



# Business IT security for non-techies

*Your data is your business. Lose it or see it stolen and your business will suffer. This is the hard truth of the internet age. This means we're all in the business of IT security now. Every business owner or manager needs to understand enough about IT security to make good decisions and ask the right questions.*

Information technology has fulfilled its promise to revolutionise our lives. It has given us the PC, the mobile phone, databases, the internet, word processing, spreadsheets and social networking. It has, in fact, changed the way we work in less than a generation. The internet, in particular, has created huge opportunities for businesses like yours. Whether your website has millions of visitors or just hundreds, it is your shop front. All your customers are online and so are your competitors, making it an essential part of any business.

Unhappily, not everyone shares your good intentions. Disgruntled employees, online criminals, unscrupulous competitors and even foreign hackers looking for valuable intellectual property can damage your business using the same tools you use to increase your competitiveness. Accidents and negligence can be just as damaging.

A breathless, hysterical response to IT security threats doesn't help anyone. The best approach is to look at IT security as another business problem to be analysed, planned for and reviewed on a regular basis. You will occasionally have IT security incidents – almost every company does – but careful planning will cut the number of problems and reduce the damage if something does go wrong. It will also make sure you protect yourself against real (not imagined) threats and that your security doesn't cost more than it should.

In short, IT security is an important business issue and not just something you can ignore or leave to the IT boffins. This guide will help you evaluate your own security in a business-like way.

## Real-world security

IT security is not much different from physical security. IT security isn't really a technical issue, in the same way that buying a deadbolt isn't a technical issue: it's a business decision. You lock your building at night when everyone goes home, right? In the same way, you need to protect your digital assets from opportunistic attacks and from viruses.

Businesses that deal with cash or valuables, such as jewellery, lock them up in a safe at night. Similarly, it makes sense to protect your most valuable assets with extra protection. For example, you might keep all your email and files on a central server and keep it under lock and key in a computer room.

Your level of security should be in line with what you would lose if you were attacked. How long could you manage without email? What would happen if all your files were deleted? If your laptop was stolen? If you had a virus infection? If a competitor got hold of company secrets?

## What are the risks?

We don't want to try to scare you into action with horror stories of businesses going bust because of security problems. Instead, by looking at each of the risks objectively, we want to give you a better understanding of what you need to do to protect yourself. For example, many people (rightly) worry about computer viruses but do nothing to protect themselves against careless or disgruntled employees.

- **Internet crime:** A 2011 [study](#) released by the Security Minister found that cybercrime in the UK cost £27 billion, with businesses taking the biggest

hit, losing £21 billion. Employees and even company directors regularly fall victim to internet scams, fraud and identity theft.

- **Data theft:** Nearly half of companies' losses were due to direct theft of intellectual property. Insiders are much more likely to steal your data than hackers working from outside. For example, a salesman might misappropriate a customer database to take to a new job.
- **Industrial espionage:** Industrial espionage was the second most harmful crime, costing businesses £7.6 billion in 2010. This is a risk even for smaller companies. For example, hackers might target junior partners in a company's supply chain rather than try to penetrate a larger firm's defences.
- **Malware infections:** Lumension's 2011 [State of the Endpoint](#) report found that malware was the most significant driver behind increasing operating costs. Internet criminals target computers by the million and without proper protection, your company's PCs could be infected.
- **Data loss:** Pricing data loss is somewhat subjective; it depends on both the type and amount of data lost. As a reference point, CIO magazine [reported](#) that data loss cost businesses an average £126 per customer record. The cost to your reputation could be much higher than the direct cost of fixing the initial problem.
- **Network downtime:** The cost of downtime is easy to underestimate, especially if only the direct costs of getting your network back online are considered. The real damage is done by the loss of productivity, which some [experts](#) have estimated at 3.6 percent of annual revenue.

## People, policies and technology

The first step is to develop good habits. This is the human side of IT security. We've all heard stories about hacked email accounts because the owner used a weak password like their pet's name, their own birthday or something equally easy to guess. Unfortunately, these stories are common because bad habits are equally common.

