Keeping 'client' data secure when working remotely

How we can manage and protect our data when not working from the office, from a privacy point of view.

The past weeks, we have seen many unexpected developments around the somewhat "traditional way of working" for organizations in the Caribbean region. Organizations are suddenly confronted with the COVID-19 virus outbreak, and therefore have to implement stringent measures to protect their employees and business continuity. According to studies, one of the best ways to help contain the COVID-19 pandemic, is to limit social contact, the so called 'social distancing' measure.

In some countries, companies have embraced remote working a long time ago, but in other countries remote working might still be the unthinkable. The possibility also depends of course on the type of service(s), the organization culture and the industry the organization is operating in. Mostly it is paradigm and mindset shift compared to 'old' ways of organizing and managing organizations. Now, during the Covid-19 crisis, governments are encouraging private sector organizations/ employers to allow employees to work from home when feasible.

Remote working of course doesn't come without any risks. The privacy and information security of your organization and clients, should be at the top of your list of concerns. Just imagine the bulk of sensitive information that employees have access to and are sending and receiving over wireless networks and storing on their laptops. Therefore, making sure your 'remote' employees remain protected is essential to the overall privacy and information security posture of your organization. Here are a few easy tips that can minimize the risk of a data breach when working remotely.

From your organization's point of view:

Make sure that sensitive business information remains secured and protected. This requires expertise of the IT department to facilitate the employees with specific software or platforms to enhance the overall information security.

Setup a VPN service: a technology that creates a safe and encrypted connection over a less secure network, such as public networks or unsecured networks.

Work in the cloud: The cloud is a beneficial way of ensuring your data is kept secure when working with remote teams.

Define clear procedures to follow in case of a data breach and/or other information security incident.

Make sure employees are aware about what sensitive data is and how important data protection is. (Information Security & Privacy Awareness training).

Communicate policies and procedures with employees and ensure practices are acted upon.

From the employees' point of view:

When working remotely, it is important to keep in mind the importance of the sensitive data you are working with. Keep thinking about the consequences that a data leakage can have for the organization or for your clients.

Use strong passwords and two (or even better multi-) factor authentication.

Make sure you connect to a trusted WIFI, preferably at home and if applicable connect to your VPN service. Don't leave your laptop unattended and always lock your laptop when not working.

If something goes wrong or you have a suspicion, report this immediately to the organization.

Danny van Haaren
GRC Business Technologist
Advisory
Grant Thornton Curaçao

Roy Jansen
Director
Advisory
Grant Thornton Curaçao