SPANNING
by EMC

Don't Gamble with Your Company's Future

The Top 5 Reasons You Need Backup for SaaS Applications

Backup and recovery can prevent data loss and alleviate most concerns about storing and managing data in the cloud.

Introduction

Protecting your data in the cloud: How lucky can you get?

As a business owner or IT professional, you may have wondered, "How safe is the information I store in SaaS applications like Google Apps and Salesforce.com?" You certainly wouldn't be alone; Cloud Industry Forum research indicates that security is the number one concern of CIOs moving their businesses to the cloud, with 84% expressing worry. Or you may be wondering about your ability to access information when you need to – now and in the future: "What if my cloud provider goes out of business? What if their servers fail?" Perhaps you've also thought about how you can continue to adhere to the growing body of regulations surrounding privacy, data protection, and more.

Rather than leaving it all to blind luck, cloud users can easily address these challenges by combining internal and external security best practices with a powerful backup and recovery solution.

In this eBook, we'll take an in-depth look into five major challenges businesses using Google Apps, Salesforce.com, and other SaaS applications face, and we'll help you understand how a solid backup and recovery plan can aid in overcoming them. In five chapters, we'll address security, reliability, and privacy in the cloud by examining the most common culprits of data loss and conclude with a discussion of the need to remain compliant in the collaborative atmosphere of the cloud. Together, these topics comprise the top five reasons you need to implement backup software for SaaS applications today:

1. Hacking
2. Insider threat
3. Human error
4. Sync error
5. Compliance

First up is hacking, and we'll be reviewing trends, research, and expert opinions to help you understand the threat and how to defend your business against it with backup and more.

CHAPTER 1

Hacking

> *"Never underestimate the determination of a kid who is time-rich and cash-poor."*
> – Cory Doctorow, ***Little Brother***

> *"Opportunity makes a thief."*
> – Francis Bacon

Someone's always looking for an easy payoff - and it always comes at someone else's expense.

Chapter 1: Hacking

The New York Times article, "The Year in Hacking, by the Numbers," shares a running joke amongst security experts: "there are now only two types of companies left in the United States - those that have been hacked and those that don't know they've been hacked." Unfortunately, according to those numbers reported, this isn't much of a joke anymore.

Hacking leads to data loss and can put business on hold

Last year clocked a record number of security breaches due to hacking. According to the 2013 Data Breach Investigations Report by Verizon that analyzes a large international sample of organizations each year, there were over 47,000 reported security incidents, 621 confirmed data disclosures, and at least 44 million compromised records. As these figures continue to climb, so too do the sophistication and variety of cyberattacks. Enter the Cryptolocker virus: the latest and greatest hack to hit the Net. Victims state that it comes in through email posing as a legitimate attachment and then quickly takes control of and encrypts all of your data so you are unable to access, edit, or export it. In an extraordinary display of human kindness, the perpetrators offer to return your information to you for a ransom, ever so reasonably priced at a minimum of $300.

Results of the Data Breach Investigations Report

Verizon's DBIR claims that 40% of all the security incidents they encountered involved some type of malware like Cryptolocker, which is created and implanted by hackers. The study also discovered:

- 76% of network intrusions exploited weak or stolen credentials;
- 75% of attacks are opportunistic (not targeted at a specific individual or company);
- 29% leveraged social tactics;
- 13% resulted from privilege misuse and abuse;
- 75% were driven by financial motives;

47,000
reported security incidents among organizations surveyed in 2013

- 78% of initial intrusions were rated as low difficulty (meaning they were easy to perpetrate);
- 66% took months or more to discover;
- 69% were discovered by external parties (even customers);
- While breaches through partners or affiliates remained minimal, the number more than doubled in 2013 compared to 2012.

Using the cloud does not equal data security

As a cloud user, it may be tempting to feel exempt from concern over data loss. However, according to an Aberdeen study, "SaaS Data Loss: The Problem You Didn't Know You Had," almost a third (32%) of SaaS users have experienced data loss in the cloud. And when some people just aren't playing by the rules, all bets are off. In the article, "Backup in the cloud - peace of mind and protection against hacking," tech expert, and Chairman of Spanning's board, Charlie Wood explains:

"Many cloud users assume that the information they store in the cloud is fully safeguarded by the security measures taken by their cloud vendors. While this holds true for several security concerns, hacking is not a threat from which the cloud is impervious. Not only can hackers use code-cracking algorithms and brute force attacks to acquire passwords, but they can also access data en route to storage if it is not fully encrypted. What's worse, cloud companies like Google may not help recover lost data once it has been deleted or corrupted through a digital affront. This means that all the data you store on Google Apps, such as your calendar, contacts, documents and spreadsheets, which often contain important financial information, can be accessed, abused, and permanently deleted by hackers with little hope of getting it back. If information is compromised in SaaS programs (such as Salesforce.com that manages customer accounts, or Workday, which contains sensitive payroll and personnel data), an entire business can be taken down. In fact, 60 percent of companies that lose crucial data shut down within six months of the loss."

44 million compromised records resulting from security incidents

What we can learn from the facts about hacking

So what do the findings on hacking tell us about the risks to your data and your business, and how can companies that rely on cloud applications keep from losing it all?

1. **Complacency leads to data loss and reputational damage.**
   The results included in the 2013 DBIR suggest that there is a high level of complacency among organizations about the risk of security breaches due to hacking. "The assumption is that these attacks only target government, military and high-profile organizations, but our data shows that this increasingly isn't true. Don't underestimate the likelihood that your organization will be a target," researchers recommend. This lax attitude toward hacking explains why so many attacks were rated as "low difficulty" and why the majority of breaches took months to discover (if they were discovered at all).

   The sharp upward trend in attacks through business partners suggests that companies are also not appropriately tuned into the consequences of cyberattacks on partners, suppliers, or affiliates; this may allow hackers access to your information through the back door, so to speak.

   Even more concerning is the possibility of becoming a vector for an attack on customers. Remember when over 40 million debit and credit card numbers were stolen from Target in the middle of the 2013 holiday season? Incidents like these are not only devastating to business continuity, but they also deeply damage brand reputation. It is your responsibility as a cloud user, business owner, or IT professional to protect your company and customers against security breaches.

2. **Education and simple precautions are an important part of defense against hacking.**
   Less than 1% of the breaches reported in the 2013 DBIR used tactics rated as "high difficulty," and over three-fourths of the intrusions resulted from weak or stolen credentials. This indicates that companies are simply unaware of or are not spending time to take basic measures to protect data. If you're a Google Apps user, download The Google Apps Admin Guide to Peace of Mind eBook to learn several vital things you can do to combat threats like hackers and malware in the cloud.

3. **Backup and recovery must be part of any complete data protection plan.**
   CNN Tech reports backup as the number one way to protect yourself from hacking in the cloud, because sometimes even the best and most well-rounded attempts to keep information safe can fail, resulting in significant data loss. That's why you must have a plan to recover from hacking. A backup and recovery solution acts as a digital insurance policy, filling in where there are gaps in your data

621
confirmed data disclosures from reported incidents

75%+
intrusions resulting from weak or stolen credentials

protection plan and allowing you to regain control of your business within your ideal RTO period. If malware infects your network and you are locked out of your files, or if a hacker corrupts or deletes critical business data, you can rely on a cloud application backup and recovery solution to hand you clean versions of files, emails, contacts, customer profiles, and other information you need to keep your business running.

