# SECURITY NOW!

Transcript of Episode #349

## Cloud Solutions

**Description:** After catching up with the week's news, Steve and Leo examine ALL of the various cloud-based synchronizing, storage and backup solutions they could find. Steve surveys each one in turn, and Leo chimes in with his own personal experience with many of the offerings. They conclude that SpiderOak looks like the winner, though Jungle Disk is still in the running.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-349.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-349-lq.mp3

SHOW TEASE: It's time for Security Now!. And Steve Gibson's doing something I'm so excited about. Have you seen all the different cloud storage solutions? There's SugarSync and Dropbox. There's Carbonite. There's Jungle Disk. It goes on and on. He's taken a goodly number of them, looked at the security ramifications of each, the price, and more. And he's got his review of something like a dozen cloud storage services coming up in just a little bit. Security Now! is next.

**Leo Laporte:** This is Security Now! with Steve Gibson, Episode 349, recorded April 19th, 2012: Cloud Storage Solutions.

It's time for Security Now!, the show that protects you, your loved ones online; your privacy, too. And here's the guy in charge, our Explainer in Chief, Mr. Steve Gibson.

**Steve Gibson:** Oh, Leo.

**Leo:** Uh-oh.

**Steve:** I really went down the rat hole this week.

**Leo:** You were going to do - when you talked last week, you said we were going to cover something that I actually like a lot called SpiderOak. You and I have been looking at a lot of cloud storage solutions like Dropbox, Wuala, SpiderOak, Crash - I mean, there's a lot of them. And I'm really looking forward to it because I just kind of empirically - maybe not even empirically, maybe a little less scientifically - chose

SpiderOak, and I've liked it a lot. But so I'm very curious what you think.

**Steve:** Well, so what happened was I started to look at it. I contacted them, and they know us and were standing by in case I had any questions. But when I mentioned last week that SpiderOak was going to be the topic of this week, I started getting all of this Twitter feedback from people saying...

**Leo:** But what about...

**Steve:** ...well, what about BoxCryptor? What about CrashPlan? What about blah blah blah? And I was just like, oh. And some guy said, well, hey, I thought you liked Jungle Disk? What about Jungle Disk? And so I started to look at some of these others, and one thing led to another. And so I ended up putting together notes for Bitcasa, BoxCryptor, Box.net, Carbonite, CompletelyPrivateFiles, CrashPlan, Cubby, DigitalBucket, Dropbox, Google Drive, Jungle Disk, HiDrive, Livedrive, Porticor, SecretSync, SkyDrive, SpiderOak, SugarSync, Tarsnap, and ZeroBin.

**Leo:** [Laughing] I think there are a few you left out, Steve.

**Steve:** I know. That's the problem. Like Wuala. When you just mentioned it, I thought, ooh, that's not on my list.

**Leo:** Oh, one more. No, no, no, no, stop, stop, stop. Stop the madness. Because I think this is a fair sampling of the choices out there.

**Steve:** Well, yes. And just as I was putting this together, then the rumor, which has been circulating for some time, as you mentioned before we began recording, is that next week, maybe on Wednesday, Google is going to drop Google Drive on the world, and with 5GB of free starter storage and who knows what features? So then I thought, well, ooh. What if that's really a good thing, and I've spent all this time digging deep?

Now, I have to say, among all of those that I just enumerated, there are a bunch that are just sort of like, okay, this is not the right solution. For example, Dropbox still in their terms of service explains that they're able to decrypt their users' data if the government issues them a warrant requiring them to do so. And interestingly, there are some add-on gizmos. A couple of things I read are encryption add-ons. I think SecretSync is that, or maybe it's SugarSync. I can't remember. Anyway, I've got it. We will be covering it here in a minute in order to, like, solve those problems. Other companies, they're sort of like enterprise-style, big-iron, don't even care about your privacy. I mean, it's collaborative stuff where other people can be editing your documents. It's like, okay, well, if that's the case, then that's not probably providing us the security that our listeners want.

However, I found some new things, to me, that are really worthwhile. So that's our topic for today is not just SpiderOak, but pretty much everybody that I could find.

**Leo:** [Laughing] All right. Well, as usual, we're going to start with security news. Then we'll get to the cloud storage services.

**Steve:** Yes. Several people tweeted me the note that Google had abandoned their plans for improving SSL latency. Remember that we talked about this months ago. Google had a pilot project, I think it was running for about a year and a half, where they were fudging the SSL spec as part of their overall "let's make the web go faster for everybody" plan, of which SPDY, for example, that we covered in detail several weeks ago, is a part. Well, SPDY, of course, runs on an existing connection. And one of the things it does is it's very good about helping you minimize the number of connections that you need. And we've seen benchmark results that are very impressive when we have SPDY. And SPDY seems to be gaining traction rapidly.

But what Google also wanted to do was to try to minimize that initial connection between the client and the server. And so they were sort of fudging the way SSL works to get more done per back-and-forth transaction. And they, pretty quickly - being Google, of course, they can have spiders roaming the web, and do, while they're doing searching stuff. They found some servers that were incompatible with this trick of theirs. And they went so far as to special-case those relatively few domains in Chrome so that Chrome would normally do the tricky SSL handshake maneuver when you were just using it unless you were connecting to any of those that Google had independently determined were going to have a problem with Chrome doing that, in which case it would back off to regular SSL.

So what the news was last week, and this came actually, I think, the first time, I have a note here, a Steve Styffe, he sent me the first awareness that Google had abandoned their attempt to make SSL faster. And I looked at Google's blog posting about this, and basically it explained that it was always sort of a grey area. They acknowledged that it was beta. They just felt that - they were working with the environments which were incompatible, trying to kind of boost them into compatibility. But it looked like the equipment manufacturers that were using SSL accelerators were the problem, and they just weren't able to make any headway there. SSL accelerators are, for example, appliances with crypto hardware to do the SSL public key stuff, which we know is time-consuming in hardware, to accelerate that handshake. And just because they're locked down in hardware, Google was never able to make any progress in getting that fixed.

So they decided, rather than sort of having what even they admitted was a flaky solution of Chrome needing to know who it was going to have a failed handshake with preemptively, which just is not very practical because new companies are going to be setting up SSL accelerators, and Chrome won't know about it, and things won't work for them. So that's not good. So they canceled that.

However, part of the SPDY protocol does allow the specification from the server that it supports this advanced handshake. So there is still a way to sort of keep it alive within SPDY, but not just in general. So I thought it's neat that they tried this. I'm really very bullish on these efforts Google is making to lay down this technology and set standards. We need someone to do it, and no one better than them.

Also, shortly after, might have been the day after, maybe the hour after we recorded last week's podcast, where we were talking about the Java exploit that was affecting Mac OS X to such a degree, and that Apple had released a patch for it, but we were expecting them to follow it up with a remover. But at that point we didn't know when that was going to happen. Well, it happened probably as the podcast was going public. What's really interesting is what more Apple did.

