THE 2020 PROBLEM

Revealed:
The ticking software timebomb that's going to disrupt half of all South Northants businesses in January 2020...
and how to prevent it

By Tony Capewell
of Your Cloud Works Ltd

YOUR CLOUD WORKS

CELEBRATING 10 YEARS 2010 - 2020

THE 2020 PROBLEM

Revealed:

The ticking software timebomb that's going to disrupt half of all South Northants businesses in January 2020...

and how to prevent it

By Tony Capewell of Your Cloud Works Ltd

Your business, like most others, relies on Microsoft software every day. It´s the software you use the most - for email, documents, to run your company´s server, and of course to run the PCs themselves.

But there's a problem. And very few businesses know about it.

Microsoft has announced that a load of its much-used software will reach "end of life" in January 2020.

What does that mean? Will it just stop working?

No, it'll carry on working. But it won't be supported by Microsoft. Which means if the software breaks or is compromised, there'll be no-one in America fixing it. It'll stay broken.

As the owner of a popular and trusted Managed Service Provider (MSP) for hundreds of local businesses, I've seen this happen before. End of life software like this becomes a keen target for hackers.

They will find loopholes and ways to use the software to get into your computer, or spread malware. **Because there's no-one to stop them.**

End of life software creates 3 major problems for your business

Problem 1
When it breaks, it'll stay broken

Problem 2
You'll become a keen target for clever hackers

Problem 3
Your business will no longer be GDPR-compliant

(as out-of-date software goes against the regulations).

The answer lies in the three Rs

Luckily, there is an answer.
And I've identified a simple 3 step process for you to protect your business: **Review – Replace - Relax**

Review – Read through the rest of this book. It'll show you the basic symptoms that your business has a problem brewing. If you recognise any of the symptoms, then please contact us and arrange for a full software audit. Better to be 100% aware what software you have what potential problems you're facing.

Replace - Some of the software, such as the Office suite, can be replaced quickly and easily. But much of it takes time... you'd be surprised how long a new server takes to get set up. We support hundreds of businesses, and are now scheduling in work right up to January 2020. Don't leave it till then to take action. This is one of those times where being proactive really will save you serious amounts of stress, time and money.

Relax - When January 2020 rolls round, I'm pretty confident the media will be full of stories about businesses and organisations that have run into major problems. "But we didn't know," they'll cry! But not your business. You'll be able to relax and enjoy business as normal.

My business is built around helping your people

Your Cloud Works Ltd is not like most IT support companies. We focus our attention on people, more than we do on computers.

Experience has told us people want fewer disruptions – they just want to get on with their work – which is why we're shouting about this problem in the area, months before it happens.

During a career that spans over 20 years in different areas of IT and communications, we've never fallen out of love with computers. Technology is in our bones, and as the industry continues to grow and present more possibilities for the way people live and work, we don't have time to get bored.

We really enjoy solving IT business problems and coming up with tailor made solutions that bring real value. For us, good business is about looking after our clients and fully understanding what they need, not bombarding them with jargon and adding unnecessary extras. Our approach is friendly, personal and totally transparent, and from the moment you first make contact we'll make it our mission to look after you. We know that just like you, your business is unique, so we take the time to understand your organisation from the inside out.

IT should empower your business to achieve its full potential, without having to worry about cyber crime. With our proactive, intuitive approach, you'll be able to enjoy all of the amazing things the Cloud has to offer and rest safe in the knowledge that your data is completely secure.

Let me now tell you more about the 2020 problem, and how to know if your business will be affected.

Making a good net profit and getting home before 8pm is hard enough. So why would you want to gamble with how your business operates day to day?

Most of us are happy to take the occasional punt on the weekly Lottery or a flutter on a big sporting event. It seems harmless enough when the most we're likely to lose is a few pounds. But we're usually far, far more reluctant to take a gamble that places our homes or businesses at stake.

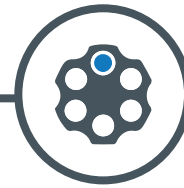
Or so you'd think. It turns out that many UK business owners are doing just that right now. Worse, they're not even aware that they're playing a hellish 'game' of Russian Roulette that places their businesses, savings, and homes, as well as those of their

employees, customers and suppliers at enormous risk.

