebrew University of Jerusalem, as well as tailor-made courses on critical infrastructure protection and others targeted for specific sectors. Finally, the IDB has produced several high-impact publications dealing with national and sectoral cybersecurity issues, and continues to update and add to this body of knowledge regularly.[1]

1. See the website of the Data and Digital Government Cluster (DDG) of the IDB's Innovation in Citizen Services (ICS) division: **https://www.iadb.org/en/who-we-are/topics/modernization-state/data-and-digital-government**.

The IDB and the INCD: Joining Forces

The challenges of cybersecurity, like those of the internet itself, are global. Thus, sharing the knowledge and tools to meet these challenges benefits everyone. In recognition of this reality, the INCD and the IDB have partnered to make Israel's expertise in this area accessible to LAC countries. This collaboration has supported the LAC region in the form of executive and technical trainings on advanced cybersecurity topics, cutting-edge conferences for LAC public officials and professionals in the field, and innovative technical assistance projects. This publication is a product of this collaboration. It consists of a series of cybersecurity methodological guides for organizations, developed by the INCD in light of its analysis of risks, attack methods, cyberincidents, and globally accepted standards. These guides have been translated into Spanish and English as a joint activity of both organizations. They are being made available in these languages with the aim of providing access to this body of knowledge to audiences throughout the LAC region and contributing to strengthening cyberresilience in the region.

The challenge of protecting the digital space will continue to grow, along with the need for proven expertise to confront it. The insights contained in these guides are a resource to promote much-needed professional training in cybersecurity in the LAC region. These guides will contribute to raise organizational standards, promote greater awareness and a culture of cybersecurity within organizations and among the general public, and inform decision makers, managers, and leaders in their cybersecurity initiatives. It is our hope that these guidelines will serve as a roadmap for professionals and leaders throughout the LAC region, working together to build a more secure and prosperous future.

Acronyms

Acronym	Definition
BCP	Business continuity plan
CIO	Chief information officer
CISO	Chief information security officer
DDoS	Distributed denial of service
DFIR	Digital forensics and incident response
DR	Disaster recovery
INCD	Israel National Cyber Directorate
IOA	Indicator of attack
IOC	Indicator of compromise
IOE	Indicator of exposure
MDR	Managed detection and response
MSSP	Managed security service provider
RPO	Recovery point objective
RTO	Recovery time objective
SLA	Service level agreement

Introduction

Ransomware is a form of malware which is intended to deny the victim access to the cyberasset and the information stored within it. As a condition for removing the denial of access, the attacker may impose various conditions on the victim, such as a demand to pay a ransom.

For organizations in the economic sector, a ransomware attack might be a highly significant cybersecurity event. As part of the attack, the attacker often encrypts the organization's information and makes the removal of the encryption conditional upon receiving a reward, such as the transfer of cryptocurrency to the attacker. In other words, the attacker blackmails the organization, demanding a reward as a condition for removing the encryption. If the organization does not comply with the attacker's demands, and the organization has no effective way of restoring the information, the organization might suffer irreversible damage, including bankruptcy.

In recent years attackers in cyberspace have been making use of a more advanced attack model when using ransomware called "double extortion," where the model is based on two main attack phases. In the first stage, the attacker leaks sensitive/confidential information from the organization. In the second stage, the attacker uses encryption to prevent access to the cyberassets and to the organizational information, following which the attacker provides the terms under which the denial of access will be lifted. The advantage of this model for the attacker is that even if the organization manages to restore the information and the cyberassets, the victim's fear of the sensitive/confidential information being leaked (and the resulting consequences) might motivate the victim to agree to the attacker's demands.

Lately several cases have come to light in which an even more advanced attack model has been used called "triple extortion," in which the attacker uses a model with three main attack stages. In the first stage, the attacker leaks sensitive/confidential information from the organization. In the second stage, the attacker uses encryption to prevent access to the cyberassets and to the organizational information, following which the attacker provides the terms under which the denial of access will be lifted. In the third stage, the attacker contacts third-party entities (such as the organization's customers) and demands a ransom payment in return for non-disclosure of their sensitive/confidential information, or the attacker threatens to launch another attack against the organization, such as a Distributed Denial of Service (DDoS) attack, unless the attacker's demands are met. The advantage of this model for the attacker is that even if the organization manages to restore the information and the cyberassets, the organization's or the third-party entity's fear of the sensitive/confidential information being leaked (and the resulting consequences), along with the possibility of yet another attack, might motivate them to give in to the attacker's demands.

In this way, even if the organization succeeds in recovering from the ransomware attack, there still remains a high level of exposure for the organization and for the information of third parties (such as the organization's customers).

It must be noted that in recent years, attackers in cyberspace have begun adopting a Ransomware as a Service (RaaS) approach, which gives attackers with limited technological capabilities, or attackers that are not inclined to invest considerable resources in research and development, the possibility of gaining access to advanced attack tools.

There are several reports from around the world about the use of ransomware that utilizes several independent encryption layers, each with a unique decryption key, and requires that a separate payment be made in order to obtain each such key. Furthermore, there is an initial report regarding the possibility of the existence of more advanced business models on the part of attackers using ransomware—for example, the sale of a decryption key that has been parametrically adjusted. Parameters might be the volume of information to be restored, the file types which can be restored, the decryption rate/expected decryption duration, metadata-only decryption, or full raw data decryption.

