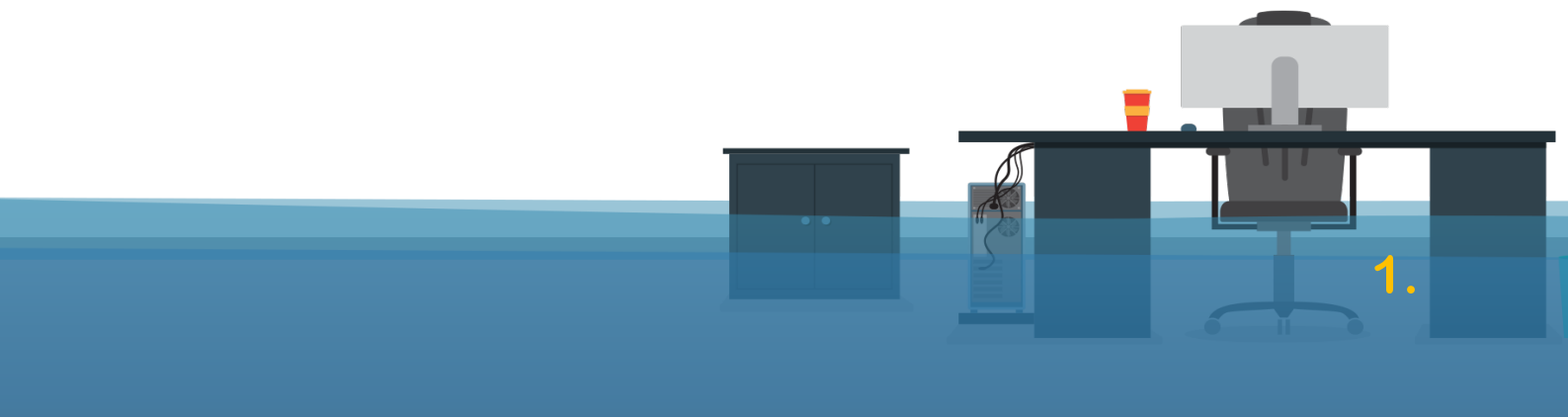
ARE YOU AT THE TIPPING FOR IT DISASTER?

Pride Solutions Derby

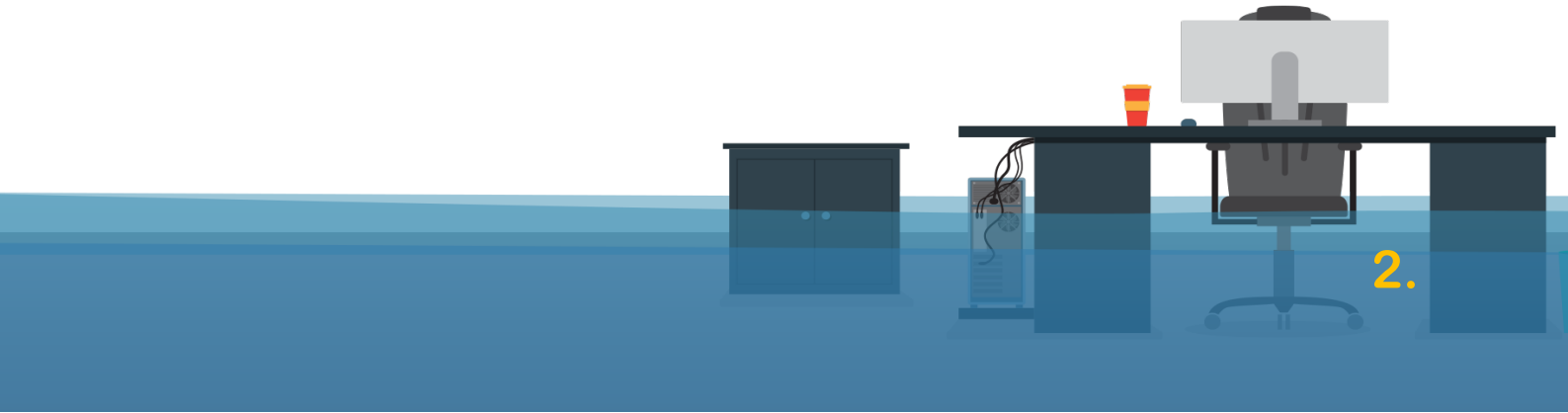
The thing about a Tipping Point is that we don't know we're there until we're tumbling head over heels over the edge. Too many businesses reach out to a managed services provider after something has gone wrong. It's not that we don't want your business, but we'd prefer to be proactive and help you avoid tipping into an IT disaster in the first place.



