IMPLICATIONS ON SECURITY FOR THE INDUSTRY SECTOR DURING AND AFTER COVID-19

FEDIL
The Voice of Luxembourg's Industry

TABLE OF CONTENTS

FOREWORD

FEDIL, The Voice of the Luxembourg's Industry, in collaboration with the **Ministry of the Economy** (Department of the e-commerce and Information Security) launched a **Forum on Cybersecurity** dedicated to the manufacturing industry (IND). This forum follows the principles of an **« Information Sharing and Analysis Center »** (ISAC). The IND-ISAC mission is to promote the cooperation in terms of cybersecurity within the manufacturing industry sector in Luxembourg and the Greater Region for the benefit of the attractiveness of the ecosystem.

As stated in the political guidelines for the European Commission 2019–2024, « *we need to move from "need to know" to "need to share"* ». The mission is achieved through (1) information and knowledge sharing among trusted representatives of the member organizations, and (2) dissemination of manufacturing industry-related risk information relevant for the public.

The IND-ISAC aims at creating a "taxonomy", common language required, to foster synergies and share common understanding of the risks within the company, the group, and the ecosystem by highlighting :

- the importance of informed governance, meaning cybersecurity governance at a sectorial, group or company level based upon as much factual information as possible (advantages for the CISO), and
- the importance of risk management and most of all the usage of as much objective and factual information as possible, and
- the importance of implementing communication between technical and organizational security by involving companies' top management.

The IND-ISAC is composed of companies' cybersecurity representatives from several industries.

The following document is the first outcome of the IND-ISAC and focuses on the COVID-19 crisis.

The IND-ISAC will continue its work by enabling companies to share information, experience, knowledge and best practices among peers in a climate of trust. It aims at indentifying sector-specific risk scenarios, vulnerabilities and threats and provides companies with a concrete guidance in conducting a risk management analysis.

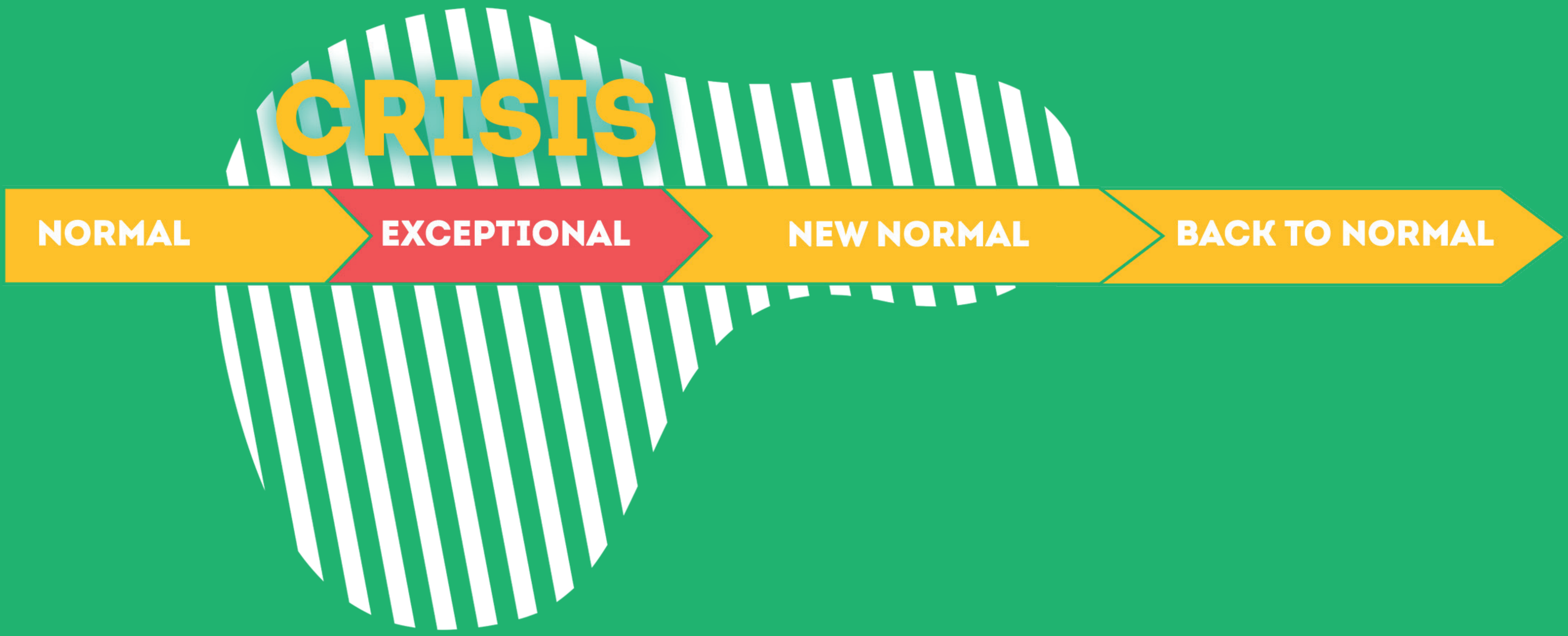
Should you wish to join the IND-ISAC and become an active member, we kindly invite you to contact our team.

