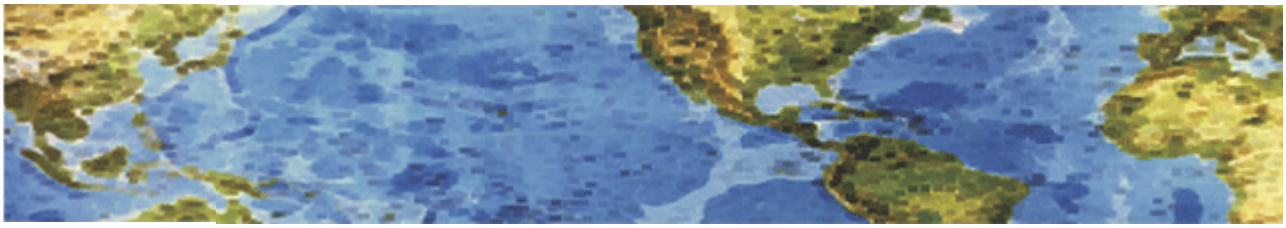
HALL ASSOCIATES



Risk-Based Decision Making Commentary
9 September 2014 Newsletter

Question: What is the cloud?

Answer: The cloud is a way of storing photos, documents, email, and other data on faraway machines. The cloud simply refers to software and services that run on the Internet instead of your computer. Apple iCloud, Dropbox, Netflix, Amazon Cloud Drive, Flickr, Google Drive, Microsoft Office 365, Yahoo Mail -- those are all cloud services. The practice saves space on your computers, smart phones, and tablets and allows users to access the same information **from any device**. Since the videos, photos, documents, games and other software that lives in the cloud are available on any device with an Internet connection, you can access your stuff **from anywhere**. And if you lose your phone, for example, you don't lose your vacation pictures. **The drawback is that you are putting your information somewhere else**, so you run the risk of a hacking attack on those systems and accounts. In fact, you might be surprised how much of your stuff is in the cloud.

That's because mobile apps and PC software are becoming inseparable from the cloud. For example, many services, including iCloud and Google+ Photos, automatically back up photos you take with your smartphone. (That can get you in trouble if, say, you take "special" photos and then delete them from your phone – there is still a copy in the cloud.) There's also a lot of personal information stored in the cloud that you didn't create. Health care providers store your medical records in the cloud, insurance companies put your claims there, and friends post photos of you on Facebook. That's a great convenience when you want to access the information -- and a bit scary when you hand the keys to your personal data over to third parties.

Question: Is the Cloud secure?

Answer: **For the most part, yes**. But only as much as you trust the company -- and your own passwords. Companies invest a lot to ensure that customers' private information stays private. The short answer is the servers that make up the Cloud are often more secure than other storage. **But that doesn't mean the system can't be compromised.** There are a lot of attackers who have a lot of time. And no system can be 100% secure. In addition, if an attacker gets YOUR account information by some scam, they can sign into your account.

Question: How can individuals make their data more secure?

Answer: **You need User Names and Passwords to access your accounts, so choosing a unique user name and a strong password is important.** You also need to have different passwords for each online account you hold, so a breach in one system won't compromise another. It is also important to have a number and punctuation mark in each password or a creative spelling of a word to make it harder to guess. Also, avoid using common words or notable birthdays as passwords. A strong password is particularly important if you store sensitive information online.

Another way to make your information harder to hack is called multifactor, or two-step, identification. That means the first time you log onto an account from a new device, you are asked for a second form of identification. Usually, that involves getting sent a code as a text on your phone or an email. A hacker who has your password still would need physical possession of your phone to get the text. But you usually have to activate the extra layer of protection.

http://www.toledoblade.com/Technology/2014/09/07/Computer-security-in-the-cloud-can-get-murky.html

HALL ASSOCIATES

So where does it all live? Instead of housing information on your hard drive or your phone's memory, your stuff is stored in massive data centers around the world. Amazon , Google, Apple, Microsoft and Facebook are among the biggest data center operators for consumer cloud services. There are 320 million iCloud users. Facebook users have uploaded more than 400 billion photos and add an average 350 million a day. Amazon's cloud services operate in 190 countries around the world. That's a lot of data.

These companies' massive server farms are so vast and so power-hungry that they are responsible for more than 2% of the United States' electricity usage, according to researchers at Villanova University. If the global cloud computing industry was a single country, it would be the fifth-largest in the world in terms of energy consumption, according to Ed Turkel of Hewlett-Packard's Hyperscale Business Unit.

Why you should be wary of the cloud

Time to consider some cybersecurity maintenance of your own – and stop trusting the cloud. Early this month, hackers broke into some celebrities' iCloud accounts and dug up and posted their very intimate photos – some of which the victims, including Jennifer Lawrence and Kate Upton, thought they had deleted. Apple, which owns iCloud, initially issued a statement explaining that there was no security breach. But by the end of the week Apple CEO Tim Cook said the company would add a security feature to alert users with a warning when someone tries to restore iCloud data.

Banks, email services and other online companies generally send users an email notice when someone tries to log in to your account from an unfamiliar device or tries to change a password**. That means your email account is your last line of defense**. So if you do only one thing to protect yourself this month, make sure you use a unique and elaborate password to access your email. The password should contain the longest string of arbitrary letters and numbers you can recall consistently (*see one of my earlier newsletters on strong passwords AND user names*). This is important because law enforcement is still investigating a break-in that involves several banks, including JP Morgan Chase. How many depositors have been affected remains unclear, but what is obvious is that these attacks are continuing.

As to whether financial institutions will ever succeed in stopping digital thievery, security professionals say don't hold your breath. Criminals are involved in an escalating battle for your accounts, and they won't stop. As bank robber Willie Sutton famously said (although he denied it), "That's where the money is." And that means you should never respond to an email or click on a link in one that asks you to log into an account – even if it is from your bank. Hackers are very adept at faking such messages, along with partial account numbers and official-looking logos. These so-called phishing attacks may look legit, but they'll take you to fake sites that ask for your password. And that's when you get hacked.

The same goes for LinkedIn requests in e-mails, or even for friends who send you a link that requires a password. **Just don't do it.** Instead, open a separate browser and go directly to the site you know before you sign in. Another question being debated is whether we can trust the cloud at all, given that more of our personal lives are being stored online. **The answer is no.**

Services that store your calendars, emails, financial data and entertainment grew exponentially as high-speed Internet became pervasive and cheap storage became commonplace. But security has not kept pace. The fact is, when you use a cloud service, you are trusting someone else to keep your records on their computers and hard drives. Like the banks, these services are embroiled in a war against criminals. And even if they have the best intentions, they are not impregnable. They may be secure enough to store your e-books, digital movies and music, but everything else? **Recommend that you keep it to yourself.**

http://www.foxnews.com/tech/2014/09/05/why-should-be-wary-cloud/?intcmp=obnetwork