While helping you recover from a hacking event is the primary way that backup and recovery supports your overall anti-hacking effort, companies providing these services can also help your business fend off hackers before they strike by storing your data as securely as possible. Any backup and recovery solution you select should ensure that your information is encrypted so content can't be read by unauthorized users, and that it is only unencrypted when you decide to access your data. Backup services should also protect data in transit via SSL protocol and require passwords for information access and decoding.

Summary: Hacking

- 40% of security incidents reported by organizations surveyed in 2013 involved some type of malware.
- Hacking is not a threat from which the cloud is impervious. Not only can hackers use code-cracking algorithms and brute force attacks to acquire passwords, but they can also access data en route to storage if it is not fully encrypted.
- **Backup** is the number one way to protect yourself from hacking in the cloud.

CHAPTER 2

Insider Threat

> *"It is easier to forgive an enemy than to forgive a friend."*
> – William Blake

> *"Et tu, Brute?"*
> – William Shakespeare, *Julius Caesar*

23%
of all electronic crime events are caused by insiders

Chapter 2: Insider Threat

It's a discouraging but well-documented trend: the insider threat is a top cause of data breaches, according to the CSO Online article, "Report Indicates Insider Threats Leading Cause of Data Breaches in Last 12 Months."

The prevalence of the insider threat has grown so dramatically in recent decades that private and government funded foundations dedicated to the investigation of the topic have been established. Most notably, the CERT Insider Threat Center, part of the Carnegie Mellon University Software Engineering Institute, has been researching the problem since 2001 in partnership with the Department of Defense, the Department of Homeland Security, the U.S. Secret Service, the intelligence community, and private firms, and has developed a database of more than 700 insider threat cases from which they draw conclusions and make recommendations.

What is insider threat?

CERT defines an insider as "anyone who has or had authorized access to an organization's network, system, or data," and points out that "current or former employees, contractors, and business partners are in a unique position to damage an organization's information systems, intellectual property, finances, and reputation." Often breach incidents are the work of malicious insiders, defined by CERT as someone "who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

Data breaches perpetrated by insiders can be triggered by several factors, including:

- recruitment from outsiders (like foreign governments or business competitors);
- monetary incentive;
- desire to destroy a company or an individual in the company (perhaps as a result of being fired, harassed, treated unfairly, or because the employee strongly disagrees with company politics and policies);
- business partners looking to leverage their privileged relationship to gain an advantage;
- unwillingness to let go of intellectual property an employee had a hand in creating.

53%
of companies experienced an insider incident in 2012 and 2011

In some instances, data breaches by insiders can be completely unintentional, yet still cause as much damage as if they were committed with intent to harm a company. Unintentional insider data breach can take the form of accidental disclosure on websites or via email, fax, or mail, the electronic entry of outsiders via an internal employee falling victim to a social engineering scheme (phishing, planted USB drives), improperly disposing records, or loss of equipment (laptops, smartphone, etc.), according to 2013 CERT research summarized in Unintentional Insider Threats: A Foundational Study.

Why should you be worried about insider threats?

Together, both malicious and unintentional insider data breaches contribute to a large portion of the overall pool of security incidents experienced by companies, and the frequency of these attacks or accidents that lead to significant data loss continues to climb.

The CERT 2013 US State of Cybercrime Survey of over 500 organizations (34% containing more than 5000 employees) concluded that:

- 23% of all electronic crime events are caused by insiders;
- 53% of companies had experienced an insider incident in 2012 and 2011;
- 53% of respondents reported that damage caused by insider attacks were more damaging that external attacks;
- the most common insider cyber incident was:
  - unintentional exposure of private/sensitive data for 34% of study participants;
  - theft of intellectual property for 34%;
  - unauthorized access and use of info, systems, networks for 30%;
  - theft of proprietary info like customer and financial records for 31%.

53%
of companies reported that insider attacks were more damaging than external attacks

Clearly, insider threats are widespread – they are also costly. The 2012 Cost of Cyber Crime Study by Ponemon found that the average cost of insider incidents is $166,251 per incident (the second most costly type of cyber crime), contributing to a total cost of $8.934 million lost to cyber crime in 2012. Insider data breaches also take the longest of all cyber crimes to resolve, requiring an average of 57.1 days for companies to recover. These findings are especially relevant for US firms, which Ponemon found to be "much more likely to experience the most expensive types of cyber attacks, which are malicious insiders, malicious code and web-based incidents."

The cloud may be a solid bet for business, but you're still at risk

As cloud users, we often assume that our cloud service providers have all the bases covered when it comes to data security. However, **"customers' systems that rely solely on the CSP for security could be at risk of damage to the confidentiality, integrity, and availability of those resources and data,"** claims CERT in their November 2013 report, Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase I.

What this means is that cloud providers diligently adhere to common security standards, but no matter how robust security credentials are, there may still be ways for data to be lost in cloud applications. While cloud vendors like Google or Salesforce can ensure that your data is not lost on their end (due to a server malfunction, natural disaster, etc.), they often cannot protect you from mishaps on your end of the equation - mishaps like insider attacks. Thus, all cloud users should be prepared to augment CSP security efforts in order to maintain compliance and a well-rounded data protection and business continuity plan.

Considering that your cloud provider may be doing less than you expected to protect your critical business data from insider threats, it may be time to start investigating what you can do to supplement existing security measures to fully protect your SaaS applications like Google Apps and Salesforce.

The most common types of insider cyber incidents are:

- unintentional exposure of private/sensitive data;
- theft of intellectual property;
- unauthorized access and use of info, systems, networks;
- theft of proprietary info like customer and financial records.

Backup is part of any well-informed strategy to handle the insider threat

Even when cloud service providers and businesses take reasonable precautions to protect against the insider threat, it is still possible that an insider will successfully execute an attack. This is why CERT insider threat experts recommend backup and recovery as one of the 19 steps companies should take to prevent and manage insider threat included in the Common Sense Guide to Mitigating Insider Threats, 4th Edition. According to the guide, "organizations must prepare for [potential insider attacks] and enhance organizational resiliency by implementing and periodically testing secure backup and recovery processes."

How do backup and recovery help mitigate the insider threat?

A strong backup and recovery solution will help you address the insider threat in two ways: most importantly, it will help you efficiently recover from a data breach due to insider attack; it can also provide an early warning that an insider has compromised company data.

1. **Recovering from an insider attack**
   "Organizations must run effective backup and recovery processes so they can sustain business operations with minimal interruption if a system compromise occurs," explains the CERT guide to mitigating insider threats. Data recovery is an especially important concept here. With rapid, accurate recovery, companies can restore their data to the last trusted version in a reasonable amount of time. Without the luxury of this kind of recovery mechanism, companies can spend precious time manually returning data to a usable form from exported backups. This is why cloud-to-cloud backup solutions are particularly effective: data doesn't live physically offsite; it resides in a separate, secure cloud structure that safely retains copies of critical business data that can be restored to cloud applications in just a few clicks.

   If the backup and recovery solution you select to protect your organization offers point-in-time recovery, when information in your cloud applications can no longer be trusted, you have the ability to choose which version of your data you want to be restored. You may choose to restore data from the

"Customers' systems that rely solely on the cloud service provider for security could be at risk of damage to the confidentiality, integrity, and availability of those resources and data."

-CERT Insider Threat Center

"Organizations must prepare for [potential insider attacks] and enhance organizational resiliency by implementing and periodically testing secure backup and recovery processes."

-CERT Insider Threat Center

day before the insider attack occurred, or even the week before. Point-in-time recovery is like a time machine that can bring your data back to the exact state it was in on the day from which you choose to retrieve it.