FEDIL

INTRODUCTION

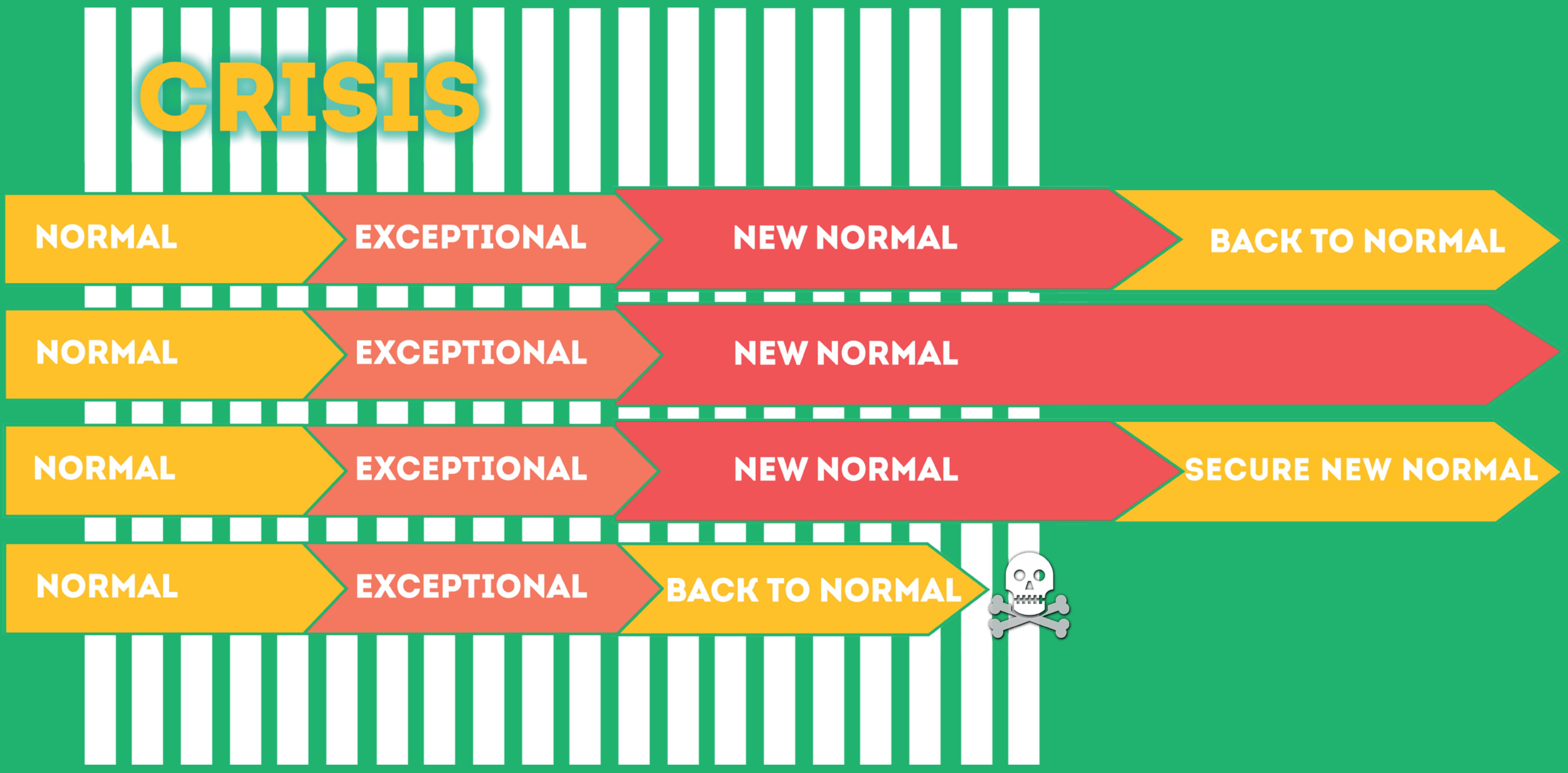
As many other sectors, the industrial and manufacturing sectors were hit hard by the sanitary and economic crisis triggered by the COVID-19 pandemic. However, the crisis also allowed to detect the weak points of business continuity and crisis management plans, thus representing a real-world test case for risk management. It is therefore important to learn from the obtained insights to improve the performance in subsequent crises (or subsequent waves of the current crisis).