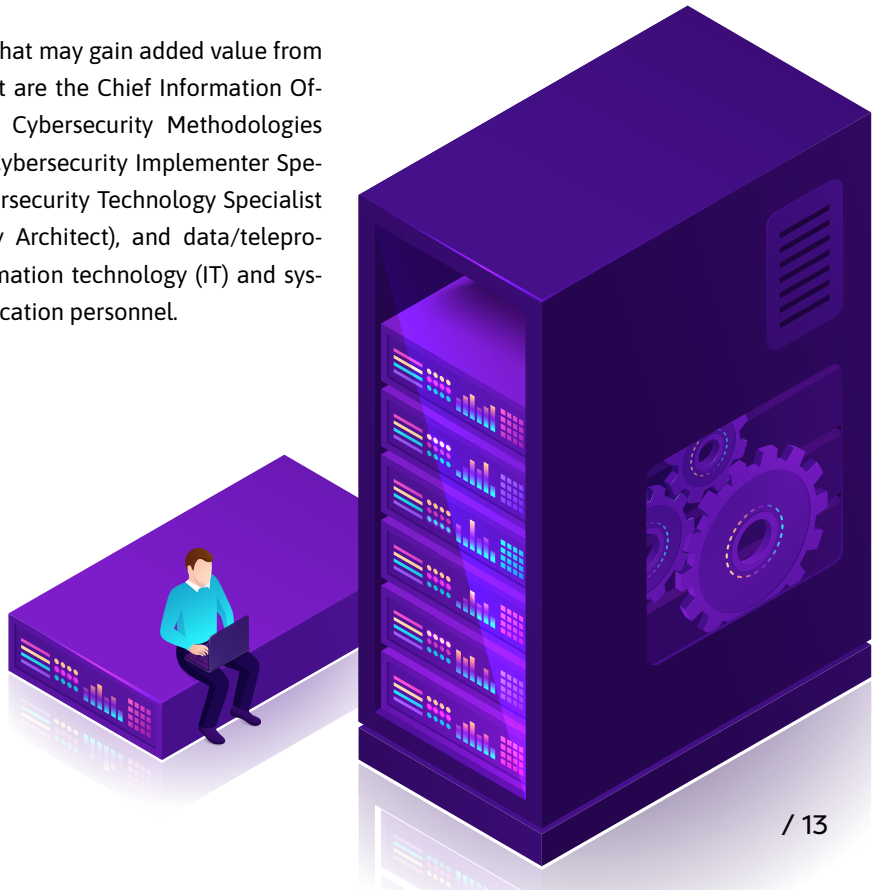
/01.
Goals and Objectives

This document is intended to assist the Chief Information Security Officer (CISO) and decision-makers within the organization in preparing for and coping with a ransomware event in the organization.

/02.
Target Audience

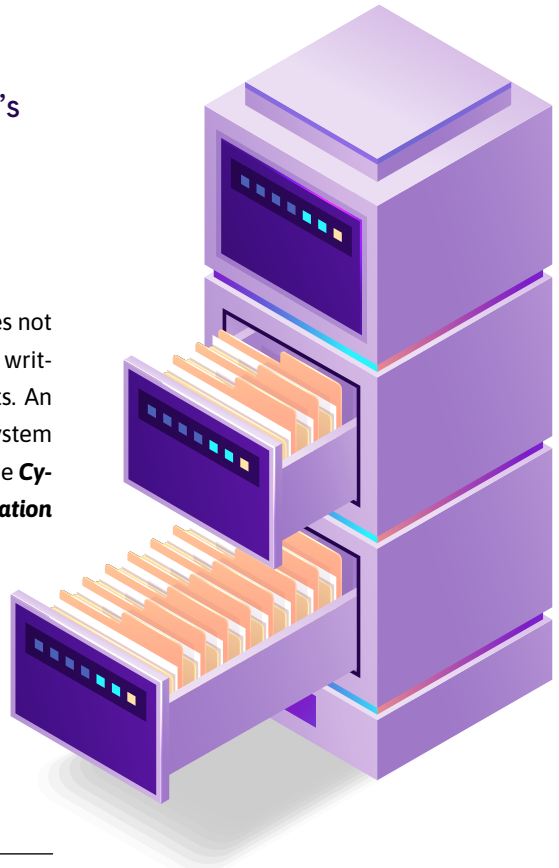
This document was written for the organization's CISO and for the organization's decision-makers.

Other actors that may gain added value from this document are the Chief Information Officer (CIO), a Cybersecurity Methodologies Specialist, a Cybersecurity Implementer Specialist, a Cybersecurity Technology Specialist (Cybersecurity Architect), and data/teleprocessing/information technology (IT) and system communication personnel.



/03.
Document Scope

This document focuses on recommendations to improve the organization's ability to prepare for and respond to a ransomware event.



It is worth noting that this document does not address subjects on which the INCD has written and published dedicated documents. An example is specific protection of the system and infrastructure, which is covered in the ***Cyberdefense Methodology for an Organization 2.0***, written and published by the INCD.[2]

2. The ***Cyberdefense Methodology for an Organization 2.0*** is available as part of this "Cybersecurity Best Practices" collection through the following link: **https://www.gov.il/BlobFolder/generalpage/cyber_security_methodology_2/en/ICDM%20V2.pdf**.

/04.
Threats Resulting from a Ransomware Attack

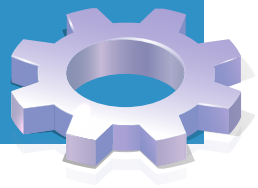
This section outlines the main threats from a ransomware attack.

Table 1. Main Threats Resulting from a Ransomware Attack

No.	Threat	Description
1	Denial of access to information	a. An attacker might encrypt the information, thereby preventing authorized access to the information. b. An attacker might delete organizational information, including existing backups.
2	Data scrambling	An attacker might scramble data, thereby impairing data reliability (for example, by changing the order of appearance or location of records in databases).
3	Leaking of sensitive/ confidential information	An attacker might leak sensitive/confidential information as a preliminary stage of activating the ransomware or in the course of its activation.