The bottom line is that backup and recovery allow organizations to return to business within a targeted Recovery Point Objective and Recovery Time Objective after a data breach by insiders. The more efficient your backup and recovery solution, the faster you can get back to normal and maintain your desired level of business continuity.

2. **Alerting you to insider attack the moment it happens**
A solid backup and recovery solution will offer a high level of transparency and insight about your data. Each time you back up data, your backup software should notify you if there are any problems with your backup. If a file did not get backed up properly, it may be because the file was corrupted by an insider attack. Knowing that an error has occurred is the first step in addressing and reversing the damage associated with an insider data beach.

Case studies on insider threat prove that backup and recovery are your pocket aces

Consider these case studies, gathered through CERT research, that illustrate the importance of backup and recovery in addressing insider threat:

An information technology support business employed the insider as a computer support technician. *As part of his duties, the insider had administrator-level, password-controlled access to the organization's network. When the insider left the organization, he lost his authorization to access the organization's computer. Three months after leaving the organization, on a late weekend night, the insider used his administrator account and password to remotely access the organization's network.*

The insider changed the passwords of all the organization's IT system administrators and shut down nearly all the organization's servers. The insider deleted files from backup tapes that would have enabled the organization to promptly recover from the intrusion. The organization and its customers experienced system failure for several days…In this case, the insider was able to remotely access and delete files from backup media.

CERT insider threat experts recommend backup and recovery as one of the 19 steps companies should take to prevent and manage insider threat included in the Common Sense Guide to Mitigating Insider Threats, 4th Edition.

If this organization had utilized a backup and recovery provider that stored backups separately from the primary storage location, this company would not have suffered such a severe loss. Critical data was lost for good, yet it could have been easily restored to the company if a proper backup and recovery plan was in place.

A mortgage company employed a contractor and foreign national as a programmer and UNIX engineer. *The organization notified the insider that his contract would be terminated because he had made a script error earlier in the month, but the insider was permitted to finish out the workday. Subsequently, while on-site and during work hours, the insider planted a logic bomb in a trusted script. The script would have disabled monitoring alerts and logins, deleted the root passwords to 4,000 of the organization's servers, and erased all data, including backup data, on those servers.*

The insider designed the script to remain dormant for three months and then greet administrators with a login message. Five days after the insider's departure, another engineer at the organization detected the malicious code. The insider was subsequently arrested.

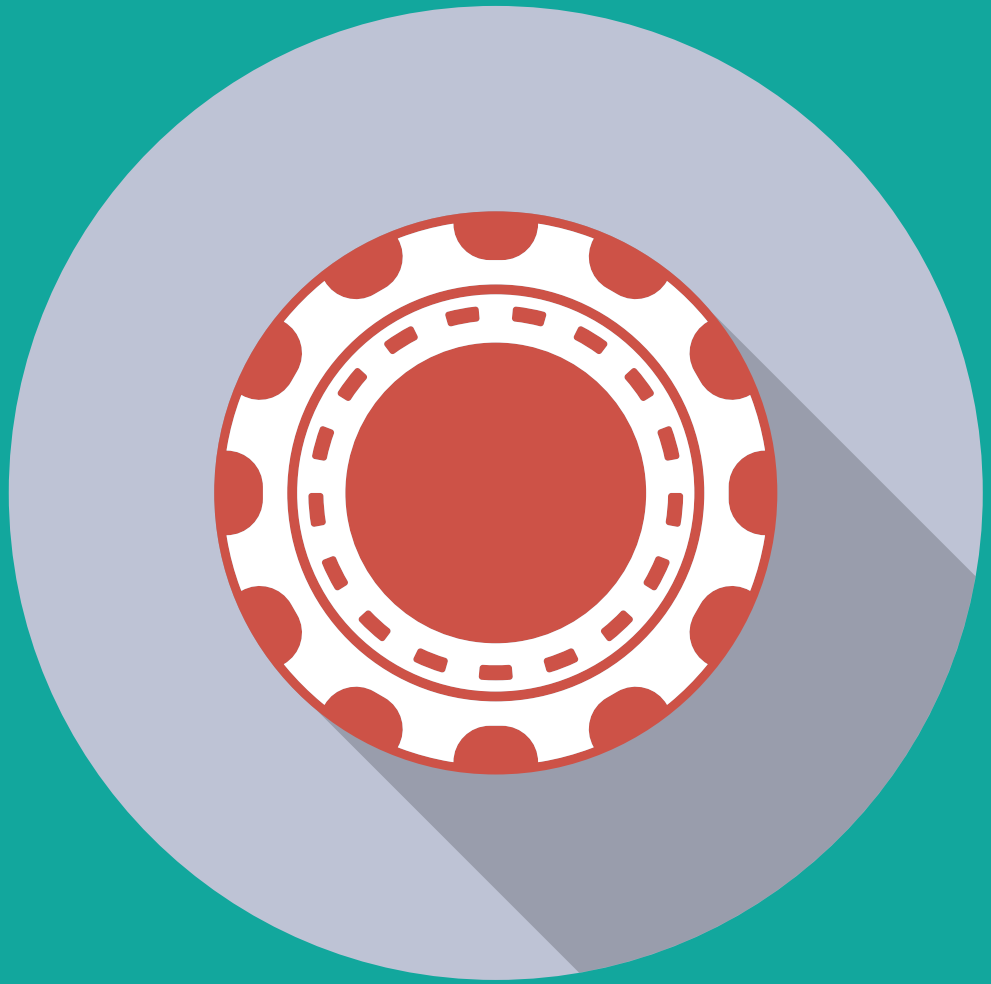
Again, this case illustrates the need for a backup and recovery solution that would allow for rapid recovery from this type of attack. What if that sharp engineer had not noticed the bad script?

Don't leave your company's future to chance. Get backup and recovery before an insider attack forces you to fold.

Summary: Insider Threat

- An **insider** is anyone who has or had authorized access to an organization's network, system, or data, including current or former employees, contractors, and business partners. These groups are in a unique position to damage an organization's information systems, intellectual property, finances, and reputation.
- Together, both malicious and unintentional insider data breaches contribute to a large portion of the overall pool of security incidents experienced by companies. The frequency of these attacks or accidents that lead to significant data loss continues to climb, with *nearly one quarter of electronic crimes being perpetrated by insiders, and over half of companies reporting incidence of insider attack*.
- *The average cost of insider incidents is $166,251 per event*, making this the second most costly type of cybercrime. Insider data breaches also take the longest of all cyber crimes to resolve, requiring an average of *57.1 days for companies to recover*.
- **Backup and recovery** help combat the insider threat in two ways:

1. **Recovering from an insider attack:** With rapid, accurate recovery, companies can restore their data to the last trusted version in a reasonable amount of time.
2. **Alerting you to insider attack the moment it happens:** Backup solutions that offer a high level of transparency and insight about your data will notify you immediately if errors occur during your backups. These issues may happen because data was corrupted by an insider attack, so understanding and addressing error can help you identify and resolve threats before it's too late.