Shortly after the crisis hit, most organizations passed from a normal to an exceptional state, during which productivity was either severely reduced or stopped temporarily. The unexpected situation was accompanied by unforeseen problems, which required quick and unconventional solutions. Some organizations managed to leave this state within days, others required weeks – but then a "new normal" state settled.



In the "new normal" state, security is often weakened, because decisions were taken in a rush, or because previous conditions (such as a secure environment) no longer held. However, the COVID-19 crisis should be seen as a unique opportunity to introduce new security concepts (especially linked to working from home remotely) and test them under real-world conditions – not only for the duration of the crisis, but also after returning to the office for a while.

For the industrial sector, the core business steps are materials, goods production and sales, which is why the most important security aspects are related to production cuts and sales drops. It turned out during the crisis that they can be impacted either directly (for example through governmental measures such as closure of borders) or indirectly through dependencies – be it customers, partners or investors.



CONTENT OF THIS DOCUMENT

This document tackles the changes in the risk landscape detected during or caused by the COVID-19 crisis. In particular, it addresses the following topics:

- important risks that were neglected before the crisis;
- new risks that appeared during the crisis;
- consideration for reviewing the evaluation of the risks (change of probability and/or impact of existing risk scenarios);
- vulnerabilities created when moving to the "new normal";
- security considerations for the move "back to normal";
- opportunities for improving security in the long term.

NEW INSIGHTS FROM AND FOR THE INDUSTRY

1/DOWNSTREAM SUPPLY CHAIN

KEY FINDINGS

The supply chain is among the most important assets for the manufacturing industry, since it has a direct impact on the production and thus on the core business. Therefore, risks related to the procurement of supplies had been largely assessed, even before the crisis. Indeed, sufficient stock and back-up suppliers were available when the crisis hit.

To date, the risks related to the downstream part of the supply chain had been given short shrift. However, the crisis did not only hit suppliers but also customers, causing a severe drop of demand for the produced goods. In a short period, warehouses filled up and production had to be cut or even stopped – even if the crisis did not have a direct impact on the manufacturer at start. The need to decrease production resulted in high fixed costs versus the comparatively low income, threatening the existence of the company.

KEY ACTIONS

A. EXPOSURE TO NEW (CRISIS-SPECIFIC) RISKS

- Include the risk “stop of production due to lack of demand” into risk assessments, taking all interdependencies of the downstream supply chain into account.

2/LOCAL VS GLOBAL RESTRICTIONS

KEY FINDINGS

When the pandemic hit Europe and the entire world, it had been around for about two months in the Far East already. By consequence, the recovery phase set off earlier in those regions as well, allowing competitors to gain advantage over companies that are still confined. Similar observations have been made on a much smaller scope as well. European governments did not coordinate the restrictions and liftings thereof in a timely manner, creating market inequalities even within Europe. A problem that is very particular for countries like Luxembourg with several borders is the taxation laws for commuters, which sets out a threshold of telework days per year which varies from one country to another.

KEY ACTIONS

A. EXPOSURE TO NEW (CRISIS-SPECIFIC) RISKS

- Include the risk “loss of customers” due to governmental restrictions that are local only or not synchronized across countries.

KEY FINDINGS

In general, the relaunch of activities took a long time (up to several weeks), even though disaster recovery plans existed. This was due to several factors.

