



Helping You Piece IT Together

Information Security, What is it and Why should I care?

Leinster CPA Society
27th September 2007

What is Security?

Confidentiality

Integrity

Availability



Why is Security Important?

- New Business Channels
- Business Enabler
- Greater Dependency
- The Internet



The Challenges

- Minimise System Downtime
- Maintain Competitive Advantage
- Legislation
- Safe Working Place
- IT = €€€€€€€€



Security is a Business Issue

Inadequate security costs money!!



Some Background

- Incidents are on the increase
 - 2000 = 21,756 ⇒ 2003 = 137,529
- Cyber-Crime costs Businesses more than Physical Crime - IBM Survey – 2006
- Average UK business has 1 incident a year at an average cost of STG£10,000



Irish Background

➤ “Irish Cyber Crime Survey 2006”

- 98% of all Companies Impacted
- 20% suffered losses > €100,000
- 33% suffered losses > €50,000
- 55% lost data as a direct result
- 90% suffered loss in productivity
- 52% Had incidents resulting in 10 man days to recover
- 25% had incidents resulting in 50 man days to recover
- 12% of internal misuse resulted in criminal cases
- 90% impacted by computer virus infection



The Threat Landscape

- Traditional Threats
- Increasing Sophistication
- Hackers Increasing
- Viruses Produced Quicker