I tweeted the fact that people - I tweeted to my Twitter followers that Mac users should check for updates again because Apple had just issued a second one to work with this. And Apple, from their own page, said, "This Java security update removes the most common variants of the Flashback malware." So in addition to fixing the Java exploit, it's a remover. "This update also configures the Java web plug-in to disable the automatic execution of Java applets," which is to say they are disabling the Java plug-in as part of this. "Users may reenable automatic execution of Java applets using the Java preferences application. If the Java web plug-in detects that no applets have been run for an extended period of time" - and they don't tell us how long that is - "it will again disable Java applets." So...

**Leo:** Wow. That's probably good; right?

**Steve:** Oh, it's fantastic. But it's also huge news. I mean, this is Apple saying, I mean, we already know they're moving away from Java. They're not going to be bundling it with future versions of the OS. So in their testing that's probably been working out well for them. So they've gone, I mean, really another big step of, first of all, disabling it by default. And even if you turn it back on in order to use some Java something on the 'Net, if you're not a frequent user of it, it will shut itself down again.

**Leo:** So that's the key is that, if you do get somewhere where you need Java, you have a kind of a checkmark or a box that says, yeah, turn it back on. I presume that that's how they'll do it.

**Steve:** Right. It'll say you need Java installed in order to use this. And you go, oh, I've got it here somewhere. And then you go turn it on. But if you leave it on, then it'll shut itself off again, which is just great. I mean, I have to say I'm a little sorry for it because I'm, I mean, I can really see the benefit of Java. I mean, look at this fantastic network analyzing tool...

**Leo:** Netalyzr, yeah.

**Steve:** ...that we talked about for buffer bloat.

**Leo:** And one of the most popular games out there right now, Minecraft, is Java. So there are people, still quite a few, millions for Minecraft alone, who use Java.

**Steve:** Yeah. And, I mean, it caught my attention, the fact that you could do that kind of network work in Java, and you get platform independence, it's like, ooh, boy, that might be something I'd like to learn for offering who knows what. Like I need any other projects. But anyway. So I was just - a tip of the hat to Apple. I'm impressed because, unfortunately, nice as it is to have it, I mean, what you'd really like is on-demand. You'd like to go to a website that needs it. You enable it for that site. Maybe much like NoScript gives us that kind of control now over Java, for example, over in Firefox, either enable it for that site, or enable it and have it, like, disable when I shut down the browser, like enable only while I'm using the computer because, as we know, the smaller your window of opportunity is, the less chance you're going to get hit. And Java had this problem that Apple didn't jump on as quickly as they should have, and they got bitten by it.

I did promise everyone last week that I would make time to analyze the Dropbox tech blog where they were proposing and put out all the code for what they were saying was a realistic password strength estimator. And I just forgot, actually. Well, by the time I saw it in my notes, it was like, oh, crap, I forgot.

**Leo:** You've got plenty of other stuff to do. I think we can live with that.

**Steve:** Yeah. So I bumped it to next week, and I will try to make time to give it a long going over. Lots has been happening with me during my non-podcast life, Leo. I actually have invented something.

**Leo:** What? Really?

**Steve:** New in computer science. I've had it for about a month. And I described it to a couple of the people in our newsgroup who are the high-end coder-capable people, and they're like, wow, that is - and this is what I've been talking about. It's the thing I've been working on all year so far, which I am excited to share with our listeners because it's just a real interesting piece. But it looks like it's a really clever algorithm, which as far as I can tell is completely new, and it solves a problem no one has ever been able to solve before.

**Leo:** Cool.

**Steve:** So anyway, I will be sharing that before long. I did get a tweet from Robert D. Walker, who is a listener, who said, "OS X 10.7 did significantly improve ASLR [Address Space Layout Randomization] and 10.8 will be improving it even further. You misstated that on Security Now!." So I said, "Whoops," and went to look. And sure enough - because I had said that Apple had added ASLR, Address Space Layout Randomization, a long time ago, promised to fix it, but hadn't. And that was correct, except that I didn't realize it did get fixed just recently in .7, and apparently, so says Wikipedia, it's even going to get better in .8. So I did want to - I wanted to correct that.

And, oh, Simon Zerafa, who tweets often and is a listener and a participant in the newsgroup, informed me of an interesting site, IsJavaExploitable.com, which is a nice way to go and see whether your Java, which we were just talking about relative to Apple, is current. So I had to tell NoScript to let it run, and then the site said, oh, yes, congratulations, you're using the latest Java.

**Leo:** Oh, that's good, that's good.

**Steve:** Yeah. So it's a nice place. If anyone's worried, IsJavaExploitable.com will tell you very quickly. And he also tweeted, just I thought this was sort of fun, things that we've said before, but he put it together. He said - this is Simon again. "If you didn't go looking for it, don't install it. If you installed it, keep it updated. If you don't need it, uninstall it." Which...

**Leo:** That's good. Very simple.

**Steve:** ...is just exactly right. Oh, and one last tweet from Eneko Bilbao in Australia. He said, "Re iOS encryption, took your advice, upgraded to alphanumeric PIN. When changed, does it reencrypt the file system? If so, it was very fast." And so I thought I would just take this moment to explain that no, the file system is not encrypted using the PIN; but rather there is a pseudorandom long key which is your file system encryption key, and that is encrypted using your PIN. And so that allows you to - so the only thing that is stored in nonvolatile memory, where it could be captured, is the encrypted version of that key for your file system. And so when you correctly put your PIN in, then that allows that encrypted token to be decrypted, allowing your file system then to be accessed. So, and that's the way most of these things work. For example, if you have an encryption password on a hard drive, same thing happens. You're actually encrypted the encryption key, rather than what you're providing actually being the encryption key. It's a second sort of a one stage of - programmers would call it "indirection," one stage of indirection, but gives you the same level of protection.

And lastly, I just had a fun note that was shared, reminding us that SpinRite can be used on strange things. Ben Stool wrote, he said, "It works great on TiVos. Just a note" - and this just came in on the 16th of April. "Just a note to tell you that SpinRite works great on TiVos. I read about it on your website and heard Steve mention it on Security Now!. Our eight-year-old DirecTV TiVos were starting to act funny. So I pulled both 80GB Western Digital drives from them, connected them one at a time to a Windows XP Service Pack 3 desktop, and ran SpinRite at Level 5.

"Interestingly, both drives reported no errors and finished in a little over four hours each. However, when I put them back into the TiVos (after blowing an embarrassing amount of dust out of them), the TiVos are back to normal. These are first-generation DirecTV TiVos, but we like them and do not want to pay the high premium to go to the new HD DirecTV TiVos that were recently released. SpinRite has let us keep our old friends going. Ben Stool, Dallas, Texas." So thanks very much, Ben. You can use it on anything.

**Leo:** Steve Gibson has done a lot of research and is now going to give you a brain dump. Stand back.

**Steve:** So I didn't know what order to put these in, so I just thought, well, let's go alphabetical. Now, Bitcasa we have talked about in the past. And I did not have a chance - it was on my list, and I just ran out of time before I was able to do a deep dig into it. This is the one people may remember which is unlimited file storage because they're doing a duplication elimination, so multiple people are sharing the same files. It was sort of controversial. And I have a link which I didn't follow, which is "The biggest problem, Bitcasa is not safe." And it's like, okay, well, I don't know what that means. So I just don't - it's on my list here, and I didn't want to skip it; but I don't have anything new to add to the prior information that we had about it.