If you've never seen 'The Deer Hunter' movie or read pulp fiction, then you might never have heard of the suicidal gun game known as 'Russian Roulette'. In this deadly game that is believed to have originated in Russia, a player puts one bullet in an otherwise empty chamber of a revolver, closes the chamber, spins it (like a roulette wheel) then puts the muzzle against his or her forehead and pulls the trigger.

If the revolver holds six chambers, the player has a one in six chance of having a very bad day.

You may not even be aware that you have unwittingly become one of these high-stakes gamblers and part of a 'game' that could cost you, your family, employees, customers and suppliers everything you all hold dear.



The 2020 Game of Russian Roulette

Like most modern games, this one is software-related. That's because 2020 is the year in which Microsoft will stop providing support like security patches, fixes and updates for a range of software and technology.

That's programmes and technology such as:

- Window Server 2008 R2. Mainstream support for Windows Server 2008 R2 ended back in January 2015. The extended support ends on January 14, 2020. According to reports, customers are already experiencing hardware-related issues including a slowdown in performance and even hardware failures. It's not optimised, and problems will continue as 2020 draws closer.
- Small Business Server 2011
- Exchange 2010. After January 2020, Exchange reaches its end of life so if you don't plan to upgrade soon, your email communications could simply shut down.

- Windows 7. If you are using Windows 7, you're far from alone. About 40% of the world's desktops and laptop computers —many of them in corporate and public-sector environments—are still using Windows 7 rather than Windows 10.

- Office 2010

50% of all businesses are affected. Is your business using soon to expire technology?

You might not be aware of what software or technology your company is using. If you're like many business owners or managers, you don't care what programmes you're using so long as they work and doesn't do any harm.

So, to help you identify whether you're using the soon-to-expire software and technology here's a quick guide to help you:

Windows 7

Does your start button look like this?

If it does, you have a big problem in 2020

You can find out which version of Windows you're using by following these instructions:

1. Click the Start button. Enter 'Computer' in the search box, right-click 'Computer', and then click 'Properties'.
2. Look under Windows edition for the version and edition of Windows your PC is running.

Outlook

Does your icon look like this?
If it does, you have a big problem in 2020

Depending on who you talk to, the old version is either brown, orange or gold (or a sort of burnt umber if you want to be fancy).

All you need to know is that if it's not blue, it's probably the 2010 version and will expire in January 2020.

Office 2010

Does your icon look like this?
If it does, you have a big problem in 2020

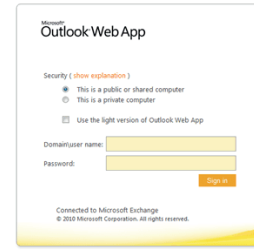
Open your 'Word programme in Office. Create or open a document. To find out which version of Office you're using, click the 'File' tab at the top of the document.

On the File screen, click 'Help' in the list of items on the left.

On the right side of the File screen, you'll see which edition of Office you're running. Under About Microsoft Word (or other Office programme), the version and build number are listed, along with whether the programme is 32-bit or 64-bit. For even more information, click 'Additional Version and Copyright Information'.

You'll see a dialogue box with additional information about the current version of the programme and your Product ID towards the bottom. Click 'OK' to close the dialogue box.

Exchange 2010 WebMail login



Does your login screen look like this?

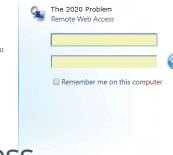
If it does, you have a big problem in 2020

If you use Webmail, and the login box looks like this, it will expire in 2020. You will still be able to login to get your email, but the software will have reached the end of its life, and won't be supported.

Small Business Server

Does your login screen look like this?

If it does, you have a big problem in 2020



Small Business Server 2011 has a remote web access, where you can dial into the server from outside the office.

Does the login screen look like this? If it does, then the software will have reached the end of its life in 2020, and won't be supported. Again, this is a security risk to your business.

Just as food has an expiry date so too does your software and technology

The software listed on the previous pages will all hit its 'End of Life' or end of extended support date at some point in early 2020. After that, the software and technology will be at risk for all kinds of bugs.

Even if programs aren't overrun with bugs, they could still grind to a halt because they'll no longer be compatible with newer software and technology. When that happens, you won't be able to call on the technical assistance of Microsoft support staff for help (and neither will any technical partner or IT support company you use).

That will mean your business' day to day operations could be seriously hampered. Think about it: slow performance, no emails, no orders, lost data, lost orders, lost records and that's just the start.

