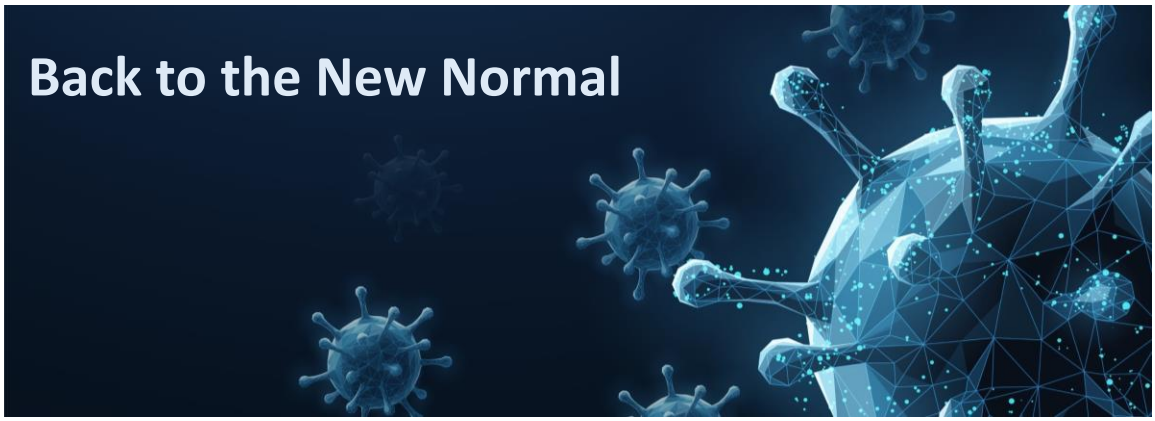

1. The recent changes in work habits require special attention to how we should re-adjust our routine. It is expected that:
    a. There will be **tools and methods we will choose to discard** and go back to former security measures that were kept prior to the Pandemic.
    b. There will be **tools and methods that we have developed** during the crisis **and that we may want to institutionalize** and implement them in order to expand working modes in the organization.
    c. There will be **tools and methods that we will want to develop to achieve a better state of preparedness in a Future crisis** or as lessons from the current crisis.
2. This document aims to highlight main issues that require attention in this era.

3. Document structure:
    a. **A recommended checklist** to perform as part of the return to routine.
    b. Detailed and **in-depth view on the changes** that have occurred.

A Suggested Checklist - Back to the New Normal

4. **Risk management**
    a. During an emergency, it is likely that a more liberal risk management approach is taken. There is a need to **re- examine policy** when going back to routine and look at all the changes in a holistic view.
    b. **Update BCP** programs according to lessons learnt.
    c. Examine changes in the **supply chain, especially** related to IT and OT. Make sure that new supplier are held to your standards.
5. **The boundaries of the organization**
    a. Redefining the **logical boundaries** of the organization (in the level of the network and in the level of the information).
    b. Examine changes done in the **infrastructure** of the network (opening a VLAN, changing DMZ)
    c. Map **external connections** assess their value.

6. **Asset management**
    a. Locate **private appliances** that were used for organizational needs and "clean" \secure them.
    b. An updated **mapping of the organization's assets** (software and hardware).
    c. Map organizational **data saving storage** and assess its value vs. protection measures.
    d. **Cancel unwanted scripts** (or update wanted ones to the organizational level).
    e. **Raise the security standards of newly used capabilities** (applications, sites, licenses, and connections).
    f. **Collaboration software** will probably become part of daily routine. There is a need to examine such software for security measures.

7. **User Management**
    a. **Re-check Identification** of users, accounts and authorizations.
    b. **Manage passwords** and make sure no changes occurred (validity and complexity).
    c. Apply **departure procedures on workers that left the organization** (especially on remote connectivity).
    d. Remind everyone the **information security processes** that are part of the organization's behavior.
    e. Close temporary accounts.
8. **Back to routine**
    a. Apply security updates that were postponed due to the Pandemic.
    b. Map tasks that were postponed because of the crisis (renewing licenses, acquiring equipment, awareness processes, risk surveys etc.) and update the work program accordingly.
9. **Run automated tools** – it is recommended to hire services that automatically map different levels so as to identify hidden gaps, such as:
    a. Identifying cloud assets.
    b. Mapping assets.
    c. Mapping attack scenarios (mainly the ability to spot unattended weaknesses).

Detailed and in-depth issues

10. **Where should we improve:**
    a. **Risk management** -during the crisis, a more liberal risk management may have been implemented, and approaching the end of the crisis it is relevant to examine how liberal we were and adjust policy.
    b. **Preserving the organization's borders** – during the crisis we have broadened the logical boarders of the organization and approaching the end

of the crisis we need to examine new networks borders that are relevant for routine and think how to better secure them (Home routers, BYOD etc).

c. **Locating organizational data**- some data might have "moved" to undesired locations (users' computerized equipment, items saved on the cloud for accessibility or backup etc.); it is required to conduct an inventory of the company's assets, software and hardware and reclaim information and clean equipment.

d. **Asset mapping update** – after using new abilities and computerized connections (inc. cloud) during the epidemic, we need to conduct a thorough asset and accounts mapping and cancel all the unnecessary ones.

e. **Organizational network structure** – we might have created changes and shortcuts in the organizational network during the epidemic in order to create extra accessibility and now we must change them to a more secure method.

f. **Mapping leftovers** – one of the most popular attack methods is finding an old untreated code; such a code might be a result of excess authorizations, untreated sites, scripts etc. A cleaning process of the leftovers is required in order to secure the organization. At least for the seen period it is advised to monitor "old" resources.

g. **New forms of information accessibility** – now is the time to return to organized and standardized working methods. An awareness campaign for the updated procedures should be considered.

11. **What lessons should be implemented:**

    a. **Integrating public infrastructure-based capabilities** – the accessibility of information (such as e-mails) through public infrastructure is a force multiplier for the organizations ability to create distant work habits. There is no doubt that these services are crucial to a period of detachment from the organizational core and of value to the organization in many aspects (scalability, elasticity etc.) These services must be developed in an organized and secure manner.

    b. **Integrative collaboration software** – there is a wide selection of collaborative software. Use this time to find the most suitable for your organization and introduce it to the employees.

    c. **Remote working ability** – it seems that this field will continue to accompany us in different volumes. The organization must define a policy in this matter and assign the means as to properly implement secure solutions for the long term.

12. **What should we develop:**

    a. Developing the **BCP program** – one should update the BCP program according to the latest threats (detachment, absence of crew members geographically from the work place, absence of crew members due to illness etc.).

    b. **The role of the CIO** – the role of the CIO must be redefined as a major contributor to the organization's activity as a major enabler of the security and operation of the organization.

    c. **Supply chain diversity** – the organization needs diversity both in IT and in CYBER all the time and especially in crisis.

    d. **Flexible response** – developing infrastructures that will allow flexible responses while conducting a reasonable risk management process.