I did get several people who tweeted, what about BoxCryptor? It's sort of an interesting solution. It's primarily a Windows solution, but they also have Android and iOS clients, so it has a mobile side, too. There's a file system known as an Encrypted Filesystem -

EncFS, sort of harkening from the way Linux labels its file systems. This encrypted file system was designed relatively recently. It's open source. And whereas a system like TrueCrypt that we've been talking about encrypts at the block level so that all of the individual sectors are individually encrypted, this EncFS, this Encrypted Filesystem encrypts at the file level.

What that means is that it's more friendly for a cloud-based solution than something that encrypted at the block level. In fact, it's not clear how you could do encryption of a file system at the block level and then remote it to the clouds. In their pros and cons, they talk about that, since they're not encrypting blocks, there is a little bit of metadata leakage, "metadata" meaning the file organization stuff. For example, if somebody looked at your encrypted file system, they could see how many files you had because, sort of like the directory tree itself they could see, the file names are encrypted; but they're rounded up to the block size of the encryption, which, for example, if it's 128 bits, that's, what, 16 bytes. So they could sort of guess the filename lengths within - with an accuracy of within 16 bytes. So it's that sort of leakage.

They do support, as I said, primarily Windows. And Mac and Linux are able to mount - Mac and Linux already support natively this, well, or as an add-on, I should say, this encrypted file system, which allows you then to mount this BoxCryptor thing on your system. They have a license - essentially, if you're a Windows user, you download their gizmo, and you select the source directory, which will store the encrypted data. And then you assign that a drive letter. So what you see is a drive letter in Windows into which you can store anything you want. And when you put things in that drive, sort of that pseudo-drive, then it's actually performing on-the-fly encryption and storing, and sort of dynamically creating a file system in the directory where you've told it to. And this is friendly, then, with being uploaded and shared.

So they have a free version - and this is sort of a problem I have with these guys is they sort of put some arbitrary limits on it. It's not clear why they did. But I guess they want to make some money from this. There are other free solutions, I think, which are maybe superior. So for free you can get up to 2GB of storage and a single drive mapping. For $40, unlimited personal, I mean, unlimited storage and any number of drives. And then just if you're a business user they want $100. Now, that is a one-time fee, so you're buying the license to the utility. You can put it on any number of machines. And if you then have some way of synchronizing folders, then this will provide the encryption side. So it's sort of an interesting solution. I'm not super gung-ho on it.

There's an Android version, and they want $6 for unlimited personal use and $9 for unlimited business. And their iOS version doesn't look very impressive at all, actually. I think it was like - you're limited to, like, three uploads or something, then it locks, and so you have to do an in-app purchase to unlock it for about the same amount of money as for Android. So it's an interesting solution. It's sort of like I'm not sure that it really, I mean, if you had some means of synchronizing folders, then adding this to that can give you strong encryption. As far as I know, the encryption is based on a well-designed encrypted file system, and so it would qualify for Trust No One (TNO), which we'll be hearing that acronym a lot here in the next 45 minutes or so because many systems do explicitly support Trust No One, and many others don't.

Also when I was looking at this, there's a company called Box.net. And it's funny because their domain is Box.com, but Box.net is what they call themselves.

**Leo:** They were Box.net for a long time, and then they bought and were able to acquire Box.com.

**Steve:** Okay.

**Leo:** So I still think of it as Box.net, but Box.com works. It's very confusing. I don't blame you for being confused. But they've been around. They may be one of the oldest that's still around.

**Steve:** Yes. And they sort of look like it, too. It's like, okay, well, I mean, it felt to me like maybe they weren't up with the times. I couldn't see any clear support for mobile stuff. You get, for their free version, single user, is a limit on file size of 25MB, and 5GB of storage. And that's - so you get 5GB of storage, but with a per file size limit of 25MB.

**Leo:** And that's kind of killing. That's a terrible limit.

**Steve:** Isn't that random? Yeah. It's like, what? Okay. But if you pay them $10 a month, then you can get 25GB and 1GB per file, so that's certainly useful. And at twice that amount, $20 per month, you can get 50GB and 1GB maximum file size. Except that, as we'll see, those are on the high side, pricewise. For example, just for comparison, something that still is in the running is Amazon's S3 service or Rackspace's service with Jungle Disk because they're $0.15 per GB per month. So that would be...

**Leo:** They also charge for bandwidth, so you've got to include that.

**Steve:** Well, Rackspace doesn't.

**Leo:** Rackspace doesn't. Jungle Disk with Amazon does.

**Steve:** Correct.

**Leo:** So with Rackspace there's no bandwidth charge. Oh, I didn't know that. That's good.

**Steve:** Yeah. And so, for example, at 25GB, these Box.net - and this is, again, we'll be talking about price because I know people are interested. Box.net is $10 a month, but Rackspace or Amazon for the actual 25GB of storage, are $3.75. And that's one of the other things, too. Everybody wants to put you in this plan. And I hate plans. It's like the whole cellular phone business where you buy this many minutes. Well, okay. But if I don't use that many, then I've overbought. One of the things that I really like about Rackspace and Amazon is you're paying $0.15 per GB rather than committing to some size of plan, and then you pay more than you're actually using unless you use right up to what that limit is. So anyway, just something to keep in mind. And I will say that Box.net does have a business plan, instead of these personal plans, which gives you 15 - I wrote

$15 per month and a terabyte, but that's less expensive than the $20...

**Leo:** That can't be right. Nobody gives you a terabyte. Nobody gives you...

**Steve:** No, that's something - something wrong with that. So anyway, if anyone's interested, check it out. Now, in my perusal I did, of course, run across one of our sponsors, Carbonite.

**Leo:** Which does not position - I want to be clear upfront - does not position itself as cloud storage. It's a backup solution.

**Steve:** Correct.

**Leo:** But you do get cloud storage.

**Steve:** Well, and as we'll see, there are a number of sort of services that are becoming sort of generic. There's the idea of synchronizing multiple machines. And several of these services that we'll be talking about offer free synchronization where, for example, you can install this on as many things as you want, and they'll keep them synchronized, but that's different than storing in the cloud, the idea being that they all share a folder on their own hard drive, and then this thing keeps them synchronized. And Dropbox, I guess, operates that way. But then you can also do storage in the cloud. And then most of these services now have a mobile component, allowing people to access these files, sometimes stream music, look at pictures and so forth, from iOS or Android devices. So there's, like, different...

**Leo:** That's how they're distinguishing themselves, I think, because you can't just do raw storage. It's like, well, what do you add to the raw storage? What is your unique point of view?

**Steve:** Right. Now, I like, I mean, having looked at all of these, I have to stay Carbonite is still in the running, in my opinion. They're $59 per year per computer, and unlimited storage, which is just a nice thing to have. One of these companies that we'll get to does something really interesting, which is, to get you bootstrapped to them, they'll send you a hard drive, which you use locally to back up your machine, and then send it back to them.