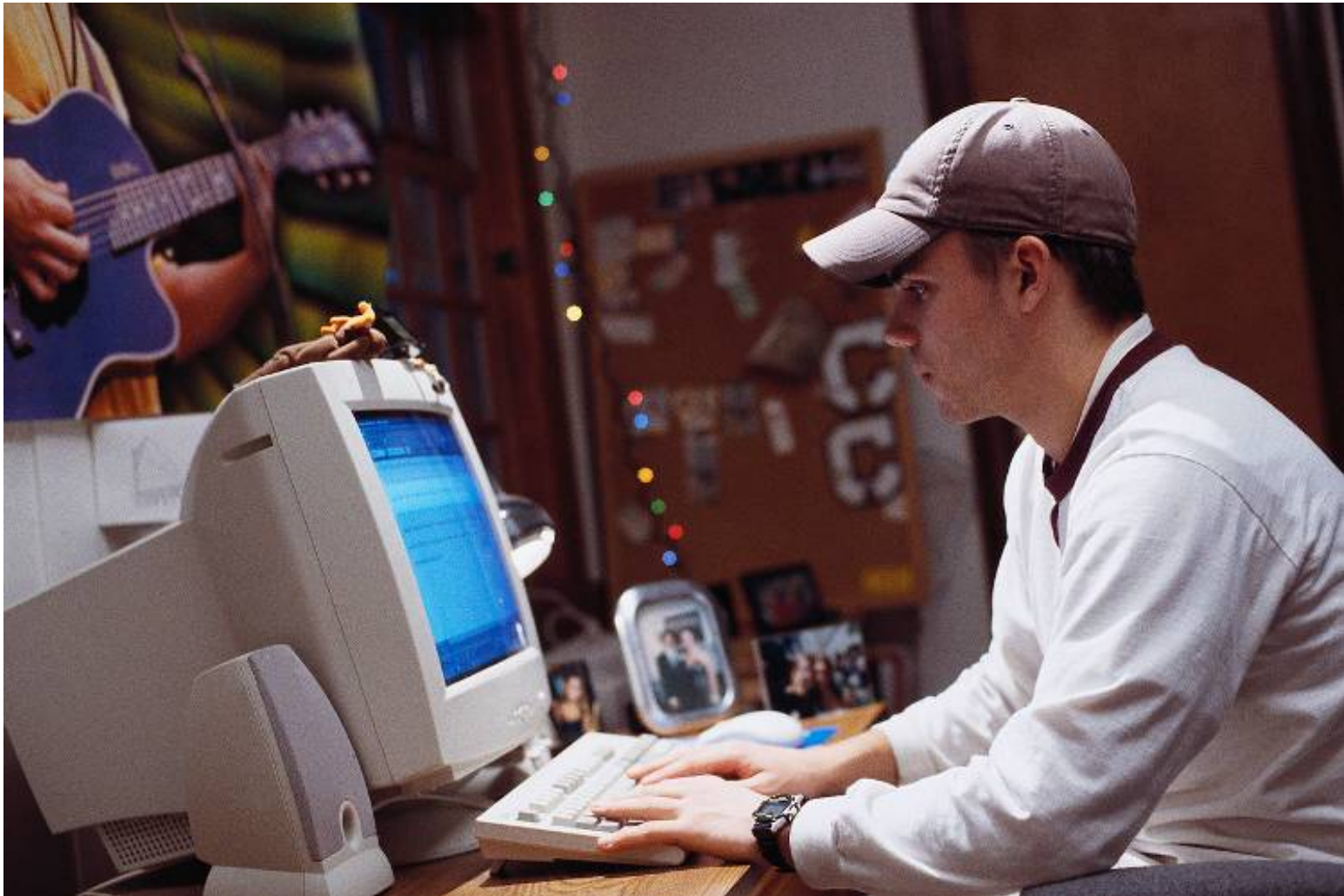


The New Threat Landscape

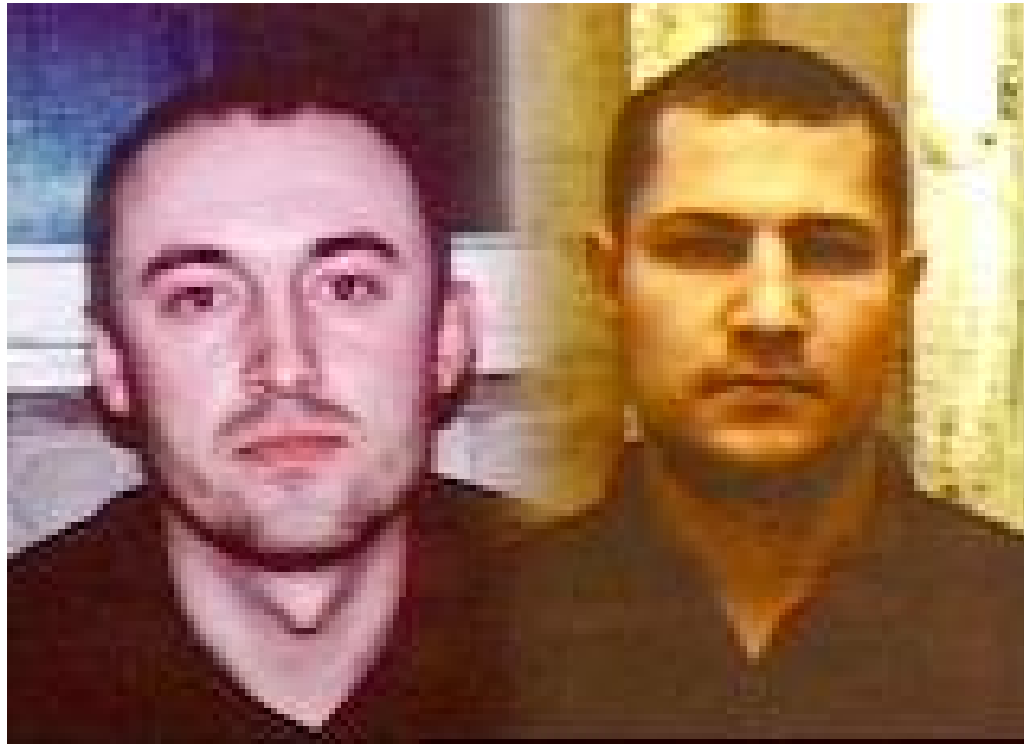
- Criminal Involvement
- Terrorist Involvement
- State sponsored Espionage
- Focus now on Profit