The bugs are a serious threat. From mid-January 2020, for example, your company will be on its own if you're using Windows 7, on any machine.

Microsoft Support says, "You can continue to use Windows 7, but after support has ended, your PC will become more vulnerable to security risks and viruses. Windows will continue to start and run, but you will no longer receive software updates, including security updates, from Microsoft."

In other words, the Microsoft security buffer or drawbridge that you've enjoyed until then will come crashing down, allowing all kinds of invaders in.

It's a bit like when the Roman army withdrew from Britain in 410AD, leaving its inhabitants to fend for themselves. Before long, invaders such as the Scotti and Picts from the North, the Angles and Saxons from the South and the Jutes from the East poured in.

Of course, the invaders you'll face from early 2020 onwards won't be paddling up rivers in long boats or waving battle axes in your car park!

In reality, you'll probably never see them coming. But the damage they will wreak on your company's reputation and fortunes will be just as deadly as the acts committed by those long-ago marauders.

If you're a gambler, you could carry on using the software. Just

like you could invite all your staff and customers for an end-of-year barbeque and cook up a load of sausages and steak that have passed their use-by-date. You could ignore what the NHS and Food Standards Agency recommend because the meat looks okay to you. But no matter how nice it might taste, you'd still be putting yourself and everyone else at risk of food poisoning.

Of course, your life won't be at risk if you carry on using certain unsupported Microsoft software after its End of Life date. Windows 7 won't blow-up as the clock strikes midnight on January 14, 2020. Robots won't attempt to rip off your head or arms when you sit at your desk. You won't hear a 'Mission Impossible'-style message that warns you "The computers in this building will self-destruct in 10 seconds... 10...nine...eight..."

But you will still be endangering your company. Cybercrime is becoming more prevalent. More than half of British businesses fell victim to some form of cybercrime in 2016, according to research from business IP provider Beaming and Opinium.

That study found:

- 2.9 million UK firms suffered cybersecurity breaches in 2016 with an estimated cost of £29.1 billion.
- Computer viruses and phishing attacks were the most common corporate cyber threats.
- The risk of cybersecurity breaches increases with business size. The larger the company, the greater the risk of falling prey to cybercrime.


CYBER
CRIME

Chris Abbott, IT Manager for US-based Accellis Technology Group, explains the security implications of continuing to use the Windows 7 Operating System after January 2020. He says the main risk is that there are "significant security implications" that occur when support is withdrawn for an operating system.

"Cybercriminals will have plenty of information about the vulnerabilities that exist in Windows 7," he says in a blog post.

"Cybercriminals can reverse engineer vulnerabilities to find the code that contains a vulnerability. Hackers can develop a workaround that exploits the vulnerability of non-updated machines (as of January 2020 that will be all Windows 7 machines) if they can find the bad code.

"Once a vulnerability is found in one version of Windows, research is conducted to identify if any other versions are affected. Microsoft attempts to combat this by releasing security updates to all affected products at once. Such a practice helps users protect their computers before a hacker can reverse engineer the vulnerability (this only applies if you apply updates promptly!).

"On January 14, 2020, cybercriminals will have a leg up on those machines with Windows 7. Any new security updates for other Windows Operating Systems will be reverse engineered in an attempt to exploit those users who have failed to update to Windows 10. Essentially, those computers with Windows 7 will have a big red target on them starting on January 15th, 2020."

This isn't just scaremongering. Big and small UK organisations have suffered recently from using out of date software (this may make you Wanna Cry)

You may think this is all scaremongering but consider what happened back in May 2017. That's when hackers, using secret cyberweapons stolen from the US National Security Agency (NSA), targeted organisations like the NHS and Santander in Europe and the rest of the world with the malicious WannaCry ransomware.

The hackers used a security loophole in Windows operating systems to encrypt data on infected computers. That prevented

organisations like the NHS from accessing their data. The hackers used a tool known as 'EternalBlue' to speed up the spread of the 'WannaCry' ransomware across 150 countries. Affected organisations were issued with a ransom demand to regain access to their data.

The ransomware attack hit more than a third of NHS Trusts.

NHS Trusts were compromised because they were still using an outdated Windows system and they hadn't followed cybersecurity recommendations, according to a National Audit Office report.