Flirting with IT Disaster

In his debut bestseller, Malcolm Gladwell wrote about The Tipping Point. It might be a magic moment before a trend takes hold or an idea reaches critical mass, but it's not always a good thing. A business can also reach the tipping point with its information technology (IT). Everything is going fine, and a business can be feeling secure, but then disaster strikes. There's a data breach. The computers crash. The backup fails. Everyone scrambles to recover.

Don't let your IT reach the tipping point. Pay attention to the signs telling you that you are flirting with the edge of disaster. Then, be proactive.



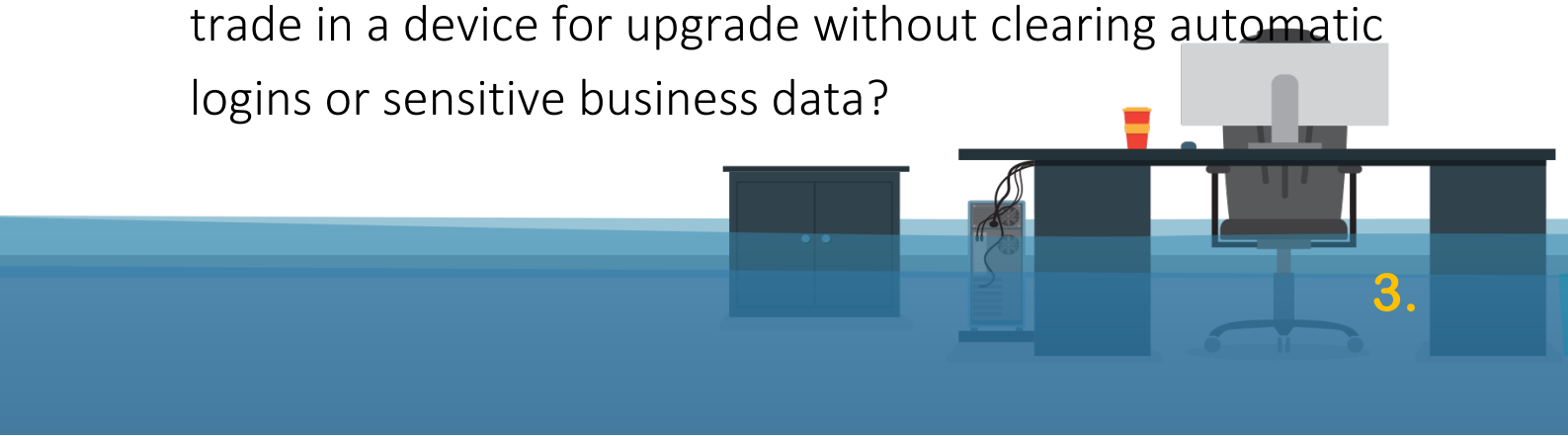
Tipping Tell #1

People like to use their personal devices at work. In a recent study nearly 80% of employers felt employees performed better using their own devices at work. (Though it may mean something that the Samsung commissioned the study.)

Many businesses allow Bring Your Own Device (BYOD) to improve morale and productivity while cutting costs. Even so, allowing employees to use their own smartphones or laptops is also a big security risk.

Employees using their own devices are going to be downloading their own apps, and they could download a mobile game with hidden malware or viruses. Then, the next time they log in to the company network, the malware spreads.

The opportunities for data loss or theft also rise. What if they send a file over an unsecured network? What if they trade in a device for upgrade without clearing automatic logins or sensitive business data?

