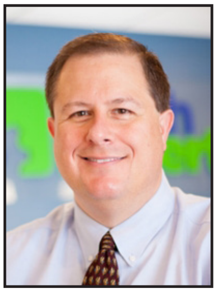
September 2022

TechTidbit.com

brought to you by Tech Experts

Who's To Blame For A Cyber Security Breach?



Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

We all know what a huge danger a cyber security breach can be for a business. And just how many businesses are being breached right now. You hear about it on the nightly news and read about it almost daily in the newspaper.

In truth, we hate having to write this. We don't want to feel like we're scaring you or sound all doom and gloom! But it's really important that you're fully aware of the risk to your business if you suffer a breach.

Last year, the number of reported data breaches rose 68% compared to 2020.

And while it's a good idea to implement the right cyber security tools to help reduce the risk of an attack, it's practically impossible (or definitely unworkable) to give your business 100% protection from attack by only using software tools. You also have to manage the human element of data protection.

Because according to research, 85% of data breaches are caused by human error.

If that happens, who's to blame for your cyber security breach? Your employee? Or you, the business owner / manager?

It's a difficult question. Sure, your employee is likely the one to have clicked the link or downloaded a bad file that turned out to be malware. They may even have disabled security features to try to speed up their work.

However, as the business owner or manager, it should be your responsibility to reduce the risk of that happening in the first place.

It all starts with training your people regularly to make sure they understand the risks and how to avoid them. But you should also have the right policies in place to remind your employees of best practices, and what happens if they fail to comply.

Employees are your first line of defense against security breaches. They can only ever be as good as your cyber security strategy. Get that in place so everyone knows:

- What's expected of them
- How to avoid risk
- What to do if things go wrong.

Be sure your systems are appropriately locked down, so that your employees can't change security settings or install random software applications.

We say, don't worry about who's to blame – just get your ducks in a row, starting with your cyber security strategy. If we can help, get in touch.

And while it's a good idea to implement the right cyber security tools to help reduce the risk of an attack, it's practically impossible (or definitely unworkable) to give your business 100% protection from attack by only using software tools. You also have to manage the human element of data protection.

Six Technology Tools You Shouldn't Use Any Longer

> *"Older systems are clunky and get in the way of employee productivity. If you keep these older systems in use, it can lead to the loss of good team members due to frustration. 49% of surveyed workers say they would consider leaving their jobs due to poor technology."*

One constant about technology is that it changes rapidly. Tools that were once staples, like Internet Explorer and Adobe Flash, age out. New tools replace those that are obsolete. Discontinued technology can leave networks vulnerable to attacks.

While older technology may still run fine on your systems, that doesn't mean that it's okay to use. One of the biggest dangers of using outdated technology is that it can lead to a data breach or infection.

Outdated software and hardware no longer receive vital security updates. Updates often patch newly found and exploited system vulnerabilities. No security patches means a device is a sitting duck for a breach.

Approximately one in three data breaches are due to unpatched system vulnerabilities.

Another problem with using discontinued technology is that it can leave you behind. Your business can end up looking like you're in the stone ages to your customers, and they can lose faith and trust.

Important reasons to keep your technology updated to a supported version are:

- Reduce the risk of a data breach or malware infection
- Meet data privacy compliance requirements
- To keep a good reputation and foster customer trust
- To be competitive in your market
- To mitigate hardware and software compatibility issues
- To enable employee productivity

Older systems are clunky and get in the way of employee productivity. If you keep these older systems in use, it can lead to the loss of good team members due to frustration.

49% of surveyed workers say they would consider leaving their jobs due to poor technology.

Following is a list of outdated technology tools that you should replace as soon as possible. Are any of these still in use on your home computer or within your business?

Internet Explorer

Many moons ago, Internet Explorer (IE) used to be the number one browser in the world. But, over time, Google Chrome and other browsers edged it out. Including its replacement, Microsoft Edge.

Microsoft began phasing out IE with the introduction of Microsoft Edge in 2015. In recent years, fewer applications have been supporting use in IE. The browser lost all support on June 15, 2022.

Adobe Flash

Millions of websites used Adobe Flash in the early 2000s. But other tools can now do the animations and other neat things Flash could do. This made the tool obsolete, and Adobe ended it.

