

The Modem Threat

The Xiscan logo features a large, stylized 'X' composed of two thick, curved lines. The word 'iscan' is written in a bold, lowercase, sans-serif font, positioned to the right of the 'X' and partially overlapping it.

iscan

Copyright 2004 Xiscan® Limited

About Xiscan Limited

Xiscan

- UK based
- Blue chip client base in the UK & Europe
 - Finance, Retail, Utilities, Local Government...
- Specialists in Modem Security
 - Through supply of our own Xiscan telephony audit tool
 - Through provision of managed modem scanning services

Copyright © 2004 Xiscan® Limited

Agenda

Xiscan

- The Problem
- Dial-out Access
- Dial-in Access
- Managing the Risk
- Questions
- Conclusion

Copyright © 2004 Xiscan® Limited

The Problem

Xiscan

- Expert Opinion
- Case Histories
- Company Attitudes
- Widespread Modem Use

Copyright © 2004 Xiscan® Limited

The Problem: Expert Opinion

Xiscan

"...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. McClure, Scambray & Kurtz. Osborne, 1999

"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

Copyright © 2004 Xiscan® Limited

The Problem: Case History 1 – Malicious Attack

Xiscan

- US based Internet Service Provider
- Disgruntled former employee dials in
- Creates bogus accounts
- Signs in later
 - Destroys data
 - Deletes new billing system
 - Takes large clients offline

Copyright © 2004 Xiscan® Limited

Most organisations will have disgruntled employees, unfortunately including those willing to destroy, corrupt or steal information.

The Problem: Case History 2 – Opportunistic Attack

Xiscan

- US Airport
- Teenager uses wardialler to scan telephone numbers
- Caused six hour loss of telephone service to local airport's:
 - Control Tower
 - Fire and Security Department
 - Weather station
- Vital aircraft landing services severely affected

Copyright © 2004 Xiscan® Limited

(A wardialler is a tool used by hackers to automate dialling of large ranges of telephone numbers).

This is a classic example of a violation performed by a person with no prior relationship to, or knowledge of, the organisation that they are attacking.

Free tools are available on the internet – with full instructions on how to use them. Some hackers are simply focussed on breaking in to any system.

The Problem:
Case History 3 – closer to home...

Xiscan

- UK based manufacturing company
- Disgruntled former support employee dials in
- Wipes production server clean
- Company rebuilds server using piecemeal techniques
- Former employee performs same action

Copyright © 2004 Xiscan® Limited

... and closer to home

The Problem: Company Attitudes

Xiscan

- Ignorance
 - “We already have a firewall”
 - “We have a digital telephone exchange”
- Complacency
 - “We physically know where each modem is”
 - “We have a no-modem policy”
 - “We don’t do anything that would make us a target”
- Blind Faith (!?)
 - “We know we have a problem – but we have other priorities...”
 - “We only have one or two...”

Copyright © 2004 Xiscan® Limited

Digital phone systems are not invulnerable.

There is a variety of devices that will plug in and support analogue modems. You may already have ‘analogue features’ installed (to allow fax machines for example).

The Problem: Widespread Modem Use - Internally

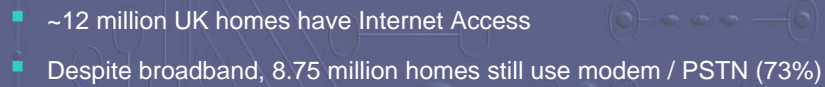
Xiscan

- Legacy business-to-business connectivity
 - EDI - electronic data interchange
 - EFT - electronic funds transfer (e.g BACS)
- Technical support
 - Internal Production support
 - Third party technical support - proliferation of computerisation
- Convenient and cheap (unofficial) route to Internet
 - Actual cost – less than £10
 - Installation easy
- In many cases – usage is not documented

Copyright © 2004 Xiscan® Limited

The use of modems within organisations is far more widespread (and concerning) than most companies appreciate. It can be as high as 5% of extensions documented as having modems attached.

XiScan



11

The Problem: Risk

Xiscan

Internally

- Increased + insecure usage
- Lack of understanding/commitment

Externally

- Increased + knowledgeable usage
- Motivation: hacking is 'cool'



Copyright © 2004 Xiscan® Limited

The Xiscan logo is located in the top right corner of the slide. It features the word "Xiscan" in a stylized, light blue font. The background of the slide is a dark blue circuit board pattern with various electronic components like resistors and capacitors.

