FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Business Blog

# Six steps toward more secure cloud computing

By: Elisa Jillson and Andy Hasty | June 15, 2020

For businesses, cloud services are kind of like clouds. At their best, they can be soothing and expansive. But for companies that fail to appreciate the security implications, their ethereal presence may hide dangerous storms within. As cloud computing has become business as usual for many businesses, frequent news reports about data breaches and other missteps should make companies think carefully about how they secure their data. The FTC has six tips for your business about making your use of cloud services safer – both for you and for the consumers who rely on you to safeguard their information.

1. **Take advantage of the security features offered by cloud service companies.** Cloud providers offer detailed guidance about their security controls and how to set up their services in a more secure fashion. But it's up to you to understand the options and configure those settings in the way best suited to your business. Keep in mind that it's not a matter of a simple on-and-off switch. Configuring your cloud security requires you to make thoughtful decisions that align with the sensitivity of the data you store and how you use it. In addition, think carefully about who at your company needs what data. Unless employees have a legitimate business reason, they shouldn't have access to your cloud resources. Require multi-factor authentication and strong passwords to protect against the risk of unauthorized access. Furthermore, never hard code passwords in cloud-based applications or source code. You may think you're saving steps, but it's the business equivalent of a "Hack me!" sign.

2. **Take regular inventories of what you keep in the cloud.** Some companies' cloud storage resembles a forgotten attic overdue for a spring cleaning. Whether you store data in the cloud, on your network, or in a file cabinet, you can't keep data safe if you don't know where it is. That's why up-to-date inventories are essential to data management. Many cloud services provide tools – for example, dashboards or management consoles – for just that purpose. But don't just set it and forget

it. In addition to staying on top of what data is where, make sure your security configurations and access rights remain consistent with the sensitivity of what you've stored. As you add data that may require more protection, re-evaluate your security settings and amp them up accordingly. Also, don't take anything on faith. Actively test for misconfigurations or other security failings that could compromise your data and maintain robust log files so you can continuously monitor your cloud repositories. We've all read reports about sensitive data stored in a cloud repository open to the internet and you don't want your company name in the next headline.

3. **Don't store personal information when it's not necessary.** One upside of cloud storage is that it's often less expensive than other methods. But as people with big basements will tell you, the list of stuff deemed "essential" tends to expand in direct proportion to how much storage space is available. As you conduct that inventory of what you keep in the cloud, resist the temptation to hold on to data "just because." Instead, be ruthless in posing the question, "Do we have a legitimate need to store this information?" If the answer is no, dispose of it securely. No one can breach what you don't have.

4. **Consider encrypting rarely used data.** "There's some information I don't have to access regularly – back-ups, for example – but I do need to retain it." We hear you and we have a suggestion. As part of your defense-in-depth approach to security, consider whether to encrypt that data at rest. Indeed, if your data contains sensitive information, encrypting that data is a basic principle of security regardless of where it's stored.

5. **Pay attention to credible warnings.** Some cloud providers offer automated tools to remind you about cloud repositories that are open to the internet. Others may contact customers with warnings like that. In other instances, security researchers may contact companies when they find exposed data online. If you receive one of these warnings, pay attention. Investigate your cloud repositories and recheck your security settings.

6. **Security is your responsibility.** Using cloud services doesn't mean you can outsource security. Throughout the lifecycle of data in your company's possession, security remains your responsibility. Even if you rely on your cloud provider's security tools, you should still have a written data security program that lays out your company's process for securing consumers' personal information, and people on your staff knowledgeable about maintaining, monitoring, testing, and updating that program. Yes, you need to review your cloud contracts carefully to spell out your expectations and clearly establish who is primarily in charge of what. But keep in mind that if it's *your* data, it's ultimately *your* responsibility.