The New Threat Landscape



The New Threat Landscape



- Ivanov and Gorshkov
 - Blackmailed Numerous Companies
 - Claimed forced to hack by organised Criminals

The New Threat Landscape



- The Bali Bomber – Iman Samudra
 - Calls for Cyber Jihad
 - Raise Funds for Terror Campaign

The New Threat Landscape



- Younis Tsouli, Tariq al-Daour, Waseem Mughal
 - Promoted Islamic Terrorism & Radicalism
 - €2.5 Million Euro Online Fraud

Upcoming Threats

- Mobile Devices
- Remote Workers
- New Technologies
 - VOIP
 - Peer to Peer Applications
 - File Sharing
 - Chat
- Increasing Criminal Activity
- Staff



Remember



➤ *Technology by Itself is not the solution!!*



Information Security Checklist

People	Check Item	Answer
Responsibility	Does a director, or equivalent, have responsibility for information security?	
Employee Buy-in	Have all members of staff given written acknowledgement that they have read, understood and accepted the information security policy?	
Employee awareness	Do all users on your computer systems receive regular training on their security responsibilities and how to identify and deal with various security threats?	
Training	Do staff members with specific security responsibilities receive proper and regular training to support their role?	
Computer security policy	Have you a documented security policy, with associated operating procedures, signed off and fully supported by senior management?	
Non-disclosure agreements	Does senior management authorise third party access to confidential and/or commercially sensitive information pending completion of appropriate confidentiality forms?	



Information Security Checklist

Process	Check Item	Answer
Audits	Are critical systems such as firewalls and routers regularly tested for vulnerabilities and are computers checked to ensure no copies of illegal software are present?	
Incident Planning and response	Are documented and frequently tested plans in place, with clearly defined roles and responsibilities, to ensure the company can respond to any security breaches such as a virus attack, fraud or natural disasters such as fire?	
Passwords	Are all default passwords on all systems reset from the default vendor installed passwords? Are users forced to use complex and hard to guess passwords?	
Software patches	Is there a mechanism to ensure that critical security patches are deployed to systems in a timely and audited fashion?	
Data Protection	Are systems and databases that store personal data secured properly to ensure compliance with regulatory and legal requirements such as the Data Protection Act?	



Information Security Checklist

Technology	Check Item	Answer
External Network Security	Are external connections, such as to the Internet, authorised by senior management, properly documented and secured using Firewalls and Intrusion Detection Systems?	
Anti-Virus	Are all computer systems protected with the most up to date anti-virus software? Are users educated on how to identify and deal with suspect files that may contain computer viruses?	
Content Monitoring	Do you properly monitor the content of emails and Internet browsing activity to protect your company from computer viruses, SPAM, or litigation due to the nature of the content?	
Monitoring	Are the log files of important security devices actively monitored to detect potential security breaches?	
Physical security	Are critical IT resources, such as file servers, secured in a secured area that is protected from unauthorised access?	

Establish External Relationships

➤ Some Skills not available In-house

- Legal
- Forensics
- Public Relations

Agree Terms & Conditions before an Incident

➤ Suppliers

- ISPs, Telecomms, Hosting

➤ Partners

➤ Customers



Law Enforcement

- An Garda Siochana
 - Garda Computer Crime Unit
 - Part of Garda Bureau of Fraud Investigation
 - How do you Report a Computer Crime?
 - Contact Local Garda Station
 - Refer to Garda Computer Crime Unit
- When Should You Contact Garda Computer Crime Unit
 - Today !!



More Information

- Microsoft's Security Resources
 - www.microsoft.com/security
- Computer Security Institute/FBI Security Report
 - www.gocsi.com
- BH Consulting Resources
 - www.bhconsulting.ie/whitepapers.htm
 - www.bhconsulting.ie/blog
- 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



Questions ?