... now let's look at the technicalities

- Dial-out access
- Dial-in access

Copyright © 2004 Xiscan® Limited

Dial-out Access

Xiscan

- Definition
- What are the risks?
- Practical demonstration

Copyright © 2004 Xiscan® Limited

Dial-out Access: Definition

Xiscan

...where a user *internal* to your premises uses a modem connected to a computer and your telephone network to connect to an *external* system (typically an Internet Service Provider)

- Internal party *dials out* to an external Internet Service Provider (ISP)
- Direct two way connection now formed

Copyright © 2004 Xiscan® Limited

Dial-out Access: What are the risks?

Xiscan

- Primarily used for Internet Access giving unrestricted access to:
 - Unauthorised software – including trojan horses / viruses
 - Offensive / pornographic (illegal!) / copyrighted materials
 - Gaming servers
- Information Leakage
 - All sorts of configuration information...

Copyright © 2004 Xiscan® Limited

Information Leakage...

As the demonstration will show, the nature and amount of accessible information is alarming...

Machine information

Company information

Data files...

Information Security Breaches Survey (ISBS) 2002 Findings - Web Access

Xiscan

Survey relates to 1000 UK businesses

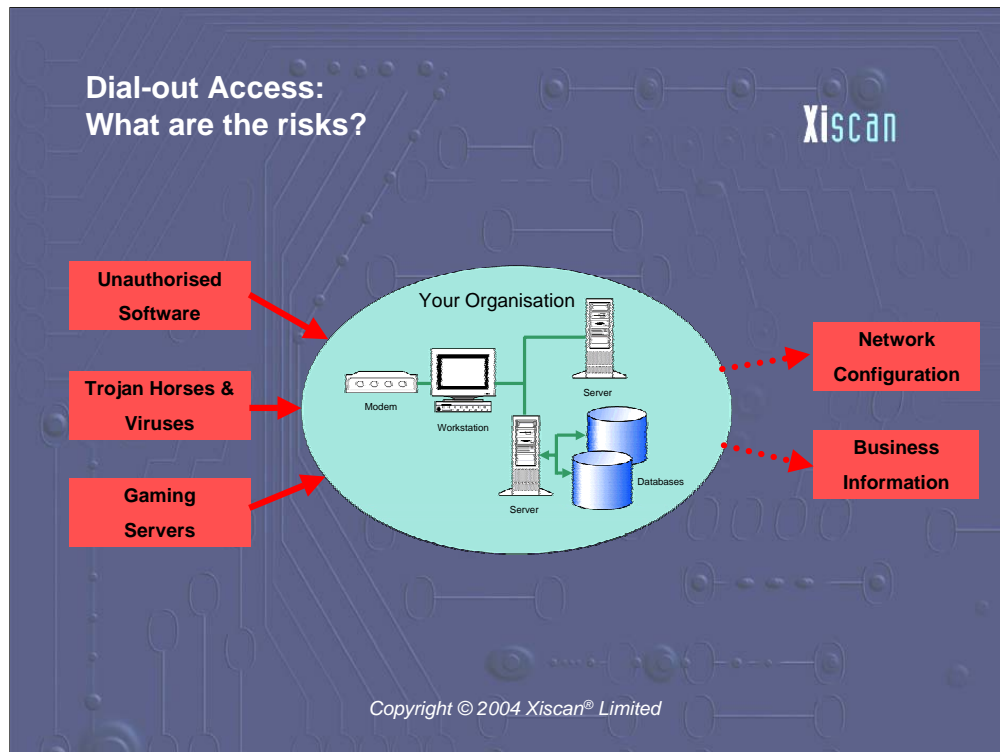
Relevant Findings for Large Businesses (250+ employees):

- 68% restrict web browsing
- 78% log and monitor which web sites staff

With good reason...

- 51% experienced security incidents related to web access
 - 36% experienced virus infection from downloaded files
 - 26% discovered staff accessing inappropriate sites
 - 11% disciplined staff for excessive web surfing

Copyright © 2004 Xiscan® Limited



The frightening aspect of dial-out access is the lack of control...

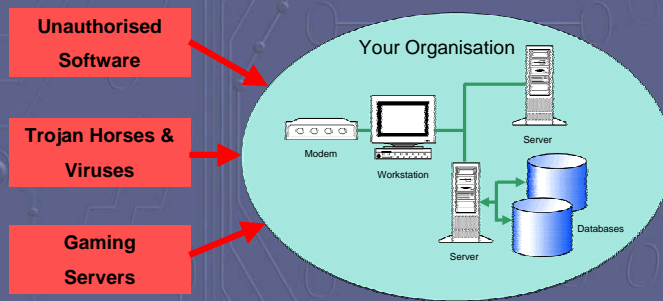
Lack of control blocking illegal and unwanted materials reaching the corporate network.

