Freshfields Bruckhaus Deringer

Navigating the impact of Covid-19

Cybersecurity during the COVID-19 emergency: the Italian perspective

The COVID-19 global emergency exposes companies to a series of cybersecurity risks, threatening their stability.

The 2020 coronavirus pandemic is giving rise to new challenges for all mankind, and governments and businesses are doing their best to cope with this emergency.

As more and more regions throughout the world opt for different forms of lockdown, our dependency on the cyberspace increases. This gives rise to new opportunities, but it also makes us extremely more vulnerable to cyberattacks.

A business' virtual infrastructure being damaged or shut down in a moment like this might have a disastrous or even deadly impact on such organization – even more so when the attack affects a hospital or a health organization, as recently happened with the US Health and Human Services Department, as well as with the Brno University Hospital.

Therefore, many commentators are urging people to care about cyber hygiene as much as they care about washing their hands and wearing face masks to avoid contagion.

This brief paper outlines the major global cybersecurity challenges and risks, also in terms of potential disputes, that companies might face in the wake of the Covid-19 outbreak together with a series of recommended measures.

Companies experimenting new or unprecedentedly widespread forms of teleworking practices, might have to face **several unique challenges**, such as:

- **Guaranteeing adequate support for a larger number of remote-workers.** As all or most of the workforce shifts to smart-working, the IT infrastructure might be under significant pressure. IT teams might have difficulties guaranteeing both the availability of the technology and its security. At the same time, a higher workload might not be counterbalanced by a larger team to process it: if recruiting freezes and some IT workers end up being either infected or having to care for someone sick, organizations might face significant disruptions in their ability to solve any emerging IT issues.

- **Managing new systems**. The rush to make a large transition to smart-working could imply companies relying on new systems or procedures, which might have not been tested properly within the organization. As a result, certain small or major incidents could be inadequately managed by both the IT staff and the rest of the organization, weakening the technological infrastructure of the organization itself. Also, employees might start to rely on software and applications (e.g. for conferencing or exchanging messages and files) which have not been previously approved or tested by the employer and might be the source of potential security breaches.

- **Training every employee in due time**. Many employees and executives of companies, public entities or organizations might be unfamiliar with many aspects of teleworking. This goes from having the security settings properly in place on their personal computer, to knowing who to call in case any problems arise – since knocking at the door of their local IT is not an option, at the moment. Furthermore, each employee connecting remotely through a personal device could represent a weak spot for the company. In-time training of every worker could prove harder during a crisis, and a safety gap could easily serve as an open door for cyberattacks.

- **Avoiding panic**. Hackers are already taking advantage of people's uncertainty stemming from the crisis. Phishing and ransomware attacks have been reported all over the world, in the past weeks.

Critical recent instances encompassed malicious emails by hackers disguised as the World Health Organization and fake Coronavirus maps and apps accessing sensitive data. Some larger security threats often start with these internet frauds. And in moments of stress and panic, people's natural defenses against frauds and fake information tend to be lowered, causing a higher risk of successful cyberattacks.

- **Ensuring business continuity**. While developing new engineering and digital safety procedures, organizations should be careful not to disrupt companies' regular work-flow, since this would inevitably harm the organizations' ability to perform its functions. An adequate balance between cybersecurity and business continuity should be achieved. Moreover, if teleworking becomes too slow for employees to 'get things done', they might be tempted to bypass secure procedures, finding unsafe alternatives to share files or messages. Proper methods for safely destroying documents at home might also be widely unavailable, which could increase risks.

Mitigating these kinds of risks might be of vital importance in times of crisis. It could save the ability of an organization to continue to work properly and get through both the emergency and any potential economic recession that might follow. It would also **prevent legal disputes and potential liability** of organizations from arising.

Indeed, on the one hand, companies might incur **civil liability** *vis-à-vis* third parties in a wide number of cases. Think, for example, of a company not taking the adequate steps to ensure the protection of confidential information of its clients or business partners, which could be seized by cybercriminals and end up in the wrong hands. Customers, shareholders and business partners could file either individual or class action lawsuits against the company, which could result in costly litigation, a weakening of business reputation and, above all, company's liability for damage.

