Computer Crime - The Emerging Threats - (1970's to 2009) -

John Austen BA MSc FBCS NEBSS

Royal Holloway University of London &

QCC Information Security Training Ltd.

Those Behind the Threats on the Internet

- Detective Agencies & Competitive Intelligence (volumes)
- Intelligence Agencies (many)
- Professional Hackers & Groups (some for hire)
- Script Kiddies (many)
- Organised Crime
- Freelance/Media
- Political Extremists

The Culture of Hacking Groups - The 2600 Club

- First formed after the Cap'n Crunch prosecution in 1972

- Issues bulletins on Phreaking and hacking with technical vulnerabilities, dialling codes and wiring diagrams

- Still in effect today – the forerunner of hacking, and hacking techniques made available to members.

The 1980's - The Growth of Hacking & Hacking Clubs - Taking Advantage of System Vulnerabilities

- Chaos Computer Club 1981 - Began in Hamburg - soon spread to other parts of Germany
- Attacked Hamburger Sparkasse & Verbraucher Banks
- Amongst other exploits, in 1989 attacked the Digital Equipment system of CERN (Conseil de Europee Recherche Nuclaire) in Geneva – took control of the Nuclear Accelerator
- Still active

L0pht (First in 1984)

- Started in San Francisco
- Concentrated initially on password crackers – l0phtcrack etc.)
- Political motivation – Microsoft etc.
- Eventually became legitimate - @stake.
- The name means 'Law enforcement nil, Phreakers & Hackers tops'.

1984 Legion of Doom (LOD)

- Started by Lex Luthor, Eric Bloodaxe, The Prophet (Robert Riggs) and 8 more
- Sci-Fi Names used for intimidation – as per Kubrick's Clockwork Orange
- Initially phone phreakers, - attacked the phone system (911) in Atlanta in 1988
- Published 'The Technical Journal' – moved onto hacking - It was considered a sport - Great concern regarding hacking throughout industry

# A Network Underground has by now been established – they used:
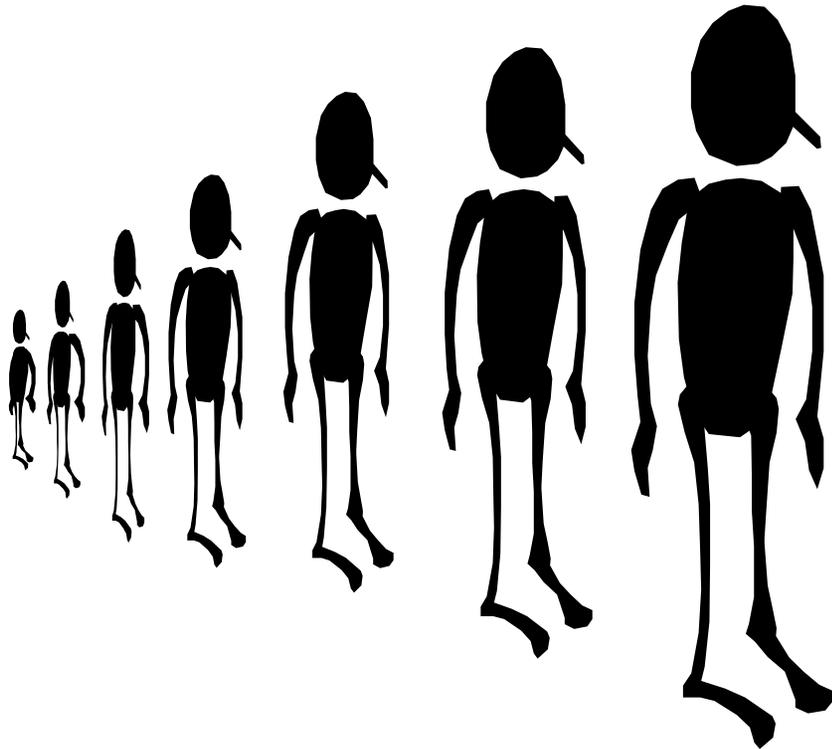
- Bulletin Boards
- Chat Sessions
- Cell Structures
- System Vulnerabilities
- Encryption
- False I.D.'s
- Social Engineering