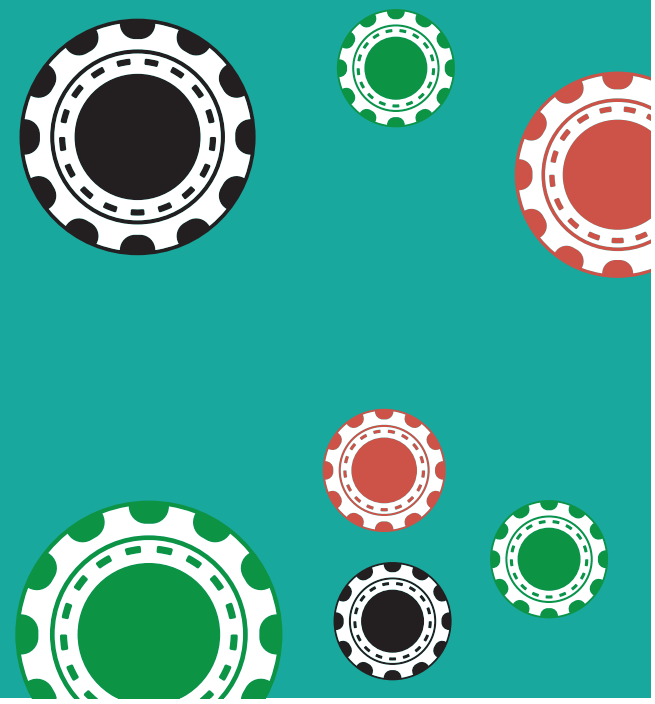
CHAPTER 3

Human Error

> *"It is unwise to be too sure of one's own wisdom. It is healthy to be reminded that the strongest might weaken and the wisest might err."*
>
> – Mahatma Gandhi

> *"As long as the world is turning and spinning, we're gonna be dizzy and we're gonna make mistakes."*
>
> – Mel Brooks

When it comes to preventing human error data loss, backup and recovery are like hitting the jackpot.

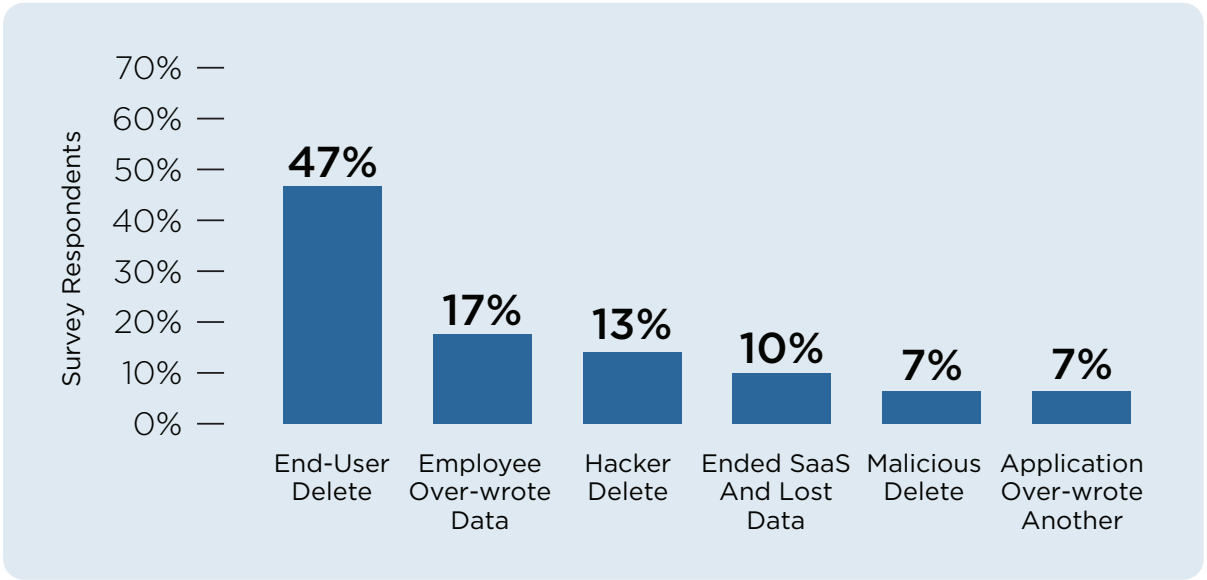


Chapter 3: Human Error

Of all the factors that put your cloud application data at risk, you are by far the biggest threat. That's right, your own unintentional mistakes are the most significant contributor to data loss in SaaS application environments.

Human error is the leading cause of data loss

Human error is not something we like to admit affects our productivity at work, but according to Aberdeen research, it is the leading cause of data loss in SaaS applications, accounting for 64% of data loss among respondents (one of every three of which had experienced significant data loss within their organizations). PC World reports an even higher estimate, stating that up to 75% of data loss may be due to human error.



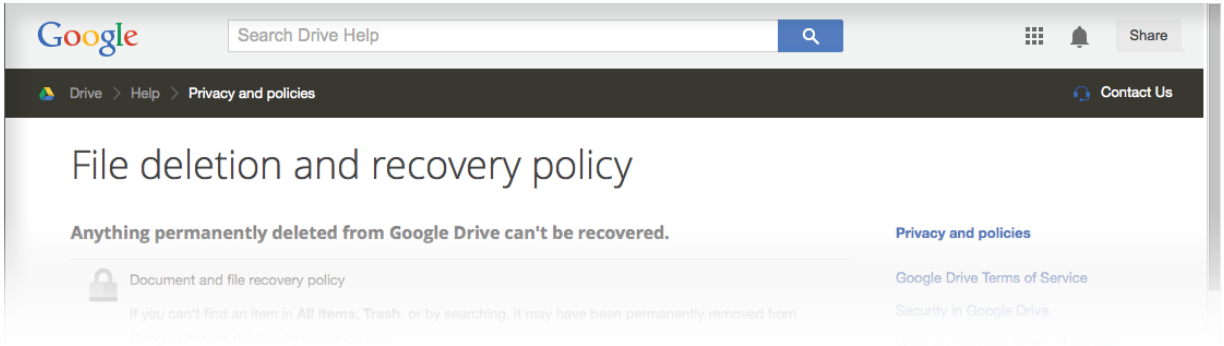
Source: Aberdeen research

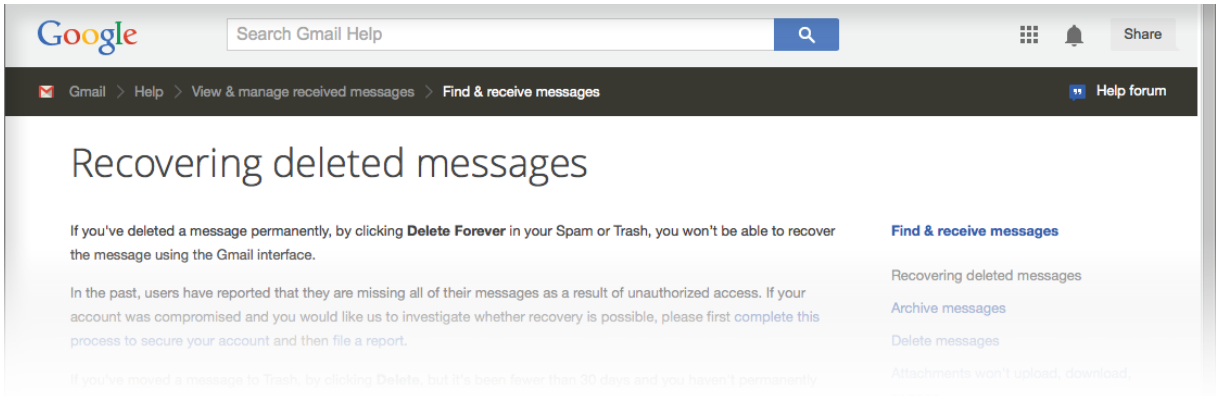
Having an incident response plan reduces the cost of data breach by $13 per record; an important part of this effort includes data loss prevention technology like backup and recovery software.

