APPLE
GROW+H
PARTNERS
Healthy Growth.

COVID-19 DATA SECURITY INSIGHT

In just a short amount of time, COVID-19 has had an immense impact on the global economy, as well as business operations around the world. How companies stay resilient and can adapt in the face of COVID-19's impact, will be a topic of discussion for many business leaders as new information continues to surface. Along with COVID-19's impact, the changes business leaders implement to respond to the ongoing crisis may introduce unintentional security and privacy risks.

Our daily routines are being impacted, along with the activities we perform. This creates opportunities for hackers, and others with malintent, who thrive in this type of environment, to take advantage of uncertainties and changes to routines. What has not changed, however, is an organization's responsibility to protect data and secure systems to reduce the risk of a breach or unauthorized access to information. The regulatory requirements, and other state and industry standards for protecting information, are as critical as the day they were implemented, if not more so. GDPR, CCPA, NYDFS, PCI DSS, CFIUS, HIPAA, HITRUST, SOX, and so on – still need to be adhered to.

The risk to an organization could increase if processes, implemented to help secure systems, protect data and information, and maintain daily operations, are not followed. Personnel, who have the assigned roles and responsibilities for managing systems and the corresponding data environment, need continued support and assistance to meet their job assignments.

To add to the complexity of daily operations, organizations have been forced to consider remote work options and telecommuting to slow the spread of the virus. There are certain technical considerations for remote workers, the first being the devices that they will use to conduct business. For organizations that provide laptops, this is generally a non-issue, however, if your workforce is typically in the office, working remotely can present some additional challenges from an equipment standpoint.

How will businesses secure remote access to company systems and data?

Businesses across the globe have been instituting remote work requirements to decrease the likelihood of spread and impact to business operations. Due to the increase of remote workers, businesses should secure access to company systems and data to ensure secure transmission of personal information. The actions below can help secure remote access to the organizations' systems:

- **Require secure connections to remotely access company systems.** A VPN solution should be leveraged to ensure transmission of data is secured over public networks. A common practice for many organizations is to use multi-factor authentication in conjunction with VPN to ensure authorized access.
- **Ensure session timeouts for connections into company systems.** Allowing remote connections to stay open indefinitely increases the window of availability for unauthorized access.
- **Ensure workstations timeouts for remote workstations.** With the increase of remote workers and remote workstations, businesses will be unable to physically secure these areas. By

implementing workstation timeouts, businesses can reduce the availability of unauthorized access if a workstation were to be left unattended remotely.

- **Require email using the organization's distributed solutions.** Organizations are so dependent on email communications and in most instances corporate email is available remotely. Employees should be reminded not to conduct corporate business over personal email accounts, text messages or third-party apps that are not managed by the organization. This is a great opportunity to pick up the phone and speak with people in lieu of other typical communication channels.

How will businesses secure mobile assets?

Businesses should consider how mobile workstations will be secured. Due to remote working capabilities, an increase of mobile workstations provided to employees will need to be secured. Data at rest should be encrypted. Hard drives on workstations are commonly encrypted to ensure confidentiality of data. Just to start.

We are all adjusting to the changes as a result of COVID-19. By supporting and reinforcing your organization's processes, procedures and solutions, which were implemented to protect your data, the risk can be better managed.