It found those NHS Trusts had not acted on critical alerts from NHS Digital and a warning from the Department of Health and the Cabinet Office in 2014 to patch or migrate away from vulnerable older software like Windows XP.

A former chairman of NHS Digital, Kingsley Manning told BBC Radio 4's 'Today' programme that a failure to upgrade old computer systems at a local level within the NHS had contributed to the rapid spread of the malware.

"The problem with cybersecurity for the NHS is [that] it has a particular vulnerability... It's very interconnected, so if you get an attack in one place, it tends to spread."

You can see from this example how vital it is to upgrade software and technology to ensure what your organisation

uses is kept secure and working efficiently.

If you continue to use unsupported Microsoft software and technology after their 'End of Life' dates, you will be playing a deadly game of Russian roulette with your company's future. It will only take one Trojan horse, one hack or one worm to breach your data and your company may be done. At the very least, your company's reputation will be damaged. At the worst, your company will be penalised under the GDPR (General Data Protection Regulation) that became law on May 25, 2018.

GDPR implications for data breaches

As you're undoubtedly aware, with GDPR every company that holds information about its employees, customers and suppliers is legally obliged to protect that data.

Organisations are also obliged to adopt data privacy by design (DPBD). This means companies have a general obligation to take technical and organisational measures to show they have considered and integrated data protection into all processing

activities from the outset.

Now, with the GDPR in force, every organisation in the UK must report serious personal data breaches like the one that hit the credit agency Equifax in 2017. That breach affected 143 million customers in the US and nearly 700,000 customers in the UK.

The company later revealed that the passwords and partial credit card details of 15,000 UK customers had been compromised in the cyber attack. It's thought that a further 14 million UK records were stolen in the attack, but only names and dates of birth were affected.

Serious data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours of discovering them. A failure to do so may result in massive fines for the company responsible.

The ICO, the independent body responsible for enforcing the GDPR in the UK, has the power to fine organisations a whopping €20,000,000 or 4% annual turnover depending which is higher.

The management of data breaches is one of the most critical aspects of the GDPR. It's why your organisation must ensure the security of the personal data you hold on employees, customers and suppliers is adequate. The more sensitive the information you hold, the tighter the security needs to be.

If you fail to comply, you'll not only damage your company's reputation but also make it more likely you'll be hit with sanctions or fines from the ICO.

That's why using unprotected software and technology is so high-risk. It's like leaving the keys to your office tucked under the front doormat. Or sharing your company bank details on Facebook. It's only a matter of time until someone somewhere seizes the opportunity to take it all off your hands.

Why you must act now - and not leave it till 2020...

As shocking as all this is, you're among the lucky ones because you're forewarned. Many other business owners and managers are completely unaware of the risks their companies face.

For example, a survey conducted by Enterprise content delivery platform Kollective, about the End of Life deadline for Windows 7 revealed that out of 260 businesses decision makers in the UK and US, two-thirds of businesses hadn't developed a strategy to migrate to Windows 10, while a fifth of those questioned didn't even know Microsoft was withdrawing support.

A quarter of businesses said they'll leave it to the employees to update and migrate their systems to Windows 10, which exposes many businesses to security risks and fragmentation if the process isn't conducted properly.

When it comes to migrating applications, time is of the essence. "It took many businesses upwards of three years to transition from Windows XP to Windows 7," Jon O'Connor, solution architect at Kollective says. "Although Microsoft has since streamlined the process, we are expecting similar migration timelines for Windows 10."

It can take at least a month for businesses to migrate to a newer computing platform, he says.

However, some businesses may experience network issues when they try to upgrade machines to Windows 10.

"For large enterprises, the key will be ensuring that the update can be rolled out automatically and at scale," O'Connor adds.

"Unfortunately, our research suggests that many businesses simply don't have the network infrastructure needed to achieve this simultaneous update, as such many will spend months—or even years—migrating their systems entirely. If the January 2020 deadline is missed, this will pose a major security threat for the world's businesses."

The real cost of IT problems

IT problems cost UK private sector companies a fortune every year just in terms of lost productivity. Employees in the UK's private sector waste a whole working day every month due to IT issues, at an annual cost of £35 billion to the UK economy, according to research by IT provider Managed 24/7 and YouGov.

It found that an average of 5.59% of an employee's productive time is wasted on IT problems. That equates to 27 minutes every day, 2.5 hours every week, or a whole day every month.

