Ministry of Finance
Cyber, Emergency
& Security Devision

STATE OF ISRAEL
MINISTRY OF FINANCE

Cyber Israel
National Cyber Directorate

Covid 19 Emergency Routine

Financial-Cyber Resilience and Business Continuity Key Guidelines

מרכז סייבר ורציפות פיננסית
Cyber & Finance Continuity Center

Ministry of Finance, Israel

12/4/2020 V3

TLP Green: Limited disclosure, the information can be shared with any recipient that may find it useful.
However, it cannot be shared in public channels as internet websites, social networks, and mass communication channels

Financial-Cyber Resilience and Business Continuity Key Guidelines
Covid 19 Emergency Routine

Background

The ongoing Coronavirus crisis might take long to resolve. Meanwhile, more and more homes become actual work places, as lockdowns challenge business continuity all around the globe. This fast-growing phenomenon directly impacts various infrastructures and infosystems that were originally designed to meet certain demands, which have probably been exceeded by now. However, it also calls for new action to be taken in the field of cybersecurity – such as adequate traffic monitoring, implementation of satisfactory security measures, etc.
There are additional aspects of shifting daily routine that call for urgent modification, such as significant reduction of work force and traffic restrictions, which imply social distancing and self-imposed isolation.
Cyber criminals can take advantage of the entire situation and increase penetration and fraud efforts.

This document's purpose is to suggest guidelines in light of these most exceptional times focusing on manpower, processes and technology.
The information below is not intended to be directional in nature but informative. It does not represent the only approach to any particular issue and there is no guarantee with regard to the accuracy, completeness or suitability of the information.
Users assumes responsibility for the use of the information, and implementing it may require professional work.

Emergency Routine - People

Actions regarding manpower:

- Work in fully separated teams, to prevent team to team infection.
- Maintain high level of hygiene when shifts change or alternatively provide separate work environments for separated teams.
- It is recommended have a qualified replacement for any key stakeholder in the organization -
- Make sure that your supply chain support has been modified to your current needs.
- Identify people that worked for you in the past or that switched roles in the organization. Can they qualify replacements for critical roles in your organization?
- Provide hygiene instructions and hygiene supplies and disinfect the work environment.
- Devise ways to support employees, both in technological and social manner.
- Plan transportation and catering alternatives for your employees in a case of a full, long lockdown.
- It is recommended to allow employees to work remotely from home as much as possible.
- In this pressure situation - be aware to ‘well-being’ and anxiety related issues of your employees, talk with them on a regular basis.

- Periodically share with your employees the organization's decisions, and the impact on them.

Emergency Routine - Processes

Actions regarding processes:

- Situation Report:
    - Collect data and maintain a DB in order to maintain situational understanding.
    - Due to the ongoing updates and dynamic situation, beware of confusion in the analyzed data.
    - Add the following appendixes to the situation report – action items and lessons learned.
    - Execute re-evaluation upon any change (operational, technological or procedural). Make sure to include also major organizational changes.
    - Update the organization's C-Suite and board of directors with the situation report and major implications of the current situation.
    - Maintain a situation report of infected and quarantined personal and contractors. Update senior management with the report.
    - Define an emergency routine activity clock, that includes status updates and periodic discussions on the situational understanding
    - Share lessons learned with organizations from the same sector or from the financial eco-system.
    - Define an exit strategy from the current situation, including: updated risk management, redefinition of organization's digital asset management, evaluation whether to continue and use new technologies that were used during the crisis, update to the identity management system, work plan to address all of the lessons learned, cyber security and penetration tests to make sure that all is back to normal, etc.
- Procedures:
    - Update the emergency procedures according to the developing circumstances.
    - Create new employee training playbooks, in case new employees will need to perform self-training.
    - Document all of the actions and operations that were taken for a the sake of lessons learned.
- Permissions and Confidentiality:
    - In case the organization has a centralized permission management system, look for available authorized employees in order to prevent bottlenecks. Map and document all changes in order to enable rollback.
    - If the permission approval processes require many approvers (more than two people in a parallel or serial manner) –examine your options in case a key stakeholder is missing.

  - If you chose to flatten the permissions mechanism, make sure to create additional controls and monitoring.
- Awareness:
  - Ransomware attacks are becoming more frequent - reinforce your protection mechanism against that.
  - Increase the awareness of your employees and vendors to fraud attacks, and encourage reporting of such events.
  - Since many employees are working from home and additional people (family members) may be in their surroundings – increase employees' awareness to business data confidentiality and privacy.
- Key Vendors:
  - Re-map the critical 3rd party suppliers that are needed for cyber security and business continuity, and ensure that this mapping is accompanied by a detailed contingency plan and a status tracking mechanism.
  - Evaluate alternatives to critical suppliers.
  - Analyze and evaluate bottlenecks, 3rd party suppliers, critical employees and contractors in an ongoing manner, and update the backup plan in case of a critical gap.
  - Evaluate all aspects regarding remote support including suppliers and tech support centers abroad.
- Consider creating of unified support center for employees, focusing on IT, cybersecurity and remote connections issues.

Emergency Routine - Technology

Actions regarding technology:

- Working Remotely:
  - Evaluate the impact of slower communication channels (for any reason), and alternative communication methods with the employees.
  - Focus the risk assessment for remote connection; Enable only the most essential operations.
  - Strengthen the cyber security measurements for remote connections.
  - Update your guidelines regarding accessing the internet from the organization's network.
  - Evaluate solutions for remote connection with multiple screens (i.e. for transaction rooms)
- Passwords:
  - Strengthen teleworkers identification methods.
  - Increase employees' awareness to strong passwords. If possible, work with 2FA.

- Strengthen passwords and identification methods when working from mobile platforms.

- Tools & Equipment:
    - Evaluate supply of tools & equipment for VCs (platform, microphone, speakers, camera). Consider using of organizational secured tools and not private or free tools.
    - Increase awareness and enforcement while using private personal computers when working from home.
    - Prepare for more people working from home, and analyze the new needs – physical equipment, identification tools, connection methods, bandwidth, increased monitoring, etc.
    - Consider tools and means to access core systems remotely.
    - Use a well-defined and formal channel to distribute messages to the employees.
    - Obtain additional HW equipment – of all types and forms.
- Monitoring & Filtering:
    - Increase DLP monitoring in order to prevent significant data leaks.
    - Re-execute risk assessment for any new digital service that is added.
    - Consider hardening policies for mail filtering and interfaces for the entire organization.
    - Run automated keep alive and effectiveness tests of the protection systems.
    - Increase the focus on SW updates, Change Management processes and Assets Management, based on risk and criticality (servers, network equipment, end points, software, etc.).
- OT
    - Evaluate systems that include programable controls. In casas they have critical impact on core or essential systems – develop a backup and redundancy plan (including a manual control option).

Regards,
FC3 - Israel National Financial CERT,
CERT-IL