Lack of control over what information external parties can actually gather about your organisation.

Lack of traceability...

Dial-out Access: What are the risks?

Xiscan

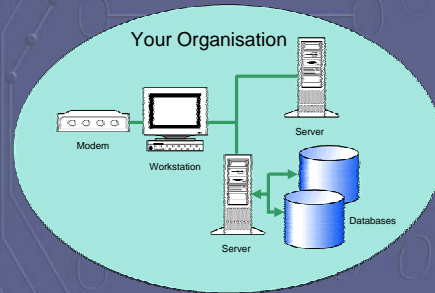


Copyright © 2004 Xiscan® Limited

A user is unaware of the information leaking out...

Dial-out Access: What are the risks?

Xiscan



Copyright © 2004 Xiscan® Limited

... Your view is even more restricted

Dial-out Access: Demonstration

Xiscan

Security issues related to dial-out access

Copyright © 2004 Xiscan® Limited

Dial-in Access

Xiscan

- Definition
- What are the risks?
- Practical demonstration

Copyright © 2004 Xiscan® Limited

Dial-in Access: Definition

Xiscan

...where someone *external* to your premises connects to one of your *internal* systems through the telephone system.

- Modem attached to your computer and the telephone network
- Auto answer set (modem or listening software)
- External party dials in
- Internal system responds

Copyright © 2004 Xiscan® Limited

It's not just your staff that pose a risk...

Dial-in (remote) access can be a contractual obligation for third party support of hardware or software.

Also, there can be lots of hidden modems: telephone systems, routers, disk arrays...

Information Security Breaches Survey (ISBS) 2002 Findings (Remote Access)

Xiscan

Relevant Findings for Large Businesses (250+ employees):

- 71% allow remote access by staff
- 91% restrict which staff can access systems
- 45% restrict access to non-business critical systems

But... that's only access that is *known* and *officially* sanctioned:

In our experience, most if not all companies of 1000+ employees have:

- remote (dial-in) access to one or more business-critical systems (including telephone systems, networking infrastructure)
- dial-in access points that are not sanctioned by IT Security
- dial-in access points located on officially unallocated telephone numbers

Copyright © 2004 Xiscan® Limited

Dial-in Access: What are the risks?

Xiscan

Dial-in (remote) access provides the potential to:

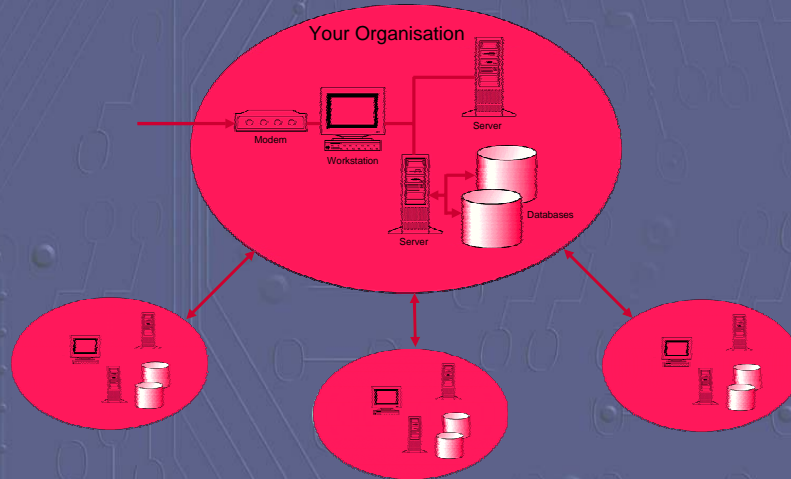
- Access the immediate machine – that's what it's there for!
- Access connected machines internal to organisation
- Access affiliates' networks
- Read, write and modify sensitive information
- Instigate an attack from your machine to an unrelated external target

Copyright © 2004 Xiscan® Limited

Dial-in access offers read-write access and the potential for significant damage.

Dial-in Access What are the risks?

Xiscan



Copyright © 2004 Xiscan® Limited

The damage may not be limited to just your organisation either – any direct links to partner organisations may be compromised – and vice-versa!

Dial-in Access: Demonstration

Xiscan

Security issues related to dial-in access

Copyright © 2004 Xiscan® Limited

How Big is the Problem?