1990's (1)

- Kevin Mitnick hacked cell-phone companies - (the methodology of social engineering was uncovered)
- Vladimir Levin(St. Petersburg) hacked Citibank systems (San Francisco) - transferred $10 million to Rotterdam. Arrested at Stanstead Airport (UK) in 1995 - 3 years in prison
- 'Satan' released on Internet - probes Internet sites for unpatched security flaws
- CERT reports 31,000 e-mail security incidents
- Music industry reports $2.25 billion loss by downloads to MP3 players
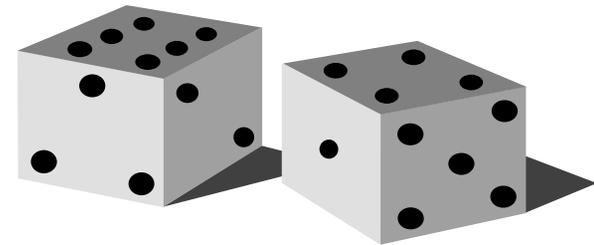
1998 - 1999

- Crack (L0phtcrack) dictionary attack launched - to crack 10,000 passwords at once
- Major vulnerability on web servers - exploits flaw in 'cgi' - (common gateway interface)
- Buffer overflow in 'stat.d' daemon (network status)
- War dialing programs now in frequent use by hackers testing for signal response
- Cult of the Dead Cow – launched 'Back Orifice' – attack on Windows 98.
- Love Bug virus released - also 'Anna Kournikova' virus – tempting recipients to execute attachments
- Web page 'kidnapping' proliferates
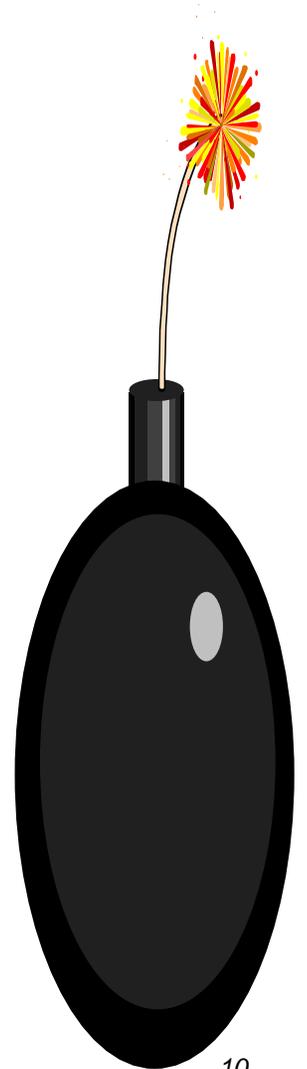
2000-2005 - Started with Worms

- Code Red worm launched – devastating effect
- Nimda, So BigF, Slammer and MS Blast worms and malware costs billions. The I.S. industry was not ready for it, and fairly impotent to act.
- Spam reaches epidemic proportions, most e-mail addresses are in the possession of spammers – domains are now well known. People can be identified by their e-mail addresses, and malware continues to be introduced by this medium.
- 2005 Phishing & Pharming cause huge losses to the financial industry in Western Europe – although the figures are not released.
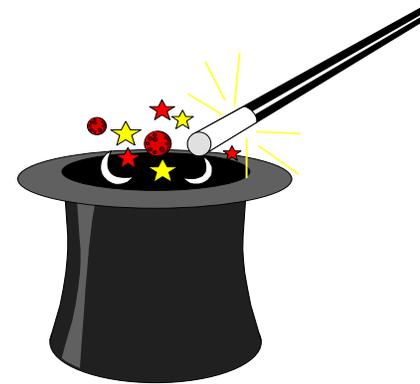
Recent trends

