Cyber security – 5 tips for organisations during the coronavirus lockdown

Marlene Winther Plas
Partner, Head of IPT, Denmark

Anders Nielsen
Attorney

Jon Lauritzen
Partner

Following the advice from the Danish Government, a large number of Danish employers have instructed their staff members to work remotely. Generally, the sudden increase in remote working - coupled with the coronavirus impact in society – will, in relation to cyber security, trigger a more critical risk landscape of an enterprise. In March 2020, the Danish Centre for Cyber Security published a revised threat assessment. The cybercrime threat was assessed to be "VERY HIGH".

Below, we have therefore put together 5 tips for enterprises facing challenges during the ongoing coronavirus lockdown.

Tip 1: Update your risk assessment

Our risk landscape has changed considerably over the last couple of months. In a crisis situation, people tend to become hungry for more information, which malicious actors will leverage by means of phishing attacks, fraudulent websites and the spreading of harmful content. Furthermore, the IT systems of an enterprise will become exposed to further vulnerabilities when, from one day to the next, the majority of its employees are instructed to work from home.

A natural step for an enterprise is therefore to address the new risk landscape - in relation to the risks of both accidental events and malicious actions - and to consider the consequential measures to be taken.

Considerations which enterprises could address include:

- Whether the enterprise in question has become a more or less obvious target in the face of COVID-19 and lockdown
- The fact that VPN services may suddenly constitute a business-critical IT asset, which could freeze the business productivity in the event of an overload (because of insufficient capacity in the event of a DDoS attack etc).
- The impact of home workplaces on physical security
- Whether sufficient IT resources have been made available to the staff members. Lack of resources may increase the risk that staff members use unauthorised IT assets, such as their personal computers, private email accounts, private storage devices (e.g. USB keys), unauthorised cloud-storage solutions (e.g. Dropbox), etc.
- The increased risk of phishing attacks and any other leverage of work-from-home users' concern, curiosity and search for information in the face of COVID-19
- Whether the use of smart devices with a voice control, for instance Google's Nest Hello and Amazon's Echo, at the home workplace is compatible with the security policy of the enterprise.

We recommend that all enterprises carry out a revision of their current risk assessment to allow for the ongoing coronavirus lockdown. The level of security should not be reduced because of the extraordinary situation.

All enterprises could also benefit from considering whether additional awareness campaigns concerning the unprecedented coronavirus situation should be rolled out and from ensuring that staff members are updated on the risks to be alert to.

Tip 2: Make sure that risks are managed in line with the enterprise's duties

As for certain security risks, it is a commercial decision how these risks are to be managed, including the decision as to whether the risk-appetite level is to be high or low. As for other security risks, the legislative framework could be affecting the options (or lack of same) open to the enterprise in question, in particular Article 32 of the EU Data Protection Regulation in so far as the protection of personal data is concerned. This framework may restrict the enterprise's risk appetite and, in some cases, maintain its responsibility if outsourced to an external provider without taking the correct measures in advance.

If your enterprise acts as a data processor on behalf of other enterprises, data processing agreements providing requirements as to the security level that must be maintained, meaning security requirements which could be subject to a review, will generally have been concluded. In this regard, it is particularly important to keep in mind that a data processing agreement may stipulate specific requirements for or preclude remote working. If such requirements impede remote working, an urgent renegotiation might be necessary.

Tip 3: The wording of the contract with the IT provider

A large number of enterprises are generally dependent on their IT providers, who tend to be considered business critical. For the time being, this is particularly the case, where a substantial proportion of an

enterprise's staff members work remotely.

At the time of writing, the majority of all European enterprises have instructed their staff members to work remotely wherever possible. This, of course, places a strain on the present IT infrastructure and capacity - to such an extent that some streaming services now reduce the quality of content delivered to their customers. This also entails an increased risk that an IT provider becomes unable to provide the promised capacity, because some IT providers sell more capacity than they can actually provide, considering that all customers never use 100% of the purchased capacity.

Some IT providers may therefore face challenges in complying with the IT contracts concluded with their customers - perhaps because their sub-providers face similar challenges.

Issues which enterprises should consider in this connection include:

- Whether the requirements to an IT provider are specified as well as defined. Does the SLA also regulate response times or just uptimes?
- The use of sub-providers and their impact
- The options open to the enterprise if the provider is prevented from performing (in whole or in part).
- Whether the IT provider may invoke force majeure due to defective supply or no supply and for how long the IT provider may invoke force majeure
- Whether sufficient security requirements are made in relation to the providers and whether these requirements are revised in line with the guidelines issued by the Danish Data Protection Agency in this regard
- Whether (spare) hardware can be supplied at short notice - especially if the enterprise is hosting its own services

Tip 4: Be prepared for the worst

The coronavirus-lockdown situation should also prompt an enterprise to reconsider its emergency plan and to prepare a temporary revised version of such plan.

The basis of a large number of emergency plans is generally that staff members meet in person and have free physical access to servers and other IT assets. An enterprise should also consider whether replacement hardware can be freely procured as well as the impact of home workplaces on the management of any restoration of IT systems should they suffer an attack.

In this relation, the enterprise should consider how it communicates to its staff members in the event of an emergency should its own communication platforms become inaccessible. Previously, it was possible to communicate orally to a large number of staff members in the event of an IT breakdown (accidental or malicious), however, this option is generally unavailable during the coronavirus lockdown.

Moreover, it should be considered whether the coronavirus lockdown will have an impact on the possibilities for procuring the right competencies in the event of an IT breakdown. It must, however, be expected that most IT security firms continue to be available for virtual meetings should their assistance be required - just like us at DLA Piper.

Finally, the staff members of an enterprise should be reminded that the obligations to make notification of any security breach still applies, even though they work remotely. In general, any security breach in a home workplace is still to be notified to the Data Protection Agency no later than 72 hours after the breach has been discovered.

Tip 5: Comply with the recommendations and guidelines from the authorities

Many public authorities have spotlight on the present situation and the special circumstances caused by coronavirus. In this connection, we wish to make a particular reference to the Danish Centre for Cyber Security (fe-ddis.dk), which several times a week issues updated data-security guidelines to enterprises and private individuals.

Other public websites offering free information on data security include sikkerdigital.dk (in Danish only) and ENISA (European Union Agency for Cybersecurity) - enisa.europa.eu.

Services	IP og teknologi
Sectors	Technology