SPANNING
by EMC

The Google Apps Admin Guide to Peace of Mind

TABLE OF CONTENTS

Introduction

You've made the switch to Google Apps. 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 starting to wonder if your organization's data protection is really handled. Is there anything you can do to protect your business from threats lurking in the cloud?

We often hear from IT professionals that have rushed into the cloud without considering data protection and now realize they need a solution after the experience of losing something important. "But it's in the cloud!" says the cloud-enthusiast IT pro. Yes, and the cloud is a good thing. But the cloud does not equal data protection just by association. It's an IT professional's responsibility to make sure that the data they've been entrusted with is always ready for the worst-case scenario.

The Cloud Is a Big Improvement, but Don't Ignore the Risks

If you've been reading any technology news lately, you've seen that it's a rough time out there for data protection. When you take a look at recent studies and statistics, the news isn't good. Consider these findings:

- Ars Technica recently conducted an experiment where they handed 3 password crackers a list of 16,449 passwords. 62% of them were cracked in an hour by one of the crackers. Another spent 20 hours and got up to 90%.[1]
- According to an Aberdeen study, almost a third (32%) of SaaS users had experienced data loss in the cloud.[2]
- A Gartner study found that 90 percent of companies that experience data loss go out of business within two years. If data is lost, most companies won't survive it.[3]
- 53% of organizations do not conduct daily backups.[4]
- Nearly one-third (32%) of IT administrators surveyed revealed their organizations do not test their backups.[4]

Sources:
[1] http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/
[2] http://blogs.aberdeen.com/it-infrastructure/saas-data-loss-the-problem-you-didnt-know-you-had/
[3] http://www.gartner.com/technology/home.jsp
[4] http://www.smbnation.com/content/news/entry/survey-says-one-third-of-smbs-don-t-test-bdr-solutions-for-effectiveness

So to summarize, hackers are having an easier time gaining access to important data, which leads to data loss. Data loss leads to productivity loss, financial loss, customer loss, and ultimately in many cases, business loss. Yet many organizations are being lax about taking steps to properly protect their data. Given the importance of an organization's data and the fact that it might be at risk, failing to take the proper precautions seems absurd.

But what exactly are all the threats that you need to protect yourself from?

Hackers: Hackers figure prominently in the list of threats to cloud computing. They're evolving better strategies and tools all the time, and it's fair to say that combating hackers is usually a game of catch-up; businesses tend to be reactive to whatever the latest hack is rather than planning for what might come next. And the hacker's weapon is usually the internet, which is accessed (to grossly understate it) on a pretty frequent basis.

Data Loss: The risk of cloud data loss is real. Accidental deletion happens a lot more often than people think, but it's not the only way to lose data. A bad sync or system failure can turn data into memories at the drop of a hat. While interruptions and business continuity can be expensive in terms of lost productivity, the bigger issue may be the way it makes you look in front of your clients. Not only could data loss cause your customers to lose faith and take their business somewhere else; depending on the kind of data lost, it could cause legal issues that could go on for years.

Malicious Insiders: We've all heard stories about malicious employees who decide to do some major damage on their way out the door. And it may be hard to see anyone around you who seems like they might do such a thing, but even so, you should make sure no one gets the chance. Ask yourself what kind of access does everyone have to sensitive data? If you were to hear that someone got fired, how quickly could you revoke their access to all of your data? What about on mobile devices? Do you have a solid BYOD plan in place? These are some of the things that, while certainly not pleasant to think about, need to be considered for the long-term health of your organization.

Lack of Due Diligence: Choosing a cloud computing provider (i.e. anything that ends with "aaS") often comes down to who has the best deal. But before you sign on the dotted line, you need to know who is responsible for what security measures on both your end and theirs. You need to know who's doing the encryption and how things are going to go when there's an outage. If you haven't asked these questions, you could be setting yourself up for some real problems when you least expect it.

If you're not sure how worried you should be about cloud data loss, consider these examples:

- "In the space of one hour, my entire digital life was destroyed." This tech writer, recounting his experience of being hacked, says the cost to recover his data was $1,690 along with a couple of weeks worth of lost time trying to figure out what happened and undo it. Some of the data was permanently lost, but thankfully, not the pictures of his daughter's first year.
- "I'm not going to name names as I don't want anyone to feel bad, but I just had a report from a member of the team that they accidentally deleted everything off the Google Drive. I had a backup from a few weeks ago which I have restored but if anyone has translated anything since then could you please reupload it if possible and check that your other work has been restored correctly. Unfortunately I think StorMyu's recent organisational spreadsheet got deleted and will need to be recreated." This is from a translation forum for a popular video game and represents a common data loss scenario in which hours of work will need to be recreated.
- Even the National Intelligence Council (NIC) in the US is not immune; their chairman's personal email account was hacked, resulting in the publication of email exchanges with 9/11 Commission members as well as documents covering the second Obama administration's transition.
- "Keys retained, enterprising employee works late into the night (well, at least until The Boss has gone home) then goes into the server room and pulls out The Big Book Of Passwords. Enterprising employee then proceeds to delete the account with the cloud computing provider, taking out the e-mail (along with many other things). 10 years worth of company e-mail nullified with a keystroke." This is a story from an IT administrator who saw firsthand how the cloud could not prevent data loss from malicious insiders.

