



Helping You Piece IT Together

Information Security for the Small To Medium Business

SBS Ireland User Group
1st September 2005

Introduction

- Brief introduction to BH Consulting.
- Overview of IT Security and what it means to the small business.
- What new threats are emerging for the Small Business.
- What you can do to ensure the integrity of a Small Business's information assets.

About BH Consulting

- Independent Consulting Firm Founded in 2004 to address lack of vendor neutral advice.
- Areas of speciality include:
 - IT Security Risk Management and Compliance
 - Service Management
 - Service Level Agreements and Service Level Management
 - Operational Management
 - Business Continuity and Disaster Recovery
 - IT Consulting

About Brian Honan

- Over 17 years experience in IT & Information Security.
 - **Certified Lead Auditor in the BS 7799 Information Security Standard.**
 - **Extensive experience in ITIL/BS 15000 standards.**
 - **Working Member of the GAISP initiative.**
 - **Member of the Information Systems Security Association.**
 - **Member of the British Standards Institute.**
 - **Published in a number of publications.**
 - **Actively involved in Global Security Week**

What is Security?

➤ Confidentiality

- Keeping people away from where they should not be.

➤ Integrity

- Ensuring what is being protected is never contaminated or altered.

➤ Availability

- Ensuring what is being protected is available to those who are authorised to access it



Why is Security Important?

- **New Business Channels to customers, partners and suppliers.**
- **Technology is a business enabler.**
- **Greater business dependency on technology.**
- **The Internet is a global public network, not managed by any one organisation.**



The Challenges

- **Small Business's face the same security issues as larger companies:**
 - Minimum interruption/disruption to systems.
 - Maximise the return on investment in their business enablers.
 - Maintain competitive advantage.
 - Comply with current legislation.
 - Provide a safe working place for their employees.
- **But with LESS/NO resources to deal with those issues.**
 - More vulnerable when attacked
- **IT is a cost for many businesses - information security a low priority.**



Security is a Business Issue

➤ **What impact would a prolonged incident such as a computer virus infection, mail server outage or loss of commercially sensitive information have on a Small Business?**

- Legal obligations and possible litigation
- Cost of recovery
- Customer confidence
- Loss of Business
- Loss of Productivity



Inadequate security costs money!!

Legal Obligations

- **Data protection Act 1988 & Bill 2002**
- **Obligations under the Companies Act 2003**
- **Criminal damages Act 1991**
- **Child Trafficking and Pornography Act 1998**
- **Theft of intellectual property**
- **Unfair-Dismissal**
 - Inappropriate use of internet and e-mail
 - Bullying and discrimination
- **Third party litigation**



Cost of Recovery

- **Loss in productivity while systems are recovered.**
- **Costs in recovering/replacing systems**
- **Opportunity costs due to system downtime.**



Customer Confidence

➤ Inadequate Security can lead to

- Loss of professional reputation
- Loss of customer confidence/trust
- Loss of partner confidence and trust



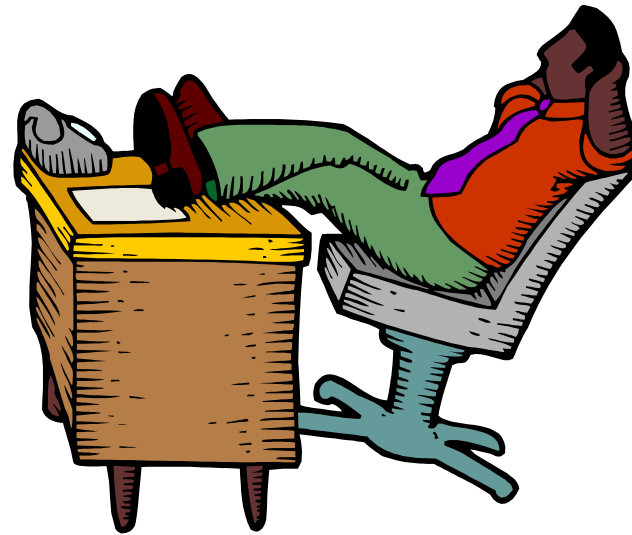
Loss of Business

- **Loss of sales/orders.**
 - Customers unable to place orders.
 - Business unable to process orders/deliveries.
- **Commercially sensitive information available to competitors.**
- **Customers move to more secure suppliers.**
- **Suppliers and Partners move to more secure.**



