



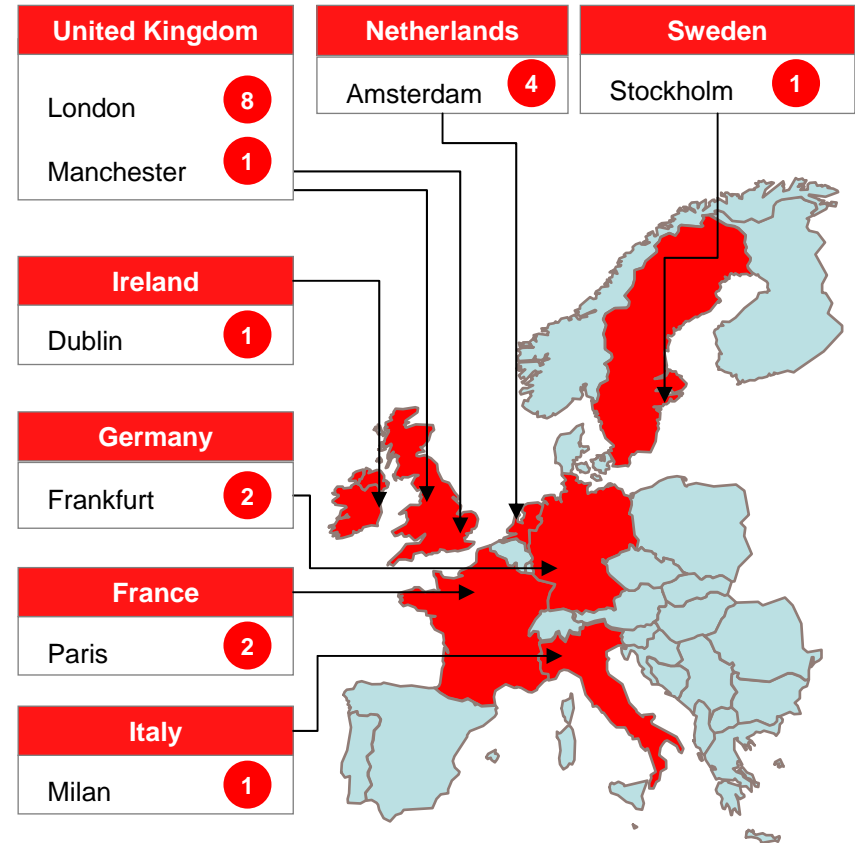
TelecityGroup

where content meets connectivity

Group overview

- **Leading pan-European operator of network independent data centres**
- Formed by **merger** of **TeleCity** and **Redbus Interhouse** (both formed in 1998)
 - acquisition of **Globix** in September **2006**
- **20** network independent **data centres** with approx 500,000 sqft fitted-out space
- Offering a **range** of **data centre** and related **managed services**
 - highly **flexible** and **scalable**
 - including bandwidth, maintenance and **security** services
- Over 3000 customer contracts
- Listed on the London Stock Exchange. December 2007 entered FTSE 250

18 + 2^(a) data centres across Europe



Insider Job

Insider Job

Data breaches are still high profile news, and can be extremely embarrassing for a financial organisation as it damages customer faith. What can an organisation do to protect itself? This will cover the technology which needs to be in place, internal IT policy, computer forensics and the legalities.

Information Insecurity

Beyond hackers, viruses and worms:

The malicious insider challenge

The Infosec theatre of war

Internal headaches

- Unaware users
- Malicious insiders
- Weak identity management
- Back doors
- Logical bombs
- Undocumented functions
- ... and more

External attacks

- Virus, worm, trojan horse writers
 - Script kiddies & other hackers
 - Zombies in DDOS mode
 - Hactivists and spoof sites
 - Organized crime
 - Cyber-warriors and cyber-terrorists
-and more

Types of attack

- Physical attacks
- Syntactic attacks
- Semantic attacks
- Corrupt data in “trusted” systems
- Make computers perform unexpected functions

Malicious insider

- Opportunity
- Knowledge
- Motivation

Insider Job

Malicious insider

- Queensland (AUS) Sunshine Coast, April 2001
- Just one example
- Disgruntled employee hacks into computerised sewage control system.
- Released one million litres of raw sewage.
- Found guilty on 46 counts of computer hacking
- Sentenced to two years in jail
- What if he and others like him had been suborned by terrorists or a foreign government?