Cloud data loss can cost you a lot of money, your reputation, your time (and everyone else's), your memories, and perhaps most importantly, your peace of mind. For as many examples as you can find by googling, you can probably think of just as many in your own life. Data loss can and will happen, even in the cloud, and if you don't want to find yourself staring down a "moment of truth" with no plan, you need to take steps to prevent damage from these threats.

Doesn't Google Take Care of This?

Among the benefits Google guarantees with Google Apps is data security, including encryption, authentication, reliable access, a high level of user control, and backup of data. But users should be aware that when Google uses the term "backed up," it may not mean exactly what they think.

Google saves your work on their servers in real time so that you are always able to access your data, even if your personal computer is stolen or crashes. This is what Google means by "always backed up." Yet what Google is truly describing on this page is syncing your data with their servers. This does indeed allow you to access your Google Apps information should anything unfavorable happen to your hardware, but it does not give either administrators or end users a way to restore their own lost data like a full backup and recovery solution would.

Many users assume full backup and recovery features come standard with Google Apps software and are surprised when they encounter an issue that Google simply can't help them solve. To be clear, Google does back up your data, but this is a different mechanism than the sync process. A data sync provides you and your collaborators with constant access, even as you are editing information, on any machine, because your data resides in the Google cloud. A backup, in contrast, provides a means to recover data should anything happen to it (a server malfunction or natural disaster, for instance). Of course, Google has disaster recovery systems in place, so if there is a problem with one of their servers that could affect your information, they are able to recover any lost data through their own internal backups. However, these backups are not accessible by end-users or even administrators, and they don't cover several common ways of losing data in the Google Apps environment.

Essentially, Google can protect you from their own mishaps, but not your non-hardware related issues. And this leaves a few notable gaps in your data protection - gaps that you need to address.

Recovering deleted messages

If you've deleted a message permanently, by clicking Delete Forever in your Spam or Trash, you won't be able to recover the message using the Gmail interface.

support.google.com/gmail/bin/answer.py?hl=en&answer=132652

File deletion and recovery policy

Anything permanently deleted from Google Drive can't be recovered.

support.google.com/drive/bin/answer.py?hl=en&answer=2405957

Recovering deleted calendars

Delete will permanently erase the calendar. (No one, including those who are sharing or subscribing to the calendar, will be able to access it anymore.)

support.google.com/a/bin/answer.py?hl=en&answer=1084819

But What About Google Vault?

We hear from a lot of people out there who are looking for a backup solution who are considering Vault. And we understand why: Vault sounds like a backup solution. And Google has a product for everything these days, right? Surely they'd have one for backup.

Vault is not it. Vault will not backup your files. It will not restore your files if they've been lost. Here's a list of what you can do with Vault, from Google's website:

- Search your domain's email data
- Place user accounts (and related data) on litigation hold to preserve email data
- Notify users of litigation holds and track acknowledgments
- Manage related searches and litigation holds under a single container, called a matter
- Share matters among authorized users
- Export search results in standard file formats
- Save your search queries
- Set email retention policies for your domain

These are all great things to be able to do, necessary things, important things. And Vault is a great solution to help you do them. But if you need to backup and restore all of your Google Apps on a daily basis, if you need to make sure that you can get your business back up and running as quickly as possible after a minor or major disaster, Vault is not the tool you need.

It's Your Responsibility

Most expert sources now include backup in their list of best practices for all cloud users, especially businesses, as insufficient data protection places revenue, reputation, and therefore, the survival of the entire organization at stake.

