Ten Ways to Protect Your Small Business in the Cloud

By Andrea Lindzey

This article originally appeared on Spanning.com

You're making the switch to the cloud. Congratulations- you're in the company of over five million businesses across the world that value agile, reliable communication and data management. But you keep hearing about serious security breaches, shrinking privacy, data loss, and other hazards of cloud computing. Understandably, you may be a bit nervous about your organization's data protection. Is there anything you can do to protect your business from threats lurking in the cloud?

Here's the truth: You company's vital information (in the form of financial records, client accounts, intellectual property, emails, and more) remains vulnerable to a host of dangers simply by virtue of being stored online, in spite of several security measures that cloud vendors typically observe. The nature of the Internet makes hacking and sync malfunctions inherent risks, but there are several things you can do to minimize threats to security and protect data in the cloud environment:

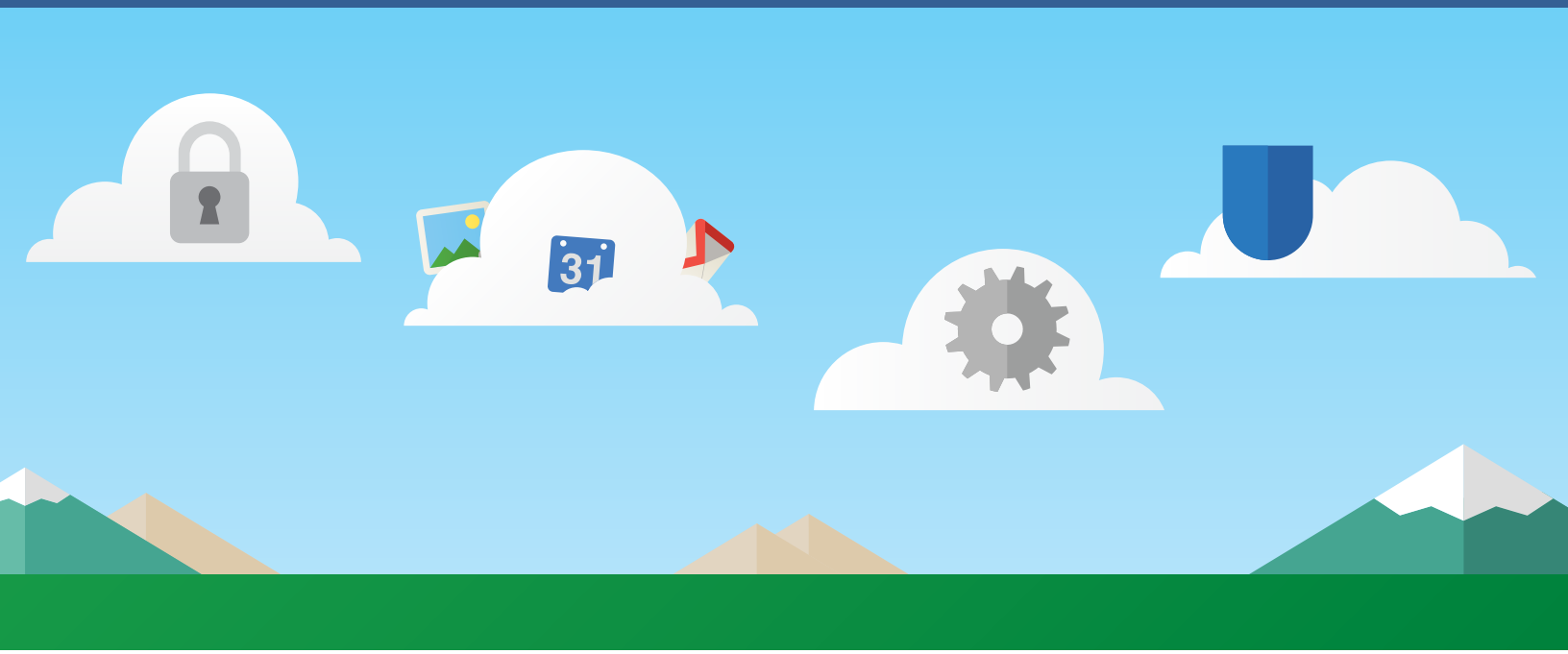
1. **Use two-factor authentication.** Google, Facebook, and others now offer a two-step sign-in process, adding a layer of account security by requiring the entry of an authentication code (usually delivered to your phone via text) in addition to your password. This prevents unwelcome guests from accessing your account from an unfamiliar machine even if they obtain your password. Make sure each user in your domain turns this feature on and carefully selects how and where they receive the authentication code.

