CORONAVIRUS: CYBERSECURITY COMPLIANCE IN TIMES OF CRISIS

Mitigating the cyber regulatory risks arising from the COVID-19 crisis

With the global COVID-19 health emergency, cyber risks are increasing:

- *Greater dependency on digital technologies*: in many countries, individuals are required to avoid physical interactions. As a result, organizations rely as never before on digital tools to maintain their activities. This has two effects: greater exposure to cyber threats and increased costs of breaches (e.g. one may only imagine the disruption that a ransomware could cause to a company whose entire workforce is confined in homes)
- *Cybercriminals exploiting the turmoil*: authorities and experts report that cyberattacks using the pandemic as a hook to lure victims – sometimes imitating trusted organizations such as the World Health Organization – are exploding[1]
- *Cyber incident response made more difficult*: sanitary measures such as mandatory remote working make it more difficult for organizations to bring together teams to handle cyber breaches, and for these teams to coordinate and evaluate the scope of breaches
- *Network saturation increasing risks of system failure*: with entire countries locking down, internet traffic is surging. This puts an intense pressure on networks and increases risks that information systems fail

At the same time, "routine" cyber-attacks continue to disrupt public and private organizations, as shown by the ransomware which recently blocked approximately 300 computers of the Marseille local authorities.

Organizations would be ill-advised to address these heightened cyber risks from a pure IT perspective. They should consider as well, as part of their cyber resilience strategy, the significant regulatory and business risks that cyber breaches bring about. Cyber regulatory risks - which differ from one jurisdiction to another - may materialize in the form of major fines for failing to comply with data security and incident notification requirements, criminal liability of managers and the organization as a result of such failures, damages

[1] Cybersecurity firm Proofpoint estimates that "*to date, the cumulative volume of coronavirus-related email lures now represents the greatest collection of attack types united by a single theme that our team has seen in years, if not ever*" (publication of 16 March 2020).

to compensate victims of data breaches, and sanctions for failing to carry out the appropriate disclosures to markets, among others.

We set out below some recommendations to mitigate the specific cyber regulatory risks arising in the context of the COVID-19 crisis, from the perspective of European Union law. Of course, there is no "one-size-fits-all" approach to handle cyber regulatory risks, so these recommendations should be adapted to each business' characteristics.

1. IMMEDIATE ACTIONS

- **Raise awareness & train**

  Most cyberattacks exploit individuals' weaknesses to penetrate organizations' systems. The COVID-19 crisis is a new occasion for cybercriminals to do just that. Already, authorities such as the UK National Cyber Security Center and the World Health Organization have warned the public about COVID-19-themes phishing attacks. In the current stressful context, phishing attacks' success rates will likely increase given that stressed individuals are more prone to fall into cyber traps.

  Regulators will likely expect organizations to be aware of these developments and have adopted the measures to face COVID-19-themed attacks. Indeed, under the GDPR[2] as well as other legislations such as the NIS Directive[3] , organizations are required to implement measures to ensure a level of security appropriate to the risk, which is appreciated in light of the "context". A first, elementary step in that direction is to (a) inform employees about the existence of COVID-19-themed attacks, (b) instruct them to follow existing policies and trainings on how to spot and react to suspicious messages, and (c) regularly remind them of "cyber hygiene" habits (e.g. password protection, authorized software installation, BYOD policy).

- **Set up a COVID-19 cyber unit**

  An organization's usual capacity to anticipate, identify and manage cyber threats may be weakened because of the COVID-19 pandemic (e.g. IT resources may be overstretched due to massive remote work). To maintain their breach response capacity at the level required by European regulations such as the GDPR, organizations should appoint a multi-expertise and cross-function COVID-19 cyber unit. That team could regularly meet online to:

  — keep track of the evolution of threats arising from the COVID-19 crisis and consider how they may impact the organization

  — design and monitor the deployment of measures aimed at upholding the cyber breach response capacity during the COVID-19 crisis (e.g. determine need for additional resources dedicated to security, assess whether complying with sanitary instructions may lead to delays in the handling of cyber breaches, integrate

[2] Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

the sanitary instructions and travel bans into the cyber breach response plan)

- **Test cyber-resilience**

  Many organisations are already strained by the COVID-19 containment measures. Yet, it is all the more important for them to test now their cyber incident response processes, given the cybersecurity challenges posed by the COVID-19 crisis and the uncertainty as to how cyber risks will evolve. Testing protocols should be designed to confirm compliance with regulatory standards[4]. The test should be followed by actions – depending on its results, systems may have to be upgraded and the breach response plan updated – and kept as evidence of compliance for regulators.

- **Review agreements with forensic advisors**

  Time is of the essence in a cyber breach. A delay in starting the breach assessment - whether caused by the COVID-19 crisis or not - may lead to several non-compliances (e.g. failure to comply with the GDPR's and NIS Directive's timing requirements for notifying regulators / individuals, late disclosure to markets, longer period during which security standards are not met). Service agreements with cybersecurity advisors should thus be reviewed to ensure timely assistance (e.g. if one advisor's team is unavailable due to COVID-19, another should step in without delay; 24/7 hotline).

- **Consider taking / reviewing cyber insurance**

  In these unsettled times, consider taking cyber incident insurance to protect against the liability exposure of a breach or reviewing your policies to ensure your business is adequately covered.

2. STRATEGIC ACTIONS FOR THE LONGER TERM

In a longer-term perspective, the cyber challenges stemming from the COVID-19 crisis may be the opportunity for a wider review of security practices, building on the lessons learned from the crisis:

- **Review the group's cybersecurity compliance**

  Once the COVID-19 crisis is over, the organization could seize the opportunity to roll out a "lessons learned" exercise, i.e. taking stock of the group's capacity to deal with cyber threats during the crisis, re-evaluating risks, listing what worked well and what did not, and improving practices where necessary to stay in line with legal requirements and regulators' expectations.

- **Investigate partners with whom data is shared**

  Partners with which the organization shares personal data may start facing economic difficulties as a result of the COVID-19 crisis. Yet,

[4] For instance, the GDPR require organisations to maintain themselves in a position to (a) establish immediately whether a data breach has taken place, (b) assess the risks posed by the breach, (c) notify the regulators within 72 hours when the breach entails privacy risks, (c) inform affected individuals without delay when the breach entails high privacy risks, (d) upgrade data security if is not in line with GDPR's standards and (e) document the breach.

that should not prevent the organization from auditing them to ensure they meet the security standards imposed by the law. Indeed, regulations such as the GDPR require organizations to ensure the security of the data they share with partners, without providing for any "emergency" exception that could be invoked with the epidemic. As a result, organizations should:

- not refrain from auditing entities with whom they share data in the coming weeks;
- request resolution of weaknesses revealed by the audit and, when it appears from the audit that the entity is not able to meet security standards, envisage discontinuing the relationship and transitioning to another partner (if possible).

CLIFFORD CHANCE

CONTACTS

Dessislava Savova
Partner

T +33 1 4405 5483
E dessislava.savova@cliffordchance.com

Grégory Sroussi
Counsel

T +33 1 4405 5248
E gregory.sroussi@cliffordchance.com

Alexandre Manasterski
Avocat

T +33 1 4405 5971
E alexandre.manasterski@cliffordchance.com

Jérémy Guilbault
Avocat

T +33 1 4405 2480
E jeremy.guilbault@cliffordchance.com

Julie Martres
Avocat

T +33 1 4405 2493
E julie.martres@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