**Leo:** Oh, that's neat.

**Steve:** That solves the problem...

**Leo:** That's interesting.

**Steve:** ...yeah, of, like, a multi-hundred gig through the cloud to get yourself set up the first time. And then of course they install - they dump that hard drive into their own servers and then catch up any changes that have been made since then and then continue. And they'll reverse the process. If you crash, and you've got hundreds of gigs in their cloud, you can say, oh, my god, I need my data now, and they will send you...

**Leo:** Here's your hard drive.

**Steve:** ...all of your data on a hard drive.

**Leo:** Wow.

**Steve:** But anyway, so back to Carbonite. We'll catch up with that...

**Leo:** Now, just to be complete, it is unlimited. But they do tell you they throttle after 200GB.

**Steve:** Right.

**Leo:** So I just want to make sure that people don't get a false impression of that.

**Steve:** So $59 per year per computer, which is, what is it - and I have, I wrote down here $5 per month, so I guess that's...

**Leo:** Yeah, it's roughly five bucks a month, yeah.

**Steve:** And support for Win, Mac, iOS, Android, and BlackBerry. Although they've got some advanced features which are currently still only the Windows platform only.

**Leo:** Right.

**Steve:** And then under PIE - Pre-Internet Encryption - where are they on Trust No One? Reading from their own disclosure, they said in their FAQ, "Can Carbonite employees see my backed-up files?" And they wrote, "Access to your backed-up files is protected by your encryption key which is kept strictly confidential. Unless you choose to manage your own encryption key (see below), a limited number of Carbonite employees are able to access backed-up files in order to assist with data recovery if needed. However, they will do so only after obtaining your consent."

And then they said, "If you are" - oh, and I loved this. This is something I learned, actually. "If you are subject to industry regulations that require no one outside your organization to have access to your backed-up files (e.g., HIPAA regulations)...." So it turns out that being HIPAA-compliant requires TNO-level security, which is great because that's going to strongly encourage companies to go in that direction. So they said, "If you are subject to industry regulations [blah blah blah] Carbonite provides you with the option to manage the sole copy of your encryption key. If you choose this option, features such as Anytime Anywhere Access" - which is their web-based viewer, and I think your mobile also is the same way, those will be unavailable to you.

"Also note that, if you lose the sole copy of your encryption key, there will be no way for Carbonite to restore your backed-up files. For these reasons, Carbonite recommends, and the majority of our customers choose, to have Carbonite manage their encryption keys." But it is significant that, if you decide to, you're able to have them do the job for you. I mean, you're able to accept responsibility, and they will not have your key.

Then I mentioned add-ons to non-encrypted solutions, and there is a company, or an offering, called CompletelyPrivateFiles, which offers encryption for Box.net. So that's an example of that kind of add-on. Again, Box.net's pricing didn't seem particularly compelling. And then this CompletelyPrivateFiles company wants to charge you additionally for that. Zero dollars for up to 5MB file size, $30 per year for up to 15MB files, $50 per year for up to 25MB files, and $80 per year for up to 50MB files. So they're charging you for the size of file that you can use them to encrypt to get stored on Box.net. So [buzzer sound], I don't think they make it.

Okay. CrashPlan is the company I was just mentioning. And every time I say "CrashPlan," I think, boy, couldn't you have chosen a more optimistic name for your company? I mean, I don't know. It's catchy, I guess, and that's what it's for. It is multiplatform: Windows, Mac, Linux, and Solaris; iOS and Android and Windows Phone mobile. And the mobile apps are free. Some of these people do charge, as we saw before, a few dollars for the mobile version of their gizmo. And this is just at CrashPlan.com.

And they say on their site, "How is CrashPlan different from other online backup services?" They say, "Unlike ordinary online backup, CrashPlan lets you back up to other destinations in addition to online. You can back up to your other computers, external hard drives, and to computers that belong to friends and family for free. If you want to back up online, too, purchase a CrashPlan+ subscription for home use. To back up your business data to the cloud, check out CrashPlan PRO or CrashPlan PROe.

So, pricing-wise, their free plan gives you no storage, but you're able to use this multiplatform set of clients - again, Windows, Mac, Linux, Solaris, iOS, Android, Mobile Phone - to do intermachine backups. So that you're essentially using storage that you, presumably on a different machine and/or different location or friends and family have, to do your backup. So they're not offering any cloud storage; but they're offering, for no money, the technology for synching all this stuff together.

Their CrashPlan+ is $2.50 per month, which is for 10GB. But then they have a one-year, two-year, three-year, four-year commitment discounting you all the way down to a dollar and a half per month if you commit to four years. And you're able to then back up 10GB and a single computer for that price. Then the CrashPlan+ Unlimited is unlimited amount of storage for $5 per month, which runs down, if you make a four-year commitment, down to $3 per month. Now, that's getting to be pretty good. Think about that. $3 per month, well, of course you've got to commit to four years. So $5 a month, one computer, unlimited.

Then they have Family Unlimited, which is two to 10 computers at $12 per month. So this is scaling pretty nicely. $12 a month - and if you commit to four years, it's half that, $6 a month - unlimited amount of storage, two to 10 computers. And then this is the company that I mentioned that has what they call "seeded backup." They ship a drive, and for a one-time fee of $125, so it's not cheap, but the idea is it will back up your entire machine. You use their client to back up your entire machine to this drive, which you then return to them. They dump into their cloud, and that short-circuits - or as they call it, "seeds" - their backup so that you're not spending lord knows how long transferring how many hundreds of gigs up to their cloud. And for the same price they'll reverse the process, if you need to get your data back.

And I thought it was sort of funny because they change the security encryption strength depending upon whether you're free or not. The free plan uses 128-bit Blowfish, and all the other plans are 448-bit Blowfish, which is great security. We know that Bruce Schneier designed it. And it's got a slow key schedule setup, which is good for security because it makes it much more difficult to try to brute force it. And they do offer full, although optional, TNO-level security. So you can set it up with what they call a private password, which is used to decrypt the encrypted encryption key, and with all the standard caveats. If you lose that, they can't help you.

But so this is some interesting packages that may fit people because, at a reasonable price, it's widely cross-platform, two to 10 computers, unlimited storage for as little as $6 a month, covering all of that, if you go with them for four years. And again, I have no experience with it. This is just pulling all the data together and drilling down to figure out how they work.

Next up is something that looks like it's sort of a Dropbox clone called Cubby, as in a cupboard. They support Windows. They have a Mac desktop app, Android, and iOS. And they distinguish themselves from Dropbox because, whereas Dropbox has, like, the Dropbox folder that you get on your machine when you install the Dropbox client, these guys allow you to share any of the folders that you already have on your machine by dragging and dropping those folders onto their app. And then that folder becomes shared with this Cubby. So this allows computer or cross-computer sharing, unlimited peer-to-peer cross-computer synching of the shared folders.