2. **Only choose complex, unique passwords.** Password strength is one of the simplest ways to combat malicious online behavior. Here's a guide to putting together a solid password:

    - Do not choose a word or phrase that would be easy to guess.
    - Select a combination of letters that cannot be found in the dictionary.
    - Incorporate capital letters, numbers, and special characters.
    - Choose a password with more than six characters.

    If account holders in your domain need help coming up with a password, suggest they look into a password management service such as 1Password, RoboForm or LastPass which can generate hard-to-guess passwords and to store them on the devices they use most often.

3. **Use multiple passwords across accounts.** Make sure members of your organization know not to use the same password for all accounts, especially those that contain sensitive information like bank statements, health records, and credit card information. Having a different password for each account will prevent someone from gaining access to more than one account if one is compromised.



4. **Change passwords regularly.** Some hacks take a long time and you don't even know when they're happening. Hackers can also crack your password but not get around to wreaking havoc on your online life for several months. For these reasons, you and all users in your domain should regularly change passwords to stay ahead of attacks.

5. **Don't link your accounts.** Often called "daisy-chaining," linking your accounts puts you at risk of losing control of all your accounts at once. If your company's social media team must link accounts, be sure they are using a secure social media manager like HootSuite. Recommend unlinking accounts to all other users.

6. **Be smart about sharing information.** Even if you are confident in your company's data protection, you don't know how secure others that communicate with your business may be. Never allow the transmission of credit-card information, Social Security numbers, or other private information via email (or any instant messaging program) in case someone targets the recipient's account.

7. **Be wary of scams and potential hacking threats.** All users in your domain should know that apps, links, emails, and websites can be faked in order to steal personal information. If company employees are using a new app, make sure you are comfortable with the service and check reviews before anyone inputs private data. Alert employees to phishing scams that use fraudulent emails and fake websites to gather private account or login information. Here are important things for users in your domain to remember:

   - If you receive an email from a business that seems suspicious, call the company to verify that communication is legitimate.
   - Don't open or answer emails from sources you don't recognize, and never click on a link or attachment contained in an email from someone you don't know.

   You can also use a cloud management and security tool like FlashPanel to monitor your domain. This software allows you to see unusual spikes in publicly shared documents, monitor the activity of a potentially hacked account, and automatically filter malicious emails sent from known sources.

8. **Install and update anti-virus software.** Use a trusted source to block and remove cyber-threats like viruses, spyware, adware, spam, and identity theft.

9. **Check for secure technology and encryption.** Make sure your cloud provider's security credentials are strong, and ensure that sites users visit and shop are secure. Here's a checklist you can provide to users in your domain to determine the security level of sites and providers:

    - Sites and cloud vendors should encrypt your data both at rest and in transit. Look for 128-bit SSL in transit and 256-bit AES at rest, as these are among the strongest block ciphers available.
    - These entities should maintain strict security credentials. Look for ISO 27001 certifications, completion of SAS-70 Type II audits, and observation of SSAE 16 and ISAE 3402 professional standards.
    - Seek intrusion protection with log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response. A good backup and recovery solution can provide these to your business.
    - Secure sites begin with "https." That "s" is important, so check for it!
    - Easily spot a secure site by finding a tiny padlock that may appear in the address bar or the bottom right of a web page.
    - Look for a statement that ensures pages are protected by a security technology vendor, and then check that vendor's credentials.

10. **Back up everything.** This is a failsafe mechanism for when your company's data or cloud provider is compromised. Data protection experts strongly recommend backup as companies increasingly manage their data online. Hackers aren't going anywhere; in fact, their methods are becoming more sophisticated. But online dangers don't have to be cause for panic if you are proactive about protecting your company. Backups create a copy of information so data doesn't permanently disappear when something happens to the original version. To be effective, backups must be paired with a recovery system that can return information in cloud applications like Google Calendar, Gmail, Sites, Contacts, and Drive to a usable form. A full backup and recovery solution can not only protect you from hacking and security threats outside your control, but it can also protect you from yourself. One of the top causes of data loss is human error. Without backup and recovery, if a user in your domain accidentally deletes an important email or file, it's gone for good. With the help of backup software, you will never have to risk permanently losing information and can quickly recover any lost or compromised data.

Do business - don't panic. Simply use the tips above to protect your company in the cloud, and be sure to start backing up data before you experience a loss.