Xiscan

From our experience of large organisations:

- 0.5 – 1.5% of telephone extensions provide dial-in access (i.e. **up to 15 extensions per 1000**)
- 3:1 ratio of dial-out:dial-in
 - Likely to increase with the prevalence of integrated laptop modems

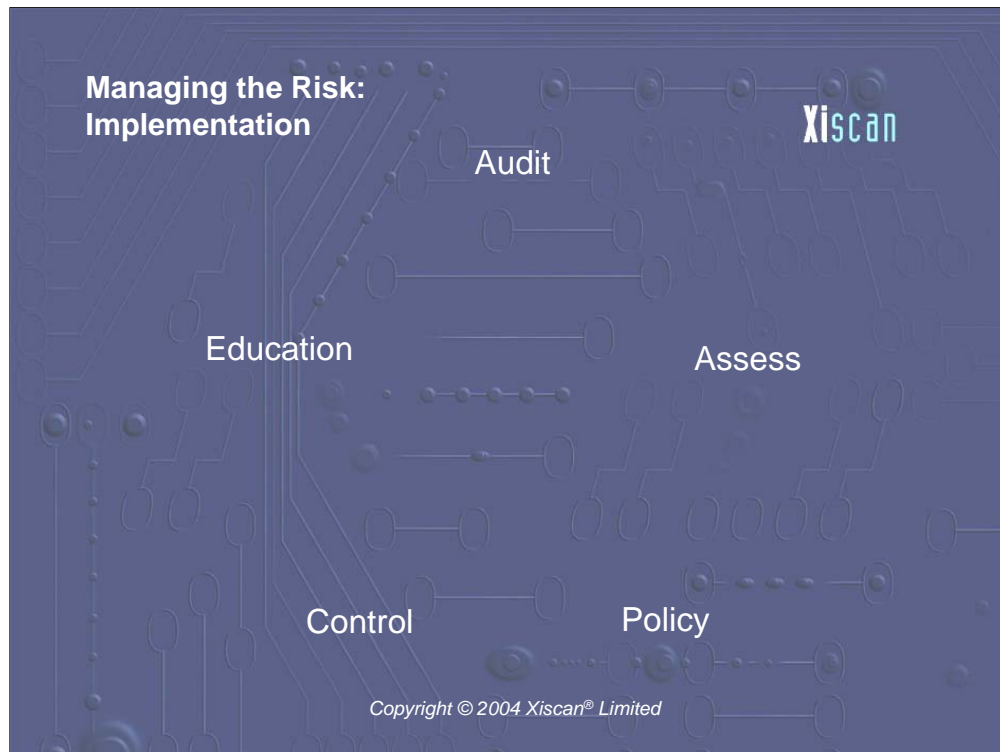
Copyright © 2004 Xiscan® Limited

Managing the Risk

Xiscan

- Strategic approach, as part of the overall Security Policy
 - Planning
 - Discrete implementation stages
 - Audit
 - Assess
 - Policy
 - Control
 - Education
 - Constant re-appraisal
- Practical issues

Copyright © 2004 Xiscan® Limited



Where you start depends on where you currently are...

You may already have a security policy that covers modem access for example.

Managing the Risk: Audit

Xiscan

- Planning
 - identify and minimise disruption
- Create a baseline understanding of the problem
- Identify where modems are:
 - Use existing telephone lists
 - Visual search
 - Automated approach
- Identify access controls on a per modem basis
- Iterative Process – several audits required to ascertain usage

Copyright © 2004 Xiscan® Limited

Techniques used to locate modems can include...

Reviewing existing telephone lists

Visual search

Automated approach – using software tools

Managing the Risk: Assess

Xiscan

From the Audit results:

- Consider each modem in turn:
 - Function / Usage
 - Business Area
- Build business cases for required modems

Copyright © 2004 Xiscan® Limited

Audit and assessment are key to providing information to feed into a modem security policy.

Managing the Risk: Policy

Xiscan

- Define a strategy that is correct for the organisation
- Document:
 - Objectives
 - Acceptable use
 - Implications for violation
 - Create an 'acceptable' modem register
- See also:
 - <http://www.xiscan.com>
 - <http://www.sans.org>
 - <http://www.cert.org>

Copyright © 2004 Xiscan® Limited

Managing the Risk: Control

Xiscan

Take control of modem access

- Remove unjustified / unwanted modems
- Ensure modems are correctly configured
- Ensure adequate security controls are in place
 - Passwords
 - Remove identifiable banners
 - Use callback
 - Avoids calls from arbitrary numbers
 - Authentication mechanisms
- Consider an integrated dial-up solution (focuses control), or a VPN