- Due to the confinement, most staff was sent home to work from home remotely. By consequence, the key personnel designated by disaster recovery plans to relaunch activities was not available on-site. However, physical presence was often needed, because either access from remote was disallowed for security reasons, or because processes were not digitalized (which is often the case in the industrial sector).
- In addition, the confinement was not lifted in one shot, but restrictions (such as physical distancing, wearing of masks, reduction of staff,...) applied so companies could not just reactivate their entire workforce. However, it turned out that it was often not clear which personnel should be reactivated first and which could stay off-site.

In Luxembourg, more than 50% of the health sector staff are commuters. Since the government considers the closing of borders as one of the major risks for this sector, health personnel was offered to live in hotels in Luxembourg. Even though the percentage of commuters is not as high in the industry sector, the same problem exists.

Another important topic to address is the reactivity in case of a crisis, as quick reaction generally implies a considerable reduction of the impact. It is important for a company to enable its capability to reduce the delay of reaction to a crisis to preserve its assets.

KEY ACTIONS

A. CONSIDER REVIEWING EVALUATION OF RISKS

- Governments might fail in correctly estimating the risk related to pandemics. If there is a potential crisis outbreak, implement own risk estimation and collect information so as to be ready before a crisis hits.

B. IMPROVE EXISTING SECURITY MEASURES

- Design business continuity plans in such a way that business processes could be managed remotely.
- Design disaster recovery plans in such a way that it can be executed remotely.
- Define priorities that allow to determine the order in which personnel is reactivated.
- Take into account crisis management capabilities of governments as well as the willingness of the population to follow the instructions from the government.
- Verify if crisis management procedures also address long-lasting crises.
- Improve capabilities to detect and process early signals of a rampant crisis.

C. CONSIDER ADDITIONAL SECURITY MEASURES

- Provide a living space for essential people if borders are closed or risk to be closed.
- Implement digital tools & solutions which could digititalize repetitive job functions.
- Stress-test crisis management.

4/EXPOSURE OF INTERNAL INFRASTRUCTURE TO THE OUTSIDE

KEY FINDINGS

Staff that worked from home needed to access the information systems or control systems, which were often only accessible from within the company network and not available in the cloud. While under normal circumstances, such an approach is more secure in terms of confidentiality, staff was unable to work from home during the crisis at first.

As an emergency measure, some companies exposed critical services (including industrial control systems) to the Internet, since companies were judging availability more important than integrity (or because they were not aware of security implications). However, in industry, such systems are often proprietary, outdated or relicts from acquisitions and thus often inherently insecure (containing vulnerabilities, poor security standards, default passwords, etc.). By consequence, many critical systems are now exposed even to non-targeted attacks, creating a huge security hole.

Another way of proceeding is the set-up of virtual private networks (VPN). However, VPN solutions were often not in place, and when they were, personal devices were not configured to connect to them.
Indeed, not only does a software client need to be installed and set up, but strong authentication tokens (which are often physical devices) need to be distributed as well.

Moreover, allowing staff to connect to the internal network with their own devices has huge security implications. Since the company has no control on these devices, more precisely on the security, most of these devices are not appropriately protected from malware and hacking. On top of that, the exposure to threats is unknown.

The crisis also highlighted flaws in the design of some security-related workflows. When the password expiration interval was set too short, passwords expired when staff was working remotely. This led to a vicious circle where staff needed to connect to the company infrastructure in order to change or reset their password, but they could not because the password had expired. When additionally, no strong authentication was in place, provisional work-arounds needed to be found that exposed internal interfaces to the public without any extra layer of security.

KEY ACTIONS

A. CONSIDER REVIEWING EVALUATION OF RISKS

- Increased threat exposure due to entry points for remote access that were hastily set up. Once this fact becomes known, criminals might additionally focus on searching for exploits, which increases the threat landscape even more.

B. CONSIDER ADDITIONAL SECURITY MEASURES

- Foresee working remotely in non-crisis times by setting up secure remote access.
- Systematically deploy strong authentication (for all critical systems and all staff).
- Consider using state of the art cloud solutions with strong authentication.