The Adobe Flash Player lost all support, including security updates, as of January 1, 2021. Do you still have this lingering on any of your computers? If so, you should uninstall the browser plugin and any Flash software.

Windows 7 and Earlier

Windows 7 was a very popular operating system, but it's now gone the way of the dinosaur. Replacements, Windows 10 and Windows 11, are now in widespread use. The Windows 7 OS lost support on January 14, 2020.

While it may still technically run, it's very vulnerable to hacks. Microsoft Windows OS is also a high-value target for hackers. So, you can be sure they are out there looking for systems still running this obsolete version of Windows.

macOS 10.14 Mojave and Earlier

Because of the cost of iMacs and MacBooks, people tend to hang onto them as long as possible. Once these devices get to a certain point, updates no longer work. This leaves the hardware stuck on an older and non-supported macOS version.

If you are running macOS 10.14 Mojave or earlier, then your OS is no longer supported by Apple, and you need to upgrade.

Oracle 18c Database

If your business uses Oracle databases, then you may want to check your current version. If you are running the Oracle 18C Database, then you are vulnerable. Breaches can easily happen due to unpatched system vulnerabilities.

The Oracle 18C Database lost all support in June of 2021. If you have upgraded, then you'll want to keep an eye out for another upcoming end-of-support date. Both Oracle 19C and 21C will lose premiere support in April of 2024.

Microsoft SQL Server 2014

Another popular database tool is Microsoft's SQL. If you are using SQL Server 2014, then mainstream support has already ended. And in July of 2024, all support, including security updates will stop.

This gives you a little more time to upgrade before you're in danger of not getting security patches. But it is better to upgrade sooner rather than later. This leaves plenty of time for testing and verification of the upgrade.

Get Help Upgrading Your Technology & Reducing Risk

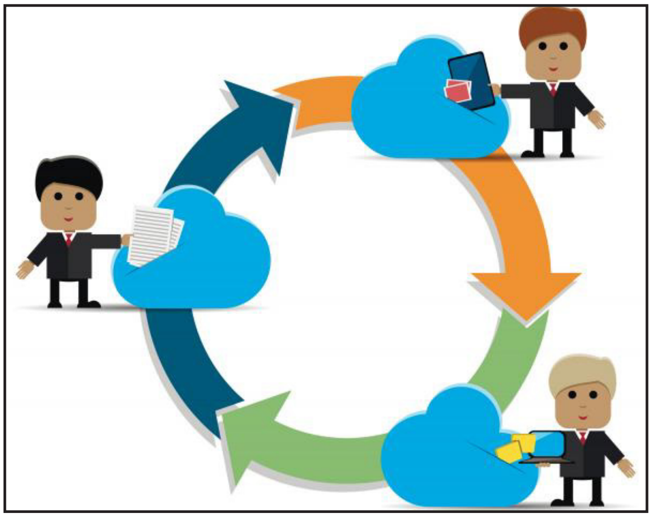
Upgrades can be scary, especially if everything has been running great. You may be afraid that a migration or upgrade will cause issues.

We can help you upgrade your technology smoothly and do thorough testing afterward. Schedule a technology review today.

Helpful Tips For Keeping Your Cloud Storage Organized

Cloud file storage revolutionized the way we handle documents. No more having to email files back and forth. No more wondering which person in the office has the most recent copy of a document.

But just like the storage on your computer's hard drive, cloud storage can also get messy. Files get saved in the wrong place and duplicate folders get created.



When employees are sharing the same cloud space it's hard to keep things organized. Storage can be difficult to keep efficient.

Disorganized cloud storage systems lead to problems. This includes having a hard time finding files. As well as spending a lot of extra time finding needed documents.

Has your office been suffering from messy cloud storage? Does it seem to get harder and harder to find what you need?

Use a Universal Folder Naming Structure

When people use different naming structures for folders, it's harder for everyone.

They often can't find what they need. It also leads to the creation of duplicate folders for the same thing.

Map out the hierarchy of folders and how to name each thing. For example, you might have departments" as an outer folder and nest "projects" inside.

With everyone using the same naming system, it will be easier for everyone to find things. You also reduce the risk of having duplicate folders.

Keep File Structure to 2-3 Folders Deep

When you have too many folders nested, it can take forever to find a file. You feel like you must click down one rabbit hole after another. When people need to click into several folders, it discourages them from saving a file in the right place.

