Managing the Modem Threat

"...most large companies are [*probably*] more vulnerable through poorly inventoried modem lines than via firewall-protected Internet gateways"
Hacking Exposed: Network Security Secrets and Solutions (2nd edition). McClure, Scambray & Kurtz. Osborne, 2001

"Unauthorised modems are one of the most overlooked security flaws in corporations today. Companies often have modem lines they don't even know are there."
Information Week

"While remote access is not the only route hackers use to attack networks, they often cite it as the easiest route in."
Information Security Breaches Survey 2004 - Remote Access. Department of Trade & Industry.

Hardly a week goes by where the news isn't full of the latest defacement of a website, or accidental disclosure or theft of credit card details or personal information. It's the Internet that attracts media attention when there is a security breach, which is hardly surprising given that that is how most organisations present their public face to the world.

However, as the quotations above reveal, there is a far more pervasive and insidious threat presented by the humble modem. In this paper we'll explain why this is the case and what can be done to both quantify and minimise the risks.

History of Modem Use

Within any medium to large organisation, our experience tells us that it is very rare for modem use **not** to be widespread, for a variety of reasons. Historically, since modems came into mainstream use in the early 1980's, it was the modem that provided data connectivity for and between businesses. The whole point of a modem was to allow a digital connection to be made across an analogue telephone system, often to allow remote support of a company's computer system(s), or else to allow the timely transmission of data between two disconnected sites. Even into the early 1990's modems were generally expensive, and (from personal experience) required some skill to install and configure correctly. For business use, hardware cost is generally less of an issue, where it can be balanced against the savings in support costs, and increased efficiency. As business use of computers increased, so did modem use. Modems started to provide electronic links **between** businesses to provide functions such as EDI and financial transfers (the embryonic business-to-business transactions), as well as fulfilling their traditional support role.

As the pace of electronic change increased, business use of modems also increased. Businesses used more complex computer systems, and automated more tasks. Data became a key asset. Availability of data, and hence computer systems became a business driver. As a consequence, the timely support of a system also became critical. Often the only way of guaranteeing the required level of support from a vendor was by allowing them to have dial-in access to the systems that they were contracted to support. Furthermore, as more and more equipment manufacturers have availed themselves of mainstream computer technology, the inclusion of a modem meant that they could streamline and rationalise their support, to the extent that this is now likely to encompass your telephone systems, fault tolerant disk arrays and key elements of network infrastructure (such as hubs and routers).

In comparison to this long history of modem connectivity, Internet penetration into business processes is a still relatively new phenomenon. For example, in 2004, although 99% of large UK businesses now have a web presence, 25% still do not offer business transactions through their website. Undoubtedly, given both the numbers of computerised systems that use modems, and the reliance on older legacy systems to conduct traditional business-to-business transactions, it is hard to imagine how modem usage within large businesses could not be ubiquitous.

The Risk to Business

So, given that we have been living with widespread modem usage for two decades, what has changed to increase the risk to business? Undoubtedly there have always been dedicated hackers who have exploited unsecured modems. In the past, before Internet connectivity was prevalent, their primary motivation was more to avail themselves of 'free' telephone calls as a means of accessing bulletin boards in foreign countries. Nowadays, there are two factors affecting risk that need to be taken into account. First, modems are far more widely used in far more business-critical systems than ever before. Consequently, there are more potential targets. The second contributing factor in increasing the risk can be attributed the PC revolution, which has increased the size of the threat.

Looking back only 8 years, there have been radical changes in the personal computer market, as the table below illustrates. (All figures taken, sadly, from personal experience.)

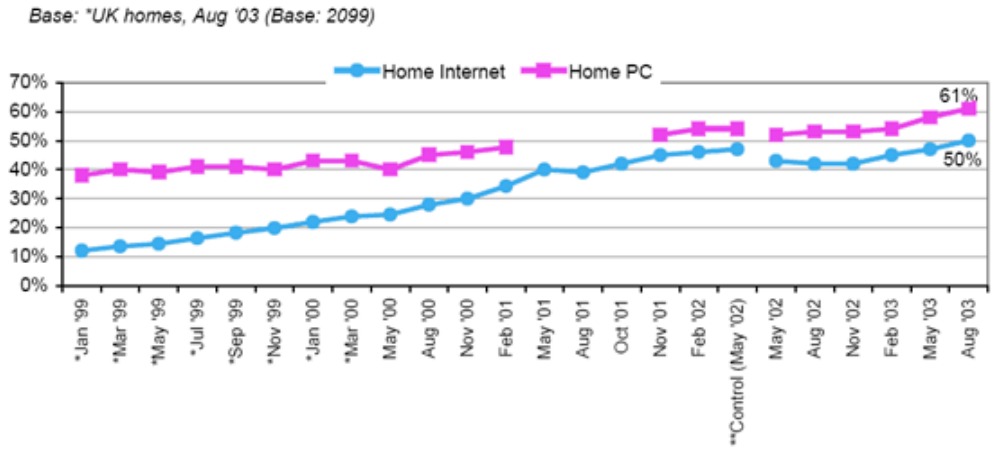
Description	Typical Cost (1996)	Typical Cost (2004)	Reduction
Entry level PC	£1500	£250	83%
Colour notebook	£2000	£500	75%
Memory (per MB)	£12	£0.10	99.2%
Disk (per GB)	£100	£0.36	99.6%
Modem	£120	£6	95%