A 2010 [survey](#) found that 60 percent of users don't change their passwords often enough, ten percent admitted to sharing their passwords and eight percent used the same password for every online account. Some even admitted to using "password" as a

## Ten questions for your IT consultant

It's important to keep communication open between you and the head of your IT department, but it can be difficult to know where to start the conversation. Use these ten questions, each covering a different facet of IT security, to initiate your IT security assessment. Remember, it's best to keep a no-blame security environment; these questions aren't meant to catch your IT off-guard. The questions should provoke a constructive and, ultimately, reassuring conversation and highlight any areas for improvement.

1. Have you tested our backup?
2. See this computer (point to one at random), how do I know it is virus-free, up-to-date, backed up?
3. What happens when someone leaves the company?
4. What information could someone get if they stole my laptop?
5. How will our website respond to a distributed denial of service attack?
6. Have we tested our firewalls and our encryption to make sure they will withstand attack?
7. Who has access to passwords for critical business functions?
8. How do we ensure that employees use strong passwords?
9. How do we manage employee permissions and restricted access?
10. How do you know our servers are safe from theft and from accidental damage?

password. Cybercriminals do the technical equivalent of walking around trying doorknobs hoping to find an unlocked one. So, remember to choose [strong passwords](#) and train your staff to do the same. It's not just weak passwords. Other simple things like downloading dodgy attachments or letting anti-virus software go out of date can open the door to malware. It's a case of changing your habits, on a personal and company level.

After establishing good habits through training and company policies, the next step is to carry out a risk assessment. This doesn't have to be an exercise in red

tape. Just take some time to think about what is valuable to your business, what you need to continue trading and what might cause problems. As a business manager, you are in the best position to do this because you know the business better than anyone else.

After identifying high-value targets, you will also need to look for less obvious, but often equally damaging, IT security threats. For example, you may have a backup but how often do you test it? You may have anti-virus software but do you do anything to stop employees wasting their time and your bandwidth cyberslacking? This is where technical advice can be valuable. A good consultant (such as Microsoft Small Business Specialist) can suggest tools that will improve your company's productivity, security and ability to trade through an IT problem (called 'continuity' or 'disaster recovery' in the trade).

To put it more succinctly, an IT security is about people, policies and technology. Establish policies that address the vulnerabilities you found in your threat assessment. Acquire the right technology to implement your IT security policies, and assign responsibility for each part of your plan.

## Understand the risks

Keep these facts in mind as you think through your plan, and do your own additional research using the resources at the end of this paper so that your plans are based on solid facts.

According to the Computer Security Institute's (CSI) 2008 Computer Crime and Security Survey, the security breaches that caused the most financial damage were incidents of financial fraud. Make sure you have good policies and procedures in place to prevent corporate fraud and identity theft.

The second most expensive incidents were "botnet" infestations in which internet criminals hijacked computers to conduct illegal activity such as sending spam. Even though the botnets weren't intended to damage these companies, between lost productivity and the cost of getting rid of the bots cost companies an average \$350,000 per incident. Botnets are usually the result of a virus infection, so putting anti-virus software on every machine and keeping it up to date is essential.

The CSI survey states that targeted attacks are on the rise. Twenty-seven percent of respondents said that they had been the victim of a targeted attack, defined as "a malware attack aimed exclusively at the

respondent's organization or at organizations within a small subset of the general business population."

These targeted attacks, the IT equivalent of professional, motivated thieves, demand the latest security software and constant vigilance.

According to the 2010 UK Security Breach Investigations reports that 18 percent of breaches were connected to an external business partner. Along with insider theft and misconduct, business partners are a dangerous blind spot. Controlling access to critical files on a need to know basis is important.

Old threats also need to be reassessed to determine whether or not the strategies you have put into place are working as planned. The CSI's survey also reported that 99 percent of companies claim to have a computer security policy in place, but 49 percent admitted to having had computer viruses infect their system in the same year. A plan is essential but insufficient. You need to implement it properly and keep it current.

### Checklist item #1: Write a plan

If you don't have a security plan, the first step is to get something in writing. It doesn't have to be perfect, and it won't be. Even if you just get a few pages detailing the outlines of your security plan, having explicit priorities and responsibilities will help you move forward. A good plan today is better than a perfect plan tomorrow.