No.	Threat	Description
4	Blackmail	a. An attacker might demand a financial or other ransom as a condition for releasing the encryption key or the scrambling key. b. Double extortion: an attacker might threaten to launch another threat concurrently with the ransomware (such as a DDoS attack) in order to amplify the damage. c. Triple extortion: the attacker might contact third-party entities demanding ransom, stating that if the ransom is not received their sensitive/ confidential information will be leaked. d. Reverse extortion: an attacker might insert "incriminating information" within the organization and demand a ransom as a condition for non-exposure/non-disclosure.

There are cases where internal players (such as system personnel) have deliberately activated ransomware against the organization which employed them. Therefore, the organization is advised to ensure that it has a clear plan for coping with an insider threat.[3]



3. For more information, see the document ***Organizational Coping in Cyberspace: The Insider Threat*** available within this "Cybersecurity Best Practices" collection through the following link: **https://www.gov.il/BlobFolder/generalpage/coping_thret/en/Organizational%20coping%20in%20the%20cyber%20space.pdf**.

/05.
Recommended Courses of Action against a Ransomware Event in the Organization

This section reviews the recommended courses of action for preparing for and coping with a ransomware event within the organization.

Table 2 below provides an exhaustive list of actions that must be implemented to prepare for a ransomware event.

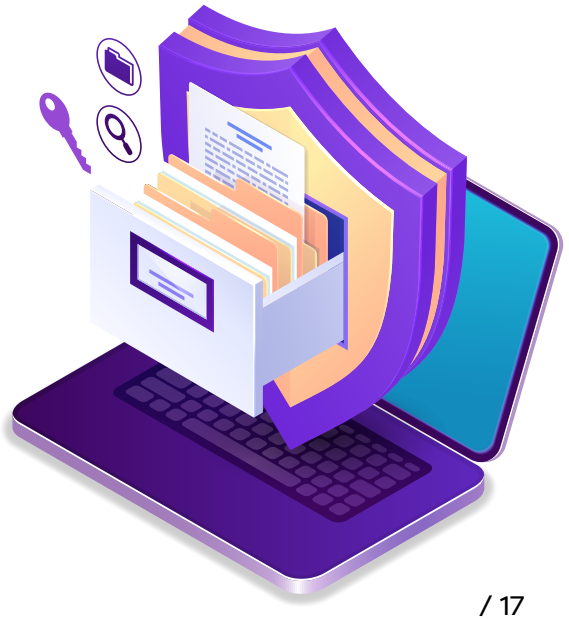


Table 2. List of Recommended Tasks to Prepare for a Ransomware Event

No.	Subject	Description	Responsible actor
General			
1	Cyberintelligence	Is the organization receiving intelligence information on ransomware attacks? How does the organization use this information to improve its protective setup and risk management process? Does the organization have prior knowledge of places where they may obtain information/support if the need arises? For example, **The No More Ransom Project**.[4]	Cybersecurity team
2	Service agreements	Does the organization have service agreements which will be of help in case of a ransomware event, and have relevant indices been incorporated into the service agreement? How is supplier compliance with the defined indices examined? In this context, the authority of the organization in case of a cybersecurity event originating from an entity within the organization's supply chain must be taken into consideration.	Information systems division
General (cont.)			
3	Human capital	Does the organization have suitable manpower to prepare for and cope with a ransomware event on a 24/7 basis? If not, is there a service agreement with a relevant supplier (such as someone specializing in digital forensics and incident response [DFIR] or in restoring information)?	Information systems division Cybersecurity team
Business continuity and backups			
4	Crisis management team	Does the organization have a crisis management team? If not, who is going to be a member of this team? Is a service agreement necessary with a third party that will be able to assist when the need arises? Who is authorized to escalate and under which conditions?	Organization management
5	Business continuity	Is there a business continuity plan (BCP)? Has a ransomware attack been included in the list of scenarios to be addressed? Does a steering committee discuss the scenarios periodically? Are stress scenarios such as deletion or loss of all organizational information addressed? Have accepted indices been defined for all of the core assets/processes (such as a recovery point objective [RPO]/recovery time objective [RTO])? What is done with the rest of the company employees during a crisis? Is the work routine maintained or does the daily routine have to be altered?	Organization management

4. For more information on this project, visit: **https://www.nomoreransom.org/en/index.html**.

No.	Subject	Description	Responsible actor
Business continuity and backups (cont.)			
6	Alternative website (disaster recovery [DR])	Does the organization have a Disaster Recovery Plan? Does the organization have an alternative website? If not, why not? When will the alternative website be activated? How long is it going to take to activate the alternative website? Does the alternative website assure compliance with the indices which have been defined for business continuity?	Organization management
7	Backups	Is the backup setup resistant to cyberattacks? How is the backup integrity checked? Does the backup policy fulfill the requirements of the BCP? Is there an agreement with a service provider that will be able to help in case of a malfunction/problem when performing a recovery? For more information, see: ***Integrating Principles of Cybersecurity in the Backup and Recovery Processes***.[5]	Information systems division
Testing readiness and competency			
8	Cybersecurity drill	Has the organization carried out a drill of the cyberprotection setup in the past year, addressing common ransomware scenarios? If yes, what were the findings? Did the drill include escalating in case this is necessary? Have the lessons learned been implemented? Have third-party entities, such as the managed security service provider (MSSP) and managed detection and response (MDR), been included? Does the Disaster Recovery Plan include a special drill chapter? Are there other issues that need to be drilled? For more information, see the document ***Cyberpractice: Creating and Conducting Cybersecurity Exercises for the Organization***.[6]	Crisis management team
9	Reducing the attack surface	Has the organization implemented the controls of the most up-to-date version of the ***Cyberdefense Methodology for an Organization****?* If not, what is the target date? What resources need to be allocated to complete effective implementation? Are there obstructions which need to be dealt with to make the process a success?	Cybersecurity team

5. The document ***Integrating Principles of Cybersecurity in the Backup and Recovery Processes*** will be available in the future within this "Cybersecurity Best Practices" collection.