The impact this has had on business is to make computers as ubiquitous a tool as the telephone. It has also added to the burden of modem proliferation, since modems have increasingly become built-ins rather than add-ons (at least within the notebook market). The very fact that computers are in more widespread usage, both at work and in the home, has also led to the rise of the knowledgeable user: users with both the skill and desire to modify and configure their own machines at work.

At the same time there has been an accelerating use of the Internet by home users. In the time that it took home PC usage to increase from just under 40% of UK households to 50% (Jan 1999 – May 2001), home Internet usage increased from 12% to 40%. Much of this early growth was undoubtedly stimulated by the introduction of free Internet Service Provision, and the reduction in call charges. (See table below as an example)

ISP	Annual Fee	Formed	Sold	User Base at Sale
Demon	£141	1992	May 1998	180,000 (in 6 years)
Freeserve	*Free*	Sept 1998	July 1999	1,500,000 (in 6 months)

Although such a meteoric increase has not been sustained, usage has nevertheless continued to increase at a steady pace. According to the last figures published by the UK telecommunications regulator (Oftel) before its being subsumed by Ofcom, by August 2003 61% of UK homes had a PC, with 50% of UK homes having Internet access. The growth in UK home Internet usage is clearly shown by the graph below (taken from *http://www.ofcom.org.uk/static/archive/oftel/publications/research/2003/q14intres1003.pdf).*



** Note – Figures up to March 2000 are based on GB population and are taken from MORI's Technology Tracker. Figures from May 2000 onwards include Northern Ireland and therefore represent the UK adult population.*

These factors have a number of indirect impacts on business. Primarily it means that more of their employees are computer literate and Internet aware. The result is more demand for Internet access from work, and more skill in configuring hardware and software (based on experience they have gained at home).

Broadband, VPN's and Modems

Technology has moved on in the 3 years since we first produced this paper. Home broadband access has become affordable, and at the time of writing is available to more than 90% of the UK population. This has lead to a growth in broadband use to more than 2 million homes. In parallel, more robust technologies, such as virtual private networks (VPNs) have allowed business to support remote access securely via the Internet, rather than through dial-up.

So, has this spelt an end to the security risks posed from modems? **Certainly not yet!**

Although there has been a surge in home broadband use, the number of users connecting via dial-up is still significant at around 8.75 million (73% of the total), and is even larger than the 8 million connecting via modems in 2001. In part the continued popularity of modem dial-up Internet connectivity has no doubt been helped by the proliferation of cheap fixed rate packages, with broadband still perceived by many home users as simply too expensive to justify the improvement in service. (Bear in mind too that many of those self-same broadband users will have migrated from a modem, that is no doubt lurking in a cupboard waiting to be used elsewhere.)

At the business end of the equation, although VPNs may be gaining some ground, there are several reasons why modem access remains as popular as ever:

- Dial-up via modem is cheap, simple to implement and a proven solution
- Many systems just don't merit the additional investment in a more complex solution
- There is a huge reservoir of legacy systems geared towards remote access via modem. Lots of systems were replaced in the run-up to Y2K, many of which will not yet be due for replacement.

In Summary

So, to summarise, businesses probably **still** have more modem access into and out-of their organisations than ever before:

- more critical systems are supported via modems through dial-in links.
- more employees inside the network perimeter have access to systems with built-in modems (e.g. notebook computers)
- more employees are computer-literate, and through experience gained at home, have the necessary skills to configure modems to access the Internet (…and they may even have one spare that they are itching to use more fruitfully elsewhere)

Even though, in this paper, we are treating modem-related risks separately from Internet risk, the two are, paradoxically, very closely linked. Employees are motivated to access the Internet from work: it's an entertaining diversion, and saves them time (if not money) at home. Similarly, the proliferation of home Internet connectivity has equipped 12 million UK households with the tools to breach your perimeter security through your dial-in connections (at a time when, more than ever, hacking is viewed as a 'cool' activity).

