CPA
Practice Advisor

enough to physically secure the paper records you had so others couldn't view them. Just as our society is adapting its laws, regulations, and definitions of terms like ...

Brian Tankersley • Aug. 21, 2022

When working papers and confidential information were stored on paper, it was enough to physically secure the paper records you had so others couldn't view them. Just as our society is adapting its laws, regulations, and definitions of terms like privacy in the digital age, accountants and their firms must adapt their work processes to incorporate security technologies like encryption and password management. With that in mind, I will use this month's column and next month's

column to address one of the key pillars of modern information technology, data

typically expect them to include encryption of the data "at rest" as well as encryption of data "in transit". We will discuss practical methods to encrypt data while it is stored on a server (we call this "at rest") in this month's column, and will follow up next month with some coverage of how to protect yourself when accessing data remotely next month when we discuss encryption of data "in transit."

Some of the tools which use encryption to protect data while it is "at rest" include:

- **Full Disk Hard Drive Encryption** – A method of scrambling all of the data on an entire drive so that it is unreadable without the password or key. Unlike piecemeal solutions which address the security of individual files, full disk encryption tools use a program which is installed on the local computer or device to automatically encrypt and decrypt data as it is written to a drive and read back from a drive. Drive encryption has little, if any, effect on speed for most computer users, and can be applied to an entire device (like a hard disk, a solid state drive, or a flash drive) or to one or more partitions (subdivisions of storage space) on a device. Some of the tools which can be used to encrypt storage devices and partitions include Windows Bitlocker, VeraCrypt, and Symantec Endpoint Encryption. I've used Windows Bitlocker for years, and while it's painful when you occasionally have to enter the Bitlocker recovery key (always back up that recovery key where you can find it, or you'll be sorry!), it has no impact on my use of Windows apps.
- **File-Level Encryption** – A method of protecting data in individual files using passwords, encryption keys, or authorization servers. File level encryption is used to protect individual files, but the rest of the disk may or may not be protected. Many tools can be used to provide file-level encryption in different scenarios, including Windows Encrypted File System (EFS) (to protect individual files or folders on a Windows hard disk), AESCrypt (scrambles individual files using a separate application), and 7-Zip (a utility which can create and access password-protected archives of files and folders). Some applications, like the Microsoft Office

applications and Adobe Acrobat allow users to encrypt a file by protecting it with a

Some IRM solutions used by businesses include Azure Rights Management ES, Windows Information Protection, and Microsoft Office 365 IRM. IRM creates some issues, but is becoming an important way businesses protect their sensitive data from interception by outsiders, and it permits companies to take away a user's ability to access data which has been inappropriately removed or stolen from its servers.

With the proliferation of new laws and regulations covering data privacy from California as well as the European Union's General Data Protection Regulation (GDPR), it's more important than ever to encrypt sensitive data wherever possible so you can meet your obligation to your clients to keep information transmitted in confidence secure from prying eyes. Next month, we will present part two of this series– how we protect data "in transit" with encryption as we access or retrieve it from a remote location.

=======

Brian F. Tankersley, CPA.CITP, CGMA (@BFTCPA, CPATechBlog.com) advises firms and companies on accounting technology issues. He has served as the technology editor for a major accounting industry publication, and currently teaches courses in the US and Canada through K2 Enterprises for professional accounting organizations across the US and Canada. Brian and his family make their home in Farragut, Tennessee.

Accounting • Technology

Sponsors.