DENTAL TECHNOLOGY ADVISOR

You Care For Your Patients, We Care For Your Technology

Bridge IT Support | February 2019

What's New

If you are considering an expansion, installing a new OP, or maybe adding a PAN or CBCT, please contact us early in the process! There are many considerations that are often overlooked when we are notified late in the process, so getting us involved early will save you time, money, and frustration.

We help make sure the specs are right, there is proper network hookup, video cables and power outlets are properly placed, and most important, who is installing each of these components.

Thank you for your business!

This monthly publication provided courtesy of Mark VanderWal, President of Bridge IT Support.

bridge IT SUPPORT

Our Mission:
To positively influence the quality of life in Michigan by directing our God-given talent of fixing and maintaining computer systems to dental practices so they can deliver exceptional care to their patients.

Do You Safeguard Your Company's Data and Private Client Information BETTER THAN Equifax, Yahoo and Target Did?

You can't deny that today we are living in an era of unprecedented technological progress. Particularly in the business world, we find ourselves more empowered day by day with the onslaught of fresh applications and features promising to extend our reach and drive success. There's a reason, after all, that business leaders like Virgin Group CEO Richard Branson argue that right now is a better time than ever to start a scrappy new company.

But this trend, in which companies become ever more inseparable from the technologies they depend on, is a double-edged sword.

Though tech continues to break down barriers to success in business, its forward motion is naturally accompanied by a newfound vulnerability. Each development is accompanied by a weakness to exploit – a back door through which hackers can wreak havoc on companies and customers alike.

This should be obvious to anyone who has even the barest awareness of the news. As the list of Fortune 500 companies that fall victim to cyber-attacks grows, we all need to learn from their mistakes and batten down our digital hatches in anticipation of a potential breach.

Last year, the country was shocked to discover that the personal data of more than 146 million people – including driver's licenses, passport numbers, Social Security numbers and a wide swath of other information – had been exposed in an attack on the credit mega-giant Equifax. Hackers infiltrated their systems through a vulnerability in Apache Struts, a tool used to develop web applications, and proceeded to lift a staggering quantity of customer data. The consequences of this attack are still being unpacked even now, but it's safe to say that even beyond Equifax's plummeting stock prices and their trip to PR hell, they've put themselves and the people they serve in a horribly uncomfortable position.

Continued on pg.2

'ontinued from pg.1

And make no mistake, the Equifax attack was far from inevitable. You would think that a company sitting on an international treasure trove packed with data from more than 800 million customers and 88 million businesses worldwide would take pains to be responsible digital stewards. But last September, under intensive government and journalistic scrutiny, company officials confirmed that, basically, this enormous breach had all come down to Equifax's failure to adequately patch their Apache Struts platform. You see, there was a known, publicly disclosed bug in the Apache Struts system the previous March. Despite the Apache Software Foundation's subsequent release of a patch eliminating the vulnerability, Equifax didn't install it in time to prevent issues, giving hackers months to easily exploit their systems and gain a foothold.

While the Equifax attack is certainly one of the most high-profile widespread data breaches in history, it's definitely not the only one to affect millions of customers. Yahoo admitted in 2016 that a data breach way back in 2013 had exposed around 1 billion of their usernames, e-mail addresses and passcodes. When Verizon acquired the company last year, they admitted that, upon further review, it looked more like 3 billion accounts had been affected. Also in 2013, hackers infiltrated Target's point-of-sale systems to steal 40 million debit and credit card accounts, thanks to a vulnerability in an

"Though tech continues to break down barriers to success in business, its forward motion is naturally accompanied by a newfound vulnerability."

HVAC company they'd hired called Fazio Mechanical Services.

Attacks like these – and the millions of similar ones aimed at small, midsize and massive companies every year – are almost always circuitous and confusing to the average business owner, but they're also preventable. Problem is, especially when it comes to SMBs, most business professionals and their understaffed, underfunded, inexperienced or even nonexistent IT departments aren't equipped to protect their precious data when the hackers come knocking.

Statistics show that, eventually, hackers are going to come for your business – it's all but guaranteed. And if they break through and bring your company to its knees, you probably won't be the next Equifax or Target all over the news with egg on your face. No, your business will probably just fold in on itself with nary a whimper, with everything you've worked so hard to build quietly buckling before your eyes.

Don't let it happen. Address cyber-attacks before they become an issue, and get a talented, experienced, around-the-clock team to defend your livelihood. It takes vigilance, research and constant upkeep to keep the wolves at bay. Protect your business or, before you know it, there won't be anything left to protect at all.