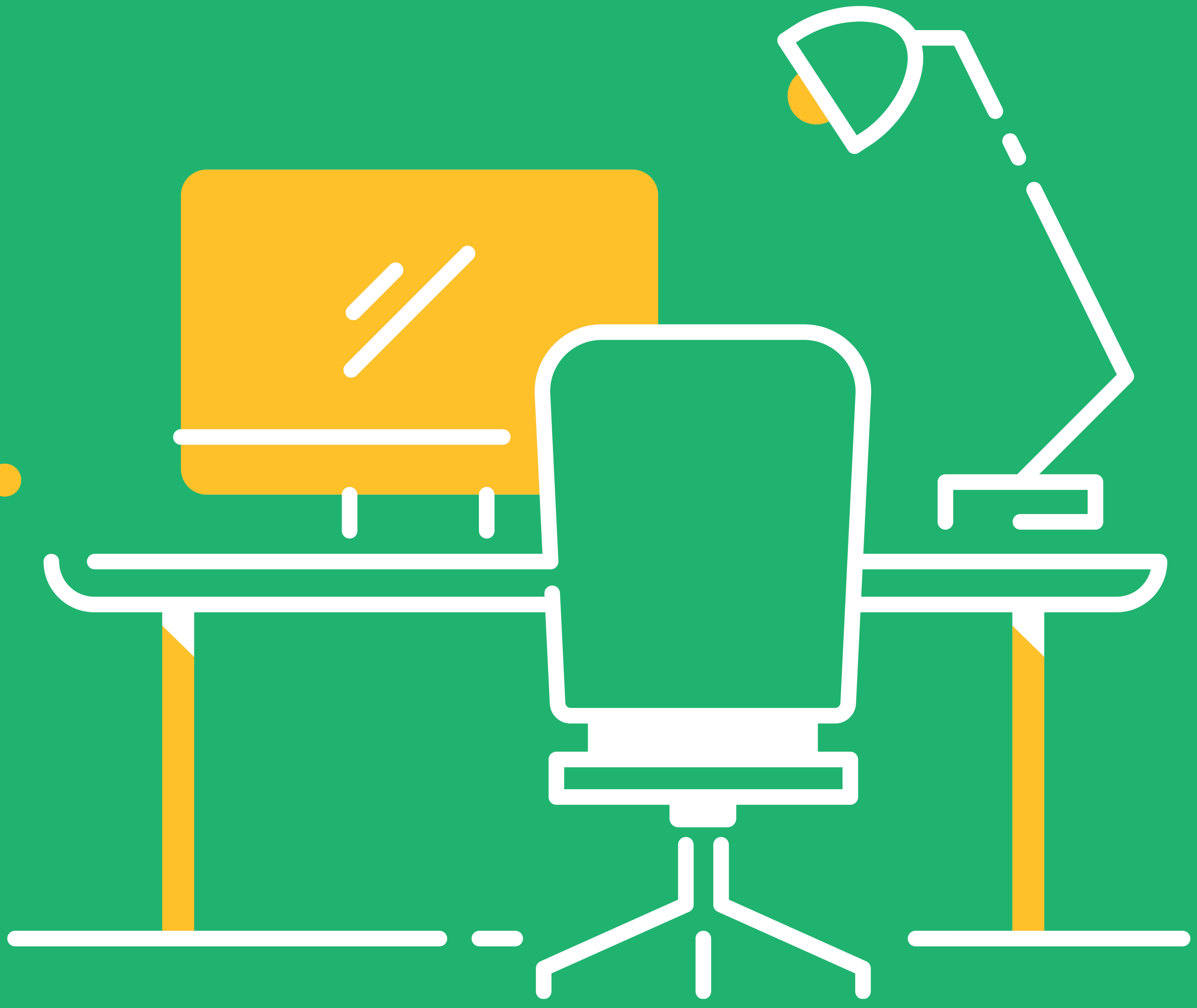
KEY FINDINGS

For those companies that had the possibility to work remotely, the crisis quickly showed its limits.

- First, not enough equipment (be it laptops, phones, or security tokens) was available to hand out to the totality of the personnel.
- Second, the infrastructure or the network itself did not handle many concurrent connections very well.
- Third, not all workflows were entirely digitalized, so that they could not be smoothly continued from a remote workplace.
- Fourth, since the crisis hit the entire economy, procurement of strong authentication tokens was largely delayed due to the huge demand (similarly as for the hygienic masks and sanitizers).