- Between 2002 and 2004, DDoS attacks were used to extort money from companies (primarily gambling sites).
- Since then, the zombie networks evolved into botnets and are used in more profitable ways, e.g. sending spam, spreading adware, and stealing users' personal data.
- Besides DDoS attacks, extortion attacks are also based on other techniques, for example, targeted malware (e.g. computer viruses that encrypt a victim's data).
- New in 2009, DoS attacks against mobile phones
  - a specially formatted text message can crash SMS inboxes of phones running versions 8 through 9.2 of the Symbian operating systems
  (see http://www.fiercemobileit.com/story/serious-new-denial-service-attack-against-certain-nokia-phones-surfaces/2009-01-07)

The Year 2006

- New DoS attack detected in late 2005/early 2006, namely the *DNS Amplification Attack*

- DNS amplification occurs due to the response packet being significantly larger than that of the query.

Defence mechanisms (according to CERT)

- Implement router filters to lessen exposure to certain denial-of-service attacks
- Install patches to guard against *TCP SYN flooding*
- Disable any unused or unneeded network services
- Enable quota systems on your operating system if they are available
- Observe your system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic
- Routinely examine your physical security with respect to your current needs

Defence mechanisms (according to CERT)

- Use *Tripwire* or a similar tool to detect changes in configuration information or other files
- Invest in and maintain "hot spares" - machines that can be placed into service quickly in the event that a similar machine is disabled
- Invest in redundant and fault-tolerant network configurations
- Establish and maintain regular backup schedules and policies, particularly for important configuration information
- Establish and maintain appropriate password policies, especially access to highly privileged accounts such as UNIX root or Microsoft Windows NT Administrator

Spyware

Spyware

- is tracking software deployed without adequate notice, consent, or control of the user, where tracking software is software that monitors user behaviour, or gathers information about the user, sometimes including personally identifiable or other sensitive information, through an executable program.

  [www.antispywarecoalition.org]

Characteristics of Spyware

- Subverts the computer's operation for the benefit of a third party
- Does not self-replicate
- Multiple infections at once (usually dozens)
- Affects mostly Windows users (not so common on Linux and MacOS)
- It is used for
  - Delivery of unsolicited pop-up advertisements
  - Theft of personal information
  - Monitoring Web browsing activity
    - Which websites does a user visit?
    - Monitor web activity to build up marketing profile
  - Routing HTTP requests to advertising sites

Effects of Spyware

- Computers often become infected with large numbers of Spyware programs
- Computer slows down due to high unwanted CPU activity, disk usage, and network traffic
- Lost time
- Spyware may disable other security software (e.g. firewalls and anti-virus software)
- May use stealth mechanisms not to be detected
- Display of pop-up advertisements
- Affiliate or click fraud
- Identity theft

Common Spyware

- *Gator/Claria* products are often delivered to end-users by being bundled with other applications or through "drive-by downloads" that pop up an ActiveX dialog and start the installation process if you say "Yes". Gator applications include eWallet, DateManager, WeatherScope, and PrecisionTime.