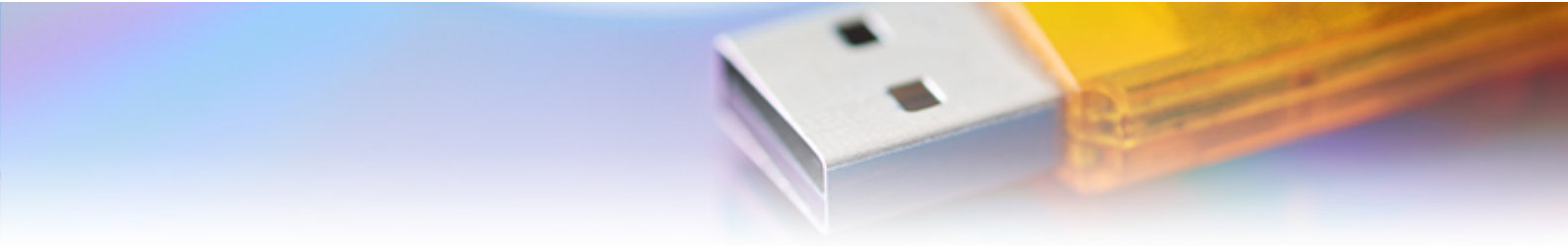


The personal device might be lost or stolen, or someone leaving the company could continue to have access to company applications after they go. You want to think the best of your employees, but a zero-trust policy can help reduce the security risk for the entire company from that one rogue device.

Tipping Tell #2

Microsoft's Windows 7 dominated the global market in its heyday. In December 2019, NetMarketShare indicated that approximately 26.6% of all Windows OS users were still on Windows 7, but Windows 7 reached its End of Life January 14, 2020.

That means millions of PCs could still be using an Operating System that is not getting any support. The OS is not getting updated or fixed. Most importantly, there are no more security patches. Hackers, meanwhile, know a large number of businesses are still working on the old



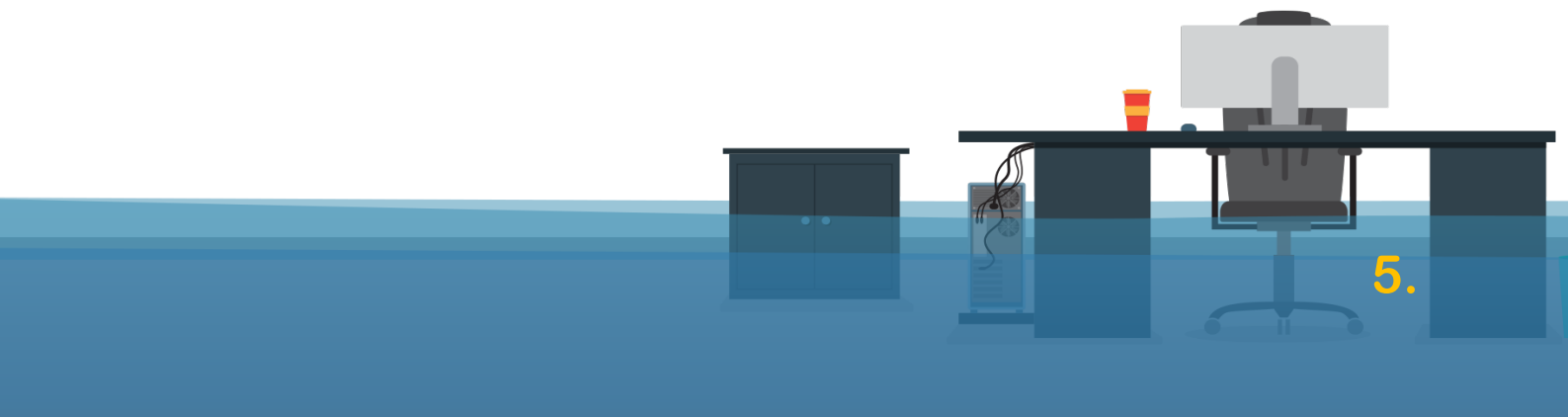
OS, and every month there are more vulnerabilities to exploit as the OS grows more exposed to cyberattack.

Your operating system won't just stop working on January 15, 2020. However, there will no longer be any updates or patches for viruses or security problems.

If you remain loyal to outdated software, you are putting your business at much greater risk of cyberattack.

Tipping Tell #3

Maybe your business still relies on email and file transfer when working together. Teams often need to get many people's input on a document, design, or proposal. The old-school approach sees different versions sent around for comments and revisions. Then, some poor person collects all that input and correlates it into a new, updated version.