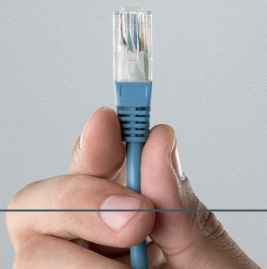
If you continue to use software and technology after their End of Life dates, you're likely to find that they are incompatible

with other software and technology, and so cause performance issues. Some applications, such as the latest version of Sage Line 50 for example, won't install on these older versions, while others will be sluggish at best.

It's why upgrading now makes good sense. Streamlined systems mean greater productivity, so with no disruption to business you'll be able to keep staff, customers and your accounts team happy.

Upgrading is good for business

There's been a lot of talk about Digital Transformation, and around 88% of UK businesses have now adopted cloud computing in some form, according to the Cloud Industry Forum. To be brutally honest, those who don't transition to cloud computing, or using it in a hybrid solution, are going to be left behind.



Taking the leap to cloud computing offers a host of benefits:

- Removal of a single point of failure – it's no longer the case that if one thing goes wrong, everything else does too
- Simplified systems – applications all work more effectively together, with less need for siloes and better collaboration throughout entire organisations
- Instant access to your files from any device, at any time
- Potential to reduce staff costs due to increased productivity, which leads to:
- Increased profits
- Reduced capital costs
- No more snow days – staff can communicate and work on files no matter where they are
- Flexibility – services can be customised and scaled up or down according to need
- Strategic value – updated systems give businesses a competitive advantage

Upgrading your software is a necessity if you want your business to stay operational.

That said, any upgrade is going to take research and a lot of thought. It's not something that you should do without expert help because IT plays such an integral role in business.

Yes, you need to upgrade, and you need to do it soon, but the choices you make will depend on how your specific organisation works.

That's why you need to talk to a trusted provider of IT services before you take the plunge. A good one will be able to provide you with honest, impartial advice based on what works for you rather than trying to flog you loads of stuff you don't need.

You need someone who knows how to keep your data safe and your systems running like clockwork. Someone like us.

If you want to avoid hardware and software performance issues (and all the costs they entail), compliance issues, and security threats, you need to take action now.

Remember, you don't want your day-to-day operations to slow down or even grind to a halt. Equally importantly, you don't want to risk being non-GDPR compliant or to lay your organisation open to cybercriminals.

So the sooner you take action, the better for your organisation.

Book your full software audit now

Migrating to updated software takes time and can be complicated, but the good news is we can take care of it all for you. We will assess your situation and advise you on what steps need to be taken.

Don't make the mistake so many thousands of companies made in the lead-up to the GDPR becoming law of leaving everything to the last minute. Just one month before the deadline, a massive 80% of UK businesses were far from being ready and fell woefully short of their new data protection responsibilities. They went into panic mode and then faced a mountain of paperwork and regulations to work through. Most struggled to keep up.

Leaving things until the eleventh hour is never a good idea in business. It causes stress, disruption and loss – especially when computers are involved. Delaying is a high-risk strategy, one that will cost your company dearly.

If you want to avoid a situation like this, act now. Kick the migration process off by booking a quick no-obligation telephone call now to discuss your needs.

Telephone: 01908 410261
Email: business@yourcloudworks.com
Website: www.yourcloudworks.com

THE 2020 PROBLEM

Revealed: The ticking software timebomb that's going to disrupt half of all South Northants businesses in January 2020...
AND HOW TO PREVENT IT

Your business, like most others, relies on Microsoft software every day. It's the software you use the most – for email, documents, to run your company's server, and of course to run the PCs themselves.

But there's a problem. And very few businesses know about it.

Microsoft has announced that a load of its much-used software will reach "end of life" in January 2020.

What does that mean? Will it just stop working? Can you ignore this and deal with it in January 2020 (spoilers... that's the worse thing you can do).

All your questions and more are answered inside this non-techy, fascinating guide to business software, written by local technology expert Tony Capewell.

Tony Capewell is a father of one with a beautiful fiance and a passion for ski-ing and snowboarding. He's also a keen DIYer who started building furniture a few years ago and has recently built an entirely new kitchen for the family home, including cabinets and dining table, as well as built-in wardrobes. When he's not at work or on a ski slope he's usually to be found in his shed, which he built himself.


Office Dog - Tigger