To avoid this issue, keep your file structure only two to three folders deep. This makes files easier to find and keeps your cloud storage more usable.

Use Folder Tags or Colors for Easier Recognition

Many cloud file systems allow you to use color tagging on folders. Using this can make a folder or group of folders instantly recognizable. This reduces the time it takes to find and store files.

Don't Create Folders for Fewer Than 10 Files

The more folders people have to click into to find a document, the more time it takes. Folders can quickly add up as employees create them, not knowing where a file should go.

Use a rule for your cloud storage that restricts folder creation to 10 files or more.

This avoids having tons of folders with less than a handful of files in them. Have someone that can act as a storage administrator as well.

This can then be the person someone asks if they're not sure where to store a file.

Promote the Slogan "Take Time to Save it Right"

We're all guilty from time to time of saving to something general, like the desktop on a PC. We tell ourselves that we'll go back at some point and move the file where it should be.

This issue multiplies when you have many people sharing the same cloud storage space. Files that aren't where they belong add up fast.

This makes it harder for everyone to find things.

Promote the slogan "take time to save it right" among the staff. This means that they should take the extra few seconds to navigate where the file should be to save it.

This keeps things from getting unmanageable. If you use a file structure that's only 2-3 folders deep, then this should be easier for everyone to abide by.

> *"Many cloud file systems allow you to use color tagging on folders. Using this can make a folder or group of folders instantly recognizable. This reduces the time it takes to find and store files."*

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

What To Do If You Lose Your Laptop (Or Other Device)

So, you're in the car on the way home from the coffee shop, basking in the glow of consuming your triple-shot, low-foam, extra-hot pumpkin-spice latte when you suddenly realize your laptop has gone missing.

You drive back like the caffeinated lunatic you are, only to discover no one has turned it in.

What do you do?

That depends on what precautions you have (or haven't!) taken.

First, if you've properly encrypted your data, password-protected the access to your device and shut down and logged off all key applications, you've got a bit more time to respond.

But the next thing to do, whether or not you've taken those precautionary measures, is to notify your IT support company that you've lost your device.

That will allow them to change passwords and lock access to applications and data a thief may gain access to via your unprotected laptop.

They can also remotely wipe your device to make sure no one will be able to gain access to the data stored on your computer. (Which is also why it's critical to back up your data on a daily basis!)

Next, change all the passwords to every website you log into, starting with any sites that contain financial data (your bank account) or company data.

If your laptop contained medical records, financial information, or other sensitive data (like social security numbers, birthdays, etc.), then you need to contact a qualified attorney to understand what you may be required to do by law to notify individuals who may be affected.

Quite simply, an ounce of prevention is worth a pound of cure, so make sure you're engaging with your IT support company to encrypt and back up your data, as well as put remote monitoring software on all mobile devices.

Set a pin-code lock or password requirement to access a device after ten minutes of inactivity and get into the habit of logging out of websites when you're done using them.

Some other tips to keep your laptop safe:

Use strong passwords, change passwords frequently, and avoid setting up automatic sign-ins. This will make it more difficult for thieves to log on to your computer and access your personal information.

Don't write down your passwords. If you must write your passwords down, don't keep the list close to your laptop (for example, on a sticky note kept in your laptop bag).

Never leave your laptop in an unlocked car or conference room.

Never leave your laptop in plain sight in your locked car. Lock it in the trunk and make sure no one sees you put it there.

Carry your laptop in something other than a laptop bag. This may seem unusual, but a laptop bag makes it very obvious to thieves that you are carrying a laptop. Use something more inconspicuous, such as a backpack or messenger bag.

Always keep your laptop in your sight. Don't leave a meeting or a conference room without your laptop - always bring it with you. You never know who could have access to that room, even if you're only gone for a few minutes.

Be especially diligent when traveling - airports are a common place for laptop theft. Also be careful in taxis, hotel rooms, restaurants, and coffee shops.

If your laptop is stolen, you'll want to make sure you have the make, model, and serial number so a complete report can be filed. Keep this information in your desk at work or at home.

Finally, if you store important data on your laptop, make sure it is being backed up! Most workers store their data on a company server, where it is protected and backed up.

If you're a mobile worker, backups are extra important since you don't have the security of a server-based backup system.