- *CoolWebSearch*

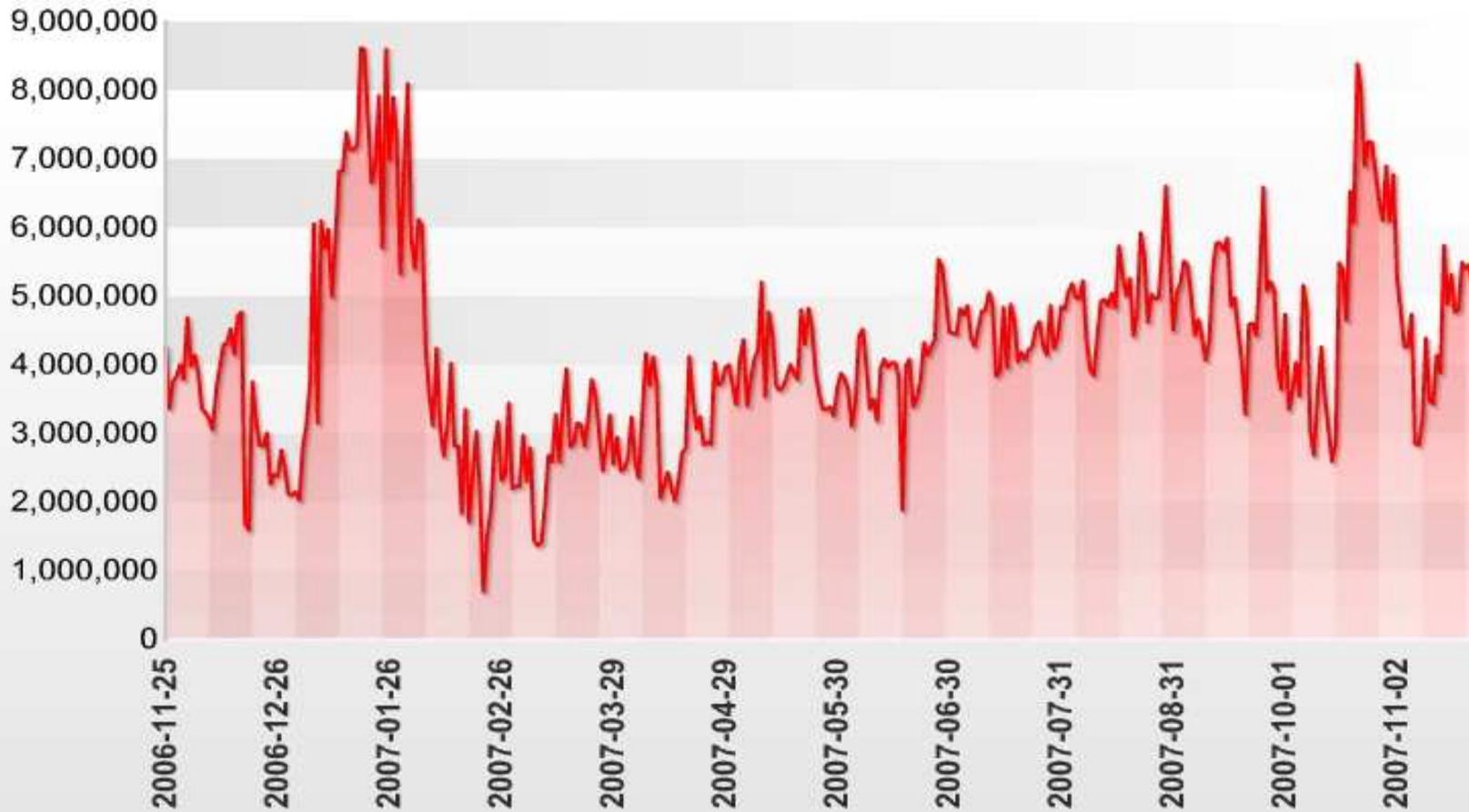- *Internet Optimizer*

- *180 Solutions*

- *HuntBar*

- *…*

Statistics

- According to Commtouch® Software Ltd.
- Jan 2008-09 – spam is physically sent from
  - US – 42.04%
  - China – 6.71%
  - Korea and Russia – about 4% each
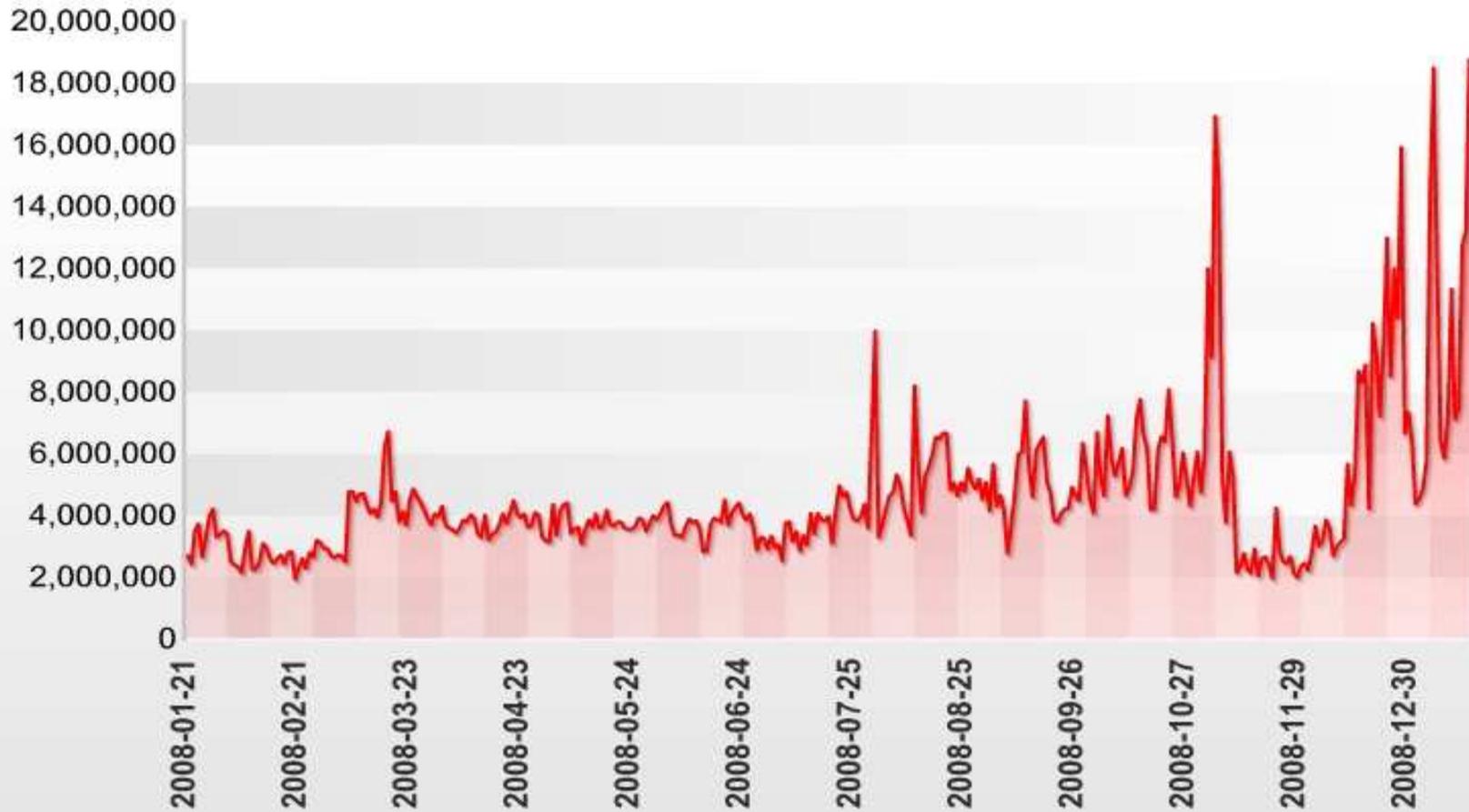 - …
  - (the top two tend to be the same every year)

Recent Spam Outbreaks - 12 Months View
Data source: Commtouch Software Online Lab

Recent Spam Outbreaks - 12 Months View

Data source: Commtouch Software Online Lab

Spam botnets

Today, most spam is sent via spam botnets.
Below, "percentage breakdown of spam received at TRACE spam traps for each spambot type. Typically a small number of major botnets are responsible for the bulk of all spam."