6. The document is available within this "Cybersecurity Best Practices" collection through the following link: **https://publications.iadb.org/en/cyberpractice-creating-and-conducting-cybersecurity-exercises-organization-cybersecurity-best**.

No.	Subject	Description	Responsible actor
Testing readiness and competency (cont.)			
10	Resiliency testing	Does the organization conduct periodic resilience tests, taking into consideration ransomware-type attack scenarios?	Cybersecurity team
11	Scanning for vulnerabilities/ weaknesses	Does the organization conduct scans for vulnerabilities/weaknesses, taking into consideration the indicators of exposure (IOEs) that ransomware frequently exploits?	Cybersecurity team
12	Cybersecurity event response procedure	Does the organization have a cybersecurity event response procedure? Is the procedure up to date? Who is responsible for updating the procedure? Has the procedure been written according to up-to-date methods in this field? Is there a hard copy of the procedure, which can be used in the event of the information and communication technology (ICT) infrastructure becoming unavailable?	Cybersecurity team
13	Continuous monitoring	Does the organization have continuous, continual control processes? If not, does the organization have a suitable service agreement with an MSSP/MDR? Are there appropriate indices for evaluating effectiveness?	Cybersecurity team

As a rule, the crisis management team should include the following representatives, as a minimum: Chief Executive Officer (CEO) or Deputy CEO, a management member representing the customer-facing business side, legal, CIO, CISO, and the spokesman's office. Appointment of a substitute for each one of these should also be considered, in case anyone in the above roles is unavailable.

Table 3 provides a list of actions to be implemented in response to a ransomware event.

Table 3. List of Recommended Tasks for Coping with a Ransomware Event

No.	Subject	Description	Responsible actor
Identification: initial inquiry as to the feasibility of a cybersecurity event, including taking immediate measures to deal with it			
1	Cybermonitoring	Who is responsible for detecting and identifying the ransomware? Who is responsible for ensuring this is not a false alarm or operational malfunction? How reliable is the source of the report (the reporting system or device)? Is there a procedure for dealing with cybersecurity incidents? According to the procedure, what are the steps to be taken? Who is responsible for carrying out each step? Who is responsible for documenting the actions performed as part of the event (maintaining an event log)? Have familiar indicators of compromise (IOCs) been identified or is there an anomaly or unusual behavior which needs to be investigated? Have measures been taken to improve the quality of the monitoring?	Cybersecurity team
Analysis: conducting a thorough, detailed inquiry of the event in order to adopt proper courses of action, while considering potential alternatives for halting and responding to the event			
2	Corporate governance	Is there a process for rapid procurement if this becomes necessary?	Information systems division Purchasing
3		Is there a BCP? Who is responsible for activating and implementing it? What are the indices which have been specified for each process/cyberasset (RPO/RTO, etc.)? Who updates the crisis management team? What happens if that person is unavailable?	Organization management
4		Is there a procedure for dealing with a crisis? According to the procedure, what are the steps to be taken?	Crisis management team
5	Initial damage control	Are the backups in good order? How do we know that the backups are in good order?	Information systems division
6		Which cyberassets have been damaged? Are there third-party entities that have been or will be impacted? Is this a smoke screen concealing a different attack? Have familiar IOEs been exploited (according to cyberintelligence, etc.)? Have new IOEs been identified? Is the means of payment traceable?	Cybersecurity team

No.	Subject	Description	Responsible actor
Analysis: conducting a thorough, detailed inquiry of the event in order to adopt proper courses of action, while considering potential alternatives for halting and responding to the event (cont.)			
6	Initial damage control (cont.)	What is the extent and quality of the information that has been hit (cardholder data, controlled unclassified information, protected health information, personally identifiable information, etc.)? Has the attacker removed the information from the organization's premises/ boundaries? Is there a demand for payment? Who is responsible for ensuring that the evidence is being collected and stored in accordance with the chain of custody principle? How is this accomplished? For how long must evidence/forensic information be kept, and what is the scope of the storage (all of the cyberassets, servers only, damaged cyberassets, full image, configuration settings only, suspected files only, etc.)?	Cybersecurity team
7		What type of ransomware is it? What are its attack capabilities? What is the entry method? How can the ransomware be removed? What is the degree of certainty that this can be done? Has leaked information been posted on the internet, social media, or the darknet?	Crisis management team

No.	Subject	Description	Responsible actor
Analysis: conducting a thorough, detailed inquiry of the event in order to adopt proper courses of action, while considering potential alternatives for halting and responding to the event (cont.)			
7	Initial damage control (cont.)	What is the attacker's goal (money, damage to reputation, etc.)? Who is the attacker (assuming they can be identified)? Has the event gained publicity outside the organization? How is disinformation addressed? Have customers/suppliers complained to the organization? Have claims been filed against the organization and/or its officers? Have complaints/accusations been made against the organization and/or officers? What is going to happen if payment is not made? How can compensation/indemnity or relevant services be obtained from the insurance company?	Crisis management team
8		If the event originated from an entity within the organization's supply chain, who is authorized to communicate with that entity? What are that entity's duties toward the organization? Is it possible to send a DFIR team from the organization to that entity?	Crisis management team