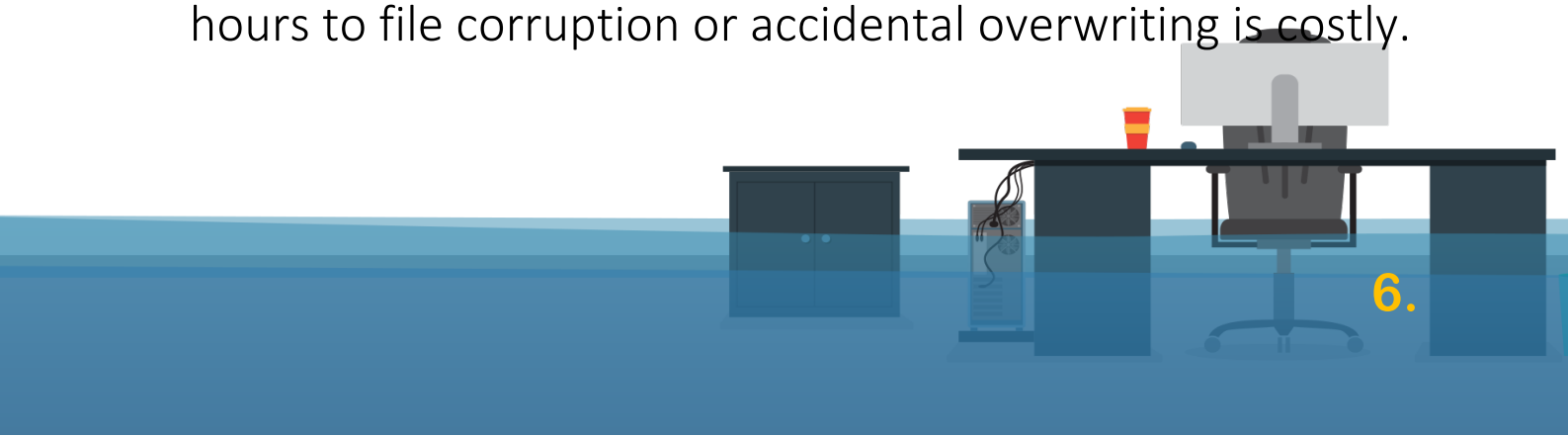


This approach slows down collaboration, plus, data can get lost. Also, with many mismatched versions circulating, it’s difficult to stay current.

Tipping Tell #4

Your business backup is non-existent or insufficient. You may back up your data to an external USB hard drive, thinking that’s good enough. But what happens if that drive is lost or stolen? If you keep the thumb drive on-site, what happens if your office is destroyed by fire or a natural disaster that takes your computers, too? You'd be left with nothing.

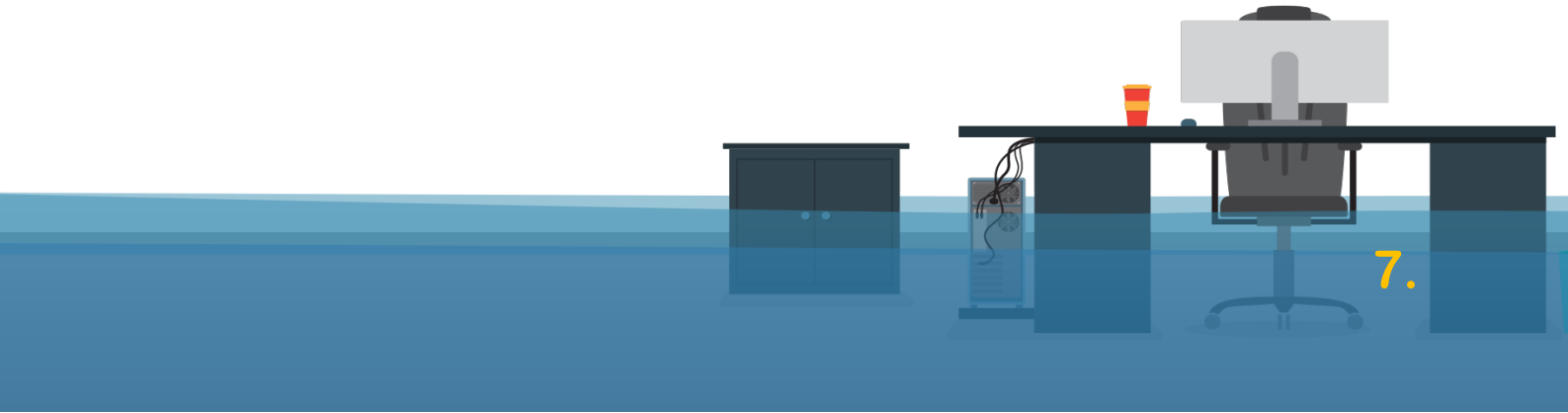
Even without that kind of dramatic damage, you may not be backing up enough for your needs. Many businesses backup at the end of the day as a habit. Depending on the amount and kind of work done daily, however, that may not be often enough. For some, losing even a few work hours to file corruption or accidental overwriting is costly.