RUSTOCK 31.5%
MEGA-D 28.4%
XARVESTER 18.4%
PUSHDO 2.2%
GHEG 1.0%
SPAMTHRU 0.9%
OTHER SOURCES 17.6%
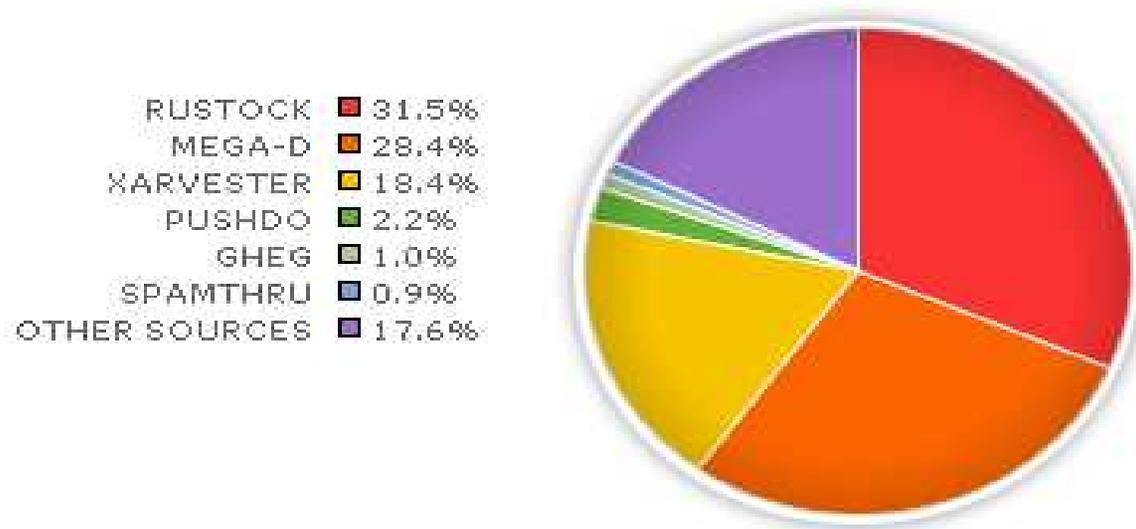
Source: Spam statistic from TRACE: Marshal

Basic spamming techniques

- Sending spam from one dedicated machine does not work well

- Instead, spammers use
  - Free webmail services (e.g. Hotmail)
  - Open mail relays
  - Open proxy servers
  - Botnets !!!

- Use spam sending software (to create dynamic text and connect to bots)

Anti-botnet solutions

Exist

- To identify and block email-borne botnet attacks (e.g. from Engate)
- To catalog and disseminate botnet characteristics derived from malware analyses and to discover and analyse botnets (e.g. from FireEye)
- To detect and isolate bot machines (e.g. from Trend Micro)

Statistics

- According to Commtouch® Software Ltd.
- Jan 2008-09 – spam is physically sent from
  - US – 42.04%
  - China – 6.71%
  - Korea and Russia – about 4% each
  - …
  - (the top two tend to be the same every year)

2007-8

- Data Loss Epidemic in Public Institutions & Large Companies

- *UK – Dept. of Health (junior doctors); Royal Cornwall Hospital (5,000 staff); Marks & Spencer (26,000 pension plans); Bank of Scotland (62,000 customers); Nationwide Building Society (laptop) HMRC (laptop & a CD 15,000 pension policies); Dept. of Work & Pensions (millions of records on Child Benefit)*

- *USA – Bank of America; Dept. of Agriculture (38,000 individuals)' 6 Universities (student details),; Transport Security Administration (100,000 employees); Texas Police (97,000 records)*

2009 (So Far)

- Theft of Laptops & Storage Devices is still increasing
- In a recent survey in the U.S.A. - half of those employees who left companies admitted copying data for their own purposes
- Conficker Worm (on Microsoft Systems) hits over 10 million PC's including governments in Europe - first public problem with Botnets - reward publicised
- First DNS Amplification Attacks reported (a form of Denial of Service)

United Kingdom - 2008 Survey by Department of Trade & Industry(1)

- 13% have detected unauthorised outsiders within their network
- 9% had fake (phishing) emails sent asking their customers for data
- 9% had customers impersonated (e.g. after identity theft)
- 6% have suffered a confidentiality breach

2008 Survey (2)

- 10% of websites that accept payment details do not encrypt them
- 21% spend less than 1% of their I.T. budget on information security
- 35% have no controls over staff use of Instant Messaging
- 48% of disaster recovery plans have not been tested in the last year
- 52% do not carry out any formal security risk assessment

2008 Survey (3)

- 67% do nothing to prevent confidential data leaving on USB sticks etc.

- 78% of companies that had computers stolen did not encrypt hard discs.

- 79% are not aware of the contents of BS7799/ISO27001

- 84% of companies do not scan outgoing email for confidential data

End