Plugging The Data Leaks

Ahmad Elkhatib
Security Consultant
khatib@umich.edu

Contents of the Leak

- RFP/RFQ
- Internal Emails
- Intellectual Property
  - Source Code
  - Design Diagrams
- Customer Records

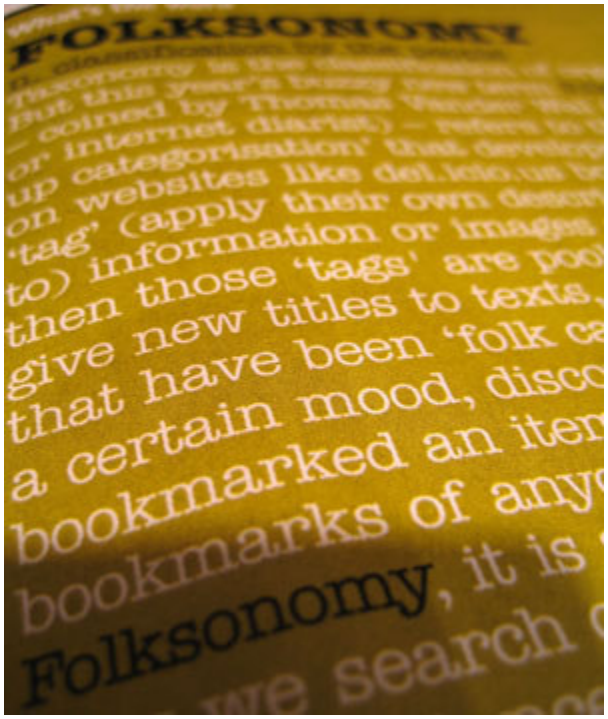
.. Those are usually stored in structured databases or unstructured documents, spreadsheets, etc..

Byproducts of the Leak

- Loss of competitive advantage
- Threats to patent applications
- Fines for violating privacy laws and regulations
- Litigating shareholder and customer lawsuits
- Customer defections due to lack of confidence in security measures
- Loss of market capitalization

How Could the Leak Happen

- Email
- Webmail
- Instant Messenger
- File Transfers / FTP
- USB
- CD/DVD
- Print
- Bluetooth
- Infrared



Is it Happening ?

- 20/7/2007 - SAIC US Military contractor transmits data in clear of 580,000 Military personnel
- 18/6/2007 - Texas A&M head of maths department loses USB flash drive with 8,000 student records while on vacation in Madagascar
- 11/6/2007 – Pfizer laptop exposes 17,000 employee records on P2P network
- 5/5/2007 – Marks & Spencer lost laptop had identity information of 20,000 employees

How to Plug the Leak

How to Plug the Leak

Two Pronged approach :

- Network
- Client

Network

- Firewall
- Content Filtering devices
- Data Leakage prevention devices
- Email / Communication Encryption

Client

- Port Control
- USB Encryption
- USB Read – Only Mode
- CD/DVD Encryption
- Print Control
- Audit / Logging