Next consider what targets might be attractive to a thief, hacker or disgruntled employee: trade secrets, HR documents, financial data, strategic objectives, your network servers. Don't forget about hard copies.

Sensitive information that has been printed out can be intercepted just as easily as something posted online. Also, think about what you need to stay in business. Consider the data on your computers, in your files and in your email system. What would happen to the business if it disappeared tomorrow?

Do a threat assessment to look for potential vulnerabilities. Think about where people interact with your company's data and network. Do you have a website? Do your employees work together on the company network? Do you use online banking? They are all avenues of attack.

Write your security policies in direct response to your threat assessment. Policies should govern what behaviours are essential to maintaining a secure work environment, from strong passwords to document disposal. Like all good business plans, your security

## A sample security plan

The first draft of your company's business plan doesn't have to win any awards, it just needs to outline your threats, establish your policies and assign responsibility for taking action. Everyone involved should take note of which policies are working and which need to be refined. You need to review the policy regularly. Large companies with more complex needs will need a more sophisticated plan than this.

**Objective:** To protect the intellectual property and financial data of Logos Ltd, a small design company.

**Team members:** Peter, head of sales; Stephen, design; Theresa, tech support. Peter will have overall responsibility and Theresa will be in charge of all the technical changes.

**Threat Assessment:** Our digital assets include all our emails, our client work files past and present, our financial records, marketing collateral, staff information, project plans, schedules and customer information including contracts and contact details. We face risks from accidental damage (e.g. dropping a notebook), natural disaster (e.g. flooding), employee negligence (e.g. accidental file deletion), employee misconduct (e.g. stealing customer data), crime (e.g. break-ins or stolen laptops) as well as external risks such as malware attacks and industrial espionage by our clients' competitors.

### Policies

- We will switch our email to Microsoft Office 365 so that we are sure that our old email gets swept for viruses, archived properly and kept securely.
- We will move our data to a central file server. We will discourage staff from storing information on their local PCs. We will back this data up online every day. We will store critical customers and business information on SharePoint online (part of Office 365).
- Only staff working on a given project will have access to that project's files. We will restrict access to business information such as the accounts and payroll to people on a need-to-know basis.
- We will set up BitLocker on all company laptops to encrypt the files on them in case they are stolen. We will also security-mark each laptop.
- We will get a security company to check our physical security, locks and alarms once a year.
- We will update our internet use policy with our lawyers and train new staff about it and security procedures. We will do revision training for the whole company once a year before the Friday afternoon round-up meeting.

policy should include regular reviews and measurable goals so that you know if the system you set up is actually working.

With your policies in place, your IT department can help you weigh the costs of various security options. If you don't have in-house IT people, consider getting help from a Microsoft Small Business Specialist.

There should be individual responsibility and accountability. Who is in charge of IT security? If you have an IT department, they will have a role but you need to involve senior managers, HR and employees too. There should be individual responsibility and accountability.

Even if you have already implemented a security plan, review it regularly in light of developing threats and a changing threat profile. Since perfect security is impossible and no budget is unlimited, you will have to make some trade-offs between security, cost and convenience. As you learn more, or as your company changes, re-evaluate those trade-offs.

### Checklist item #2: Check your PCs

- As the main interface between your employees and your corporate network, not to mention the primary tool for many of your employees, your first practical task for is to rid your PCs of security vulnerabilities as best you can. Here is a quick checklist to apply to each PC:
  - **Update the operating system.** Use Windows Update to update the system software and set it to download automatically the latest patches and updates.
  - **Update applications.** You can use third-party tools like [Secunia](#) to check that other applications and software is up-to-date.
  - **Anti-virus software.** Make sure it has up-to-date anti-virus protection. For small businesses and personal users, [Microsoft Security Essentials](#) is a good choice. Make sure your anti-virus software is updated automatically with the latest virus 'signatures'. Don't let staff switch it off. Using multiple antivirus programs might seem like a good idea, but in practice you won't be much safer and running every file through multiple scans can create a noticeable delay and loss of productivity.
  - **Double-check.** You can check if your Windows computer is up to date in the Security Center in Windows XP SP2 and Windows Vista and in

the Action Center in Windows 7.