In some cases, especially for international groups, not all workers had a reliable internet connection at their disposal, and 4G hotspots needed to be provided by the company.

Remote working also created new security problems. For one, every person that connects from remote represents an entry point to the internal systems and thereby increases the attack surface. Unfortunately, it is very hard to protect these endpoint devices, let alone the endpoint networks. Moreover, since all internal communication was now done via e-mail, phishing and other social engineering attacks became much simpler and more effective.



Videoconference platforms have been used extensively. It turned out that not all of them were sufficiently secure (e.g. lack of encryption) and thus inappropriate for internal meetings. A lot of cases of conference bombing (uninvited participation) were reported in the beginning of the crisis.

In general, companies did not experience a lot of end-user IT problems, but set up a permanently manned IT support just in case. Most support could be provided remotely over VPN.

When employees are working remotely, the normal security measures (anti-virus, SIEM, patching and back-up servers) were not necessarily available, especially when employees did not connect to the VPN. So alternative solutions were needed, such as making the respective services accessible from the public Internet. Employees were encouraged to use cloud storage for saving their files – but it was very hard to make sure that they actually used cloud storage and not their local file system (which is not backed up).

KEY ACTIONS

A. CONSIDER REVIEWING EVALUATION OF RISKS

- Increased risk of phishing and social engineering.
- Personal (non-surveilled) devices are connected to the internal networks. Sensitive data can possibly leave the perimeter of the company.
- Communication between members of the company is mostly done over the Internet.
- Increased risk of data loss due to back-ups not being made remotely.

B. EXPOSURE TO NEW (CRISIS-SPECIFIC) RISKS

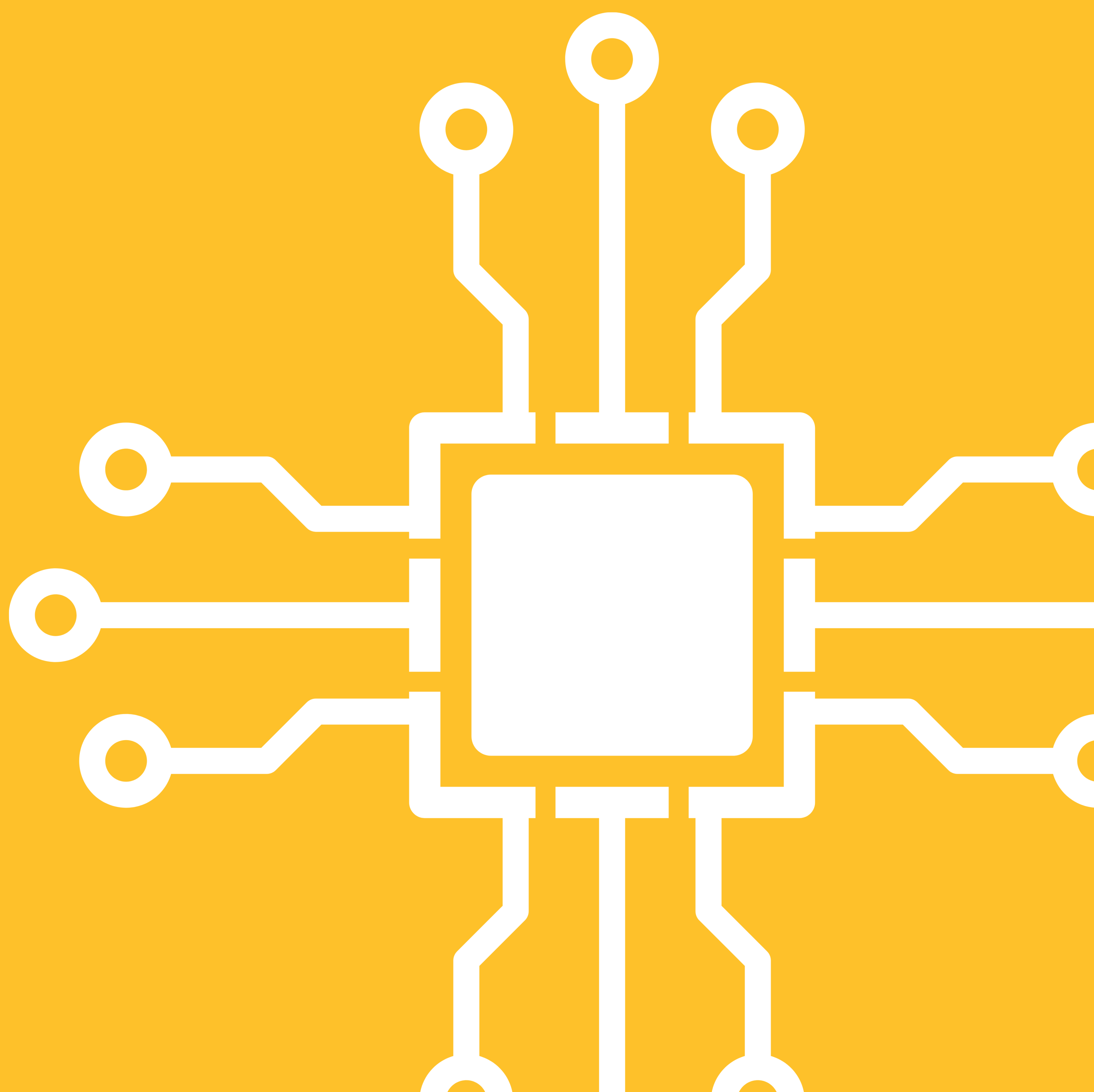
- Consider the situation where telecom lines and IT infrastructure will be exhausted due to an accumulation of connections (consider the logfile storage for preparing for an incident).