On the other hand, higher risks of cyberthreats, lowered security for IT systems and the inability to effectively face potential breaches could intensify the risk of crimes committed by or through the company's devices. This could result in corporations' quasi-criminal liability under Legislative Decree no. 231 of 2001 (***Decree 231***), possibly leading to heavy penalties, such as monetary sanctions, interdictory measures and seizure of illicit profits, should any of the offences listed by Decree 231 be committed by company representatives, directors or employees in the interest or the benefit of their corporations. Think, for example, of the offence of abusive access to IT systems when committed by an employee to manipulate data and information for accounting purposes.

Accordingly, companies should ensure that all their employees and members are aligned in taking the **necessary precautions** to avoid cyber threats. Among them:

- **Organizations would have to consider relying on secured means of remote access, transmission of information and messages**. More specifically, encrypted communications channels, such as Virtual Private Networks, as well as Multi-Factor Authentication might prove useful, especially for accessing particularly sensitive areas of the network. Each organization should guarantee efficient and secure means for employees to perform their tasks, so that they are not forced to rely on software or applications not approved by their employer and potentially unsafe. Whenever corporate computers or devices are not available to employees, their personal devices should be adequately secured.

- **Employees should be properly informed on what not to do and how to telework effectively**. Raising awareness is pivotal in order to prevent cyber threats. For example, businesses could consider making clear that company devices cannot be used for personal activities, nor shared with people not belonging to the organization, and that personal devices can be used for company activities only insofar as they are equipped with adequate security systems. Unapproved software and applications should be banned. Also teaching how to behave when a disruption of the network occurs could be crucial to enhance cybersecurity.

- **Employees should receive adequate training to detect phishing or other attacks and to react to them properly**. This would require providing cues in order to promptly identify potential hacks, as well as adopting a clear policy aiming at making each member of the organization

immediately aware of what to do and whom to contact, in case of emergency. Training and simulations (even remote ones) should involve all levels of the organization, since executives are often targeted by more sophisticated forms of attacks, which might result in higher risks – given also their ability to access larger amounts of sensitive information.

- **Ensure network's resilience**. Organizations should consider testing and improving their networks to sustain large amounts of users even before a lockdown is declared or recommended by public authorities.
- **Try to get IT resources focused on the problems that really matter**. Given the risk of having excessive workloads for IT teams to handle, establishing a specific Incident Response Plan, pinpointing a clear ranking of priorities to be addressed during the COVID-19 emergency, might be life-saving for organizations. Additionally, the deployment of effective instruments, allowing employees to report suspicious communications and to receive immediate assistance, should also be considered.
- **Companies should enhance their compliance programs**. In this time of emergency, corporations should carefully consider rendering their compliance programs even more robust with respect to the potential commission of cybercrimes, for example, by enhancing the role and powers of the internal supervisory body; by setting up dedicated instruments to report suspicious communications and potential cyberattacks; or by upgrading the information and training of their employees. Comprehensive, company-tailored and adequately implemented compliance programs would allow companies to limit or even exclude their quasi-criminal liability under Decree 231.

All these and other measures, taken together and in due time, could prove very helpful to make organizations, if not immune, certainly more resilient to the difficulties that they are increasingly facing and to the ones that lie ahead.

The information contained in this note is general and does not represent legal advice. You can receive more information and tailor-made legal advice by contacting Freshfields Bruckhaus Deringer LLP.

Reference persons

Fabrizio Arossa, Partner

Disputes, litigation and arbitration
Global investigations

Rome
Via Barberini, 86
00187

T +39 06 695 331
E fabrizio.arossa@freshfields.com

Federico Mercuri, Associate

Disputes, litigation and arbitration
Global investigations

Rome
Via Barberini, 86
00187

T +39 06 695 33 386
E federico.mercuri@freshfields.com