ARTICLE

Business security in times of furloughs and home working

The need for extra vigilance is now

The effects of COVID-19 have led many companies worldwide to take drastic measures. This includes applications for temporal layoffs or furloughs, with the additional uncertainty of definitive layoffs for vast numbers of employees.

The COVID-19 pandemic has forced many employers to close their businesses, whilst others have found that there is a reduction in their workforce requirements.

Many companies have had to enable working from home; the majority in a time crunch and without the necessary experience or preparation, resulting in their technological resources being pushed to the limit.

Companies´ compliance, legal, audit, technology and security departments have all been working for years to create and improve control measures and put in place procedures for action and adaptation to regulatory requirements (GDPR, competition, etc.). However, as a result of COVID-19, many companies are beginning to feel vulnerable as several of the implemented measures and policies, which were rigorously employed, are becoming difficult to apply and maintain in this complex situation.

The combination of teleworking and furloughs can lead to situations not covered by the security and control protocols of companies. Therefore, it is essential to consider the importance of information security and implement the necessary measures to preserve and protect company data.

The most relevant factor is that millions of employees are making intensive use of the technological means made available by their companies for their professional duties (laptops, smartphones, tablets, email, the cloud, etc.). In this context, it is critical to define protocols for work, monitor and control employees, of their use of technology and access to company servers and information. Additionally some of these employees could unfortunately be affected by a furlough.

Company IT systems must continue to operate at full capacity to enable workers carrying out their professional activities. However, due to the uncertainty of the present situation, the security and safeguarding of sensitive business information may land on a back burner. The risk of suffering losses of data and information increases significantly in these circumstances, which can lead to economic losses, reputational damage, etc.

Various measures can be implemented effectively and efficiently, to safeguard and guarantee the integrity of information.

Some examples of these measures would be as follows:

— Review and update the company **electronic device inventory** for all employees. The objective is to have them identified, always located and be able to claim them back if necessary.

— **Control of electronic signatures:** Increased control over employee authentication methods in operations where required (e.g., transfers requiring the approval of two people). Today more than ever, companies must remain vigilant regarding the notorious CEO and CFO frauds.

— Many companies use **cloud storage systems** (*OneDrive*, *G Suite*, *Dropbox,* etc.), which allow different levels of access control and file management. It is important to take steps to understand and ensure the proper implementation of these controls to know which ones are used by employees.

— The **activity records (**logs) (Internet access, file sharing, external device connections, etc.) **generated by employees while they are online or using their corporate devices** are usually stored on company servers for a limited period (30, 60 or 90 days), after which they may be automatically deleted or overwritten. It is important to adapt log rotation and retention policies, to extend this storage period and safeguard activity records from destruction.

— **Monitoring the access to the network/servers by employees** (e.g. those subject to temporary layoffs), or access control during unusual hours. Moreover, it should be considered that each home working employee could be connected to a Wi-Fi network with a lower level of security than recommendable and used in the business environment (double authentication, etc.).

— The **systems from external suppliers or third parties (anti-virus, security, etc.)** may store a lot of sensitive information and activity records. You must ensure that the level of contracted service includes the safeguarding and possible access to this information if necessary.

— **Review or implement management systems for corporate mobile phone devices,** allowing the company to control and maintain a record of connections, installations, and deletion of applications, as well as irregular activities that may be committed with those devices (mass deletions, improper access/ connections, etc.).

— Ensure the **creation, safeguard and extension of the corporate mail system backup**, **of data stored within company servers and records**, as well carrying out regular reviews, to confirm that the intended data is indeed stored and that its content remains accessible and unaltered.

If these measures have not already been implemented, companies should take note and adopt as soon as possible all the necessary measures to protect and secure their data, as well as those devices and/or corporate media that may store them.

GRAINNE BRYAN
Managing Director
+353 87 7393089
grainne.bryan@fticonsulting.com

JAVIER GARCÍA-CHAPPELL
Senior Director
+34 600 83 76 28
javier.garcia-chappell@fticonsulting.com

0982 - 04/20