They say that it keeps unlimited versions of friend-shared files. So I guess, as I understand it, if you share files with friends, and there's a means to do that, and they alter the files, then this is keeping versions of those. And then you also get a free 5GB. We're going to see a lot of this. It makes Dropbox's free 2GB look a little stingy now. Everyone pretty much seems to have gone to 5GB for their free offering. And I should mention this is from the company LogMeIn are the people that produce Cubby.

However, nowhere, anywhere that I could find, was any mention of security, encryption, and privacy. That is, that just is missing from their site. It's all very nice and polished looking. But they don't tell us anywhere about what they're doing for us from a security standpoint. So it's like, okay, until I knew that, of course, if that was a concern for people. And I love the idea that HIPAA regulations require this. So maybe they'll be addressing that in the future.

I ran across something called DigitalBucket which I didn't spend much time at. There's no Trust No One option. They use Amazon S3 cloud storage as their backend cloud provider. And they're expensive. An individual plan is $99 per year for 50GB. Their professional plan is $30 per month for 100GB plus three subaccounts. And their small business plan is $125 a month, that's a lot of money, for 500GB and 10 subaccounts. So it's like, okay, well, I was following some links and thought, well, what's DigitalBucket? And it's like, well, doesn't sound like it's for us.

**Leo:** It's a terrible name, too.

**Steve:** I know. I thought exactly the same thing.

**Leo:** Spell it carefully.

**Steve:** So proceeding alphabetically, after DigitalBucket we come to Dropbox. We know that they're free. They give you 2GB, which as I mentioned seems a little stingy these days. $10 a month or $100 per year, and we'll see that many people we're going to encounter offer you essentially two free months if you sign up for a year, is what everyone seems to be doing, probably cloning off of Dropbox's policy.

**Leo:** And they do an affiliate - you get a link that you can ask others to use, and then you get extra storage.

**Steve:** Oh, boy, strong social networking on these sites.

**Leo:** Very viral, yeah.

**Steve:** Oh, boy. Yeah, I had to keep clicking through all that. It's like, yes, yes, I know. It's like, you're three clicks away from an extra 250MB. It's like, oh...

**Leo:** I find that very annoying.

**Steve:** I do, too. It's like, okay. If it's good, I'll recommend it, but I'm not doing it because I need an extra quarter gig. So for $10 a month or $100 a year, you get 50GB in the cloud. Or for twice that, you get twice that much storage. And it's interesting because, for example, $20 a month is, if you stored all - if you filled up 100GB at $20 a month, then if we compare that to Rackspace or Amazon, that same 100GB only cost you $15 per month, and that's only if you use it all. Again, it's like, the idea of signing up for such a huge amount of storage and having to pay a fixed amount of money sort of rubs me the wrong way, relative to Amazon or Rackspace, where you're really only ever paying for what you use. I'm an S3 user. I'm still using Jungle Disk with Amazon. And I get a little ping in the email every month saying, oh, we just charged you $3.15. It's like, okay. I like that. Because I have a ton of stuff up there, all Pre-Internet Encryption, from Jungle Disk, that we'll get to here in a minute.

And so also from Dropbox, under security, under their "Compliance with Laws and Law Enforcement" section, they said, "As set forth in our privacy policy, and in compliance with United States law, Dropbox cooperates with United States law enforcement when it receives valid legal process, which may require Dropbox to provide the contents of your private Dropbox. In these cases, Dropbox will remove Dropbox's encryption from the files before providing them to law enforcement." So I salute them for being clear, but it's clearly not providing anyone protection who wants that kind of protection.

Consequently, we will run across a couple solutions. It's one of those "Sync" things, either SecretSync or SugarSync. I think it might be SecretSync. In fact, I'm sure it's SecretSync because SugarSync I was very impressed with, and SecretSync is just sort of encryption for Dropbox to solve this problem. Alphabetically proceeding, we hit Google Drive.

**Leo:** But one thing I want to say about Dropbox, one of the reasons I use it, I know it's a bad deal, because every app, for instance, on the iPad and the iPhone has an interface for it.

**Steve:** Yes.

**Leo:** And so it's convenient, even though - I guess that's what I'm paying for is the convenience; right?

**Steve:** Yeah. And it is very popular. I didn't want to leave it out.

**Leo:** Popularity is why it wins.

**Steve:** Yes, yes. And I did not want to leave - well, in fact, you and I were using it for quite a while.

**Leo:** I still use it. I wish I didn't have to because I know I'm paying a lot more than - I love Amazon, or Amazon S3 using Jungle Disk, which you turned me on to. And I'm going to have to use Rackspace now because that's even better.

**Steve:** Yes, because no transit cost. What I like about - I ought to just take this moment to say what I like about S3, Amazon, is the apps we use to talk to it are decoupled from it. I'm buying the storage and transit, which in my case isn't much. Mostly I'm using it for archival stuff. But I'm not dependent on some company that I don't know about and don't know if they're going to be here tomorrow. Essentially, I don't know, it seems more granular to me. I like that I'm only paying for what I'm using. And, for example, there are many S3 frontends. There's a beautiful frontend for Firefox that I really like where I can just open this - it runs in the browser. I open my Firefox and I'm looking at this really nice S3 Explorer app add-on for Firefox. So I like the idea that I'm not being insulated from my files by sort of an all-encompassing Big Brother, don't worry, we'll take care of you sort of thing.

And so Google Drive. We don't know what it's going to be. We've heard the rumors that it's going to be 5GB, which would be keeping with the current what you get for free these days. Drive.google.com now resolves, but doesn't have anything on it yet. And the rumors are that we'll see an announcement next week. So we'll see what they're going to offer and what it'll be. I'll update, obviously, everybody with that news when we know.

And again, it was a tweet that reminded me about Jungle Disk, the thing that I use. Good multiplatform support - Windows, Mac, Linux, iOS, and USB. And Leo, do you know, were they purchased by Rackspace?

**Leo:** Who?

**Steve:** Jungle Disk.

**Leo:** Oh, yeah. That's why they - yes, that's the whole point. They got bought by Rackspace. And they continue to offer their S3, but obviously Rackspace gives you a better deal. And it's otherwise the same, I would guess.

**Steve:** Yeah, well, they've moved forward.

**Leo:** I thought, when they bought them, I was a little nervous, to be honest. I thought, oh, boy.

**Steve:** Yes, yes. And back in the day, when we first encountered Jungle Disk, I purchased the lifetime something or other for $20, and they're still honoring that. They do have something else, I think it might be the web access, which they don't bundle in if you were grandfathered into the original deal. But for Rackspace you pay only for storage. And as I said, it's $0.15 per gig per month, with free transit and free requests. I say that because Amazon actually charges you by request. It's not much, but it's not nothing. So Amazon is the same storage price, but there is a transit fee for moving data back and forth. I think it might be $0.15 per gig and $0.15 per request. So it's really not meant to be a CDN. Amazon has other offerings that are much more content delivery network oriented.