Categorising Modem Access

From the above, we have touched on the fact that there are really two distinct aspects to modem access. **Dial-out access** (where a user *internal* to your premises uses a modem to access an external system) and **dial-in access** (where someone *external* to your premises uses a modem to directly access an internal system). Each poses its own risks, and its own management issues.

Dial-out Access

For most organisations, the risks from dial-out access come primarily from employees subverting the firewall to access blocked content on the Internet. The risks associated with this type of access are twofold:

- Unregulated access to the Internet re-exposes your organisation to precisely the risks that the firewall was designed to keep out. The result is that your systems can be exposed to viruses and trojan horse programs. Equally, an unauthorised connection can be used to download illicit or illegal material (not just pornography, but also copyrighted works) for which you are then legally responsible.
- All kinds of information can leak out about your organisation: user names, company and machine identification, protocols and programs that you use. All of which can be used indirectly as valuable intelligence by a potential hacker. (See http://grc.com.) *[If you have a PC and a software firewall (such as Zone Alarm), it's quite alarming to see the frequency with which a PC connected to the Internet is probed while it is online.]*

Dial-in Access

One of the common misconceptions is that dial-in access doesn't pose a significant threat because of cost:

"*Why would a hacker bother to dial thousands of numbers within my organisation when it would incur hundreds of pounds in telephone costs?*"

The answer is: **because it doesn't**.

Dialling most organisations at night, only a very small percentage of numbers will be answered. Many of the numbers that do answer are precisely the ones that a hacker would be interested in: modems configured for dial-in access.

Dial-in access poses all of the risks of dial-out access, but with some additional twists.

- As we've covered earlier, your business-critical systems are likely to permit remote access, either as a contractual condition of support, or else as the result of an ad-hoc installation by support staff. So, if someone manages to exploit a dial-in modem, there is an increased chance that it will be attached to a business-critical system.
- A modem which has been added unofficially is far less likely to have been configured securely.
- The attack is more likely to be planned rather than opportunistic: someone is deliberating probing one of your systems, rather than a user stumbling across a site with malicious content or being randomly port-scanned.
- It is easy for a hacker to explicitly target your organisation. All they need is a telephone number to start from and then they can dial your numbers sequentially.
- A hacker is more likely to have time to exploit the system.
- An attack is likely to be untraceable. Organisations do not usually monitor incoming calls, and there is little on the attacked system to be of use forensically to allow a determination of where an attack came from.

As a result of all of the above, it would be our view that an attack from a disgruntled employee is far more likely to be through an unsecured dial-in connection than through an Internet connection. (They may have even installed the modem in the first place.)

Managing the Problem

One of the initial stumbling blocks to effectively managing modem access can be the attitude of Management itself. Sadly, these have not changed substantially over the last three years. Some of the common statements we still come across are:

Attitude	Statements	Analysis
Ignorance	*"We already have a firewall"*	• Modems subvert the firewall (and hence jeopardise the considerable investment made in the firewall and content-filtering)
	"We have a digital telephone exchange"	• Devices are available to allow digital ports to be used by analogue devices (e.g. modems) • Ordinary fax machines use analogue ports.
Complacency	*"We know where each modem is"*	• How? • What about embedded modems? • Unlikely for any but the smallest organisations, or those with an existing proactive agenda to manage modems.
	"We have a no-modem policy"	• Is the policy effectively communicated? • How is the policy enforced?
Blind Faith	*"We know we have a problem but we have other priorities"*	• Is this the result of an objective assessment of the *relative* risks against current priorities?
	"We only have one or two…"	• Is this an assumption or based on knowledge? • That's all it takes!

Given these attitudes it is perhaps not surprising that in 2004 only 4% of UK businesses surveyed even check for unauthorised access via modems[1]. Yet there are substantive reasons for securing modem links. Apart from any inherent benefit, you may need to adopt a proactive approach in order to comply with an externally recognised or enforced standard. For example, both ISO/IEC 17999 (BS7799) and the VISA AIS Standards make specific recommendations regarding modem access.

Once you have overcome the hurdles of the perception of lack of risk, it is important to realise the limitations of what can be achieved practically. For almost any business, modem access in some form is essential. There is little point in trying to impose a no modem policy on a supplier if that is the only way that they can achieve a contracted level of service. The key point is to understand the level of modem access that is genuinely required, to remove access where there is no corresponding business justification and to ensure that any required access is managed effectively.