No.	Subject	Description	Responsible actor
Analysis: conducting a thorough, detailed inquiry of the event in order to adopt proper courses of action, while considering potential alternatives for halting and responding to the event (cont.)			
9	Manpower	Are the relevant members of the system team available and do they have access to the cyberassets? Is it necessary to augment the system team with third-party resources (such as a backup expert)? If so, what is the service level agreement (SLA)?	Information systems division
10		Should the organization augment the existing team with third-party professionals? If so, is there a contract with those professionals? What is the SLA?	Crisis management team
11		Does the organization have a DFIR team? If so, what is the organization level agreement (OLA)? If not, is there a contract with external professionals? And if not, who will we summon? What is the SLA?	Cybersecurity team
12	Cyberinsurance	Does the organization have valid cyberinsurance? What is the name of the insurance company? Who is the organization's insurance agent? Does the existing insurance cover cybersecurity issues? If so, what services does the insurance include? What is the SLA for each service?	Crisis management team

No.	Subject	Description	Responsible actor
Analysis: conducting a thorough, detailed inquiry of the event in order to adopt proper courses of action, while considering potential alternatives for halting and responding to the event (cont.)			
12	Cyberinsurance (cont.)	Are the external entities the organization is interested in summoning recognized and authorized by the insurance company? Does insurance company approval need to be obtained before continuing an action? What is the size of the compensation/indemnification? Is it worthwhile to contact the insurance company? Who in the organization is authorized to be in contact with the insurance company/agent? Is the agent/insurance company available for consultation at this time? Do we have a specific point of contact within the insurance company who is available 24/7?	Crisis management team
13	Inspecting the backups	Are the backups in good order? How do we know that the backups are in good order? What is the date of the last backup? How long will it take to restore the asset/information? How much information/work time will we lose after the information has been restored? What is the restore sequence? What is this sequence based on?	Information systems division

No.	Subject	Description	Responsible actor
Analysis: conducting a thorough, detailed inquiry of the event in order to adopt proper courses of action, while considering potential alternatives for halting and responding to the event (cont.)			
13	Inspecting the backups (cont.)	What will happen if the backup copy is found to be defective or infected? Can built-in capabilities within the storage network/virtual environment setup be used to restore a specific "snapshot"? Is it possible to bring in an additional backup system to shorten the restore time? Does the system team have licenses, images, and software from a reliable source that will facilitate the performing of a restore or install from scratch if necessary? Would the restore function destroy required evidence, and if so, what measures are required to protect it?	Information systems division
14		Do the organization's backups contain malware? How can we ensure that the restored information does not contain malware?	Cybersecurity team
15	DR site	What is the level of readiness and fitness of the DR site?	Information systems division
16		Is there a need to fail over to a DR site? How likely is a failover to be successful, according to the indices that have been specified?	Crisis management team

No.	Subject	Description	Responsible actor
Containment: gaining initial control over the event in order to contain it and stall the exacerbation of its impact on the organization			
17	Reducing the damage effect	Is it necessary to sever the connection to external interfaces such as the internet? What are the potential implications of this? Who is authorized to approve this? Is it necessary to sever the connection to internal interfaces such as the connectivity to the DR site? What are the potential implications of this? Who is authorized to approve this? Is it necessary to disconnect the backup/storage setup from the network? What are the potential implications of this? Who is authorized to approve this? Have affected cyberassets been disconnected from the network? If not, why not? Is it necessary to take additional measures to reduce the attack surface/raise walls? Is this familiar malware? Are there ways of extracting the key? Does the use of the key enable restoration of the information? Does the organization have documentation (logs, history files, other) and other artifacts that can help with the investigation? Does the organization have suitable tools for conducting the investigation? Are there indications as to the level of complexity (for example, stealth capabilities) of the malware? How long has the attacker hold been in effect?	Cybersecurity team

No.	Subject	Description	Responsible actor
Containment: gaining initial control over the event in order to contain it and stall the exacerbation of its impact on the organization (cont.)			
18	Duty to report	Who are the stakeholders to be reported to? Customers? Suppliers? Regulators? What is the reporting channel (email, phone, other)? Is it necessary to use the traffic light protocol (TLP) when transferring information?[7] Is it necessary to verify the successful delivery of the report/notification? What is the time window for reporting? Are there cases where it is necessary to provide updates on the evolution of the event after the initial report? What is the trigger for continued reporting and who is the authorized entity for sending a report? Has the INCD been updated about the event? If not, why not?	Crisis management team

7. For more information on this protocol, see the document ***The Israeli Cyber Emergency Response Team (CERT) Principles of Operation*** available within this "Cybersecurity Best Practices" collection through the following link: **https://publications.iadb.org/en/israeli-cyber-emergency-response-team-cert-principles-operation-cybersecurity-best-practices**.