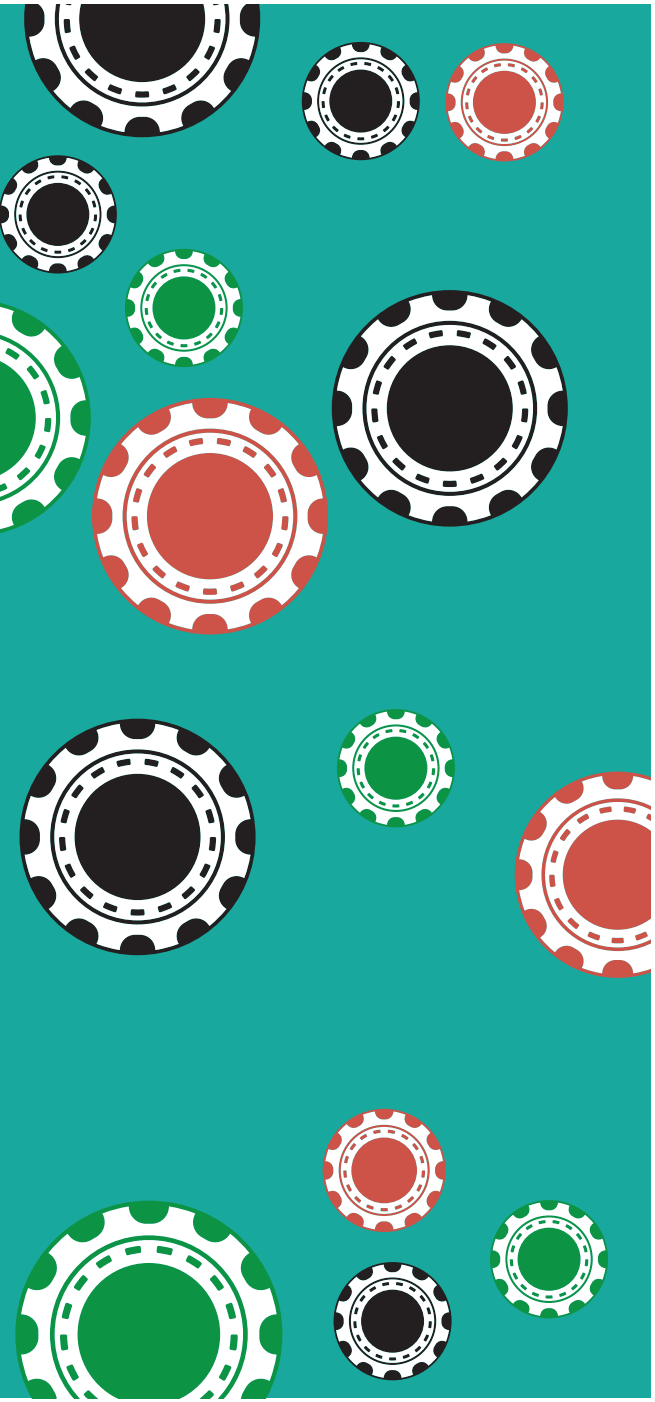
CSPs can't protect you from yourself

The cloud may be a great place to store and manage data, but you can still manage to lose data through accidental deletion and other mistakes - mistakes that cloud providers can't help you recover from.

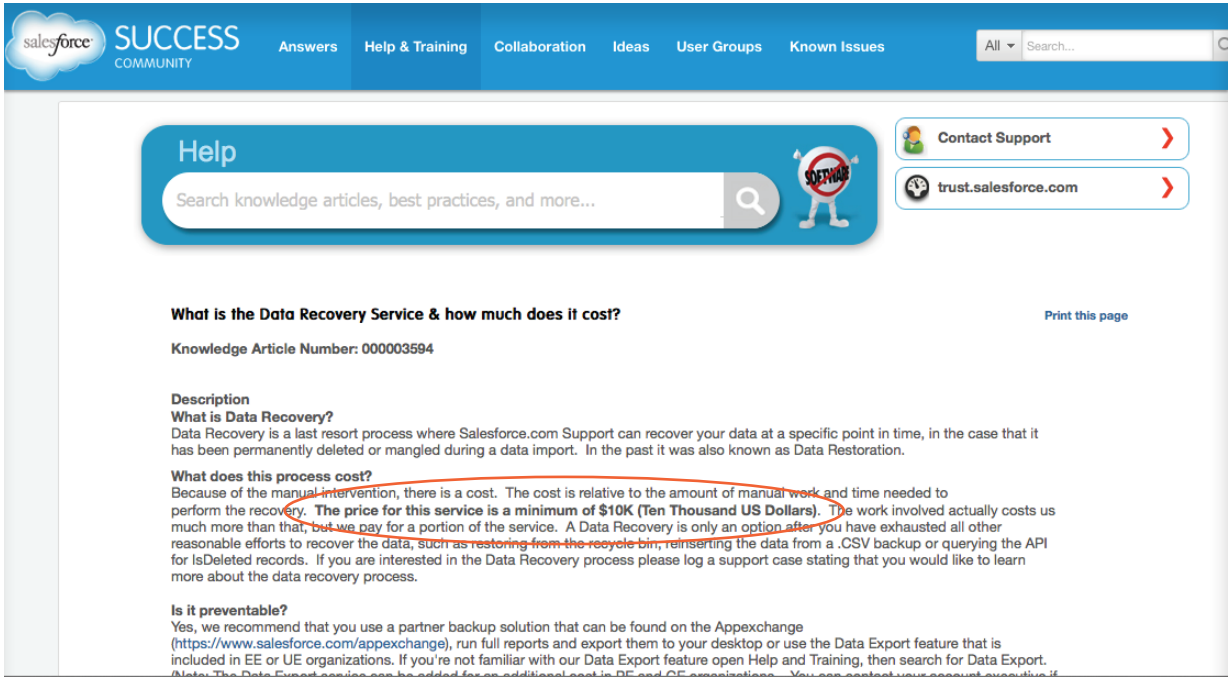
For example, Google stresses that they can protect your data from accidents that happen on their side of things, but if anything happens on your end, they don't provide a convenient recovery mechanism for their users. See the Google Drive and Gmail recovery statements below:







Like Google, Salesforce enables you to rescue deleted items by retrieving them from the Recycle Bin. But your window for doing so is even smaller than Google's - just 15 days. After that, you can initiate a data recovery process, but the price is steep. As Salesforce describes it:



salesforce SUCCESS COMMUNITY

Answers | Help & Training | Collaboration | Ideas | User Groups | Known Issues

All ▾ Search...

Help

Search knowledge articles, best practices, and more...

Contact Support

trust.salesforce.com

What is the Data Recovery Service & how much does it cost?

Print this page

Knowledge Article Number: 000003594

Description

What is Data Recovery?

Data Recovery is a last resort process where Salesforce.com Support can recover your data at a specific point in time, in the case that it has been permanently deleted or mangled during a data import. In the past it was also known as Data Restoration.

What does this process cost?

Because of the manual intervention, there is a cost. The cost is relative to the amount of manual work and time needed to perform the recovery. **The price for this service is a minimum of $10K (Ten Thousand US Dollars).** The work involved actually costs us much more than that, but we pay for a portion of the service. A Data Recovery is only an option after you have exhausted all other reasonable efforts to recover the data, such as restoring from the recycle bin, reinserting the data from a .CSV backup or querying the API for IsDeleted records. If you are interested in the Data Recovery process please log a support case stating that you would like to learn more about the data recovery process.

