

ScotlandIS Trust in Software

Information Security
in Financial Services

26 February 2007

Information Security

- **Information security is evolving**
- **We learn from managing our issues, trends and best practice**
- **We develop our skills and maintain career development**
- **We ensure we continue to improve what we have**

We know ‘some’ of the threats out there and we take action to actively manage them?

Emerging Threats

- **The emerging threats in Financial Services will not be radically different from those experienced in other industries**
- **At a technical level the skill requirements are similar**
- **Regulation will differ**

The emerging threats discussed today should be similar to those experienced by others

**The source of the threats discussed today
have been taken from the public domain.**

**The content of this presentation does not
relate specifically to the views, opinions
or experiences of RBS Group**

“My current top 10”

- 1 Increasingly more sophisticated attacks
- 2 BotNets
- 3 Phishing
- 4 Data theft from out of office working / home working
- 5 Stolen or lost media
- 6 Insider threat
- 7 Unauthorised machines accessing internal network
- 8 WEB 2.0
- 9 Legislation, regulation and compliance
- 10 Global impact

Sophistication of Attacks

- **We all learn from the incidents which we deal with, but so do the attackers**
- **Malware, including more sophisticated Trojans**
 - Selective and developed with predefined targets
 - Operate in ‘stealth’, and so not always visible
 - not always detected by Anti-Virus software
 - e-cards
- **Microsoft’s Malicious Software Removal Tool**
 - 290 Million PC(s) scanned, 4 Million infected, 2 Million were “bot infested”, i.e, used to stage another attack

Botnets

“...refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure”

- Usually where security is poorly maintained and a side-effect from an age where machines are always on
- Source for SPAM, Phishing, Trojans, etc
- Not helped by the lack of control around being able to acquire domain names

Points to ponder

- Can machines be turned off when not in use?
- Are patches, anti-virus signatures, SPAM filters up to date?

... and Phishing

- **There has been considerable publicity relating to Phishing**
- **Sources of Phishing sites are Geographically distributed**
 - Including countries where there is challenge around time zones, language
- **“FIRST” is a global Forum for Incident Response and Security Teams**

Points to ponder

- Would you know where to report a possible Phishing site?

Also, APACS site: <http://www.banksafeonline.org.uk/>

Data theft



- **Wireless machines**
 - Increased ability for Wireless DDoS
 - An attack to stop a Client and Access point from talking to each other
 - An issue, the Wireless standard IEEE 802.11 (early stages) were not built with initial security input
- **Wireless users are not confined to the office**
 - Will use in public areas

Data theft (continued)

- **Stolen or lost laptops, some examples**

- “FSA fines Nationwide £980,000 for information security lapses”

<http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml>

- There have been several press articles in relation to lost laptops which have sensitive information

- “81% of U.S. firms lost laptops with sensitive data in the past year” (16 August 2006)

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002493>

Points to ponder

- Are your laptops encrypted?
- What data is on your laptops?
- Does this data have to be on the laptop?

Data Theft (continued)

Media in transit

- We need to transfer data on occasion
- A long time ago, we used disks.
 - Small, held very little information
- We now have to consider the use of
 - CD / DVD
 - memory Sticks
 - Removable Hard Drives
 - Laptops
 - Other multifunctional devices...

*How many track
the 'life' of each
storage device,
each CD, etc?*

Point to ponder

- Do you know what data is being transmitted?

Data Theft (continued)

Convergence in devices

- Devices are smaller
- Have many converging functions
- These devices can store data
- e.g., Mobile phones, iPod(s), PDA(s), etc

Points to ponder

- Do we know which devices are being used?
- Can we tell if a device has been connected to our network?
- If data has to be stored, then how do we protect the data on the device?

Data Theft (continued)

Email :- a business enabling tool

- Easy to use and may feel secure
- It enables faster business engagement
- Maintains a personal record of an action taken
- Our data may be e-mailed out without us knowing

Points to ponder

- Should you monitor usage / content?
- What if it is sent to wrong address?
- How to enforce appropriate use?
- When should we not use email?
- How do we protect business content?
- We need to retain email, but for how long?

***“An ohnosecond is the fraction of time in which you realize you made a big mistake and you can't undo it.**”*

Source Wikipedia

Insider threat

The threat of attack from insiders is real

“... Respondents who identify the culprit indicate that 80% of the attacks come from outsiders and 20% from insiders”

(Source: 2005 E-Crime Watch survey, United States Secret Service, CERT® Co-ordination Centre and CSO Magazine, <http://www.cert.org/archive/pdf/ecrimesummary05.pdf>)

“.... The impact from insider attacks can be devastating. One complex case of financial fraud committed by an insider in a financial institution resulted in losses of almost \$700 million”

“...Another case involving a logic bomb written by a technical employee working for a defense contractor resulted in \$10 million in losses and the layoff of eighty employees”

(Source: Computer Emergency Response Team - Carnegie Mellon University, <http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.1-1-070118.pdf>)

Insider threat

Staff / contractors / suppliers

- Screening / vetting
- Contact enforcement for contractors / suppliers
- Know what is being connected to the network
- Event logging for connections

- Qualify appropriate risk indicators / thresholds
- User Access controls, e.g., default minimum access as defined by role

Points to ponder

- Do we know how and what is being connected to our networks?
- Is access appropriate for job requirement?

Unauthorised access to an internal network

- **Protect the network**
- **Regular scans**
- **Penetration tests**

Point to ponder

- Do you know that your network is secure?

Topical example

“TJX had thought the intrusion into its customer data files took place between May 2006 and January 2007, but has since learned its computer system also was hacked into in July 2005 and other periods during that year.

Credit and debit card data from transactions at its U.S. and Puerto Rican stores and credit card-only transactions at Canadian stores from January 2003 through June 2004 were stolen.”

and also

“...believed stolen are some drivers' license numbers”

(Source: <http://www.businessweek.com/ap/financialnews/D8NE5GGG0.htm>)

Web 2.0

- **Blogs / Wikis**
- **Personal Blogs**
- **Content Management is a concern**
- **Potential for disclosure of sensitive information**

Points to ponder

- Can this activity be controlled through Policy?
- How would you monitor use?
- Or, what opinions will be expressed?
- Who would be liable during a dispute?

Legislation, Regulation & Compliance

- **Regulatory Compliance comprise 65% of initiatives which were planned for 2006**

(Source: [Deloitte 2006 Global Security Survey](#))

- **Always a hot topic in FS**
- **Some legislation currently lacks enforcement**

Point to ponder

- **If Information Security is thorough, do we have much to meet other compliance requirements?**

Global impact

The world is getting smaller

- Jurisdiction
- Culture and awareness
- Effective Global Governance
- Effective Risk Assurance
- Incident Management

Threats Summary...

- 1** Increasingly more sophisticated attacks
- 2** BotNets
- 3** Phishing
- 4** Data theft from out of office working
- 5** Stolen media
- 6** Insider threat
- 7** Unauthorised machines accessing internal network
- 8** WEB 2.0
- 9** Legislation, regulation and compliance
- 10** Global impact

Thank you