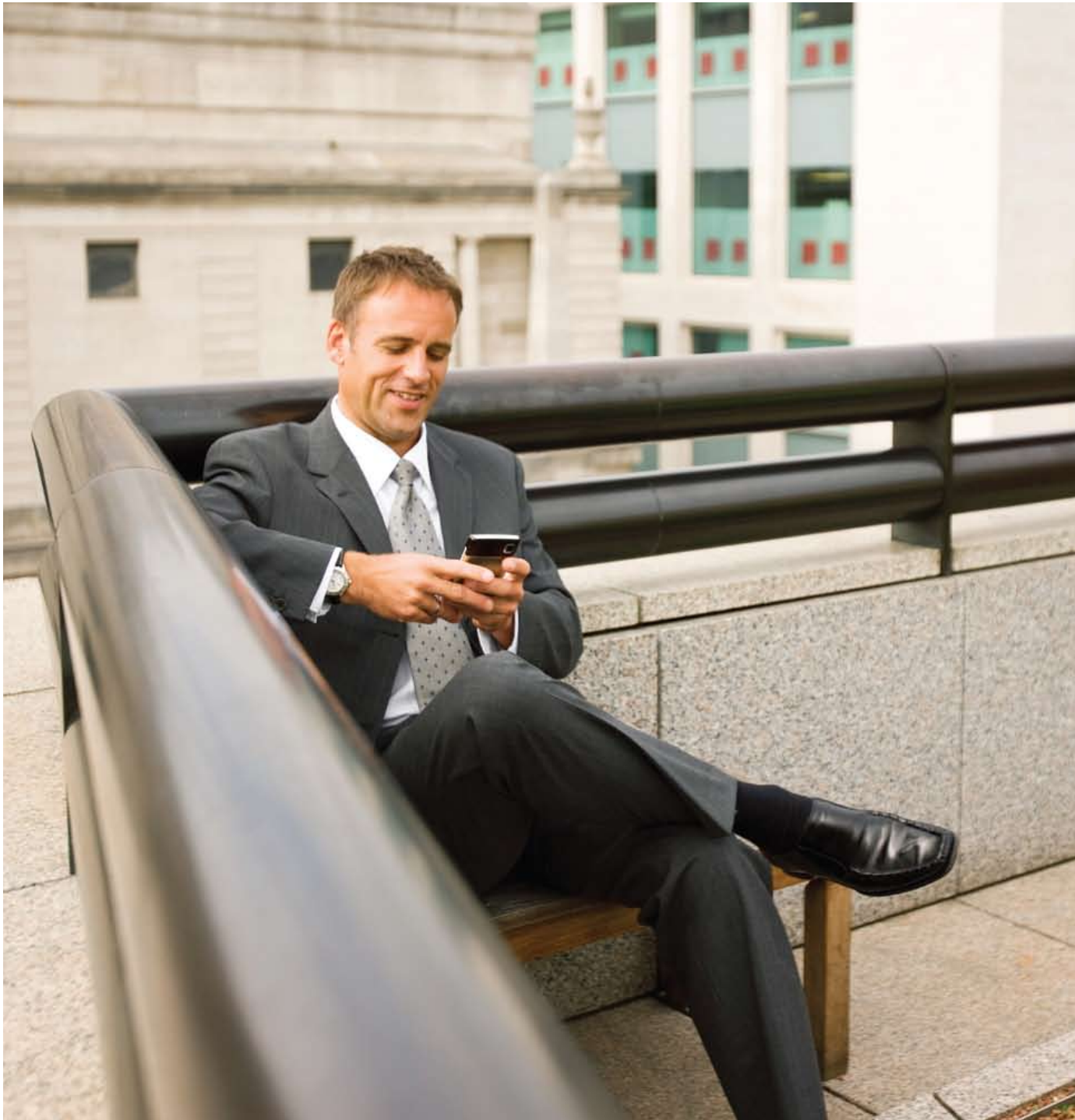




Cisco Problem Solver Guide

Making the most
of IT – ten essential
tips on security for
your business



If you're in business then you're involved in security. The security of your information, your premises, your customer data – it should all be vital to you even if it's not part of your business' main mission. The difficulty is that there is so much information out there, not all of it helpful. The non-expert is constantly asked to make decisions like: I'm told I need a firewall but there's one built into Windows nowadays. So do I need one?

In this guide we'll aim to talk you through a number of the issues you need to look at and we'll make a start in equipping you with the information you're likely to need. We'll also bring out some of the managerial rather than strictly technical issues facing people who are concerned with protecting their business.