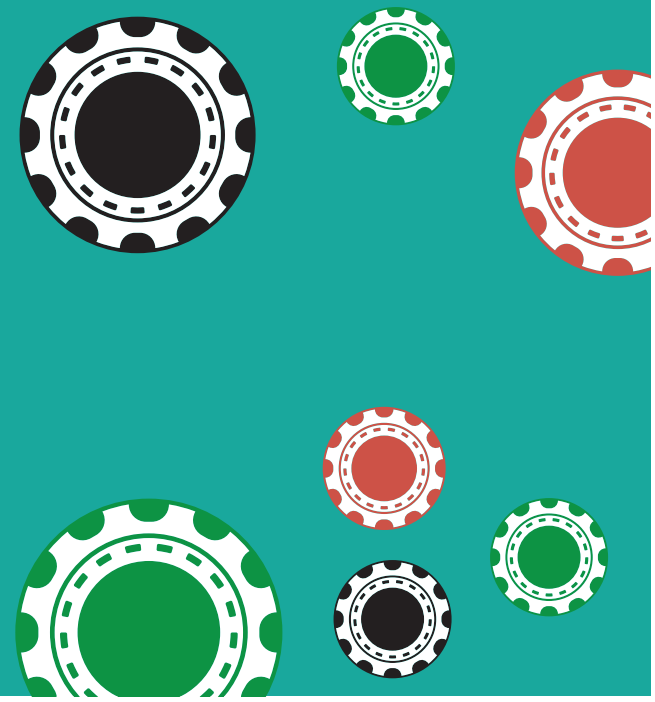
Is it preventable?

Yes, we recommend that you use a partner backup solution that can be found on the Appexchange (https://www.salesforce.com/appexchange), run full reports and export them to your desktop or use the Data Export feature that is included in EE or UE organizations. If you're not familiar with our Data Export feature open Help and Training, then search for Data Export.

You read that right: Salesforce's Data Recovery process starts at $10,000.

For **individuals**, backup and recovery means:

- never having to retype an email from memory that you accidentally deleted from drafts;
- closing sales instead of spending precious time trying to replace contacts that made their way into the trash.



Human error can cost your company greatly

Ten thousand dollars to try and recover your Salesforce data is a lot, but it's not the only price that a data loss can exact. CSO Online points out that data loss due to human error can be devastating to its victims, both emotionally and financially, in their summary of research by Symantec and the Ponemon Institute. "Eight years of research on data breach costs has shown employee behavior to be one of the most pressing issues facing organizations today, up 22 percent since the first survey," explains Larry Ponemon, chairman and founder of the security research think tank. The cost of these types of data breaches is constantly on the rise, says CSO, with the global average cost of a data breach increasing from $130 per compromised record in 2011 to $136 per compromised record in 2012. However, there are ways to mitigate the effects of human error data loss.

How to reduce the negative consequences of human error

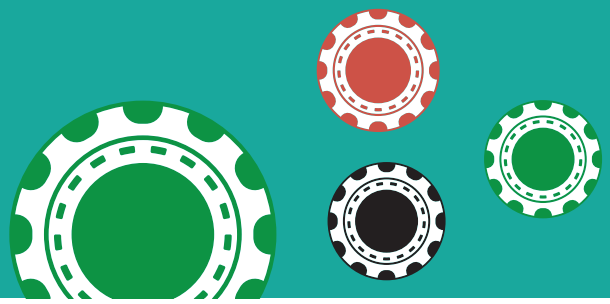
"The key to reducing data breaches for the vast majority of reasons is really to educate employees," says Robert Hamilton, director of product marketing at Symantec. Providing training on data security and how to handle important data can lessen the incidence of data loss due to human error.

Poneman research also revealed that having an incident response plan reduces the cost of data breach by $13 per record. Part of this effort includes "deploying technology like data loss prevention technology," recommends Hamilton. Anil Chakravarthy, executive vice president of the Information Security Group at Symantec, agrees:

"Given organizations with strong security postures and incident response plans experienced breach costs 20 percent less than others, the importance of a well-coordinated, holistic approach is clear."

For **businesses**, backup and recovery means:

- being able to operate smoothly and efficiently even when employees inevitably make mistakes;
- hitting numbers and expected profits instead of losing the customer records, financial documents, and communications upon which business depends;
- making customers happy and instilling confidence in your products, services, and brand instead of apologizing for mistakes that put customer privacy and faith in your company in jeopardy.

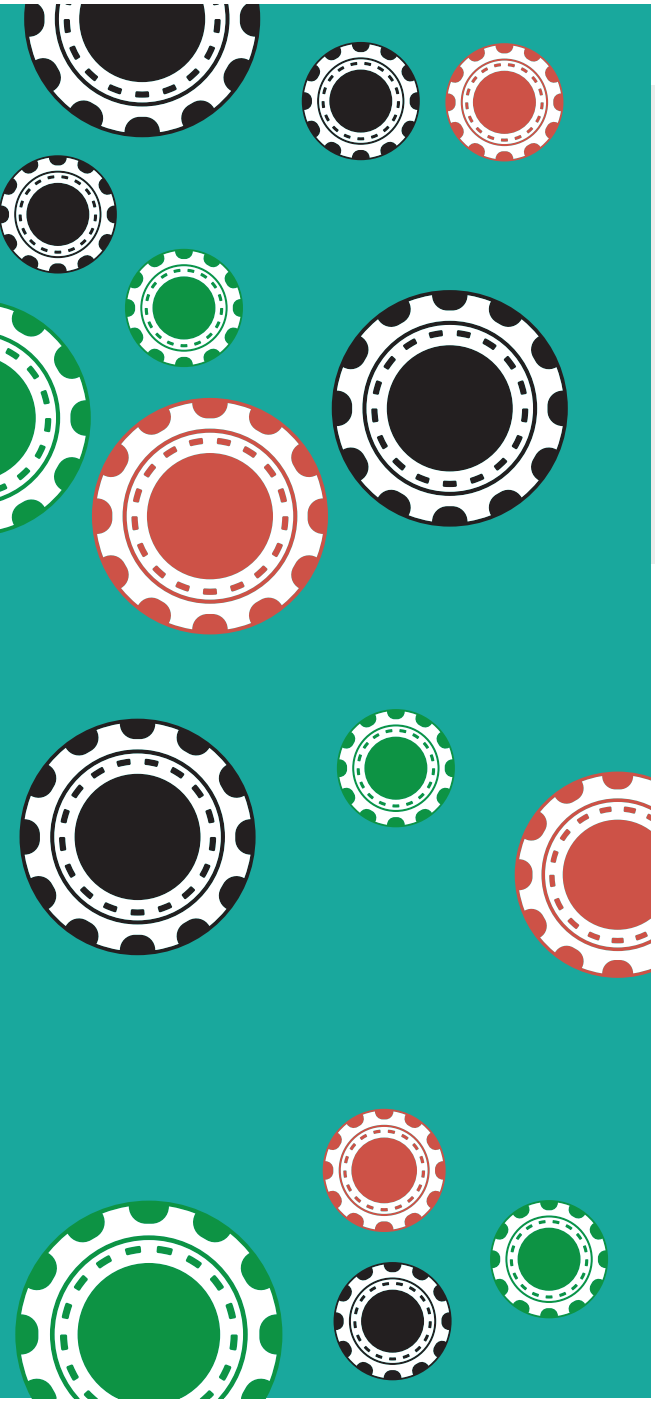


Backup and recovery are an important part of eliminating human error data loss

A major piece of a well-coordinated, holistic approach to data protection is a strong backup and recovery solution. This is because backup and recovery software for SaaS applications can virtually eradicate data loss due to human error. Recovery features allow users to look back in time and restore files they've accidentally deleted, thought they didn't need anymore, mistakenly altered, or lost for any other reason. Even if a user introduces malware or a virus to a company's network, backup and recovery software allows companies to go back in time to restore the last trusted version of all affected data with minimal interruption to business continuity. Without such a solution, companies that experience data loss must spend countless hours - and sometimes even weeks or months - making up for the lost information.