For me, I like it because Jungle Disk we absolutely know is Pre-Internet Encryption. You put the password in, Jungle Disk encrypts it locally, and it goes nowhere else. And their USB version is cross-platform, that is, it's Win, Mac, and Linux all bundled into a single thing which you then - you can put it on a USB drive, and you stick it in whatever computer you're at, no matter who made it, essentially, Windows, Mac, or Linux. And Jungle Disk figures that out and runs, which is neat.

Now, they offer web access to cloud files, but I don't know how that works with Pre-Internet Encryption. We know that it's possible that the decryption could occur in your browser, if you provided that key. But might be that web access is only available if you don't encrypt with your own key. And that is an option. You have the ability to do that or not, as you choose. But if you do, it's full TNO security.

And, let's see. Oh, they also offer public sharing of specific files. So of the stuff that you've got stored up there in your Jungle Drive, you can get a web URL and set a date of expiration, which you can then share with other people. So you can email this URL to someone and say, hey, here's a file I want you to grab, go get it at this link. They do put a maximum of 5GB on file size and 50 downloads per file, saying that it's not their intention that this be a free content delivery network. But that gives you some security.

Anyway, so I'm still a Jungle Disk user, more from inertia than anything else and also because, as I've said, something feels right to me about the use of Amazon and only paying for the storage I'm actually using and because I'm not a big - I'm not using it to constantly back up my system, so there's not lots of transit that I'm paying for. I think, if that were the case, I would opt for Rackspace as my storage provider, and then we get free transit, which makes a lot of sense.

I ran across HiDrive, which is from a company called Strato, and they're not U.S.-based. I remember - I didn't write down where they were, but I noted, because prices weren't coming up in dollars, that I had to convert to dollars. Nothing really jumped out about them for me. They're iOS, Android, and Win Mobile 7 for their mobile side. 5GB for free, as many people are now doing. $13 for three months, which seemed odd, and they call it a "three-month commitment," and that gets you 100GB; or $39 for three months gets you 500GB. And on the security side I'm not impressed. They mention, probably because they're European, ISO 27001 certification. That is, they're compliant with that. But who knows what that means? That didn't - I even...

**Leo:** Only somebody in Germany knows what that means.

**Steve:** Yeah. I looked it up, and it's like a long Wikipedia page of gobbledy-gook. And it's like, okay, well, I don't think anyone's going to be jumping on these guys anyway.

So Livedrive. Good multiplatform support - Windows, Mac, iOS, and Android. Although I kind of got kind of a creepy-crawly feeling from these guys. On their homepage they say, "Resellers, sell online backup and more. Sell our full range of online backup, storage and sync products to your customers. Custom brand everything, manage it all from the web. Sell unlimited backup accounts from just $59.95 per month, instant setup." And it's like, okay. That's - okay.

**Leo:** That always makes me nervous, too. That's, yeah.

**Steve:** Yeah, it just sort of seems a little slimy somehow. So they have their offerings. $8 a month is backup with no storage limit for one computer, and additional computers $1.45 per month. $16 per month is their so-called "Briefcase" plan, where you get 2TB and Windows and Mac synchronization, and you can also share it with friends and family, specific files. So that's cloud storage with ability to access it. $25 per month is their "Pro Suite," which brings you up to 5TB. And they store 30 previous versions of files. They can restore deleted files and stream music. And for $8 you can add NAS backup. So they will back up your own local network-attached storage to the cloud.

And they're, as many people, purchase for one year and get two months free. But again, it's like, okay, I think they're, I mean, obviously this is a huge and exploding market segment with cloud storage being the buzzword these days. And so there are a lot of companies that are there, and it's not really clear to me what they have to offer.

I ran across, speaking of that, a company called Porticor that seems very enterprise-oriented because $162 per month. It's like, ooh, okay. I'm not sure...

**Leo:** [Whistling] Wow.

**Steve:** ...who they're appealing to. But you can register for a free evaluation, Leo, if you'll give them your email address. And so I said, uh, I don't think so. Yeah. And when you do that, you get three virtual disks at 2GB per disk, and then they start sending you email. So, uh, no, thank you.

Okay. SecretSync is what I referred to before. What they're doing is they're an add-on for Dropbox that puts another folder on your desktop, and anything you drop in there, they pre-Internet encrypt before dropping it in the Dropbox for you. So it uses the Dropbox API, probably. But it's not free. You get up to 2GB of encryption in that encrypted folder for free. But it's $40 per year to expand that to 20GB of encryption, or $60 per year for a terabyte. So of course that's their own metering of the encryption. Then you have to pay Dropbox's fees for the actual storage. So it's like, okay, well, they're there.

**Leo:** That's why I rejected that one. I didn't want to pay twice.

**Steve:** Exactly. And of course, going alphabetically, we've got Microsoft SkyDrive, which, eh. It doesn't seem to have any strong Mac support, not surprisingly, although there is an SDK available for apps, although only apparently running Windows, iOS, and Android. Now, Microsoft does give you more free storage than anybody, 25GB, I didn't see anybody that was at 25GB, with a 2GB per file limit. They do support - SkyDrive supports Windows, iOS, Windows Phone, and Windows 8 Metro-style. But again, no real clear focus on security. No explanation about how keys are handled or crypto and so forth. And I wouldn't be at all surprised if they also can and would respond to someone telling them that they need to hand over your data. Do you know anything more about SkyDrive that's beyond...

**Leo:** Well, I think it's going to expand. The thing is you're working with Microsoft. So at some point they're going to add to it. It's probably enterprise-focused. It does support the mesh synching, but only 5GB of that can be dedicated to Live Mesh synching.

**Steve:** And it does have a nice web interface, too.

**Leo:** And Mac. So, yeah, I mean, I think it's something. It doesn't seem to play at the same level as some of these other solutions, however.

**Steve:** No. And the 25GB is kind of compelling, except, like, well...

**Leo:** You can't really do much with it. There's no, for instance, there's no interface; right? There's no - you want to be able to mount it, for instance, as you do Dropbox. That would be cool. You can't do that.

**Steve:** Exactly. Exactly. So, SpiderOak. I'm impressed. Good platform support - Windows, Mac, Linux, iOS, Android. They are really upfront. I mean, these guys, what hooked me immediately was they have what they call their "Zero-Knowledge Privacy" policy. They don't want anything to do with your key. You don't have an option to give them your key. You can't misconfigure this so that they have your key. They never get it. So, I mean, and that's just like a big deal for them. And of course we know for certainly a segment of our listeners, that's a big deal. Certainly is for me. I'm not sending my data off to the cloud without it being encrypted. That just isn't what's going to happen. My company's accounting data, and backups of images of my main machine which is up there, that's going to be encrypted.

I'm probably going to spend some time looking more closely at them because they are saying they offer things which seem really interesting. So you get 2GB for free. That seems, again, five seems to be the norm now, but for these guys 2GB. But if you want 100GB, that's $10 a month, and they also do the two free months per year, so $100 a year if you did it for a year with them. That buys you 100GB. And as soon as you cross 66GB, that's the breakeven with Amazon and Rackspace. So if you're storing less than 66GB on the 100GB plan, Amazon or Rackspace are cheaper for storage. But if you're doing more than 66GB, then SpiderOak is cheaper.