Ten Essential Tips

1. Antivirus:

An antivirus package is an excellent thing but not all of them go far enough. You're possibly aware that an AV package works by drawing on a database of information on what's around that's posing a threat at any given time (which is why it's vital to keep your antivirus subscription up to date).

This means, however, that if your AV package doesn't 'know' about a particular virus then it can't protect you. This is why Cisco® advocates not only an AV system but also an Intrusion Prevention System. The difference is twofold; first an IPS will inspect a whole packet of information for anything it doesn't like, second it will also monitor for unusual behaviour from a piece of software on your computer. So in other words it'll not only look for viruses it knows, but if a piece of code starts doing things it probably shouldn't – deleting other files, inspecting your customer database, whatever – it will stop it. Security experts call this a zero day attack – one that exploits a vulnerability or hole in a program or system before it's known by the manufacturer. By watching for unusual behaviour rather than known code we can stop it.

There are different levels of IPS – host-based and network-based. A network-based IPS sits at the entry point to your network. A host-based IPS sits on your laptop rather than your network – so when you're connecting to another network out in the field you're still protected.

2. Firewall:

There is a great deal more to a firewall than ticking a box that says 'I've got a firewall'. Some are built into the operating system, others are on separate machines on the network.

Something that's even more important is what the Firewall is going to look for. Many of them look out for what they perceive to be an attack on the network, which is an essential part of what you need. At Cisco we also offer application-level protection so that if a piece of code looks likely to make an individual program start behaving oddly it'll be detected. It's essential to have a firewall that isn't actually on your computer but on another computer, router or other device that acts as a gateway to your network. If this is the only gateway through which traffic must pass to get to your computer system then clearly putting a guard of some sort into it makes sense. Cisco has numerous levels of security in its offerings.



3. Employees:

Before we go any further into technology it's worth considering just how much of the risk to a business is of a non-technical nature. Here are a few areas in which people have lost data or found it compromised:

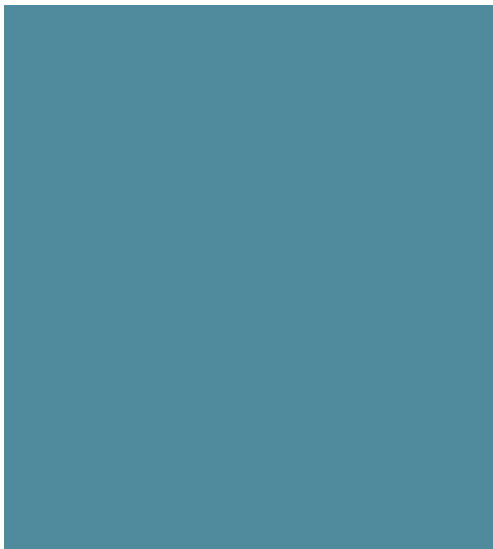
- Instituted a rigorous policy on who may look at what when it's stored electronically – then forgotten to apply this to print-outs, which get left on trains, in hotel lobbies...
- Fail to impress upon people that they need to switch their screens off when vacating their desk – visitors can and will read confidential stuff on monitors (you might want to note at this stage that screen savers use electricity unnecessarily and the days when they protected the screen from anything are long gone).
- Forgive the old chestnut but it still happens – the name of someone's dog/partner/road name is not a secure password and neither is p-a-s-s-w-o-r-d.
- Generally not having a clear policy on what needs to be done to make a network secure, who needs to do it and the sanctions when someone fails to comply. Treat people like intelligent adults and you'll be amazed how quickly they'll want to co-operate.
- Include in that policy that people simply may not download software at will. A lot of it will be harmless but you need to be in control of software licenses and to insulate yourself against the risk of malware.

4. Devices:

The devices that come into and out of a building: If you worked for the Ministry of Defence, so it's been reported, you would have to check your mobile phone or music player in at the door and not get it back until you're leaving. This isn't because people aren't trusted to do their work on time but because phones, cameras and similar devices can contain data. An iPhone 3G (picked purely because it's a best seller) contains 16 gigabytes of space in some cases. They can connect to a USB port on a computer and people can walk away from work having transferred your customer list to whichever medium they happen to be carrying. Alternatively someone could introduce a virus into your system.

You might not want to be as draconian as to ban all forms of personal data carrying devices from your workplace but you can take precautions:

- Computers can be configured not to accept USB devices;
- Intelligent monitoring software like that preloaded with all of Cisco's products will detect unusual activity on your network and report it to you.
- If you have guests logging on to your network then it is imperative that their equipment (if they're using their own laptop) be virus-checked and as secure as your own. Once again, equipment from Cisco will check these computers and other devices as they log on, looking not only for known viruses but for unusual activity.



