itguy

Friendly. Efficient. Sorted.

10 POINT CHECKLIST TO SAFEGUARD YOUR COMPANY'S IT

Information Technology (IT) is the beating heart of your organisation. When it stops working properly, your whole business can grind to a halt, costing you dearly in time and money. Add to that the new and existing laws that say you must take responsibility for your company's IT, and it soon becomes even more complicated.

Don't panic. You can keep your company's IT safe in just 10 simple steps. If you follow our 10 point plan and always remember that prevention is better than cure, you can't go far wrong.

WORK BACKWARDS FROM THE DISASTER

If you've ever written risk assessments before you'll know that it makes sense to start with the worst-case scenario and work backwards. So, when thinking about what you need to do to avert disaster, ask yourself a few questions first:

- If a fire hit your office and all your computers were destroyed would your data be safe?
- What would happen if a ransomware virus hit your accounts computer?
- Do you leave your backup device plugged into your PC?
- How would your business be affected if you had a burglary?
- Are the computers and internet in your organisation becoming slow and sluggish? (It's a widespread problem, especially as businesses grow).

Downtime is costly, frustrating and wastes valuable time that could be much better spent on other important business tasks. If nobody's looking after your IT and doing everything they can to prevent that downtime, it's far more likely that a disaster will strike.

It's important that you understand the applications your staff are using and that they're totally safe. Anti-virus protection is the bare minimum you need to stay safe online, so make sure it's up to date.

ITGUY has supported a wide variety of organisations for over 10 years. Most issues that arise are due to inadequate backup systems, poor data security and lack of investment in IT overall.

This guide will take you through the 10 key steps you'll need to take to keep your computer systems and your business safe.

1. BACKUP

Nothing lasts forever and eventually all computer hardware will fail. Just like you need regular maintenance and breakdown cover on your car so you're not stranded in the middle of nowhere, you must think ahead. Backing up your important business data is absolutely essential and if you don't take precautions now, it will become a case of once it's gone, it's gone.

Vital business data must be backed up in multiple safe places. Computers and servers can be replaced but that's not the case with data, and if you can't get it back, will you still be able to function as a business? Probably not.

IT backup is not a procedure to be set and forgot. Repeated and regular checks must be made to ensure that:

- The specific data that must be stored is being properly backed up.
- The backup methods are adequate for the type of data in question and how important/sensitive it is.
- The backups that have been made are restorable (this means that the backup process must be checked and be seen to work).

The "Three-Two-One" backup rule

Three backup copies maximise your chances of being able to retrieve your files. **Two formats** could mean one as a set of files on your computer and another on a USB backup disk. **One offsite copy** means that the data is backed up in the cloud, or simply a backup disk is taken to another location (in case of theft, fire or any disaster).

What data?

When you're working with multiple data streams it's tempting to decide to save time by only backing up the life and death stuff. Don't get caught out by this. The fact is that every tiny bit of data in your organisation is important - all the emails, quotes and documents must be kept safe because they're all important parts of the fabric of your entire organisation. Without a clear audit trail, you could find yourself at risk of customer complaints and serious financial losses - so the sensible thing to do is identify everything that is important and back up all of it.

How to back up?

There are many ways (external drive, flash drive, cloud storage, etc.) and methods (full, incremental, etc.) you can back up data. What's important is that whatever you choose allows you to retrieve any lost information quickly and easily and keeps you totally compliant with any business continuity requirements.

Rule of thumb: the more important the data, the more time and process is required to ensure it has been saved. Large financial institutions will spend much larger sums of money and time on ensuring there is no data loss than say a freelance copywriter, so understand what your business needs to function effectively and guard it with your life.

Test your restore procedure

Some types of data, like text-based documents and image files, can be opened from a backup source and a simple visual check will suffice. However, a database or email store such as Microsoft Exchange Server will be much harder to check.

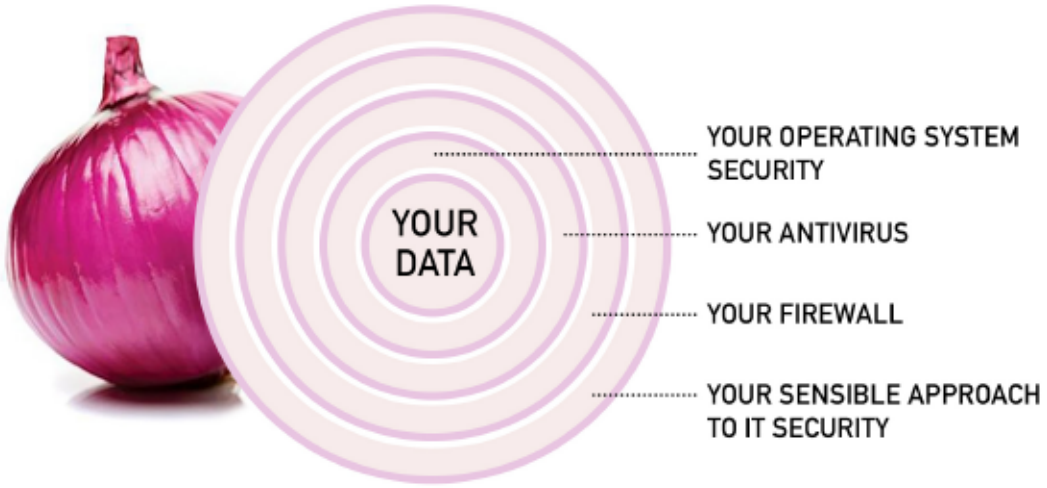
After an agreed backup procedure has been established and you think it's going to work for you, a restore procedure must be defined and tested to prove that data can really be retrieved.