Copyright © 2004 Xiscan® Limited

Managing the Risk: Education

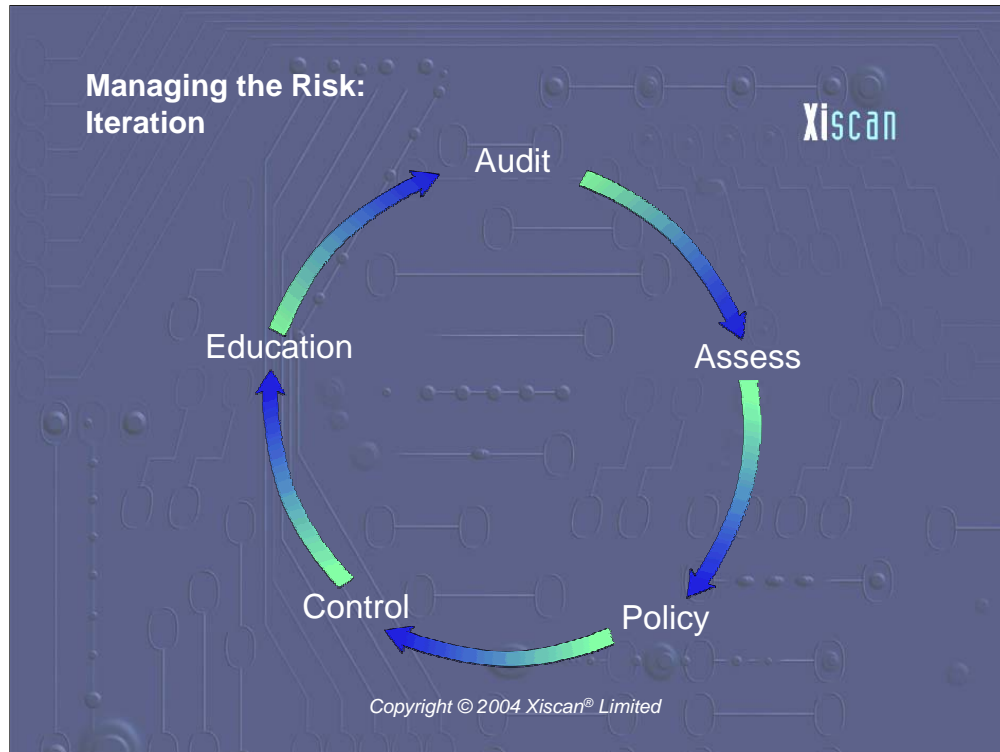
Xiscan

- Effective communication of policy
 - Acceptable use
 - Violation implications
- Prevention rather retribution
(take care not to drive the problem underground...)

Copyright © 2004 Xiscan® Limited

Prevention is better than cure...

Educate users to the risks posed by unauthorised modem access.



Just as when you buy a virus checker, you have to keep it up to date, iteration is key to managing the modern risk. Business requirements, telephone systems and IT systems are not static. All of the above processes must be iterated through.

Managing the Risk: Practical Issues

Xiscan

- Audit & Assess
 - Time and Effort
 - Coverage
- Policy & Control
 - Policing - tools
- Education
 - Effective communication
- Cost of iteration

Copyright © 2004 Xiscan® Limited

Modems can be very difficult to locate...

Telephone lists go out of date

Modems can be difficult to see (under floors, built into equipment, etc)

If you have a policy – how do you enforce it?

How do you educate staff within your organisation?

Business Benefits ...Is It Worth It? (1)

Xiscan

- Increased understanding of IT infrastructure
 - Increased responsiveness to security events
 - Indirect Savings
 - e.g. organisation with 3,500 staff and 20,000 telephone numbers
- Protection of investment in:
 - Business-critical systems
 - Infrastructure (e.g. firewall)
 - Brand/Image
- Promotion of Security Awareness
 - Prevention is more cost-effective than cure

Copyright © 2004 Xiscan® Limited

Business Benefits ...Is It Worth It? (2)

Xiscan

- Compliance
 - Legal obligation – data protection
 - BS7799
 - Visa AIS Security Standards
- Competitiveness/Business Advantage

Copyright © 2004 Xiscan® Limited

Summary

Xiscan

- Basic introduction to the problem
- Dial-out access
- Dial-in access
- Practical solutions

Copyright © 2004 Xiscan® Limited

Questions

Xiscan

Copyright © 2004 Xiscan® Limited

Conclusion

Xiscan

The single most important point to take away from this seminar :

“Any modem configured incorrectly poses a very real threat to the security of your organisation...”

Copyright © 2004 Xiscan® Limited