So under their list of features they say backup, sync, share, access, and storage; multiplatform support we know, Mac, Linux, and Windows; they're 100 percent zero-knowledge privacy, so they're just storing pseudorandom data. They're storing noise for us. Any number of computers at no additional cost, so you're just paying for storage, and there's no transit cost. They say "storage and time-saving de-duplication." This is one of the things that I'm interested in. It's like, okay, how are they doing de-duplication if they're doing pre-Internet encryption? So that's something I'd like to understand.

They said "perpetual deleted file and historical version storage." So they're also doing some versioning of some sort. And they're saying they're saving deleted files forever. So you can go all the way back to the beginning of when you started using them. And then, this is interesting, 10 to 15 times faster than traditional backup solutions. So it's like, what? Okay. And I've got the name of the techie there who I can have a conversation with because I'm interested in what they're doing. And they make a big point of being wholly fault tolerant. So the idea is not only is it in the cloud, but they've really looked at being fault tolerant.

Now, I noticed also in perusing that they say they securely synchronize folders across multiple computers and operating systems using their free online sync. So you pay for, as I said, $10 a month or $100 a year for 100GB. But then synchronization is free. So, and on any number of machines you're able to use SpiderOak for performing synchronization. And they say "discreetly share selected folders with friends, family, colleagues, and clients." So, now, this is interesting because they must be doing it and maintaining TNO. So I want to find out how that works because presumably, I don't know if you have to install their client in your friend's, family's, or colleague's machine, or if that's a web-based interface. And I think it's web-based because they have something called "Share Rooms" where you can share folders instantly over the web in share rooms, and then you can also subscribe to an RSS feed to be notified of modifications in there.

And under "Efficient Versioning" they said, "SpiderOak keeps historical versions of every file. This is an extremely important safety feature in a backup application. Consider this scenario: You accidentally save over your thesis paper with a different document. The easy solution is just to go back to your backup software and retrieve the old version, except what if you don't notice for a few days? If your backup software doesn't keep historical versions, it will save the new wrong version of your thesis into your next backup, making recovery impossible. SpiderOak's historical versions are space efficient. Even though your historical versions are encrypted and only stored on the server, SpiderOak detects the similarity between those historical versions and your new versions, only saving the parts that actually changed."

Now, somebody tweeted something that's kind of ringing a bell here. There was some mention of not wanting to store data redundantly on your own machine.

**Leo:** Ah.

**Steve:** Yes. So maybe...

**Leo:** That's how they do it.

**Steve:** Yes. So maybe what they're doing is they're creating an archive region on your hard disk. They're seeing the differences and maintaining that and then encrypting and only sending, for example, the deltas after encryption up to them so that there's a way to piece this all back together. I mean, that, as I'm reading this, the thing that I remembered someone saying is they didn't like the idea of, like, this blob of space being taken up on their hard disk. That may be what SpiderOak is doing.

I should mention, though, and actually this came from another tweet, apparently they've got work to do over on iOS because their iTunes store reviews for the iOS client are, like, horrifying.

**Leo:** Really, really, huh.

**Steve:** It's one star, and people just shuddering at how bad it is. You have to, like, remove it and then reinstall it, and then it kind of works. And I just think that they - I don't know what the - I'm sure they'll explain to me, if I pursue this, what's happening over there. But that's not the client, apparently. People are trying to use it to read PDFs, and it's doing horrible things to them. So...

**Leo:** I think - I'm looking at a SpiderOak interface. And it says here, there's a checkbox that says "Keep my own copy of all archive data blocks." So you don't - looks like you don't have to.

**Steve:** Ah. Okay.

**Leo:** "Enabling this option will cause SpiderOak to send a copy of all new encrypted data blocks to the location you've chosen. SpiderOak will then check this location first when restoring data. This can increase the speed of larger stores." Oh, maybe this is just - I don't know if this is where the versioning - maybe not. Maybe this is just for bandwidth-limited folk. It has, I mean, a slew of features. I mean, this thing is amazing. So I've been using it for some time. I haven't had to restore from it at all. But I'd be very - so you're going to do some more conversations with them.

**Steve:** Yes, yeah. Because of all the offerings, I feel the same way. This is one that, like, survived this whole process of looking closely into the corners. And we're down to three left. Actually, really only one because the other two don't qualify. In fact, I'll do them first. I'll go to "Z." ZeroBin, I ran across it, somebody mentioned it, I figured out what it was. It's an encrypted Pastebin. So we're familiar with Pastebin, which is sort of just random catch-all. Anybody can put stuff up there. Of course the malware/script kiddie kind of folks and hackers use it as a rallying point, essentially. But everything normally is in the clear.

And ZeroBin is browser, that is to say, client-side encrypted Pastebin. So you could upload a file, protecting it with a password, and then get that password to someone else somehow. I was going to say email, but you want to do it over a secure channel somehow. And then they're able to get and decrypt it, to download it into their browser and then decrypt it. So it's sort of a means of having 'Net-shared files which are cryptographically secure because they use AES-256 encryption in the browser. So in case that was useful to anyone, I just wanted to note that it exists, called ZeroBin.

Then the other one that sort of didn't - I didn't spend much time on is Tarsnap. I'd run across it before.

**Leo:** I like the name.

**Steve:** Tarsnap. No Windows support except through Cygwin, which is the library for sort of limping along with Linux or UNIX support under Windows. They do support BSD UNIX, Linux, OS X, and Solaris. And they provide storage at twice the price of Amazon for storage and transit. So I'm not sure what they have to say for themselves. But that's as far as I went with those guys.

The last one is a company called SugarSync. And, boy, they've got the widest platform support I've seen. Win, Mac, iOS, BlackBerry - you don't see BlackBerry except, what was it, I think Dropbox offered BlackBerry also. So that's uncommon. Android, Symbian, Kindle Fire, a web interface, and an Outlook plug-in that gives you access. They have a comparison chart with comparing themselves to lots of other people. Of course it's their comparison chart. So every one of the things that they compare against has a green dot on them, and various of the other guys are missing dots in various places.

And it's, until you get up to the really big storage, it's not even compatible with Amazon or Rackspace. You get 5GB free, as most people do; 30GB at $5 per month or $50 per year, so that's also the two free months deal. 60GB for $10 a month; 100GB for $15 a month; 250GB for $25 a month, or 250 a year, for example; 500GB at $40 per month. So it wasn't until you got to 500GB at $40 per month that pricing was better than Rackspace or Amazon. Otherwise, on all those other ones, you were paying more than Amazon or Rackspace and, if you weren't using all of that storage, then paying a lot more than those guys. It does allow you to back up any folder. So it's a little bit like Secret - no, not SecretSync.

**Leo:** [Laughing] You're losing track now, aren't you.

**Steve:** I'm losing track. One of those that I talked about. But it does not look like they support TNO-level security at all. So not at all clear what they're, I mean, everybody, of course, supports secure transit, just even using just SSL. But I saw nothing that convinced me that these guys were really good from a long-term storage security standpoint. Their storage is expensive. Huge cross-platform support. But again, it's not clear how secure our stuff is. So of all of those things, Leo, I think you chose wisely, SpiderOak.