2. PHYSICAL AND REMOTE DATA SECURITY

Data security is an essential aspect of IT for organisations of every size and type. In a world where anyone can buy a DIY hacking kit for as little as £50, bad guys are waiting around every corner to steal your data. Serious hackers can penetrate any network and use that access to steal, delete or encrypt your data and blackmail you - so you need to work hard to prevent an attack.

Internet security

Cybercrime is now the biggest threat to UK businesses and one of the most commonly reported crimes in the country. Cybercriminals are developing more and more sophisticated methods of attack. You must be prepared. Think of **internet security like the layers of an onion**. Each layer is a different "shield", designed to make it hard for the bad guy to do bad things to your precious systems and data.



Operating system security

Windows and Mac operating systems run regular updates to add extra security and patch newly discovered vulnerabilities. These vulnerabilities can allow data theft, password theft and ultimately compromise the entire computer network.

It is vital that all your computers have the latest security updates installed – this is precisely how the NHS got hacked in May 2017; put it off at your peril!

Malware

This is the generic term for all malicious codes (viruses, spyware etc.) that make their way into unprotected computers and steal bank credentials or other valuable information. Many people are fooled into thinking that Apple devices are safe from malware and other viruses - wrong! Macs, whilst natively less vulnerable than Windows PCs, can be infected with viruses just like any other computer so it's important that this myth is busted and all users understand the importance of being fully protected on any device.

A free anti-virus product that requires frequent user input or one that's out-of-date/expired is simply not safe.

It's a high priority that all your computers are fully protected with a quality, up to date anti-virus product at all times.

Ransomware

We've all read the news about the NHS being hit by the malicious Wannacry virus. If it can happen to a large national organisation, then nobody is safe. Ransomware software encrypts all the data on a PC and the network it's connected to (think Dropbox, shared folders of the USB disk plugged into your computer) and demands a ransom to decrypt the files. Even if you pay the ransom – what guarantee is there that you will get it back?

If your organisation does not have adequate anti-virus protection or is not kept up to date with operating system updates, your business is seriously at risk.

Physical access

Would you want your loved ones walking down a dark alley at night with no way to protect themselves from attack? Of course not. Your organisation's data is also vulnerable and keeping it as safe as possible is crucial.

How physically secure is your office? Is your server locked away out of site? Even if your company data is not of value to a would-be thief, computer theft is common and clearly bad for business continuity. Add in embarrassment with the cost of replacement and this becomes downright mad-making.

When any computer is physically vulnerable, data theft is a real possibility. And if you're holding sensitive data (credit card details?) on your computer it MUST be encrypted. Windows and Macs both have built-in encryption software that can stop

unauthorised access, but by default, they are switched off. It's therefore vital that you configure this properly to ensure your sensitive data is being encrypted.

3. NETWORK SECURITY

It's important to protect your data during transmission, so internet security that protects you from intruders is essential.

Firewalls

A firewall only allows certain kinds of data in and out of a network. Certain data types are far more likely to transmit a dubious code that may attempt to access data or applications that can compromise a network. A proper firewall defence is as important as a decent anti-virus application, so don't skimp on it.

Network traffic

We all spend so much time online these days that we're constantly at risk of attack. Even the most innocuous day to day applications like emails, web browsers and social media all carry significant risks. Trusted sources (such as a Facebook "friend") may send you a link to an unknown site or application, which when clicked on could cause a major breach of Internet security.

One way of dealing with such issues and protecting your network is to limit what websites your office internet is permitted to access. Sticking to sites that are for work only can also have added benefits, like more focus and productivity from your team.

4. STAFF AND SOFTWARE USAGE

Can your staff install any program they like on their PC? Do you monitor what programs they run? It's important that you do. This isn't about Big Brother watching your team's every move and checking they're working, it is about making sure they're not running any applications that are unwittingly malicious and can cause network-wide chaos.

Educating your staff is a crucial step towards preventing such issues. The majority of cyber-attacks happen when a well-meaning user clicks on a link by mistake. If people receive appropriate training and know what to look out for, your whole organisation will be in far less danger of an attack.

