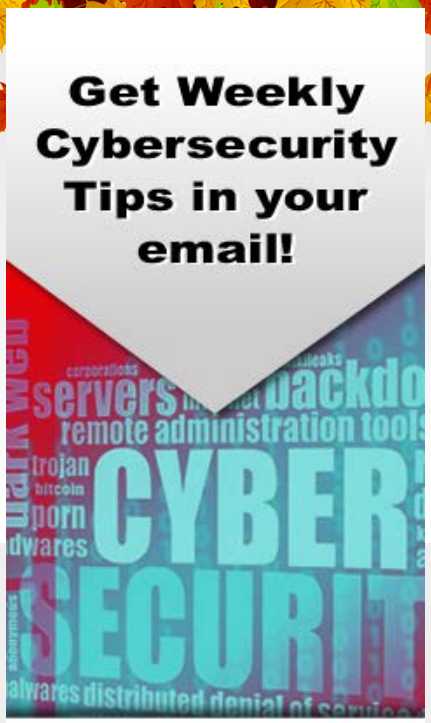
The Bensinger Beacon

MONTHLY INFORMATION TECHNOLOGY NEWSLETTER



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), what's next? You call your IT services partner –

Continued on pg.2

This monthly publication provided courtesy of Ed Bensinger, CEO of Bensinger Consulting.

As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Continued from pg.1

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

"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!"

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!

Get a FREE, No Obligation, Security And Network Assessment!

Would you like a 2nd opinion about your IT Services, but don't want your current IT company to know? Would you like discreet confirmation that your security services are really keeping you secure? And that your backups are really backing up?

Contact us for your FREE, No Obligation, Security And Network Assessment!

We will contact you prior to beginning our assessment. Nothing will be installed on your network. When we're done, we'll provide you with written documentation of our findings at NO OBLIGATION to you.

Visit: bensingerconsulting.com/data-backup-and-recovery/
or call our office at (602)362-0202.

Do These Things To Protect Your Business From Getting Hacked

Train Employees.
Your team needs to know how to identify and handle today's IT security threats.

Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

Hold Employees (And Yourself) Accountable.
Training and company guidelines don't mean much without accountability.

When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone who does not accountable.

Have A Disaster Recovery Plan.
Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen.

This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved?

Who do you notify in the event of a breach?Who do your employees call in the event of disaster? SmallBiz Technology, Dec. 26, 2019

Is Working From An Office More Secure Than Working Remotely?

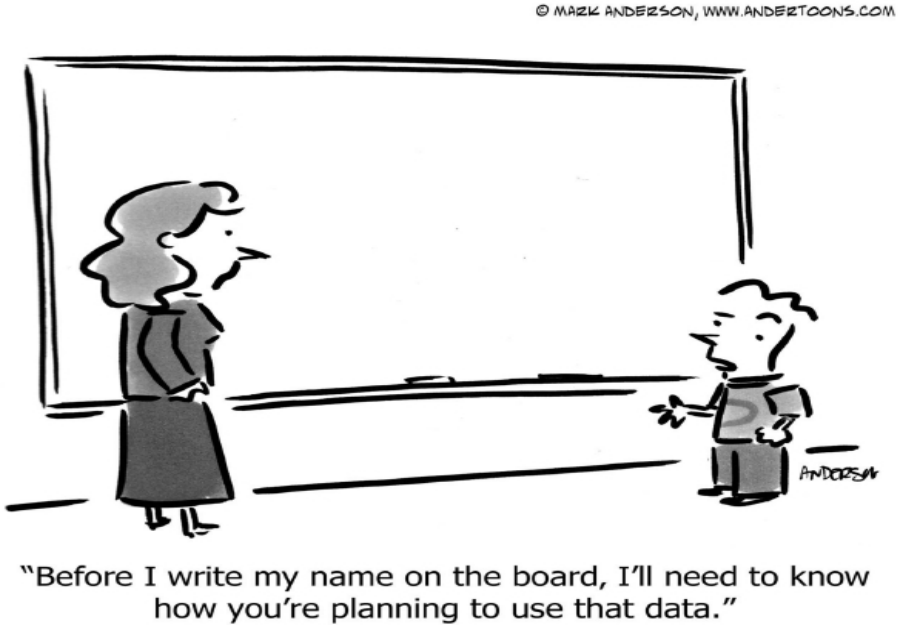
It may come as a surprise, but working remotely can be just as (or more) secure than working in the office. If done right.

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



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

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

Ed Bensinger