- **Install a modern browser**, such as [Windows Internet Explorer 9](#). This will reduce your vulnerability to fraud and malware.
- **Enforce policies**. Consider restricting people's ability to install software, run internet scripts, and use USB or other removable media. Your IT partner can help you control these settings using group policies.
- **User account control**. In case one of your computers does get a virus despite your precautions, enable [User Account Control](#) (in Windows Vista and Windows 7) to mitigate the damage. UAC limits applications to standard user privileges. In other words, viruses aren't given permission to make serious changes to the operating system. That doesn't mean they are completely neutralised, but the scope of their potential damage is decreased. In Windows XP, you set up restricted accounts for users and only use an administrator account for, well, administration.
- **Enforce password policies**. Make sure that users have to choose a strong password and change it regularly. Set each computer so that it requires a user password if it hasn't been used for a while.
- **Password discipline**. You can prevent unauthorised access by requiring passwords, but make sure that employees get in the habit of signing out and securing their passwords. Using last names or taping passwords to the office door defeats the whole purpose. Also, turn off guest accounts. If you want to give someone access to your system you can create a new account; no one without an account should have access.
- **Use a firewall**. Windows XP Service Pack 2 and later versions of Windows have a built-in firewall. Make sure it is switched on (check in the Security Center or Action Center). Buy and install a desktop firewall on older versions of Windows. Turning on your computer or network firewall is almost the literal equivalent of locking your door. As you work online, your computer is trading information with a large number of other computers. Your firewall prevents hackers from pretending to be part of your usual traffic, entering your system and

having a look around.

While you are deciding on which best implement your new security policies, consider investing in a security management suite like Windows Intune that provides an intuitive graphical dashboard that makes most security-related tasks straightforward.

Finally, you need to address the physical security of your system both from attack and from accidents. Marking company computers with irremovable stencils prevents employees or visitors from trying to pass off your equipment as their own and acts as a deterrent against theft. Secure servers to prevent unauthorised access, and they should be kept off the ground in case of flooding or leaks.

### Checklist item #3: Backup

Moore's Law, which posited the exponential increase in computing power, is often written about in tech articles. But there has been an equally dramatic drop in the [cost of storage](#). Even for large corporations, storage space is becoming a minor expense, and so there is no excuse for not backing up your data. The bigger problem is deciding which type of storage you want to use. Flash memory is convenient, but it isn't reliable so you probably shouldn't use it to back up your system.

Storing a backup file on your server is one option, but if the entire server dies, then having multiple copies on the same machine doesn't really help you.

You can create a hard copy of your data on tapes or CDs. The data is stored more or less permanently, which is good if you need to retrieve your data but bad if the data is confidential, since the hard copy is one more version that must be guarded.

[Cloud computing services](#) offer security through redundancy. Your files are stored in multiple locations across the cloud, which is a specific type of network architecture, so that if any one location crashes you are guaranteed to have multiple copies in other places. Most likely, you will use multiple backup solutions in tandem. For backing up routine tasks, it may be enough to use [Microsoft Backup and Restore](#). Regularly backing up the system on local servers and storing particularly important files in multiple locations. When backing up your work, the devil is in the details. Setup a regular schedule for creating backups and stick to it religiously.

It is also good practice to test-restore some files from your back on a regular basis and to store backups

offsite in case of a fire or other catastrophe.

#### **Checklist item #4: Staff policies and training**

If you have staff, it can be difficult to keep everyone on the same page in regards to IT security. Working with employees has to start with education; you can't hold people accountable if you haven't explained what is expected of them. Incorporate computer security into your new employee orientation. Many new employees will believe that they know what is necessary to be secure, but it is important to address the topic rigorously so that there aren't any knowledge gaps.