Free Report: What Every Dental Practice Must Know About Hiring An Honest, Competent, Responsive, and Fairly Priced Computer Consultant

Bridge IT Support recently released their latest report for the dental industry, which includes:

- The "dirty little secret" of the computer support industry
- 20 Revealing questions you should ask
- 4 costly misconceptions about computer maintenance
- And more……

Visit our website at www.bridgeITsupport.com for your copy, or email us today at info@bridgeITsupport.com

Security Byte

This section of the newsletter will remove the veil of ignorance and fear concerning cybersecurity and how it relates to your practice and home.

In an earlier newsletter issue, we discussed cybersecurity best practices are to utilize LAYERS of security in your network, like the combination of fences, walls, alarms, guards, dogs, and camera's surrounding the precious gold of Fort Knox.

What is a Firewall?

Your first line of defense against attacks from the outside is your Network Firewall, which is normally a small box located in your network closet. This device acts like a guard shack between the public internet outside of your building, and the private network inside your building. Each public visitor requesting access to your private network is processed by the firewall to make sure they have not been classified as "a bad guy". This is similar to checking fingerprints against known criminals to see if there is a match. If it is a known criminal, their request to enter your network is denied.

The list of criminals changes every minute of every day, so how do you keep the guard (firewall) updated on who the bad guys are? Next month, we will discuss Intrusion Detection Services that should be part of your network...

You Shouldn't Trust Your Backups! But You Should Get Them VERIFIED...

Ronald Reagan said it about the Russians, and it applies to your practice data backups: "Trust…….but VERIFY"

If you're reading this right now and your backups give you a nice green checkmark or a "Success!" email, and you haven't had anyone fully check them, I've got some bad news for you: unless you've had those backups VERIFIED, they can't be trusted. You could be in a situation where your backups could be silently failing or giving a "false positive" without you knowing it, a situation all too common.

Backup verification is a multi-step process. First, you have to verify all the data is identical to the "live" server. If a backup failed to copy correctly and it didn't warn you, how would you know? Your tapes could be blank, or filled with corrupted data, and the only way to know for sure is to check.

Second, you have to make sure you can restore. You may have a situation where the data copied correctly, but isn't in a format that can be restored. The disk could have errors or be damaged, or the backup could be missing core files or configurations. By actually rebuilding a Server with the data, you can prove that it is all there and working, beyond a shadow of a doubt.

Even if everything else is configured correctly, systems that use databases (like almost all EHR and Practice Management Systems) require special care. If, as an amateur would do, you

simply copy the files, **your backup will fail, and it will never warn you**, because it will look like it succeeds. It won't be until the day you try to restore that you find that your database is corrupted and unreadable, requiring costly DB repair services and upwards of weeks of downtime – if the data can be recovered at all! Backup verification can discover these issues before they become a disaster.

If you're currently rotating a set of disks or tapes, taking one home… is your backup encrypted? Do you know for certain it is? Has anyone tested and verified the encryption? Not only that, but how often are drives rotated? All too often, we find such a situation where a business owner believes the drives are rotated daily, but the staff member in charge isn't doing it. What does that mean? If there was a fire, flood, or theft, there would be no recovery – everything would be lost.

"What about Carbonite, Crashplan or other Cloud Backup?" These can suffer from data corruption or database configuration issues just

Continued on pg.4

Continued from pg.3

like a tape or disk system. Even if you have cloud backups that are configured directly, a situation like server hardware failure or ransomware can be far more costly than it seems. For an average-sized practice, your data could take upwards of **eight hours** or more to download from a cloud service! After that, you then need an IT professional to spend upwards of four to eight hours of time to set your system backup, restore those backups properly, reconnect all the computers, etc. Basically, consider having no computers – no X-Rays, no electronic insurance claims, no patient charts, nothing – for two full business days, minimum. How many thousands of dollars would that cost you? How much trust would you lose from your patients, having to send them home?

As an example, Bridge IT Support recently went in to a dentist office in the West Michigan area. They thought the backups were rock solid – every day, they got an email that said it was successful, and the office manager was dutifully swapping the disks. When we attempted to verify, we found that the backups actually contained no practice data at all! The basic "Windows" operating system was backed up, but the disks were completely missing their medical records, charts, and X-Ray images. The kicker was that this was a Server that was only 3 months old, and we verified that the backups were simply set up wrong at that point.

bridge
IT SUPPORT
6080 Fulton St. E
Ada, MI 49301

"Before I write my name on the board, I'll need to know how you're planning to use that data."