

Inside This Edition:

4 Deadly Mistakes You're Making
With IT Security



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.



I'm really not into spring cleaning.



Come to think of it, I'm not into summer, fall or winter cleaning either.



DENTAL TECHNOLOGY ADVISOR

You Care For Your Patients, We Care For Your Technology

Bridge IT Support

April 2019

What's New

Just like the dental industry, the IT industry changes fast and significantly every year. To help us keep up, Mark recently participated in a computer industry conference focused on improving our business, delivering better and faster service to our clients, and keeping up with technology and cybersecurity threats to keep our clients systems "lock-down" safe and running efficiently.



4 Deadly Mistakes You're Making With IT Security

For something so instrumental to the success of your business, technology can be an incredibly unstable, confusing and ever-changing tool. Just when you think you've got a handle on the latest cyber security trend, hackers find a way to circumvent the process completely. A new patch arrives for an essential piece of software, and the next day, another patch is required to repair the vulnerabilities the previous patch created. It can seem impossible to stay on top of the constant technological arms race, much less stay relevant amid the exponentially increasing pace.

Today, more and more businesses are switching over to a managed services model for their IT needs. A managed services provider is a company that partners with businesses to proactively manage their networks inside and out. With MSPs, you get a full team of professionals who become intimately acquainted with the entirety of your IT structure, not only ensuring that problems are fixed long before they hit your bottom line but offering recommendations and tweaks to optimize processes and save

time, money and headaches down the line.

By leaving your network up to an organization that takes the old break-fix approach, you're leaving the health of your entire business up to chance. Here are four ways the adage "If it ain't broke, don't fix it" is putting the security of your company in jeopardy.

1. YOU'RE BASICALLY PRAYING NOTHING EVER GOES WRONG.

The break-fix approach is pretty self-explanatory. The thinking goes that instead of shelling out a monthly fee for daily management of your network, you only pay your IT partners when a problem needs to be addressed. Typically, they're almost entirely hands-off until something goes wrong.

Certainly, this strategy saves money in the short term, but it will invariably come back to bite you in the long term. Hiring a break-fix IT company is a bit like opting for the lowest level of insurance coverage. You may not fret about it now, but you definitely will when an accident happens and you're

Continued on pg.2

Continued from pg.1

forced to pour thousands of dollars into repairs. And sadly, the threat of your business being hacked is actually greater than the chances you'll be in a serious car accident!

2. YOU'RE LEAVING HOLES IN YOUR DEFENSES.

Today's tech world is a constant game of whack-a-mole, with security experts frantically hammering down on every digital threat that rears its ugly head. For the entirety of your security structure to be equipped with the latest and greatest, it takes a team of genuine experts keeping an eye on your systems and ensuring everything is up to snuff.

With a break-fix approach, it's likely you don't detect flaws in your system until long after they've already been exploited, costing you dearly. And it's important to remember that every data breach has the potential to be utterly catastrophic, doing so much damage that it can close down your business for good. Better to stay one step ahead with an MSP by your side.

3. YOU'RE OPENING YOURSELF UP TO COSTLY SERVER DOWNTIME.

When the very survival of your business depends upon staying online and serving your customers, every minute your network is down – your assets are locked down behind ransomware or your tech is fried to the point that you're at a standstill – is a minute that you cannot afford. According to Gartner, the average cost of IT downtime is a whopping \$5,600 per minute, and that doesn't even

“... you're leaving the health of your entire business up to chance.”



factor in disgruntled clients or missed communications.

The top priority of your IT infrastructure should be to prevent downtime from ever occurring, not to minimize the amount of downtime you suffer when something goes wrong.

4. YOU AREN'T OPERATING AT PEAK EFFICIENCY.

One of the most insidious costs of the break-fix approach doesn't have anything to do with your network breaking down. It chips away at your bottom line gradually and silently, without causing much of a fuss.