Tipping Tell #5

Cybercriminals constantly find new ways to exploit operating systems, software, and applications. It’s their primary business. But your focus is on other things. Protecting your data and systems is something you know you need to do but can’t always find time to get around to doing.

You may not have a good way to keep all your IT up to date with the latest upgrades and security patches. You leave it up to employees to install the software security patches, for instance. But they're always getting notified about an update, and those notifications come at the worst times, so they put it off until later. Then, they forget. This leaves a vulnerability for exploitation that can put your network at risk.

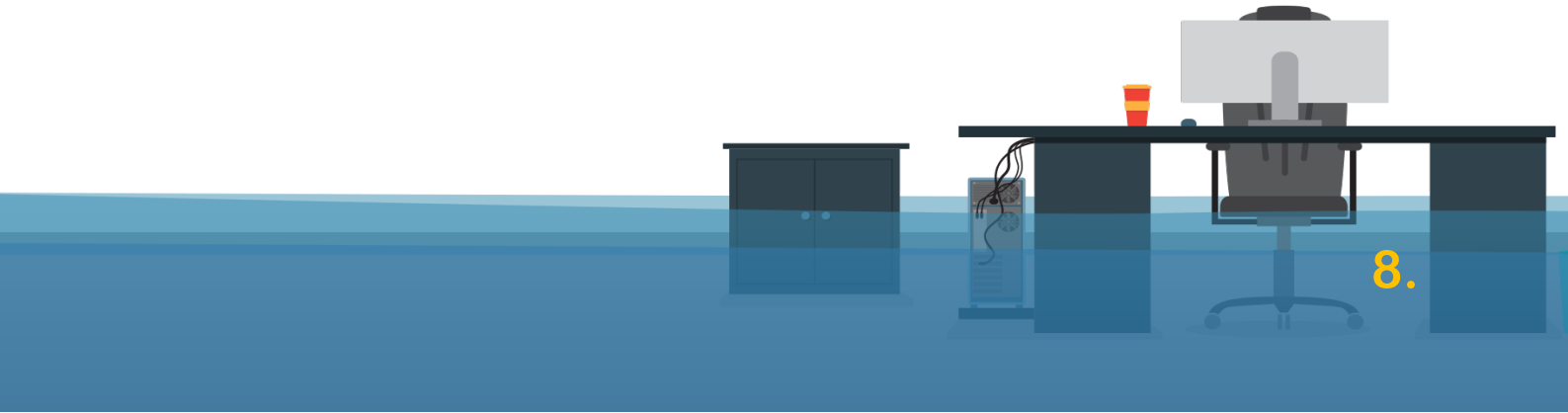


Tipping Tell #6

Growing your business may not seem like a bad thing, but landing big contracts and bringing in more employees can also cause IT problems. Adding new people can slow your email server, and putting new people on your software licenses adds up.

Plus, you've got to invest in more hardware to give every worker access to the technology they need to get the job done.

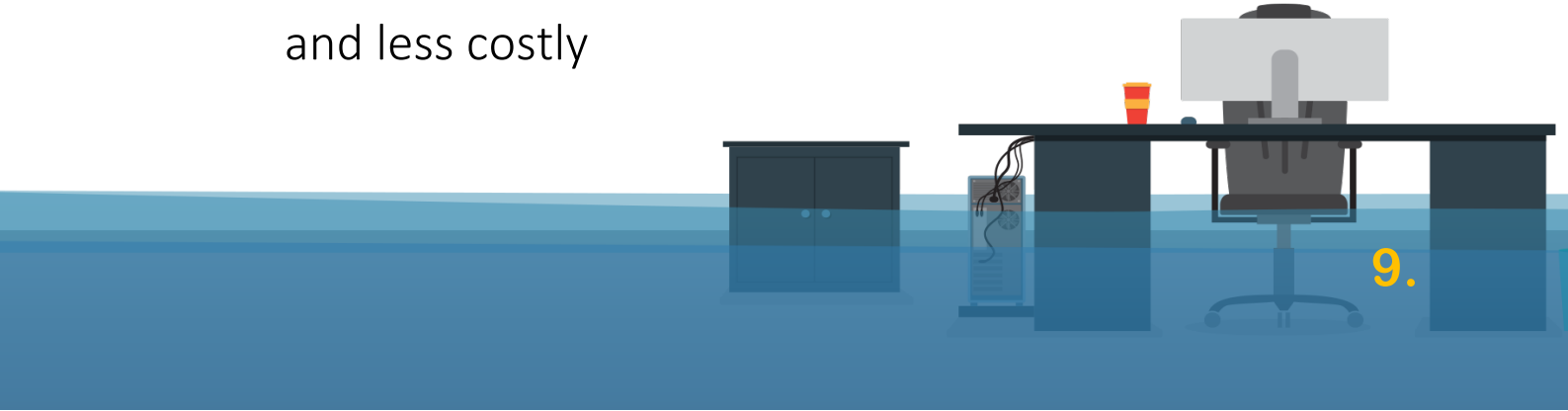
But when are you supposed to find the time to set all this up? You've got people to train and projects to deliver on! You can try to make-do until the money starts rolling in from all this new business, but that can hurt employee morale and your brand reputation.