Standard internet behaviour should be taught: don't open attachments, don't divulge personal or corporate information to unknown parties online and don't give programs access to your computer. One ironic attack claims that a virus has been detected and offers to scan the computer for further infections; of course, accepting the scan allows the site to install viruses on your machine. You may also want to specify guidelines and limits on personal and acceptable internet use. Employees should be given explicit rules when choosing their passwords. Requiring both uppercase and lowercase letters, letters and numbers, and

## **Get help if you need it**

### *How to choose an IT partner and what they can do for you.*

Information should be empowering, but sometimes a glut of information can have the opposite effect. When it all seems like all bad news, as is so often the case with cyber security, it can become downright disheartening. You need someone who can provide a solution that you can rely on without blowing your budget.

If you are a small company without a dedicated tech department, and no one feels comfortable taking responsibility for your company's IT security, it may be time to bring in outside help. As a long-time supporter of small businesses, Microsoft has developed a network of resources and Microsoft Partners, all accessible at our Small Business Centre. The [Small Business Centre](#) has a wealth of information about Microsoft's products and IT services that are designed to help your business tackle IT challenges. Just as importantly, it provides information about Microsoft's Small Business Specialists, the team that Microsoft trusts to discuss Microsoft business solutions with start-ups and small-to-medium businesses.

Our training and certification programme ensures that the Small Business Specialist you work with has sufficient knowledge and experience to deal with issues that are specific to small businesses like yours. Because our specialists regularly work with small businesses, they are used to working within the constraints that you currently have and can help your IT solutions grow with you.

Microsoft's Pinpoint application lets you search for a Small Business Specialist by postcode or by specialty. Once you have selected a Specialist he or she will come to your business and guide you through the entire process.

The specialist will work with you to assess your needs and provide you with options that best match your business. Our specialists' in-depth familiarity with Microsoft products means that you will get the best combination of products and services for your venture. If you are specifically concerned about IT security, Small Business Specialists can work with your team to conduct a threat assessment and then draft security policies that are in line with your employees' skill set, your company's budget and your corporate culture. Service doesn't end just because you have made a purchase. Small Business Specialists stay in touch to monitor your system, provide corporate training and troubleshoot problems as they arise.

When it's time to upgrade your system, working with Microsoft's Small Business Specialists provide a continuity of service that is normally only possible with an in-house IT department. You won't have to waste time bringing a new consultant up to speed. Instead, your Specialist will help you decide the best way to move forward combining industry expertise with first-hand knowledge of your specific firm.

prohibiting dictionary words are good rules to start with. Passwords shouldn't be shared between co-workers. If a file needs to be accessed by more than one employee than it should be stored in a location where all of those employees can get to it using their own log in names.

If something does go wrong you want to know about it as soon as possible. Create a no-blame security culture so that you learn from mistakes rather than punish them. Even when an employee's mistake costs the company money, if that mistake is covered up and allowed to fester it will compound the damage many times over.

Your training also needs to address social engineering attacks with your employees. Social engineering attacks are essentially con jobs. They persuade people to take actions that circumvent your security system, either by revealing confidential information, providing insecure access or revealing their password. As technical security improves, social engineering becomes more likely and more important to defend against.

While you want to trust your people, compartmentalising data on your network limits the amount of harm that any one employee can cause should he or she decide to hurt the company. Your system administrator can give employees permission to access data on a need-to-know basis and then restrict access again once the need has passed.

Employees who have access privileges also need to respect the divide between secured and unsecured sections of the network. Accidentally saving a restricted file in a public workspace opens it up to all eyes and is a serious breach of security.

When someone leaves the company, whether on good terms or bad, make sure that you delete their access privileges immediately.

#### **Checklist item #5: Protect remote workers**

Working from home from creates its own unique security challenges. First, you have to make sure that your home PC is just as secure as your company workstation. Even assuming that is the case, you put your data at risk every time you move it from one location to another. Even an impenetrable system can be compromised if you store information on your smart phone and the phone is stolen.

Situational awareness goes a long way in these cases.

You shouldn't leave anything as expensive as a laptop lying around, and if there are sensitive files stored on it you should be even more vigilant. Laptop locks and secure briefcases help keep your laptop safe.