On an individual level, backup software means never having to retype an email from memory that you accidentally deleted from drafts; it means closing sales instead of spending precious time trying to replace contacts that made their way into the trash. For businesses, it means being able to operate smoothly and efficiently even when employees inevitably make mistakes; it means hitting numbers and expected profits instead of losing the customer records, financial documents, and communications upon which business depends; it means making customers happy and instilling confidence in your products, services, and brand instead of apologizing for mistakes that put customer privacy and faith in your company in jeopardy.

Accidents can and will happen in cloud applications, but they don't have to lead to data loss with backup and recovery on your side.



Summary: **Human Error**

- **Human error** is the leading cause of data loss in SaaS applications, accounting for 64% of data loss.
- *Cloud service providers like Google and Salesforce.com cannot protect you from accidental deletion and other mistakes due to human error.*
- The average cost of a data breach is approximately $136 per compromised record.
- **Backup and recovery** software for SaaS applications can virtually eradicate data loss due to human error. Recovery features allow users to look back in time and restore files they've accidentally deleted, thought they didn't need anymore, mistakenly altered, or lost for any other reason.

CHAPTER 4

Sync Error

> *"We are stuck with technology when what we really want is just stuff that works."*
> – Douglas Adams, ***The Salmon of Doubt***

> *"It's supposed to be automatic, but actually you have to push this button."*
> – John Brunner, ***Stand on Zanzibar***

How can you lose? It's easier than you think when you're trying to sync information in the cloud.

- Adopting a new device, updating an existing device, or syncing an existing device with your app can make files, emails, and contacts vanish.
- Losing connectivity while you're syncing could corrupt files, making the information in them inaccessible to you.
- Integrating third-party apps and services can cause on overwrite or complete deletion of your information.
- Deleting unnecessary applications can result in deleting your original data in addition to the copies synced in the applications.

Chapter 4: Sync Error

In the age of the consumerization of IT, our personal and professional lives are increasingly merging, relying on multiple devices, accounts, and applications to keep us connected and informed. We think we're on a roll as these tools sync information to make us as productive as possible. The problem is that every time all those things sync in the cloud, you're rolling the dice on technology that doesn't have 100% of the bugs worked out; if something goes wrong, you could come up with "snake eyes" when you go looking for your data.

Out of sync, out of luck

Although not formally researched, sync errors are one of the most common problems reported by users of cloud applications. In fact, sync errors are so pervasive that Google even has a webpage dedicated to "Error messages for sync problems." If you see this error: "This file points to an invalid online Google document," Google lists the following as the most likely reason: "The original Google document is no longer available online (e.g. your Google document was deleted while you were offline or paused a Google Drive sync)." This may understandably leave you wondering, "Well, who on earth deleted it while I wasn't online? I certainly didn't pause any sync!" Even worse, you may receive this error: "An unknown issue has occurred." And the likely reason: "Something unexpected has happened." Cloud applications like Salesforce that work heavily with third-party applications may have worse odds when it comes to syncing because there's that many more sources exchanging information with each other, and thus, more opportunities to fail.

How sync errors lead to data loss

As Google aptly puts it, "something unexpected" can happen at any time in the cloud due to weak connectivity and a host of other glitches that come with using online technologies. Sync errors happen for a variety of reasons, some of which can result in the loss of information you need most. Here are some of the most common ways a sync error can lead to data loss in cloud applications:

1. **Adopting a new device, updating an existing device, or syncing an existing device with your app**

   - Smartphone users complain about files, contacts, and emails disappearing (sometimes by the hundreds) when they sync a new phone with their account information.

Sync errors are so pervasive that Google even has a web page dedicated to "Error messages for sync problems."

- Several devices, like the Blackberry and iPhone, are reported to drop contacts and more upon updating.
- Sometimes when you have duplicate contacts between your phone and a SaaS application, one list can override or delete the other list when you are updating your device or re-syncing that device with the SaaS application.

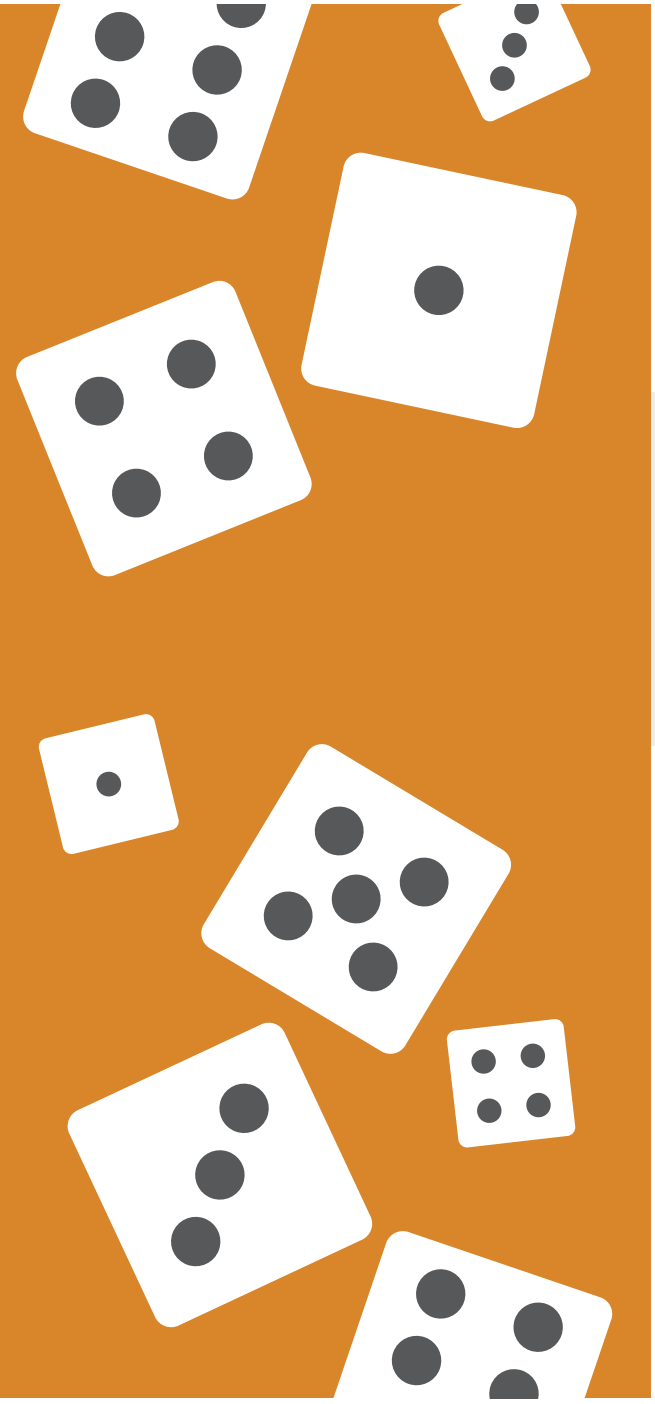
2. **Incomplete or bad syncs**
This can happen when:

- you close your laptop before you are fully synced;
- you lose connectivity while syncing;
- something goes wrong while converting between file formats (from Microsoft to Google Drive, for example).