No.	Subject	Description	Responsible actor
Containment: gaining initial control over the event in order to contain it and stall the exacerbation of its impact on the organization (cont.)			
19	Internal/ external communication interfaces	Will the organization be talking to the media? Does the organization have prepared boilerplate messages to be posted? Who is authorized to talk about the event with the media? Have the organization's employees been briefed about the sensitivity of the issue and the dos and don'ts, and has the circle of personnel handling the event been briefed accordingly in terms of messaging, etc.? Has a transparency process been specified with customers and suppliers regarding the situation? Will information be provided regarding what has happened, the estimated damage, and recommendations for suppliers/customers whose information is at risk? Will they be notified as to what they should do? Will they be informed about how the organization is coping with the event and what is expected to happen? Will they be given a phone number or email they can contact? Have there been reports about the event in the media? Have there been reports about the event on social media? Has the stock value been impacted? Have there been calls from investors? Have there been calls from other entities?	Crisis management team

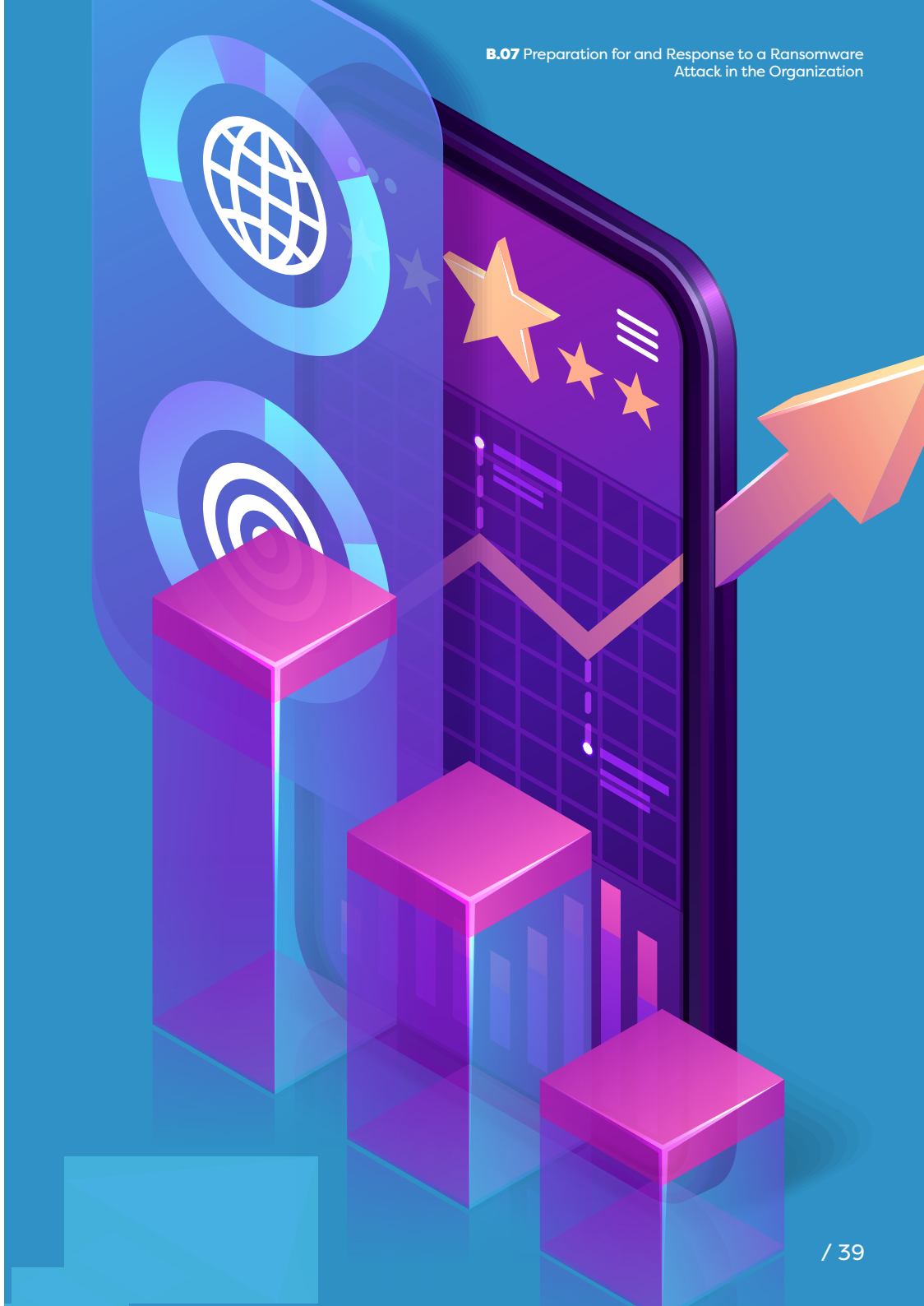
No.	Subject	Description	Responsible actor
Containment: gaining initial control over the event in order to contain it and stall the exacerbation of its impact on the organization (cont.)			
20	Negotiation	Who is in charge of the negotiation? What are the organization's objectives in the negotiations (buying time)? Who is supervising this activity? What is the attacker's goal? Is it possible to stall until the emergency measures have been completed? Are there any special demands from the attacker? Has the attacker uncovered any unique information? What will be done if it is not possible to restore the information? Have any specific instructions been received from a regulator or from any other body?	Crisis management team
Conclusion: neutralizing the attack components within the organizational systems with the intent of minimizing the damage caused by the attack			
21	Malware removal	Has the malware been removed? Are all the cyberassets clean? What can prevent repeat infection of the cyberassets? Are there identifiers (such as indicators of attack [IOAs] and IOCs) that can be calibrated in the security setup? Are there any orderly guidelines for removing the malware? How can it be ensured that the malware has been removed, that there is no additional malware, and that it is not affecting the organizational infrastructure and systems?	Cybersecurity team