**Leo:** Interesting. Because I did not get as comprehensive as you did.

**Steve:** Yeah. I don't know, what was it, Wuala, now that I'm...

**Leo:** Yeah, Wuala has an unusual idea, which is that you contribute some of your hard drive space to the Wuala...

**Steve:** Ugh. Okay. I'm out of that.

**Leo:** I knew that would give you - and if you want more, it runs in Java, just in case you wanted another reason not to do it. So I don't think you have to worry about Wuala.

**Steve:** Okay. I don't know who I forgot. I'm sure Twitter will let me know. But of everything we just looked at, I mean, I am still using Jungle Disk for now. I like it. I like the incremental, pay for what I use. Although I am on S3, so I'm paying for transit. If I were doing a lot of stuff, SpiderOak is no charge for transit, cross-platform. As you said, it's got features coming out of every pore. And, boy, are these guys security conscious. So I want to find out how they do what they say they do. I imagine we will have the podcast I thought we were going to have this week, which is really, really drilling down deep into SpiderOak to figure out how they work. And maybe we'll figure out what's wrong with iOS because I don't think they quite have that figured out yet. But other than that, I like everything I see.

**Leo:** Apparently Wuala got rid of the space-sharing feature, so maybe others had the same reaction that you had to that. That's actually why I did it, because I wanted to get - because it's free if you donate 100GB or whatever.

**Steve:** Right. And so, like, they're encrypting somebody else's data on your drive.

**Leo:** Yeah, exactly. Maybe pieces thereof. Pieces thereof.

**Steve:** There are some interesting ways, using state-of-the-art block-level error correction, where you can sort of spread your data out among some - it's almost like a RAID, where you spread your data out among some number of nodes.

**Leo:** Right, exactly.

**Steve:** And you don't need every one of those nodes to be alive in order to...

**Leo:** I believe that's what they're doing, exactly.

**Steve:** ...reassemble and essentially do ECC on the data to algorithmically work around what's missing.

**Leo:** Right. I should say that's what they were doing because they don't do it anymore. According to the chatroom, anyway. Yeah, good. Well, this has been really, really valuable. And you see there's nothing perfect out there.

**Steve:** Yeah. And, well, and what I wanted to do was, when I realized how many choices there were, I thought, okay, wait a minute, let's step back and get an overview, like what's going on out there? And our sponsor, Carbonite, if, for example...

**Leo:** I'm pleased to hear that they're good.

**Steve:** I set Jenny up with Carbonite because she doesn't need all these kinds of features. She just needs her laptop protected. And that's a good price for unlimited storage of a laptop, of a single machine. It makes, I think, lots of sense.

**Leo:** There is a Wikipedia article called "Comparison of File Hosting Services" that has a very large chart with checkboxes and things that might make it a quick way to kind of get a survey of features in many, many, many, many more. I don't know how many they're doing.

**Steve:** I'm glad somebody else did that.

**Leo:** Yeah. And we're going to do - we have a new show we're launching, Iyaz Akhtar and I are going to launch a show, a how-to show. And one of our first episodes, I think it is our first episode, how to roll your own cloud services, using things like Pogoplug. So that might be the best way to do it. If you've got a couple of - you need, of course, in order for it to work, you need a couple of premises so that you aren't all in one spot. But I think it's possible to do your own, as well. Certainly a lot cheaper. Depends what you need. And yes, I don't know how accurate the Wikipedia article is or whether vendors go in and modify it and all of that. It's really not a review. It's more like a list of features.

**Steve:** Oh, and that's super useful. I mean, the one thing that I liked, although I didn't like SecretSync because they didn't talk about security, and they were pricey, but it was interesting to see their - well, and of course it is their comparison chart. But it was interesting to, like, sort of see them lined up next to a bunch of these other guys because all the other players are there, too.

**Leo:** This does not seem to have any information about pre-Internet encryption, which is unfortunate because that's, for us, the thing we care most about.

**Steve:** Oh, Leo. If our data is going to go up to the cloud, it's got to be safe.

**Leo:** Yeah, yeah.

**Steve:** I mean, it just has to be. So, yes. From all of this, as I said, I'm using Jungle Disk, but I'm going to be looking closely at SpiderOak. And they were really responsive to saying, hey, we'll tell you anything you need to know. So I expect I'll start using it a little bit, see if it, like, passes just the usability test. But you are using it and have been for, what, a year?

**Leo:** Yeah, a year, yeah.

**Steve:** Oh, okay. Cool.

**Leo:** Yeah, yeah. I use it, mostly I use it to sync the computers, my documents folders across a bunch of computers.

**Steve:** Nice.

**Leo:** And of course, as a side effect, you get a backup, as well.

**Steve:** Yeah, and that's free. The cross-machine synching is just thrown in.

**Leo:** Right, right.

**Steve:** Cool.

**Leo:** All right, Steve. Steve Gibson lives at GRC.com. That's where his Gibson Research Corporation is hosted. You can get SpinRite there, of course, the world's best hard drive maintenance utility. You must have it, if you have a hard drive. But he also has lots of free stuff which I highly encourage you to check out, GRC.com. Next week a questions episode, so post your questions there, GRC.com/feedback. There's also a users group there, a forum for people to share their security tips. Oh, there's so much stuff. And of course this show. And he offers 16Kb versions and transcriptions, which we do not offer at TWiT.tv. So if you need a small file, or you want the transcription, GRC.com. We do this show normally Thursdays, so - go ahead, I'm sorry.

**Steve:** I was going to say we don't have - I was just about to say we don't have you next week; right?

**Leo:** Yes.

**Steve:** You're off in Norway or something.

**Leo:** I'm going to Norway. We do this show Thursdays at 11:00 a.m. Pacific.

**Steve:** Wednesdays, Wednesdays.

**Leo:** I'm sorry, Wednesdays at 11:00 a.m. Pacific. We're doing it Thursday because I was out of town for NAB, and we had already done iPad Today. Those of you tuning in for iPad Today, I'm sorry to have disappointed you. However, we've already done it, and it'll be on the feeds any minute now. And we're going to replay at, I think, 11:00 - I'm sorry, 1:00 p.m. Pacific tomorrow, if you want to watch live-ish.

**Steve:** So I'll be here regular time.

**Leo:** 11:00 a.m. Pacific Wednesday.

**Steve:** Wednesday. But not with you.

**Leo:** With Iyaz Akhtar, I think. But I'm not sure. Might be Tom Merritt.

**Steve:** Yes, yes.

**Leo:** All right.

**Steve:** Iyaz is what Eileen and I talked about.

**Leo:** Good. Then that's who it'll be.

**Steve:** Cool.

**Leo:** All right. Hey, thanks, Steve.

**Steve:** Thanks, Leo.

**Leo:** Thanks, everybody, for joining us. We'll see you next time on Security Now!.