Often, these types of sync errors cause files to become corrupted, rather than deleted altogether - but this still means that your original data is inaccessible to you.

3. **Third-party integrations and syncs**
Integrating third-party apps and services can cause an overwrite or complete deletion of your information. Suppose you are using an add-on or plug-in with one of your SaaS applications that pulls in data from your existing calendar. But when trying to sync the data between the two, your calendar gets overwritten by the add-on or plug-in. Without a backup plan, there's no way to get these calendar events back.

4. **Deleting unnecessary applications**
When you decide you no longer need an application and want to remove it from your smartphone or computer, you may be surprised to find that that action may also delete your original data in addition to the copies that were stored (synced) in the application. A recent blog post from Alan Davies describes exactly that: *"OK, I admit it, I was fiddling. Fiddling with some new calendar apps on my phone, and when I decided that I no longer wanted one, I deleted it. And it told me that deletion would also delete my Calendar, and I didn't believe it. How could an App be so dumb as to delete my data when all I really wanted to do was get rid of the App from my phone? Well I was wrong, and after clicking on 'OK,' I'd lost all my Google Calendar. And the truly surprising thing was that Google has no restore capability."*



How backup saves you from data loss due to sync errors

Since cloud syncing can be a roll of the dice, you'll want to make sure your data is fully protected from loss with a backup and recovery plan, so that even when you get those snake eyes, there is no cause for panic. Sync errors may make your important information inaccessible, but with backup software for your cloud applications, you can quickly restore your files and get back to work with minimal delay.

Summary: Sync Error

- **Sync errors** are one of the most common problems reported by users of cloud applications.
- Data is at risk during syncing due to weak connectivity and a host of other glitches that come with using online technologies.
- **Backup and recovery** is essential to restoring files lost to sync errors.

CHAPTER 5

Compliance

> *"The price of greatness is responsibility."*
> **- Winston Churchill**

> *"Each player must accept the cards that life deals him or her. But once in hand one must decide how to play the cards in order to win the game."*
> **- Voltaire**

Stop taking chances with regulatory compliance.

- Observe the same standards for your data that were imposed before you moved to the cloud.
- Be prepared for regulations to multiply and evolve to address the adoption of cloud and other technologies.

Chapter 5: Compliance

The February 2014, Forrester Research, Inc. Report, Back Up Your Critical Cloud Data Before It's Too Late: Cloud-To-Cloud Backup Emerges As A Practical Option For Cloud Data Protection, by Rachel Dines, Senior Analyst at Forrester Research, discusses the fact that backup for data stored on-premises has long been a standard best practice, yet backup for SaaS application data hasn't been getting dealt the same cards. However, companies are rapidly finding that not only are backup and recovery for the information they store in the cloud just as critical as for any other type of information, but they are also an important part of passing audits and maintaining compliance with regulations surrounding data storage, management, accessibility, and recovery. There are two things to keep in mind about compliance and cloud technology:

1. **Moving to the cloud does not mean that all your compliance issues are handled by your cloud provider.** You must still observe the same standards for your data that were imposed upon you before moving to the cloud.
2. **Regulations are constantly being added and changed to address the adoption of cloud and other technologies.** Companies should be vigilant to these developments and be prepared to handle them as they multiply and evolve.

Business continuity controls make backup a key investment

Here are some of the most common regulatory frameworks for IT and what they mean for you:

- **COBIT DS11**
  What it requires: COBIT stands for Control Objectives for Information and Related Technology. The DS11 objective deals with the management of data. It requires that companies store and transport data strategically and responsibly, as well as provide mechanisms for backing up and recovering this information. "Management should implement a proper strategy for backup and restoration to ensure that it includes a review of business requirements, as well as the development, implementation, testing and documentation of the recovery plan," according to section 11.23. This is measured by "percent of user satisfaction with availability of data, percent of successful data restorations, and number of incidents where sensitive data were retrieved after media were disposed."

What it means for you: Particularly important here is the recovery aspect of this clause, as the quality of data management is measured by both subjective and objective experiences of the data restoration process in particular. Thus, not only must businesses have backup and recovery in place, but that solution must also be high quality - reliable and easy to use. Companies should therefore be extremely discerning when choosing a provider, looking for the best possible recovery features and examining the user-friendliness of the solution as a whole.

- **NIST CP-9**
  What it requires: This code mandates that "the organization conducts backups of user-level and system-level information (including system state information) contained in the information system."

  What it means for you: This implies first that businesses must backup critical data, and secondly that backup is required for customizations of that data. That means that the custom settings, organization, and metadata attached to company information should be retained in the backup and recovery process. Not all providers are capable of accurately achieving this goal, so businesses should look carefully at the capabilities their selected backup and recovery solution provides.

- **AICPA SOC2**
  What it requires: The SOC2 reports on an organization's ability to maintain security, availability, processing integrity, confidentiality, and privacy within their systems. Companies wishing to receive high marks and prove trustworthy to customers, users, partners, and shareholders must prove sound policies and practices in these areas. And backup plays an important role in nearly all of these domains.

  What it means for you: A backup and recovery solution ensures that data is always available, even when original copies are compromised, because it keeps secure copies of information stored and accessible for recovery in a matter of clicks. The more efficient the backup solution, the more quickly data can become available again after a data loss event. Backup solutions that follow security best practices protect data with encryption and password protected access so that only appropriate parties are able to access information, thereby allowing companies to develop robust claims concerning their privacy, confidentiality, and security efforts.

- **HIPAA 45 CFR 164**
  What it requires: CFR 164, part of a comprehensive code covering the treatment of health and human services information, states a requirement to "establish and implement procedures to maintain retrievable, exact copies of electronic protected health information" and to "establish and implement procedures to restore any lost data."

What it means for you: Clearly, secure, efficient backup and recovery are a recognized necessity in dealing with sensitive records and healthcare data.

How backup and recovery help keep you compliant

Based on the above standards imposed on countless businesses, and the guarantee that more will come into play as companies increasingly rely on the cloud, it is exceedingly apparent that backup and recovery are vital to companies using SaaS applications. Not only does a backup solution for SaaS applications enable compliance with regulations regarding data storage and management, but it also provides the kind of peace of mind that allows a business, from decision-makers to end-users, to utilize the cloud without the fear of being dealt a bad hand.

Summary: Compliance

- **Backup and recovery** are an important part of passing audits and maintaining compliance with regulations surrounding data storage, management, accessibility, and recovery.
- Regulatory frameworks that impose backup requirements include COBIT DS11, NIST CP-9, AICPA SOC2, and HIPAA 45 CRF 164.
- Not only does a backup solution for SaaS applications enable compliance with regulations regarding data storage and management, but it also provides the kind of peace of mind that allows a business to utilize the cloud without fear.

Place your bets on Spanning – You literally can't lose!

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.

Follow us on Twitter @SpanningBackup | Follow us on LinkedIn | Follow us on Google+ | Read our Blog

www.spanning.com | +1 (855) 295-8111

SPANNING by EMC