No.	Subject	Description	Responsible actor
Conclusion: neutralizing the attack components within the organizational systems with the intent of minimizing the damage caused by the attack (cont.)			
22	Malware removal (cont.)	Who is responsible for tracking/controlling the execution of the required tasks? What will be done if it is not possible to restore the information? Have any specific instructions been received from a regulator or from any other body?	Crisis management team
23		Does the system team know what it must do to remove the malware? Does the system team have to reinstall the operating systems from scratch? Does the system team have to remove the malware using scripts, or using a different method? Is it necessary to back up information which has been encrypted, such that it will be possible to restore it in the future in case the key is discovered?	Information systems division
24	Removing leaked information	Is it possible to remove information that has been leaked on the internet, darknet, or social media? How is this done?	Cybersecurity team
25	Damage control	What is the damage which has been inflicted on the organization so far? What are the short-term and long-term effects? Can the damage be minimized? What happens if it is discovered that the event has not ended and that it might even have escalated?	Crisis management team

No.	Subject	Description	Responsible actor
Resumption: return of the organization under attack to normal functioning and full-scale business			
26	Restoration of information	Is the rate and quality of the restoration compliant with the required standards? If not, what can be done to improve the situation? Were the restoration activities completed successfully from the system team's perspective?	Information systems division
27		Is the environment to which the information is going to be restored free of malware? Who is responsible for checking that the attacker does not have any further hold on the organizational network for repeat infection and escalation of the event? How will this be checked? Are there indications (such as IOAs, IOCs, or tactics, techniques, and procedures [TTPs]) that the event is recurring?	Cybersecurity team
28		Who are the business entities that check that the restore has functioned as expected, and that the assets are fit for work?	Crisis management team
29	Cyberinsurance	Is it financially worthwhile to claim compensation/indemnity from the insurance company? How can compensation/indemnification be obtained from the insurance company due to the damage that has been caused? What is done if the insurance company refuses to pay?	Crisis management team

No.	Subject	Description	Responsible actor
Resumption: return of the organization under attack to normal functioning and full-scale business (cont.)			
30	Supervised return to routine	Are there conventional processes for returning to supervised routine (a period during which intensified measures are taken to detect and identify an attacker)? How long will this period last (75 days as a minimum is recommended)? What happens if it is discovered that the event has not ended and that it might even have escalated?	Crisis management team
31	Conducting a debriefing process and drawing conclusions	Is the debriefing investigation done by an independent entity that is free of internal pressures? What are the deficiencies in the security setup that allowed the attack to succeed? What has to be improved in the security setup? Who is responsible for improving the security setup? How can it be verified that the protection controls are effective in order to prevent the event from recurring? Who is responsible for conducting a cybersecurity drill to test the organization's readiness and competency, and when will it be performed?	Cybersecurity team
32		Who is in charge of the debriefing and when? What are the debriefing's findings? What has to be done to prevent the event from recurring?	Crisis management team

No.	Subject	Description	Responsible actor
Resumption: return of the organization under attack to normal functioning and full-scale business (cont.)			
32	Conducting a debriefing process and drawing conclusions (cont.)	Who is responsible for implementing the recommendations from the debriefing? How does the organization verify that the recommendations from the debriefing have been implemented effectively? Who is responsible for allocating resources to the upgrade/enhancement plan for the computing infrastructures? Do the findings from the debriefing have to be sent to the regulator or to any other entity? Do the findings have to be published in public reports (such as a stockholders report)? If so, what information is required and how can the unnecessary disclosure of sensitive/confidential information be prevented?	Crisis management team
33	Rebuilding the reputation	What has to be done to rebuild the organization's reputation (recovering customers' and investors' confidence)? Who is responsible for doing this? What resources are required? How can it be ascertained, at the end of this activity, that the rebuilding efforts have been successful?	Crisis management team
34	Return to normal routine	When can "return to normal routine" be declared? Are there any regulatory sanctions in place against the organization or its officers? Who is handling them? Are there any lawsuits against the organization or its officers? Who is handling them?	Crisis management team



Appendices

Appendix 1. Workflow for Preparing This Document

This section will share with the reader how this document was developed, the factors involved in the writing process, and how feedback on the content is being received in order to improve transparency and proper disclosure of the process and all the different factors involved.

How This Document Was Created: Market Survey, Syllabus, Worldwide Comparison

01

Examination of documentation and standardization from around the world such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), etc. (the primary examples are presented in **Appendix 2: Applicable Documents**).

02

Examination of accepted publications in the field (the primary examples are presented in **Appendix 2: Applicable Documents**).

03

Public feedback and comments on the drafts of the document that have been published:

- Mr. Mario Lichtman
- Atty. Vered Zlaikha

Appendix 2. Applicable Documents

This appendix contains the sources of information used for the preparation of this document.

Sources of Information in English

Israel National Cyber Directorate (included in this "Cybersecurity Best Practices" collection)

- Cyberdefense Methodology for an Organization 2.0. Available at: **https://www.gov.il/BlobFolder/generalpage/cyber_security_methodology_2/en/ICDM%20V2.pdf**.
- Cyberpractice: Creating and Conducting Cybersecurity Exercises for the Organization. Available at: **https://publications.iadb.org/en/cyberpractice-creating-and-conducting-cybersecurity-exercises-organization-cybersecurity-best**.
- Integrating Principles of Cybersecurity in the Backup and Recovery Processes (available soon).
- Organizational Coping in Cyberspace: The Insider Threat. Available at: **https://www.gov.il/BlobFolder/generalpage/coping_thret/en/Organizational%20coping%20in%20the%20cyber%20space.pdf**.
- Suppliers' Questionnaire to Strengthen the Supply Chain. Available at: **https://www.gov.il/BlobFolder/generalpage/expsupplychain/en/Suppliers%20Questionnaire%20v1.3.xlsx**.

Israel National Cyber Directorate

- National Cyber Concept for Crisis Preparedness and Management. Available at: **https://www.gov.il/BlobFolder/news/cybercrisispreparedness/he/Management%20of%20crisis%20situations%20english%20final.pdf**.