Switch on the [BIOS](#) password on your laptop and the SIM password on your smartphone (process varies depending on your model of PC or phone but is normally very straightforward) so that thieves can't turn on your computer and see what you have stored. Again, make sure that your passwords are strong (a mixture of letters and numbers, no dictionary words, etc.) and don't let anyone else know what your passwords are. If you are working in public, look around before typing your password to see if someone is trying to look over your shoulder.

Passwords won't prevent the most sophisticated thieves, who may simply try to analyse your hard drive. Fortunately, data encryption can prevent unauthorised access even if someone has physical access to your laptop, but only if the encryption is strong enough. On the other hand, strong encryption makes it less convenient to look at your own files. Certain versions of Windows include built-in drive encryption services called [BitLocker](#) that will protect critical data on a laptop.

#### **Checklist item #6: Encrypt wireless networks**

Wi-Fi, or wireless free internet, is great for casual surfing at a coffee shop, but it has dangers. In the office, you should use your Wi-Fi router's security settings to encrypt and password-protect your connections. This will stop people stealing your bandwidth or, worse, casually hacking into your network. For extra security, you may want to consider using a Virtual Private Network over your Wi-Fi connection. An IT consultant will be able to help you set one up. Make sure that your employees don't set up their own ad-hoc wireless networks by plugging in their own Wi-Fi routers into your network. This can create an insecure back door for intruders.

When your employees are roaming, it's best to rely on trusted, paid-for networks such as [BT OpenZone](#), rather than jumping on any free, unencrypted Wi-Fi connection. Hackers sometimes use free, open connections as bait to break into people's PCs.

#### **Checklist item #7: Make sure you're using cloud computing safely**

More and more businesses are taking advantage of

cloud computing, such as Microsoft Office 365, to improve their business performance, cut costs and access big-business features at a small-company price. If you use a webmail application like Windows Live Hotmail or an online service such as Facebook, you're already using a type of cloud computing. Unlike conventional software, which runs on your own PC, cloud computing (also called software-as-a-service or SaaS) means running applications over the internet. Examples include web-based email, customer relationship management or web conferencing. Typically, you pay for cloud computing applications on a per user, per month basis rather than paying up front for hardware and software. Often this combination of advanced technology and predictable pricing makes it very attractive. However, it raises some new security challenges. First, it is important to select cloud computing services that are secure by design. Second, it is important to use them in a secure way. So, when you're looking at new services, check the following points:

- **Size and reputation.** Will the supplier be around for the long haul? Do they have a good reputation? Has anyone recommended them?
- **Business focus.** Do they have a track record of working in your industry sector or with small and medium-sized businesses? Is this a scaled-up consumer product or a built-for-business service?
- **Support.** What support options do they offer? Do they have a partner network, which can give you local support, if you need it?
- **Future options.** Does the supplier offer options to move to in-house systems or other platforms if your business changes or grows?
- **Familiarity.** How much training will your staff need to use the new service? Is it like anything that they already use?
- **Data protection.** Look for detailed information about how your data is protected, backed up, stored and how you can get it back if you want to move suppliers.
- **Service level agreements.** Look for a strong commitment to meet promises, such as money back guarantees if the provider fails to meet uptime requirements etc.

- **Pricing.** Are you paying per month or per year? What happens if you change the number of users?

## Next steps

For a small business, writing a basic security plan shouldn't take more than a couple of hours. Checking each PC in your business will take 20-30 minutes per computer – at most – and running through the other checklist items in this guide may take perhaps an hour or two. With help from an IT consultant, it could be much easier and quicker. If you can browse the web, edit a document and run an application you already know enough technology to protect your business. Don't let anyone put you off. Compared with the risks, any investment in IT security has a massive return on investment.

## For more information

- [Consumer Security Software Providers](#): Choose from among our list of trusted security software providers to ensure you get a quality product.
- [Get Safe Online](#): Get Safe Online provides you with free, expert advice for all your online questions.
- [Security Newsletter](#): Keep up with what Microsoft is doing to keep you safe with our monthly security newsletter.
- [Security TechCenter](#): A key resource for IT professionals tasked with keeping your system secure.
- [CSI](#): The Computer Security Institute is a leading professional association for IT security professionals.
- [SANS](#): SANS provides IT security training around the world, with a large variety of courses designed to meet your needs.