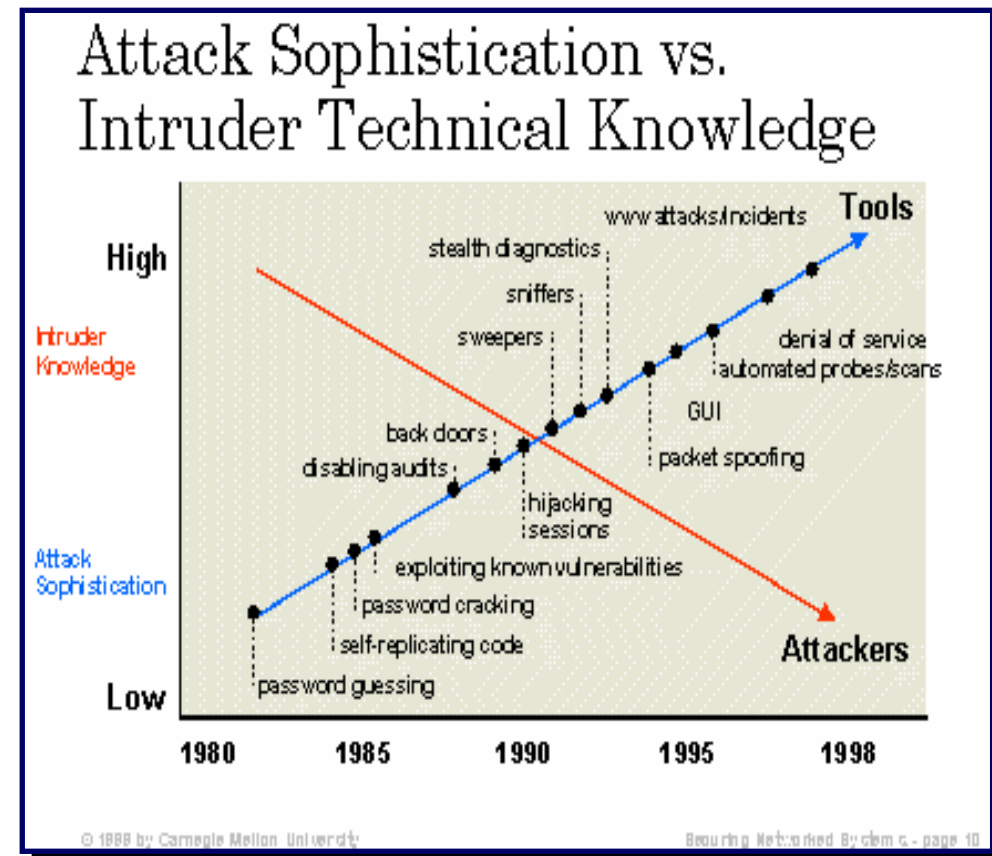
Loss of Productivity

- **System downtime due to security breach.**
- **Missed deadlines**
- **Manual tasks implemented while issues being addressed**
- **Inappropriate use of resources**
- **Loss of valuable staff**



Current Security Threats

- **Sharp increase in hacking attempts from Internet**
 - Honeynet Project
- **Increasing Sophistication of threats**
- **Number of hackers increasing**
 - Hacking tools easier to use
 - Hackers don't work 9-5.
 - Automated attacks
 - If you are on the Internet, you are a target



Current Security Threats

➤ 31% of Information Security breaches are internal

- Accidental/deliberate misuse by employees.
 - CSI/FBI Computer Crime & Security Survey 2005

➤ Increasing Criminal focus

- Phishing
 - Spear Phishing
 - Pharming
- Online Blackmail
 - DDOS
 - File Encryption
- Scams

➤ Wireless networks



Current Security Threats

- **Bot networks**
- **80% of companies reported internet abuse by employees.**
 - CSI/FBI Computer Crime & Security Survey 2005
- **Confidential information**
 - Spyware a major problem
 - keyloggers
- **Exploit code within 6.4 days**
 - Slammer 6 months
 - Zotob 4 days
 - CNN, US Dept of Homeland Security??
 - Sasser 36 hours
- **Instant Messaging**



Computer Virus & Email Threats

- **86% of Viruses spread via email**
- **1 in 4 companies do not scan for viruses**
- **SPAM accounts for over 60% of all email messages**
- **E-mail**
 - Is becoming most popular file transfer solution
 - Can contain unsavoury content
 - Can contain defamatory, unprofessional or libellous content



Upcoming Threats

- **Mobile Devices**
 - PDAs
 - Blackberry's
 - Smart Phones
 - USB Devices
 - Bluetooth
- **Remote Workers**
 - Teleworking on own computers
 - Company computers
- **VOIP**
 - External Connections
- **Peer to Peer Applications**
 - File Sharing
 - Chat
- **Increasing Criminal Activity**



How to Protect Your Assets

- **Conduct a risk assessment;**
 - Mitigate the risk
 - Transfer the risk
 - Accept/Ignore the risk
- **Develop Policies and Enforce them.**
- **Conduct regular security audits.**
 - Check logs for suspicious activity
 - Check for new vulnerabilities
 - Check compliance with policies
- **Educate users on how to deal with threats.**
 - Encourage them to practise safe HEX



How to Protect Your Assets

➤ Electronic Mail Guidelines

- E-mail can appear to be from anyone
- Never open an email attachment unless you are expecting it.
- Don't participate in chain mail
- Assume a permanent record of messages sent
- Use appropriate, professional and courteous language

➤ Use Strong Passwords

- Treat Passwords like a toothbrush
 - Use it regularly
 - Change it often
 - Never Share it with anyone



How to Protect Your Assets

- **Secure Remote Users/Devices**
 - Encrypt sensitive data.
 - Guidelines on protecting computer equipment.
 - Use Personal Firewalls
 - Deploy Secure VPN
 - No Split tunnelling
 - Quarantine facility
- **Prepare an incident response plan.**
 - When do you contact the Gardai?



How to Protect Your Assets

- **Patch systems regularly.**
 - WSUS,
 - Windows Update for remote machines
- **Deploy a Firewall.**
 - Apply Strict rules.
 - Check logs regularly
 - Check rules every 6 months
- **Use Anti-Virus Software and Update regularly.**
- **Implement Content Filtering tools for email and internet.**
- **Secure Wireless Networks.**
- **Lock down workstations**
 - Group Policy

- ***Be Aware-Technology by Itself is not the solution!!***



More Information

- **Microsoft's Security Resources**
 - www.microsoft.com/security
- **Computer Security Institute/FBI Security Report**
 - www.gocsi.com
- **Irish Chapter ISSA**
 - www.issaireland.org
- **Information & Communications technology law in Ireland**
 - www.ictlaw.com
- **The Security and Administrators network**
 - www.sans.org
- **Global Security Week**
 - www.globalsecurityweek.com
- **Information on the BS 7799 Information Security Standard**
 - <http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter>



Questions ?