General

- The No More Ransom Project. Available at: **https://www.nomoreransom.org/en/index.html**.
- RTF Report: Combating Ransomware. Available at: **https://securityandtechnology.org/ransomwaretaskforce/report/**.
- Technical Guideline on Incident Reporting under the EECC. Available at: **https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc**.

National Institute of Standards and Technology

- Draft NIST SP 800-137A: Assessing Information Security Continuous Monitoring (ISCM) Programs. Available at: **https://www.nist.gov/news-events/news/2020/01/assessing-information-security-continuous-monitoring-iscm-programs-nist**.
- NIST SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Available at: **https://csrc.nist.gov/pubs/sp/800/137/final**.

Regulations

- Reporting of Technological Failures and Cyber Incidents, Proper Conduct of Banking Business 366, Bank of Israel. Available at: **https://boi.org.il/media/p2ndlmdf/366_en.pdf**.

Standards

- PCI Security Standards

Sources of Information in Hebrew

Israel National Cyber Directorate

- Strengthening User Identification in the Organization's Systems and Infrastructures through the Use of Multi-factor Authentication (MFA). Available at: **https://www.gov.il/he/pages/mfa**.

Legislation

- Archives Law, 5715-1955
- Electronic Signature Law, 5761-2001
- General Data Protection Regulation (GDPR)
- Privacy Protection Regulations (Data Security), 5777-2017
- Prohibition of Money Laundering Law, 5760-2000
- Protection of Privacy Law, 5741-1981

Regulations

- Cyber Guide: Compliance with the Terms of the Cyber-Related Toxins Permit in Industry, Ministry of Environmental Protection. Available at: **https://www.gov.il/he/pages/cyber_industry_toxins_permit**.
- Form for Reporting a Severe Security Event, Privacy Protection Authority. Available at: **https://www.gov.il/he/pages/reporting_security_breach**.
- Legal Position No. 33-105: Cyber-Related Disclosure, Israel Securities Authority. Available at: **https://www.new.isa.gov.il/images/Fittings/isa/asset_library_pic///SLB_105-33_cyber.pdf**.
- Refresher on Duty of Disclosure in the Event of a Cyber Event According to Legal Position No. 33-105: Cyber-Related Disclosure, Israel Securities Authority. Available at: **https://web.archive.org/web/20211229054747/https://www.isa.gov.il/%D7%92%D7%95%D7%A4%D7%99%D7%9D%20%D7%9E%D7%A4%D7%95%D7%A7%D7%97%D7%99%D7%9D/Corporations/Hodaot_segaL/General/Documents/HODAA211220.pdf#search=%D7%93%D7%99%D7%95%D7%95%D7%97%20%D7%90%D7%99%D7%A8%D7%95%D7%A2**.

Ransomware is a form of malware which is intended to deny the victim access to the cyberasset and the information stored within it. For organizations in the economic sector, a ransomware attack might be a highly significant cybersecurity event. If the organization does not comply with the attacker's demands, and the organization has no effective way of restoring the information, the organization might suffer irreversible damage, including bankruptcy.

This publication is intended to assist the Chief Information Security Officer (CISO) and decision-makers within the organization in preparing for and coping with a ransomware event in the organization. Other actors that may gain added value from this document are the Chief Information Officer (CIO), a Cybersecurity Methodologies Specialist, a Cybersecurity Implementer Specialist, a Cybersecurity Technology Specialist (Cybersecurity Architect), and data/teleprocessing/information technology (IT) and system communication personnel.

Cyberspace is a field of opportunities in terms of technological progress, connectivity, integration, and global connection to the internet. But it is also a field of threats and risks. Cyberattacks can harm organizations and inflict significant financial and image damage. To be prepared to defend against cyberthreats, an organization must master a large number of specializations, whether they are technological, organizational, or process centered. The list of documents presented below reflects the state of the collection at the time of publication of this document.

Volume A: A methodological approach

Volume B: A technical approach

- **B.01** Securing Internet of Medical Things (IoMT) Components
- **B.02** Securing Access Point Name (APN) Infrastructure
- **B.03** Hardening Computer Systems
- **B.04** Reducing Cybersecurity Risks in Video Surveillance Cameras
- **B.05** Reducing Cybersecurity Risks at the Organization's Endpoints
- **B.06** Securing Enterprise Resource Planning (ERP) Systems
- **B.07** Preparation for and Response to a Ransomware Attack in the Organization
- **B.08** Reducing Cybersecurity Risks for Industrial Control Systems (ICS)
- **B.09** Cybersecurity Risk Survey Template for Industrial Control Systems (ICS)
- **B.10** Securing Voice over Internet Protocol (VoIP) Infrastructure
- **B.11** Advanced Multi-Factor Authentication against Cybersecurity Threats
- **B.12** Major Cybersecurity Threats of Remote User Support Platforms
- **B.13** Prevention of and Response to Border Gateway Protocol (BGP) Hijacking
- **B.14** Preparation for Distributed Denial-of-Service (DDoS) Attacks
- **B.15** Reducing Cybersecurity Risks in Building Management Systems (BMS)
- **B.16** Cybersecurity through Mobile Device Management (MDM/EMM) Systems
- **B.17** Securing Managed File Transfer (MFT)
- **B.18** Cybersecurity Aspects of Commercial Message Distribution (SMS)
- **B.19** The Israeli Cyber Emergency Response Team (CERT) Principles of Operation
- **B.20** Securing Multimedia Systems
- **B.21** Integrating Principles of Cybersecurity in the Backup and Recovery Processes

Volume C: Secure software development