To achieve this goal, we recommend an approach that includes the following steps.

- audit
- assessment
- control
- policy definition
- education

The sequence of the individual steps will very much depend upon an organisation's existing culture, and hence the position from where they start. (The ordering of steps above is

[1] *Information Security Breaches Survey 2004. Department of Trade & Industry*

suitable for an organisation that does not have an existing modem security policy, for example.)

Audit
The purpose of the audit is to create a baseline understanding of the problem.

- Identify where modems are through:
  - Existing telephone lists
  - Visual search
  - Automated approach
- Identify access controls on a per modem basis
- Iterate through the process – several audits may be required to reveal the full picture (to cover daytime and night time usage patterns, for example)

Tools (specifically telephone system scanners, such as our own Xiscan product) can be of real assistance in the audit process, in that they allow repeated scanning of large volumes of telephone numbers. However, whereas they are ideally suited to detecting dial-in access, they cannot accurately reflect the level of dial-out access.

Assessment
Assessment is dependent on the audit results:

- Consider each modem in turn in terms of:
  - Business Area (where are they?)
  - Function/Usage (what are they used for?)
- Build business cases for required modems

Control
Take control of modem access:

- Remove unwanted modems
- Ensure modems are correctly configured
- Ensure adequate security controls are in place
  - Restrict modem access to the specific time window when it is required
  - Use good password security
- Remove identifiable banners from internal systems where possible
- Use callback to block access from arbitrary numbers
- Rather than relying solely on password security, use additional authentication mechanisms (e.g. challenge/response, token-based)
- Consider the suitability of an integrated dial-up solution as a means to focus control

Control is often a difficult step to implement, particularly where it extends to controlling access of third party suppliers. Password security should ideally reside internally, but be aware of the needs of suppliers to provide support within contracted timescales.

Policy Definition
Policy is an important cornerstone. Ideally, the policy should not permit **any** form of unauthorised access, and should aim to reduce the risk presented by modem access. It should:

- Define a strategy **that is suited to the organisation**
- Document:
  - Objectives
  - Acceptable use
  - Implications for violation
- Create an 'acceptable' modem register

Education
Effective communication of policy is one of the most difficult and often overlooked aspects of the process. It should reinforce:

- Acceptable use
- Implications of policy violation

One of the dangers implicit in the ad hoc use of modems is that users are ignorant of the wider implications of such an apparently trivial act. The aim of education is not just to communicate policy but also to raise awareness to the dangers, and thereby get user buy-in. Effective education (backed by policy) is the best tool to address dial-out access. (In this respect, our own Xiscan product is unique in that it can provide automated assistance for education, as well as being used in policing of policy. See **www.xiscan.com** for the technical details.)

Be Prepared for the Size of the Task

Auditing a telephone network is not a trivial task. The telephony infrastructure must be understood, and any potential impact on normal business processes planned for and contained. Once past the planning stage, there are tools that can help with the job. Telephone system scanners, for example, can provide a great deal of assistance in the audit process, and contribute to education and control. However, identifying where modem access exists addresses only one half of the problem. The other half is a management issue: physically finding them and negotiating their removal.

How big the problem turns out to be for your organisation will depend on many factors, not least how seriously the threats posed by modem access have been perceived. In our experience, in organisations where modem usage has been openly permitted in the past (and hence where there is no incentive to hide modems) it is not unusual for 5% of all telephone extensions to be documented as modems. This covers everything from the mainframe computer support down to the catering department! Of these, up to 30% will be configured to allow dial-in access. Put another way: in our experience for every 1000 telephone extensions, 5 - 15 lines may be providing a direct route into your network through a modem configured for dial-in access.

As with all aspects of security, the process must be iterative. Policy must adapt to changes in technology and business practices. Having the procedures and tools in place allows you to keep pace with these developments, and to monitor whether your policy continues to being effectively communicated and adhered to.

Resources

UK Internet statistics:
http://www.ofcom.org.uk/static/archive/oftel/publications/internet/index.htm
http://www.ofcom.org.uk/static/archive/oftel/publications/research/2003/q14intres1003.pdf

Useful sources of Internet statistics:
http://www.clickz.com/stats/
http://www.nua.com

UK population statistics
http://www.statistics.gov.uk/pdfdir/popu0801.pdf

Modem awareness
http://grc.com
http://www.xiscan.com

Security Awareness
http://www.dti.gov.uk/industries/information_security
http://www.visaeu.com/acceptingvisa/datasecurity.html
http://www.visaeu.com/acceptingvisa/pdf/selfassessform.pdf