To get your plan started, I suggest you begin with the most widely accepted rule for creating a good backup plan, called the *3-2-1* rule:

- **Keep three copies of your data.** One copy is your primary copy, the one that is accessed every day. The other two copies are backup copies.
- **Use two different types of media.** If you keep all three copies on the same type of media, all three copies will be subject to the same risks. Therefore, you should use at least two types of media. Local disk storage is used for the primary copy, but at least one of the other two copies should be something other than disk, such as cloud-based storage or tape.
- **Keep one copy off-site.** If all three copies are stored together, a physical calamity such as a fire can destroy all three copies. Therefore, at least one of the backup copies should be stored somewhere else.

The 3-2-1 rule has been around for decades and has served us well, but I think it needs an update in light of today's environment. Here's my new version of the 3-2-1 rule:

- **Keep three backup copies of your data.** One primary and two backup copies are no longer sufficient in today's world, where threats to our data are constant and sophisticated. So I recommend you plan for three backup copies in addition to your primary data.

  TIP

  A bit later in this chapter, I discuss the concept of backup *restore points,* which refer to how many date-specific copies of your data are contained in a backup. When I say you should keep three backups, I don't mean to keep three restore points. Instead, you should keep three distinct sets of backups, each stored on different media and in different locations. Each of those three backups can and should contain more than a single restore point.
- **Keep two copies off-site.** Your main backup copy should be kept close to your primary data for fast recovery. It isn't so important that you have two distinct types of media, but it is imperative that you keep backups off-site to protect your data in the event of a physical disaster. One option for off-site backups is the cloud. The other is a backup target that is located at a different site, such as at a branch office.
- **Keep one copy offline.** Off-site is not the same as offline. These days, your off-site backup copy is likely to be either an off-site backup appliance or the cloud. As safe as these backup locations may seem, they are not completely safe from the efforts of a highly motivated and high skilled cyberattack. If all your backups are online, a hacker can break into them and delete your backups. And that would be the ultimate nightmare scenario: That you come in to work some day and find that your primary data has been erased, your