CPA
Practice Advisor

cost millions of dollars to mitigate, they also cause untold reputational damage, violate the privacy of clients, and result in federal compliance headaches.

Sep. 15, 2015

It should come as no surprise that the financial industry suffers from more cybercrime than any other industry, due in large part to the valuable information the industry traffics in, including bank information, social security numbers, and other personal financial details.

As a result, management at financial institutions should maintain security as a

absolutely no excuse for denial when it comes to data breaches, and security must move to the front of mind—and action.

So what steps can CPA management take to ensure that the appropriate steps are being implemented when it comes to securing sensitive client and company information? Here are a few that I've seen be particularly useful:

Embrace the cloud.
All the recent data breaches, from Target to Sony to Premera, have occurred on outdated legacy network systems with gaping security vulnerabilities. The cloud has the means to be safer than on-premise systems as long as everyone's using it correctly. What's more, your CPAs are probably already using the cloud, whether it's officially sanctioned or not.

The truth is that 80 percent of employees nationwide admit to using unapproved software. They use the cloud in their personal lives, and it's only natural that they want to translate its benefits to their work lives, too. Often, it's a no-brainer: Cloud platforms like Dropbox or Google Drive boost productivity and efficiency and let employees work seamlessly from home or on the go.

However, these workarounds ought to be a major red flag for IT: If the company's not approving cloud software, it's not controlling its security either. A savvy IT department will make the switch to the cloud sooner rather than later and deploy security measures tailored to the cloud.

Educate your staff about BYOD.
"Bring Your Own Device" (BYOD) culture is on the rise with everyone, and CPAs are no exception. Approximately 90 percent of companies have BYOD policies in place already, which certainly helps CPAs be productive in and out of the office, have access to client files at their fingertips, and be efficient and responsive. But it's important

that with BYOD policies comes BYOD knowledge. Staff members need to know how

The CPA brings his tablet to the meeting, which contains the client's financial and tax information. If he leaves that tablet on the subway on the way home, say, that client's confidential financial data can be easily exposed, damaging the client and the CPA. More than 70 million smartphones alone are lost each year, and only 7 percent of those are recovered—so it's absolutely essential for everyone to know what's going onto their mobile devices and how to properly secure the data.

Encrypt sensitive data.
Encryption is the key to using the cloud securely, and while most cloud platforms encrypt files by default, their encryption does not generally extend to files synced to mobile devices. Make sure you're reading the fine print when you transfer to the cloud, and add an extra layer of protection to your files by deploying file-level encryption.

Knowing that the files themselves are encrypted—not just the place where they reside—ensures peace of mind. This way, whenever a file is synced, shared, or emailed, it will remain encrypted, accessible only to authorized users. Separating the encrypted content from the encryption keys is also something to keep in mind: When the keys are separate, neither the cloud provider nor the encryption provider can access your files, either—or give them up, in the event of a breach.

Revisit security often.
Switching to the cloud and establishing security protocols are essential steps, but security doesn't stop there. Technology is evolving at a rapid pace, and so is hackers' sophistication. Once you've implemented necessary safeguards, make sure you're changing passwords often, maintaining an audit trail, and updating security measures regularly.

———————

Asaf Cidon is CEO and co-founder of Sookasa, a cloud security and encryption company