T. Daniels Consulting

THE T. DANIELS TIMES

Microsoft SMB Cloud Champions Club

Microsoft Partner | Silver Cloud Platform, Silver Small and Midmarket Cloud Solutions

What's New

This season of Thanksgiving, we want to say **Thank You** to our clients and newsletter readers. We love watching you manage your business, especially during these challenging times, and we learn so much from your commitment to excellence in customer service. From the blogs you follow to the books you recommend, we appreciate your desire to learn. We think of you each month when we write our newsletter. We want it to be full of information — to help you be a better boss, manager, and business professional. And because of that goal, you (unknowingly) push us towards excellence every month, as we plan articles for you. Happy Thanksgiving wishes to you and your family.

November 2020

This monthly publication provided courtesy of Timothy D. Ricketts, President of T. Daniels Consulting.

"Thank you for the confidence you have given our entire team to manage and protect your valuable assets. We take great pride with our goal to exceed your expectations every day!"

4 Questions Your IT Services Company Should Be Able To Say "Yes" To

Out with the old and in with the new! For far too long, small businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services company and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT specialists are an in-demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong.

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence),

Continued on pg.2

Continued from pg.1

what's next? You call your IT services partner – if you have a partner – and tell them you need help. They might be able to restore lost or stolen data. That is, if you routinely backed up that data. You don't want to find yourself in this position.

And you don't have to.

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

If you work with an IT services company that only comes out when something breaks, it's time to get them on the phone to ask them four big questions. These are questions they absolutely need to say "yes" to.

1. **Can you monitor our network and devices for threats 24/7?**
2. **Can you access my network remotely to provide on-the-spot IT support to my team?**
3. **Can you make sure all our data is backed up AND secure?**
4. **Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?**

If your IT services partner says "no" to any or all of these

> **"When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!"**

questions, it might be time to look for a new IT services partner.

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security). They would rather pay for things as they break. But these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

FREE Executive Guide: 12 Little-Known Facts Every Business Owner, Non Profit Organization, And Government Leader Must Know About Data Backup, Security And Disaster Recovery

You will learn:

- The only way to know for SURE your data can be recovered if lost, corrupted or deleted – yet fewer than 10% of businesses have this in place.
- Seven things you should absolutely demand from any off-site backup service.
- Where many backups fail and give you a false sense of security.
- The #1 cause of data loss that businesses don't even think about until their data is erased.

Get your FREE copy today at:
https://www.tdaniels.com/protectyourdata1120/

Shiny New Gadget Of The Month:

Arlo Pro 3 Floodlight Camera

In the era of porch pirates, more people are investing in outdoor security cameras. The Arlo Pro 3 Floodlight Camera delivers security and practicality. It features an ultrahigh-definition camera delivering 2K HDR video and color night vision combined with a 2000 lumens light. Nothing goes undetected!

Plus, the Arlo Pro 3 is wireless. It connects to WiFi and doesn't need a power cord (it just needs to be plugged in for charging periodically). Because it's on WiFi, you can check the feed anytime from your smartphone. You can even customize notifications so you're alerted when it detects a car or person. And it has a speaker and microphone so you can hear and talk to anyone near the camera. Learn more at: **Arlo.com/en-us/products/arlo-pro-3-floodlight.aspx**

Should You Cut Your Technology Budget For 2021?

It goes without question that budgets were impacted by COVID-19. Many business leaders immediately adopted a conservative approach to any form of spending, including IT, in their budgets.

And now with 2021 on the horizon, many business owners are asking themselves an important question: what should we be doing with our technology budgets? Across the board, a new key differentiator for businesses will be their ability to be agile and adopt new trends that encourage the efficiency and security of their remote workforce.

One thing is for sure, there isn't one set answer on whether you need to increase your IT spending, lower your technology budget, or keep things status quo. A lot is going to depend on your situation and future plans. However, here are a couple of things we think you should consider…

There Might Be Reasons to Cut Back

Let's face it: this could be a time when you need to decrease your technology spending. If your bottom line has taken a big hit, then the last thing you want to do is to continue as if it's business as usual, particularly if that puts important investments (like payroll) at risk.

If you do need to trim your IT budget, there is a right way and a wrong way to go through such an exercise. Don't simply look for the most expensive items on your list or cut services that seem unnecessary without first considering the consequences. As an example, halting your expenditures for managed support services or backup and disaster recovery might save you a few dollars today, but could cost you huge amounts in the future.

Cyber Security Is Critical- Now More Than Ever

It's not just businesses that are noticing the technology changes brought on by the events of 2020, cyber criminals are as well. Organizations that have newly deployed remote workforces and are expanding their cloud capabilities have also increased their security vulnerabilities, especially related to ransomware attacks, via inexperienced employees, new systems, and processes.

One thing is for certain, operating a business with cloud-enabled technologies is very safe and secure when the proper cybersecurity protections are in place. There are numerous cybersecurity solutions that can be implemented to improve security, provide training to your employees, and monitor your networks.

Need Help Finding Good Business Technology Answers?

Even if your IT budget isn't quite as big in 2021, it makes it even more important to ensure your IT investments are in the areas most vital to your company's success. If you're looking for real insights that can help you manage plans, budgets, and more, contact us at https://www.tdaniels.com or 810-629-0131.

The T. Daniels Difference

25 YEARS
1994 ~ 2019
T. DANIELS CONSULTING

For over 25 years, T. Daniels Consulting has provided Small and Medium sized organizations with excellent customer service. Our Microsoft Certified Professionals and Engineers have an average 10 years' experience benefiting you by fixing problems quickly and correctly the first time. No other competitor comes close to our level of knowledge, experience and professionalism. We are continuously adding new and improved services to meet your ongoing needs. We never stop improving. That is the **T. Daniels Difference**. Thanks to all of our customers for making us one of Michigan's fastest growing IT consulting and service companies.

Is Working From An Office More Secure Than Working Remotely?

It may come as a surprise, but working remotely can be just as (or more) secure than working in the office. *If* done right.

Those are the three operating words: *if done right*. This takes effort on the part of both the business and the remote employee. Here are a few MUST-HAVES for a secure work-from-home experience:

Secure networks. This is nonnegotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

Secure devices. All devices used for work should be equipped with endpoint security – antivirus, anti-malware, anti-ransomware and firewall protection. Employees should also only use employee-provided or approved devices for work-related activity.

Secure passwords. If employees need to log into employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board. *Entrepreneur, June 17, 2020*

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. Regularly update your passwords. Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2. Say no to sharing. Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. Connect the camera to a SECURE network. Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better. *Digital Trends, May 7, 2020*