Acceptable Usage Policy: Many organisations have a written guide (which must be signed by all employees) detailing which software can be run and installed on company computers. This makes it clear to people what applications they are able to run and what sites they can access.

5. INTERNET DOMAINS

Does your company own a domain? An Internet domain is very much a corporate image and intellectual property - it links to the company website, email and possibly other services linked to the company.

If the domain data is wrong or expires, this could mean email delivery could fail or that the website may become unavailable. It also leaves you open to any other company coming along and taking it, preventing you from using your existing website or email addresses.

What would happen if you couldn't send or receive emails? What would your clients think if they got an error message when sending emails to you saying this email address does not exist?

Take responsibility for your company's domain data, login details and expiry date.

6. DOCUMENTATION

IT documentation is vital for the smooth running of an organisation. Access to passwords for computers, servers, routers, internet domains and email addresses can easily be recorded in a central location and this can itself be encrypted if necessary.

Does your current IT company (if you have one) have all your IT passwords? Will they share them with you? Are they keeping them safely?

Documentation about your IT setup, the contact details for service providers and support should also be held centrally to enable a quick response to any IT issues that may arise.

Failure to have such data held centrally can cause major problems in resolving issues and, whilst resetting passwords is possible, recreating pre-existing configurations costs time and money.

7. SOFTWARE LICENSING

Is all the software installed on your work devices legal? The Federation Against Software Theft (FAST - www.fastiis.org) will prosecute or fine where it feels there has been software piracy. Commonly, this happens when disgruntled ex-employees report their old company and business owners often don't realise there's even a problem until it's too late.

8. COMPANY'S LEGAL REQUIREMENTS FOR IT

The 2006 Companies Act stipulates specific issues surrounding the duty of care of company directors regarding business continuity. In the event of any disaster, a company must be able to get back on its feet and function again within a reasonable amount of time. All the points made in this checklist are crucial for ensuring you're fully compliant.

The General Directive on Data Protection (GDPR), which will replace the UK Data Protection Act 1998, comes into force in May 2018 and all UK businesses will be expected to adhere to it regardless of Brexit. The directive has very specific requirements regarding the personal data of any EU citizen, which even covers something as simple as an email address. The substantial change that all businesses must grasp is that they themselves are responsible for the data held about other EU citizens, **no matter where that data resides**.

All data held must be stored safely:

- It must be encrypted.
- It must be backed up adequately.
- In the case of any data breach, your company has 72 hours to report the breach to the relevant supervisory authority.
- Fines are onerous if the criteria are not satisfied (up to 4% of turnover).

For more information read this summary:
http://www.dataiq.co.uk/blog/summary-eu-general-data-protection-regulation

9. ENERGY EFFICIENCY

Older computers have less efficient power supplies in them. Computers use a lot of energy and those left on all day (and sometimes all night) consume a significant amount of power (and thus cost money!).

Newer power supplies are vastly more efficient and therefore should be considered.

Do you have multiple servers? If so, think about whether they could be relocated to a newer server that supports virtualisation to help you become more energy efficient. New IT technology now allows for just one single machine to house several types of operating system, which can all run at once and can be moved from one physical location to another as required. This is another way to reduce energy costs and do your bit for the environment.

10. MACHINE PERFORMANCE

Are your computers running slowly? Underperforming computers are annoying and can slow productivity considerably. Sometimes a new machine may be needed, but not always. By reducing the amount of unnecessary software running on a computer and scheduling in regular services, you can greatly improve your users' experiences and save valuable time and money. To put things into perspective, if your staff waste just five minutes a day waiting for their computers to start up or open programs, that equates to more than three lost days of work per year per person. You could buy them a new fast computer and save money!

YOUR 10 POINT CHECKLIST

Now that you have read through our 10 points, here is the checklist to safeguard your business:

- [ ] 1. BACKUP
- [ ] 2. PHYSICAL AND REMOTE DATA SECURITY
- [ ] 3. NETWORK SECURITY
- [ ] 4. STAFF AND SOFTWARE USAGE
- [ ] 5. INTERNET DOMAINS
- [ ] 6. DOCUMENTATION
- [ ] 7. SOFTWARE LICENSING
- [ ] 8. COMPANY'S LEGAL REQUIREMENTS FOR IT
- [ ] 9. ENERGY EFFICIENCY
- [ ] 10. MACHINE PERFORMANCE

WANT TO KNOW MORE?

ITGUY offers a free consultation at your office to go over this checklist in detail. Once agreed, we can support your organisation to implement any remedial work required.

We can either implement the work on your behalf or work with your admin team to go through all the individual points and make sure the IT in your business is fit, safe, resilient and fully compliant.

Contact us today on 0207 241 2255

itguy
Friendly. Efficient. Sorted.

www.itguy.com

Follow us:

Contact us:
020 7241 2255
info@itguy.com

ITGUY London Limited is a registered company in England and Wales. Registered Number 09390513.
Registered Office: Unit B10, 3 Bradbury Street, London N16 8JN