



The Psychosis Quick Guide to Security (August 2004)

IT security is often thought of as just a technology issue, but that is far from the case. It is, first and foremost, a business issue. If you had all the firewalls and virtual security in the world, and an insider leaked the access details to your network, your protection would be worthless. That's like installing a state-of-the-art alarm at your home, and then leaving the keys and code on the doorstep.

If you think security is not an issue for you, think again. If you think that security is a firewall between your network and internet connection, you are mistaken.

At Psychosis we can help you ensure that your systems and technology processes are secure. Security is an ongoing process and something that is beginning to affect small and medium sized businesses more than ever before.

More than anything, securing your business data is a matter of understanding and working with the people in your business, which is why we have created this short guide to security.

Security policy

The first task is to create a realistic and enforceable security policy. If you don't have one, you need one. This doesn't need to be a long or formal document, and the way you present it depends on the style and character of your company. In a small team where communication is good, you could discuss it at a meeting or individually with each team member. In a larger organisation, it may be better to introduce the policy formally in your office manual or other operational documents.

The best security policy strikes a balance between flexible working practices, security measures, and controlling budgets. It needs to inform staff of all aspects of their security responsibilities, provide guidelines on the use of company resources, and make it clear how sensitive information should be



handled. The policy should leave no doubt about what is acceptable use of your facilities and what is prohibited.

An important benefit of the security policy is that it involves all staff in the process of securing the company's communications. If you get that right, it will significantly cut the risk of security breaches arising from human error, such as the inadvertent disclosure of information to unauthorised parties, or the insecure or improper use of the internet.

An effective policy will cover a range of issues including:

- Using and recording login names and passwords
- Handling sensitive information
- Monitoring access to sensitive data
- Defining, logging and responding to security incidents
- Secure use of computer networks and the internet
- Using the company's email system
- Anti-virus software and facilities
- Content filtering

Threats

The internet is an obvious source of external threats. Potential risks include damaging your data, transmitting sensitive information, or simply shutting down your systems and your business. You can be exposed to all of these while browsing the internet, viewing emails, downloading attachments or using instant messaging. Powerful technologies have been developed to protect you from such threats, but just as your immune system can sometimes take time to build a defence against infection or disease, your protection software may not always be ready to deal with threats when they arise. It is important to understand these limitations. A combination of technology and sensible use is what is needed to keep the threats to your business data to a minimum.

On-line risks are not the only threats to come in from outside. Viruses or Trojans (remote-control applications developed by hackers) can be picked up outside the network on notebooks and bypass the perimeter defence when



they are plugged into the company's network. In the same way, removable media such as CDs or drives may contain malicious code.

Internal system access is often overlooked as a source of risk. If your own passwords are weak or not kept secret, internal users could reach data that only you should have access to. Worse still, if your network has remote access capability, unknown outsiders may get to it too. All systems that need to get into the company's network - including home systems - must be protected from infection and attack. The security of system back-ups, which typically contain all your data at a given time, is also a key factor in avoiding the risk of leaking sensitive information.

Solutions

It's important to recognise that no system can be watertight. Don't think about if - think about when your network will be compromised, or infected by a virus. Minimise the likely extent of the problem and optimise the effectiveness of your response. It is true in technology as elsewhere that prevention is cheaper than cure, but this makes it all the more important to have the tools and resources available to deal with an infection when it occurs.

In recent years most businesses have started using firewalls as part of their security infrastructure, but they are often not used properly. Do you know what the firewall does for you, and whether it is set up correctly to do what you expect? Have you tested it? Installing a firewall without making sure it meets your needs is like hiring a night watchman but not telling him what to do, nor checking whether he's asleep on the job.

Small and medium businesses often have insufficient expertise or staff in-house to provide fully for their security needs. Relying on external providers can result in unnecessary costs, particularly if they have little knowledge of the business or if they are not geared to your scale of operations. The Psychosis approach is to work with you in a way that enables each of us to do what we are good at, by developing a security policy that is rooted in the reality of your company and building your solutions on that.

You could start by asking us to review your existing security. Or, if you prefer,



you can get the process under way by looking at our free and regularly updated White Papers on this topic at www.psychosis.co.uk/security.

Firewalls: Hardware or Software?

Software

Pros

Easy to install and configure

Little IT knowledge required

Change configuration 'on the fly' as you need

Low cost

Cons

It's not advisable to have individual users make security decisions in a network environment

The protection ceases if the software or the PC on which it is loaded fails

Slower and less effective than hardware firewalls at processing large volumes

One installation per PC, and software needs to be managed

Hardware

Pros

One dedicated, centrally managed unit

Only administrator changes rules and policies

Can process large volumes of data

Extras such as VPN connections on many units

Easily monitors all traffic entering the network

Cons

More expensive for systems with very few users



Why would someone hijack my system?

Joyriding

Joyriders take over computer resources, telephone and internet connections so they can use these services without paying for them. Joyriding is not usually destructive, but it can be costly for the victim.

Vandalism

Vandals may be motivated by almost anything: amusement, a taste for anarchy, or a grudge. The intruder does not need to be inside your network to vandalise it. Viruses can be appended to files or emails. A common type of attack, known as Denial of Service, can be launched externally and flood a network device with data or corrupt information so that it cannot fulfil its normal function. This could be used, for example, to shut your network off from access to the internet. Other common acts include damaging systems and files, deleting, corrupting and altering data.

Theft

Theft of data has become a significant business issue now that remote access is a common requirement. Thieves can steal entire databases as well as financial assets, personal information and so forth, and they are increasingly aware of the possibilities.

Extortion

There have been cases where extortionists have planted a destructive programme in a business network and then threatened to activate it unless payment is made.

Which password is more secure?

password
aaa123bbbb
SecureD
Lucy
abcdefg
76543210
Ona3277(sA



Further information

www.psychosis.co.uk
0845 072 3444