



The View from Lori's desk...

Special Edition

Brought to you by ComVida

Jan 29th, 2020

I know it's only been a few weeks since my last view, so you're probably wondering what exciting things I'll be talking about this time... Well, do I have a treat for you! The focus of this special edition is, "Be Prepared!". Ok, maybe not the most exciting topic, but it is one that is close to my heart...

Yes, that's right, folks... I'm talking about taking a look around and making sure your hindquarters are protected (so to speak), and if you don't have a good handle on what you'd do in the event of a disaster, this is a great time to **meet with your IT team and make sure you're prepared**. I'm talking about BACKUPS – specifically off-site backups! Ransomware isn't just something you read about in the news, it happens... some of our own sites have even been hit, and it's not just ransomware... Picture this: You've securely backed up everything to a portable drive, and that drive is sitting on your desk so that it's within easy reach, and then the water main breaks... right over your desk... never happen? Actually, it did...

But hey, what about that handy backup folder on your server, full of backup files? Convenient, when you need to restore back to yesterday or last week... but what happens when that server gets hit with ransomware? That handy set of backups is not going to do anyone any good anymore...

In fact, here're some interesting statistics from an online blog published at the end of last year by phoenixNAP:

A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021. (Source: Cyber Security Ventures)

1.5 million new phishing sites are created every month. (Source: webroot.com)

Ransomware attacks have increased over 97 percent in the past two years. (Source: Phishme)

34% of businesses hit with malware took a week or more to regain access to their data. (Source: Kaspersky)

In 2019 ransomware from phishing emails increased 109 percent over 2017. (Source: Phishme)

There's no harm in hoping for the best, as long as you're prepared for the worst.
- Stephen King

Every organization is unique, but they all have one thing in common – data stored on a server somewhere, and that data is relied on for everything, from schedules to pay cheques, client information to financial statements. It is integral to your day-to-day operations, and the cost of recovery without a good backup is often measured in *weeks* of lost time.

But it's not all bad news. That sinking feeling of trying to recover from an attack can **easily be avoided with a good backup and recovery plan**. In fact, that's one of the many reasons why third-party hosting is so popular, and off-site storage is normally a standard part of the package.

So, please... *meet with your IT team, make sure you're prepared!* (Yes, I know I said it twice, that's how important it is!) Some questions you might ask: What is our recovery plan in the event of a malware attack? What do we do if the server fails? Is everything being backed up? How often are backups performed and the backups moved off-site? (directly correlates to the number of days you'll have to manually recover.)

And now for a word from your friendly ComVida support team: *A Secure Socket Layer (SSL) certificate is a critical part of your self-hosted website security! In fact, get 'em while they're hot – an SSL connection will be required for CVC51 by the end of 2020. Your webmaster or IT team can set one up if you don't already have one. If you're not sure, check your url (website address) – it should start with https.*

One last thought: It happens to be Bell Let's Talk day, why not ask someone how they're doing, or even just give them a smile - it might just make all the difference.

This view features a fun shot from the movie Twister – another disaster in which off-site storage might've been handy...?