Without a proactive eye on your systems, chances are you aren't implementing the processes and software that keep everything working at its highest potential. You'll be using clunky work-arounds to simple problems without even realizing you're doing it. The seconds you waste on Internet bottlenecks will add up over time, especially when multiplied by your entire company.

The fact is, the break-fix model of doing business is, ironically, broken. Consider partnering with an MSP and invest in the long-term future of your company.

Security Byte

This section of the newsletter will remove the confusion 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 cameras surrounding the precious gold of Fort Knox.

What is Managed Services?

For the past 15 years, Bridget IT Support has provided “on demand” computer support to practices in Michigan. This on demand, or “break-fix” style of support is a reactive, “call us when it breaks” model of business. For many years, this reactive model has worked well. However, over the past few years, the cybersecurity threats have matured, and tools available to computer support companies have evolved, along with demands on your IT infrastructure uptime. As a result, a more proactive model has developed in the IT business called Managed Services. This proactive model allows your IT company to constantly manage your system for optimal security and uptime.

Bridge IT Support continues to offer the on-demand, break-fix model of support, but now offers managed services with their Full Support program. For a fixed monthly budget, we take care of all your computer system needs, including free Helpdesk calls, network security devices, automatic backup, disaster recovery testing, system optimization and much more.

Contact us today to learn more about how managed services can improve your business.

Great CEOs Give Their Teams Freedom to Choose

Something surprised me the other day. A colleague, who had (sniff!) previously left to work for a big company, told me the reason she'd returned to my company, ghSMART. She'd left a couple of years ago to become a senior executive at a top-tier fashion company. It sounded like a dream job at the time, but within two years, she came back to our firm.

I was happy she'd returned, but it was a mystery to me *why* she'd decided to come back. When I asked her while sitting next to her at our firm's annual summit, she paused for a second. “The real reason is our culture of freedom here at ghSMART,” she said. “It's not like that in Corporate-land. There was no freedom there. Meetings, meetings, meetings. And if anybody above me, or below me, called a meeting, I had to be there, as their culture requires. It's like nobody trusted anybody to think or act on their own! Everything was by committee. Drove me nuts. Here, we're way more empowered to make decisions, to use our talents, to team up with colleagues when it makes sense and to take initiative and make things happen for our clients.”

Her story made me feel good. As chairman and founder of ghSMART, one of my two big goals for starting our company was to provide a career “home” to exceptionally talented people. At one point, I had to make a key decision about our culture. I had to pick between hiring not-so-smart people and boxing them in with excessive meetings, processes and bureaucracy to limit their ability to do damage; or to hire smart people, as in *ridiculously* smart and capable people, and give them the freedom to make choices.

In the end, I chose the path of “talent and



freedom,” of course. It just made a lot more sense to me. I worked to create a culture in which my team had the freedom to choose which clients to serve; which types of problems to help them solve and how to go about doing that; to choose their own career path at the firm; and to choose which colleagues to work with along the way.

This decision wasn't original though. It came from watching some of the best CEOs in the world hire the most skilled folks in business and learning about the results those employees produced when they were given an unusual amount of freedom to make decisions. It became clear to me over the years that the mark of a *truly* great CEO is the ability to hire super-talented people and give them the opportunity to forge their own path. The best leaders are able to attract the best talent and give their colleagues the choice to make life-and-death decisions swiftly and effectively.



Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book, *Who: A Method For Hiring*, and the author of the #1 Wall Street Journal best seller, *Leadocracy: Hiring More Great Leaders (Like You) Into Government*. Geoff co-created the *Topgrading* brand of talent management. He is the founder of two 501(c)(3) nonprofit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in economics with honors from Northwestern University, and an MA and Ph. D in psychology from Claremont Graduate University.

Are You Prepared for January 14, 2020?



This is the day Microsoft will no longer support Windows 7, making all computers running this operating system vulnerable and non-compliant.

Do you have any computers running Windows 7? If yes, we need to put together a plan to make the conversion to Windows 10 in your practice.

Contact us today for a free Technical Business Review to map out a plan for your computer system. 616.682.5450 or info@bridgeITsupport.com