C. IMPROVE EXISTING SECURITY MEASURES

- Strengthen security awareness training and adapt it to the new situation (work from home).
- Review complex workflows to make them crisis-resistant.
- Stress-test the remote access infrastructure (the remainder of the crisis being a good opportunity). Consider acquiring VDI (virtual desktop infrastructure) solutions.

D. CONSIDER ADDITIONAL SECURITY MEASURES

- Digitalize processes by setting up secure cloud and e-signature platforms.
- Ensure that all staff can work remotely when required.
- Make sure that enough spare authentication tokens are available.
- Address the endpoint security problem (provide corporate material for users working at home to prevent privacy issues and be able to enforce security).
- Explicitly prohibit employees to use their private mail for corporate usage.
- Companies should invest in open source platforms hosted within their premises or with a service provider from a trusted company. Encryption of these conference streams should be standard, which is not the case for most of them for the moment.



6 / THREAT LANDSCAPE

KEY FINDINGS

At the beginning of the crisis, it became apparent that cyber criminals quickly reacted to the fact that most companies, prepared or not, started to work from home. Especially scam and phishing but also ransomware were quickly on the rise. In some cases, small-scale DDoS attacks were observed on communication infrastructure.

Home office also had a direct impact on the threat landscape. Before the lockdown, threats were to be stopped at the premises. This implies that within the premises, all traffic was predictable and well-known, and any deviations were suspicious.
When staff started to work from home, the detection mechanisms also needed to cover home devices and networks, and were thus facing much more noise than before. This increased the number of alerts and made attacks much more difficult to detect than before. However, the strengthened endpoint security also allows attacks to be detected earlier.

Dedicated security awareness training was given so as to address the increased risk of (phishing) attacks. To organise the training, online learning platforms were used.