Insider Job

Who is an insider?

-
- Employees
- Temporary appointees
- Interns
- Contract employees
- Consultants
- Visitors good at social engineering
- Others who have regular access:
 - Maintenance personnel
 - Cleaners
 - Anyone else within the security perimeter

Protection Against Insider Threats

- Stage 1: Policies, monitoring and compliance
- Stage 2: Building protection features into systems
- Stage 3: Operational administration and monitoring
- Stage 4: Investigations and digital forensics

Stage 1: Policies and compliance

- Appropriate use of ICT resources
- Authentication and identity management
- Access rights “need to know” or unrestricted
- Irresponsibility, impropriety and fraud
- Computer crime and audit strategies
- Monitoring
- Validation of worker credentials

Without monitoring for compliance, policies are worthless

Stage 2: Building features

- System design safeguards and controls
- Back doors and logical bombs
- Partition of data in support of “need to know”
- Authentication systems
- Storage safeguards
- Review and validation
- (no Easter Eggs, no undocumented functionality, no unknown superusers, etc)

Stage 2: Building features

- Stronger than passwords...
- Gadgets generate a one time password every 60 seconds
- Access to systems requires something that
 - The end user knows (a password)
 - The end user has (the gadget and an unpredictable password)
- The next step up in security requires biometrics

Stage 3: Operational matters

- Identity management and MACs
- Superuser rights management
- Data rights (C, U, R)
- Disclosures and social engineering
- Monitoring tools, privacy and ethics
- Sys Admin

MAC = moves, additions and changes

CUR = create, update, read only

Quality requires discipline

- Clarity in roles and responsibilities
 - Awareness briefings and training
 - Monitoring for compliance with policies and best practices
 - Operational practices documented and applied
 - Appropriate controls for changes, exceptions and emergencies
-
- Blame storming after the event is of little help

Stage 4: Digital forensics

- Determining point of access and containment
- Setting up traps
- Evidence preservation and custody chain
- Evidence analysis and forensic tools
- Collaboration between HR, Internal Audit and I.T.

Insider Job

After the event

- Incident response
- Intrusion detection
- Emergency Response Team
- Problem containment
- Problem resolution
- Restoring normal operations
- (also called digital autopsy)

After the event

- Digital Forensics
- Determine attack mechanism
- Review adequacy of arrangements
- Search for evidence
- Action plan for internal causes
- Action plan for external causes
- Be prepared to trace and prosecute

Evidence

- Legal requirements for seizure, storage, handling, volume and manageability of logs
- Indexing & classification
- Retention & archival
- Media & software
- Right to access
- Right to remove
- Right to destroy

Evidence (2)

- Headaches
- Hard to trace, particularly cross-border
- Hard to quantify losses
- Lack of clarity what is court-admissible
- Litigation
- Contractual issues
- Harassment, bullying, impropriety
- Containable fraud

Evidence (3)

- Criminal litigation
 - Sabotage
 - Industrial espionage
 - Major fraud
-
- Out of court settlements are common

Insider Job

Tests, audits, certification

How do you know you don't have a malicious insider ?

How do you know that your arrangements will work ?

- Tests
- Audits
- Digital autopsy
- Certification e.g. ISO 27001

- Like your annual medical
- It's no guarantee of good health, but it might diagnose a problem
- Who tests the testers?

Organization's metabolic rate

- Ability to recruit and train
- Career progress criteria
- Background vetting/clearances
- Flexible remuneration
- Fast procurement processes
- Budgetary room to breathe
- Culture of openness

From cybercrime to sabotage+

Same skills, same tools, different intent

- Achieve media coverage
- Impact economic systems
- Destabilise civilian life
- Asymmetric warfare against law enforcement
- Hurt trust in governments' ability to protect citizens
- Use “successes” to gain more support for their cause

AND/OR

- Guns, explosives, chemical weapons, bacteriological weapons

Planning for defensive success

- Are traditional infrastructure operations, audits, etc still good enough
- How do we learn how bad guys think and operate
- What can we learn from the “bad guys”
- How do we incorporate this culture into our defences