5. Securing home and remote workers' data:

There is of course no point in securing your network internally if it's going to start leaking information when it's outside your office. This means a number of things. First, ensuring any link into your network from the Internet is done through a proper Virtual Private Network with all the security features that will go with it. Second, make sure the non-technical parts of your employees' activity are subject to the same security it would be if they were in the office. So if they're not allowed to print things out, transfer items onto USB sticks etc. when they're in the office they shouldn't think it's OK to do so at home.

Much of this can be achieved through installing an intelligently-switched network in the office and securing its gateway with the right set of Cisco products.

6. Wireless networks:

A subset of the point about securing home and remote workers' data is to examine the wireless networking set-ups, both internally and externally when they are within your control. Don't rely on the network showing up as 'secured' when a laptop or smartphone finds it; this might mean it has only WEP security which is pretty dated now

and any seasoned hacker can get around it. In the office all networking equipment supplied by Cisco will have security built in as standard and this can be configured by our expert partners. Outside the office your employees may be using their own wireless equipment. It's reasonable to insist it's secured with the following elements:

- If it has a WEP set-up this needs to be upgraded to something with WPA;
- Default passwords that came out of the box with the home equipment should be changed.
- The computer and the network router will have an identifier called the SSID, which can be found in the set-up menu for the router. Change this and also stop the SSID being broadcast, so others won't be able to see your computer if they're looking for networks to hack.
- Switch auto-connecting to WiFi networks off so that the user only connects to networks you trust.
- Assign a static IP address to your devices. The alternative is that your network randomly assigns these addresses, which causes you problems when you want to shut a particular device out.
- Your router will have a firewall, probably – make sure it's switched on as many are shipped with them off by default.
- Turn off the network if it's not going to be used for any length of time.



7. Hacking – how likely is it?

So far we've discussed how to avoid being hacked and how to ward off unwanted intrusions in your computer network. But how probable is it that someone is going to try to get into your system? Many Cisco customers are smaller enterprises and surely, they ask us, nobody's really interested?

In the days of human-only hackers this was probably truer than it is now. The problem is that many 'hacks' and intrusions are automated at the moment. Think of the hacker as the organiser of a lot of thieves, who have to break into unguarded houses to see whether there's anything worth stealing. In this instance the houses are the computers and look identical, so the only way to see whether they're worth turning over is to get in first and have a look.

This is done by automated 'bots' on the Internet, and they do something called 'port scanning' – basically they come to your network's 'door' on the Internet and the first thing they do is to see whether it's locked. Clearly it's in your best interests to make sure it is.

(And don't forget your real doors as well. Cisco offers cameras which can be linked to the Internet so that you can look at what's happening in your office regardless of where you are. Some are activated by motion so you can be alerted anytime someone is in an unauthorised place).

8. Online business:

If most or all of your business happens online then you'll clearly need to take action to protect both your stock information if it's confidential and your customer data. All of the measures we have mentioned so far will contribute to that protection but there are a few more – once again these are as much managerial as technical and include not doing what the Government has been known to do and leave unencrypted CDs lying around to be found on buses, for example! (Remember to encrypt CDs – then nobody can read the data even if they get past the password).



9. So how does it pay off?

Many smaller businesses, particularly at times of financial stress, will be concerned that every investment in technology needs to be seen to be paying for itself. This is slightly tricky in terms of security spend because it's an intangible; you've probably paid to have locks put on your house at some point but at no stage have you calculated how long they've taken to pay back, you just know what you could lose when they get broken.

There is some return on investment from security expenditure that's easy to talk about, though. If you run an e-commerce site and can't reassure customers that their data is safe, for example, you can stand by and watch your business fade away. If you have guests on your premises and they link to your network and walk away with a new computer virus because of your security set-up, you can watch them stop trading with you. And so on.

It's worth stressing, though, that little of the basic equipment costs a fortune. A small office with a handful of employees can get a suitable wireless router with a firewall and full security and have change from £150.

10. Outsourcing Security:

If you still find it intimidating it's worth looking at outsourcing the whole of your security infrastructure. There are many Cisco partners who specialise in making small enterprises more secure than they were before and because they're experts they have economies of scale and skills you won't want to take the time to acquire. Taking all of your data offsite and having a suitably qualified and trustworthy company keep it is an extra layer of security that many smaller enterprises welcome.

As we said at the outset, if you're in business in any capacity then you're in the security business whether you want to be or not. Fortunately the starting points to securing your network don't cost the earth and there is a lot of expertise on hand to help you set it up.

Good luck!