KEY ACTIONS

A. CONSIDER REVIEWING EVALUATION OF RISKS

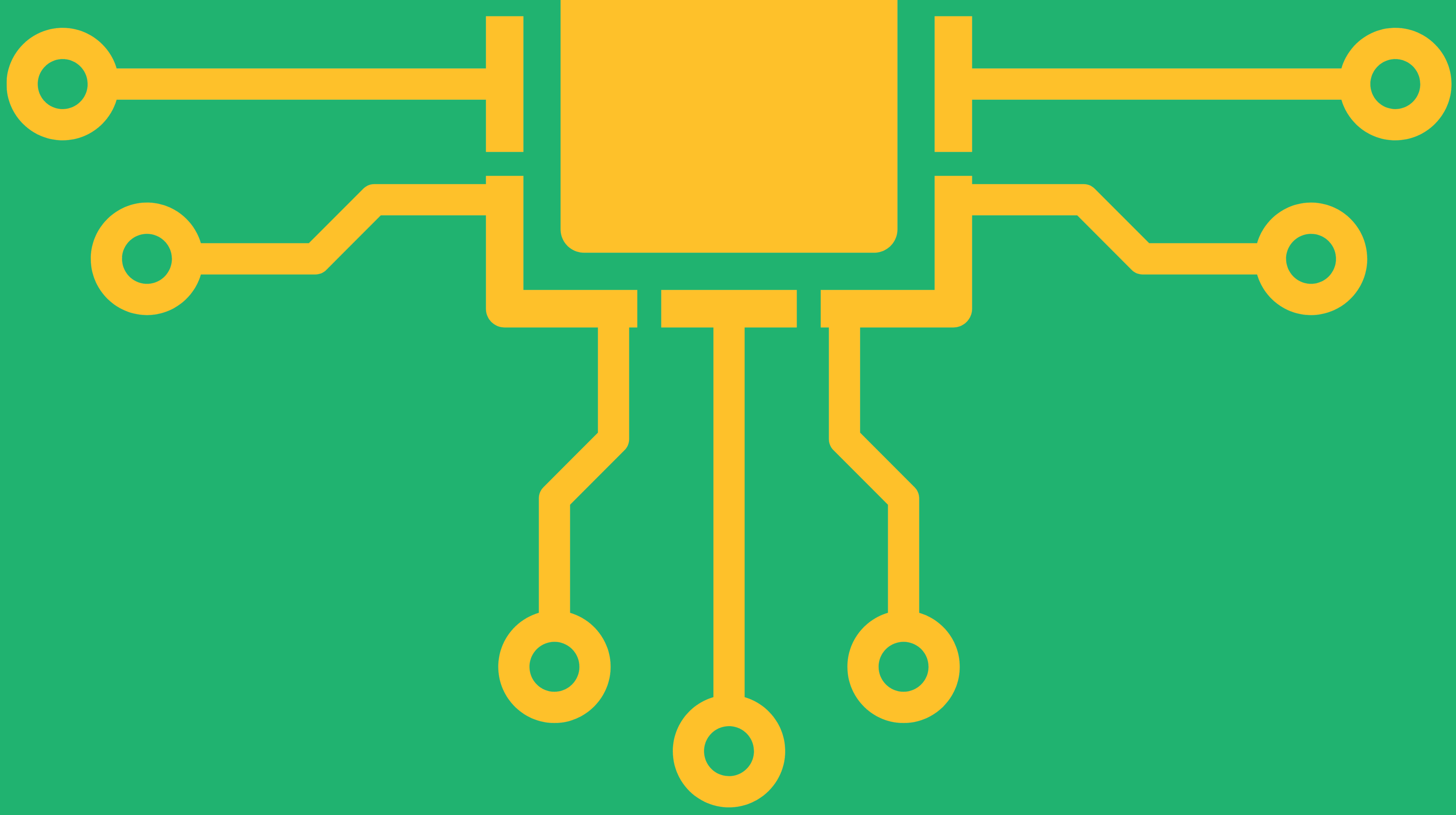
- In an unexpected situation, such as one which threatens their health, employees are avid for updates and information. In this situation, it is easy for a scammer to make people open dangerous attachments.
- Remote access gateways have become single points of failure, which must be protected against loss of availability.
- Governmental decisions might impact the availability of personnel (social leave).
- Geopolitical tensions.

B. IMPROVE EXISTING SECURITY MEASURES

- Key people must stay available even if they have a right to leave (e.g. social leave). These key people must be highly committed and loyal to the company and be motivated to stay available. Foresee the possibility to cope for their children by organizing kindergarten on premise.
- Strengthen security awareness training, focusing on social engineering.

C. CONSIDER ADDITIONAL SECURITY MEASURES

- Continuously provide employees with information about the situation, make them aware about scams.
- Foresee DDoS mitigation techniques or infrastructure.
- Be able to handle a cyber-incident in times of a crisis, that is, even when resources will not be quickly available on-site.



FEDIL reminds you that the Cybersecurity checklist concerning devices, e-mails, access to the cloud and to the network as well as videoconferences set up in collaboration with SECURITYMADEIN.LU is available on the FEDIL website: Cybersecurity Checklist

Should you wish to join the ISAC, please, contact:

Céline Tarraube
Adviser Digital & Innovation
celine.tarraube@fedil.lu
(+352) 43 53 66 610