But a recent survey conducted by Opinion Matters on behalf of GFI Software revealed some serious negligence in the area of data protection due to lax backup and recovery policies. When you take a look at the reasons for neglecting backup and recovery, areas that everyone knows are best practices, it's not hard to see why they're getting short shrift. Consider these findings:

- More than half (53%) of the organizations surveyed revealed they do not conduct daily backups.
- IT administrators indicated the biggest reason for not backing up data every day is that it's not an efficient use of their time, according to nearly one-third (32%) of respondents.
- Some respondents – including 75% of those who work at organizations with 50-99 employees – said daily backups are disruptive to workplace productivity.
- Other respondents suggested they do not conduct backups every day because they lack the resources, efficient technology or sufficient storage space.
- In order to protect critical information, companies need to regularly test their backup solutions to ensure they work properly. However, nearly one-third (32%) of IT administrators surveyed revealed their organizations do not conduct such tests.
- Many IT administrators surveyed revealed that a failed backup has led to a loss of revenue and important company documents, including financial records, employee emails and confidential information such as social security numbers. As a result, respondents indicated that failed backups have affected customer relations, business operations and brand reputation.
- Those respondents who indicated they were not able to recover data due to a failed backup cited loss of revenue and critical business documents as the biggest impacts on their business. Other IT admins said their organizations suffered the following consequences:
    - The loss of data "caused weeks of problems with clients."
    - "We lost records pertinent to our organization that were unable to be duplicated and had to be reinvented."
    - The impact of the data loss was "...huge, in terms of meeting deadlines and productivity."

When you hear these types of stories about what can happen when you lose data, you HAVE to take the problem seriously. There are just no excuses for being negligent towards data protection; the threats are real and could strike at any time.

Now, we realize that protecting your data, performing and testing regular backups and working on your business continuity plan is not associated with being fun, and these things have traditionally been a pain in the neck with little return. But it has to be done if you want to keep your business up and running at all times.

Think of it this way: we buy insurance for our cars, our houses, our health. We wear helmets, we stop at red lights. We install security systems. We apply sunscreen and do background checks. We update our passwords. We wear a seatbelt. We put on a lifejacket. We stow our tray tables and return our seatbacks to the upright position. We're constantly guarding against threats to our well-being so that we can go about our lives without running into that awful panicky feeling that comes with a moment of crisis.

There is such a thing as cloud data loss. People get hacked. People accidentally delete things, important things. There is a long list of potential threats to your data to think about, and if you're too busy or simply don't want to do so, one of them will find its way to you. And on that day, you'll start spending a lot of time thinking about what you should have done.

What do you do?

The Game Plan: 13 Steps to Protecting Your Google Apps Data

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. Try setting up a monthly or quarterly Google Calendar reminder for everyone to change their passwords.

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. **Keep up with cyberthreats in the news.** When a new kind of attack comes out, some kind soul almost always publishes a step-by-step guide to what you need to enable/disable in order to keep yourself safe. And any time a new hack is announced, go ahead and change your passwords in whatever password management system you're using (which you definitely are using, right?).

11. **Back up everything and everyone.** 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, and if you're backing up some people but not others, you're leaving holes in your security plan. But what kind of backup solution do you need? Your backup solution should be:

    - **Easy to install and implement.** If you're spending a ton of time wringing your hands over basic setup, how's easy is it going to be when you actually need to use it? If the installation process doesn't go smoothly, run.
    - **"Set it and forget it."** You should be confident that you'll be notified when there's a problem so you don't have to constantly monitor for them. If you're spending more than 15 minutes a week dealing with backup and recovery, something's wrong.

- **Recovery-Focused.** The data recovery should be as fast as your internet connection will allow, and the longest part of the data recovery process should be waiting for the files to move around, not figuring out how to get them back where they're supposed to be.
- **Selective.** You shouldn't have to restore an entire account to get to a single lost file. You should be able to restore a single file, a section of an account, an entire account or an entire domain as needed.
- Easy to test. You shouldn't have to wait for a disaster to find out whether or not your backups are working properly; you should be able to do a quick, 5 minute test once a week to ensure that it is.
- Easy to access and use. Are you the one restoring data? Why not let your users do it? If they can handle Google Apps, they should be able to restore their own lost data. Managing their own restores saves you time, and it makes them happy because they don't have to open a ticket and wait for you.

12. **Check the status of your backups.** Backup is key for data security, but if your files are not recoverable before you get hacked, they won't be recoverable afterwards either. This process should only take a few minutes each week to complete.
13. **Schedule regular data security tests.** Make sure all of your data is hard to get into from the outside, make sure it's backed up, make sure it's properly encrypted and make sure it's easily recoverable. And then test all of that on a regular basis. Nuke something important and make sure you can get it back. Make sure nothing has changed that you're not aware of.

Do business – don't panic. Use this game plan to protect your organization so that you can be fearless in the cloud.

About Spanning

Spanning, an EMC company and a leading provider of backup and recovery for SaaS applications, helps organizations to protect and manage their information in the cloud. We provide powerful, enterprise-class data protection for Google Apps, Salesforce, and Office 365. Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world.

Start a free 14-day trial at Spanning.com/try-it-now