Is Your Data Security Plan Ready For COVID-19?

cyber security pandemic

Summary: While most community financial institutions had a formal data security plan before the COVID-19 outbreak, cyber risks have increased as staff was moved to working remotely. Tips to secure your data security plan during the coronavirus situation.

In a Gallup poll from April 3-5, 71% of Americans said that they would "wait and see" what happens with the coronavirus before getting back to a routine, even after the government lifted COVID-19 restrictions. This hesitancy to change is understandable when you consider the tremendous changes we have experienced in the past few weeks. Cyber risks have changed too, so reviewing your data security plan for coronavirus-readiness is critical.

While most community financial institutions (CFIs) had a formal data security plan before the outbreak, cyber risks have since increased as staff moved to working remotely. But, CFIs can make sure they have the required procedures and controls to continue safeguarding customer data through COVID-19.

NuData Security VP Robert Capps notes that the precautions already used by financial institutions, such as data loss prevention software, antivirus and malware removal tools plus behavior analytics and anomaly detection should cover most of what is needed. But, there are definitely challenges that need to be addressed too.

Many layers of security. With the swift move to work remotely, there were many moving parts for CFIs. Computers and other hardware needed to be outfitted with the proper software, and system access credentials needed to be updated. A greater number of devices and connections set up in a short period of time could cause problems, if care is not taken. Also, an extra layer of security should be considered with increased online collaboration. Multifactor authentication through a virtual private network (VPN) is a secure way to access shared documents and programs. You will also likely encrypt more documents as your staff is sending them electronically more often these days. These types of adjustments should be included in your data security plan.

Stay vigilant even at home. But, a plan is only as good as its participants. Once employees are working in a different environment, such as in a living room or at a kitchen counter, they may feel more comfortable and less professional. That can lead to an opportunity for cyber thieves. Remind your employees how important it is to have the same protocols at home as they did at the office. The computer should only be used for work-related projects, anti-malware and anti-virus protection should be run regularly and emails with links should be expected or followed-up. They should also continue to lock their computer when they take a break to ensure no one else in the household has access to it. Sending them regular updates on the latest ways that cyber fraudsters are trying to fool banking employees will keep them on track too.

Customer communication is needed. Last but not least, a good data security plan calls for educating the very customers it protects. Communicate with your customers in short and focused ways. Tell them how you are keeping their information safe while reminding them what they should (or should not) do to help keep their data safe.

We know this situation has been an adjustment for everyone. We will all get through this together.

SAVE TIME AND MONEY WITH OUR STRESS TESTING SERVICE

Now more than ever, it is important to stress test loans of all types from multiple perspectives and on a portfolio basis. Get expert help to save you time and money. Learn more about stress testing today.