What Can You Do?

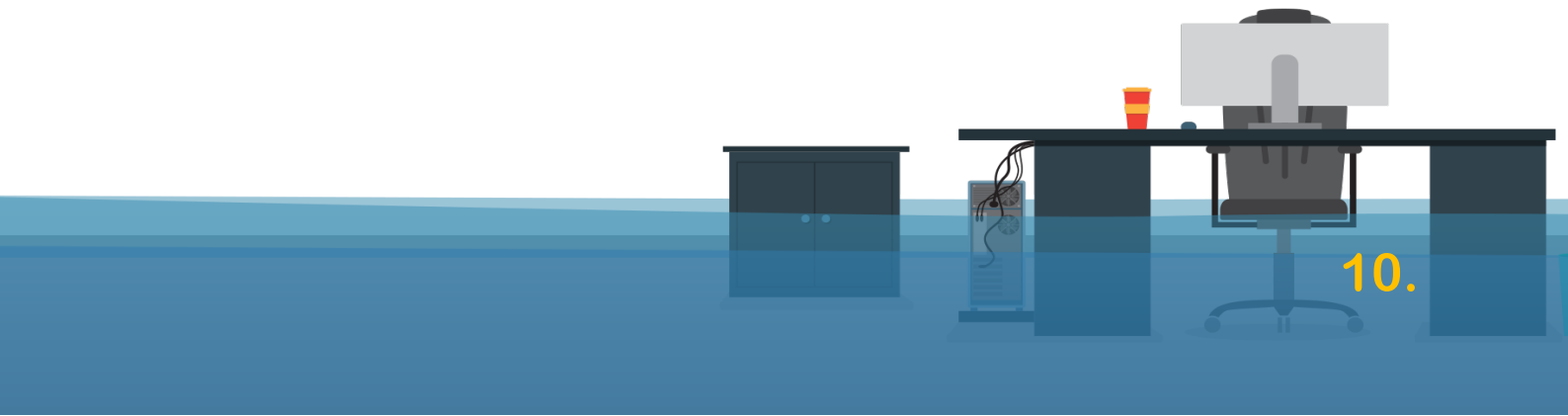
Don’t wait until the damage is done to reach out to IT experts. A managed services provider can help with each of these areas of concern:

- implementing mobile device management for BYOD
- overseeing an upgrade to Windows 10 for those still using the old OS
- introducing software to support online, real-time business collaboration and streamline processes
- upgrading backup so data is on physical devices (on-site and off premises), as well as in the cloud
- determining incremental backups or versioning needs throughout a business day
- putting a disaster recovery plan in place to help a business get back on its feet quickly
- monitoring and managing upgrades and security patches to keep IT current and safer
- providing cloud options that make scaling up easier and less costly



Your business has momentum, and you don’t want to lose that. Still, you can’t ignore IT growing pains. These tipping points may not feel like a priority but leaving them unattended can bring huge problems.

Partner with a managed services provider to pull your business away from a dangerous precipice. You’ll enjoy increased productivity and improved cost efficiencies while gaining the support of IT experts. Contact us today.



Pride Solutions Derby

Pride Solutions Derby Ltd
Thulston
Derbyshire
DE72 3UL

Phone: 01332 949706
Email: enquiries@pridesolutions.co.uk

Web: www.pridesolutions.co.uk

Facebook: www.facebook.com/pridesolutionsderby