How secure is your company data during a lockdown?

By Paula Sartini

4 May 2020

Many businesses have developed business continuity plans (BCP) to mitigate risks and reduce the impact of a crisis. Further, they would have conducted a business impact analysis (BIA) to determine which functions are critical for the company to remain in business. However, the Covid-19 lockdown is the first time that many companies will be implementing a work-from-home contingency plan and putting their BCP and BIA to the test.

Paula Sartini, founder and CEO at BrandQuantum

To equip employees to work from home, many companies have put fundamentals in place, arranging laptops, providing connectivity for employees and access to virtual private networks (VPN) to continue with business-as-usual. These are the basic tools that employees need to conduct their daily tasks and meet the business needs but employees will need additional tools and resources if they are to succeed in working remotely at this time.

Increased data threats

With many employees sent to work from home during the Covid-19 lockdown, this is a prime time for hackers to target businesses. Employees have been given tools and access to secure company data without the stringent security in place or necessary training to prevent data breaches. This is supported by various reports stating that hacking attempts surrounding the Coronavirus are on the rise.

According to Wired, coronavirus phishing scams already started circulating in January, preying on people's fears about the virus. This is supported by Cnet which reported that the coronavirus is one of the fastest-growing tactics used for hacking attempts with phishing attacks and malware campaigns being the main categories of attack.

While companies strive for business, as usual, they need to have measures in place to protect their employee and customer data. Customers have taken precautions to safeguard their personal information and verify the companies they provide personal information to, trusting that these companies have measures in place to keep their data secure.

Whether employees are working from home or the office, customers expect them to keep their data secure at all times.

How safe is your brand in the hands of a remote workforce?

Paula Sartini 23 Mar 2020

Securing data

There is no single solution to keeping data secure, particularly with a remote workforce as often homes have fewer security defences than that of an office. Hackers are aware of this. Further, they prey on the vulnerability of employees and customers that would be distracted by the circumstances surrounding them and more likely to fall for a scam.

To help prevent employees and customers from falling victim to these scams companies should incorporate layered security measures to boost security and add extra peace of mind. Many companies have VPN access as a security mechanism for employees to access company information. For companies that do not have a VPN or those looking for added security for their VPN, a cloud network should be used to keep company documents and data secure.

Secure access to resources

To perform their jobs effectively, employees will need quick and easy access to the most up-to-date company resources. They will also need relevant content that is consistently branded and compliant that can be shared with customers timeously.

This content should be housed securely on a cloud platform to allow easy access to relevant documents via the internet. Access should be restricted to those departments and individuals that need access to perform their job function. In addition, access should be tracked to monitor which employees access what documents and when.

All company documents should also be saved and managed centrally to allow for changes to be made and shared rapidly and easily with employees, ensuring that all employees use the most up-to-date and relevant documentation. To prevent non-compliant documents from being sent to customers and prevent possible fraud, no employees should be able to save documents to their desktops for future use as these can easily be tampered with or shared with employees that do not need access to them.

Secure email communications

Emails solutions used by the remote force should be designed with the segmentation of risk in mind. This means the

solution uses independent silos to safeguard the content of the email as the content is not associated with the context of the email. This is key to preventing security breaches and keeping employee and customer data secure.

To give the recipient's peace of mind that the emails are authentic, emails should have built-in verification that allows users to verify the emails sent from one user to another with a pass/fail verification report. In addition, users can check if the content of the email has been tampered with when receiving replies to emails. To prevent false reports, emails should have email signatures and banner applied during the drafting of the email to prevent the need for system intervention as this could impact on emails reaching recipients and being flagged as spam.

By putting your customers and employees security needs at the fore, companies demonstrate their commitment to their customer's safety, building brand trust and establishing the foundation for a long-standing partnership.

ABOUT PAULA SARTINI

With over 20 years' experience helping leading organisations overcome various business challenges, Paula understands the challenges that companies face in delivering a consistent brand experience and the impact this has on their bottomline. An analytical thinker that strives to solve business problems with innovative solutions, Paula believes that technology plays a major role in solving critical business and branding challenges. As such, she established BrandQuantum to help businesses overcome their branding challenges in the digital age.

- How secure is your company data during a lockdown? - 4 May 2020
- Marketing and IT: Will the great divide continues in 2020? - 17 Dec 2019

View my profile and articles...