CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Responding to Data Breaches

October the 23rd, 2009

Brussels, European Parliament

Pascal Lointier
President, **CLUSIF**
Regional IS Risks Advisor, **Chartis**

Agenda

- ☞A wider concern than « Telecom Package »
- ☞French SME-SMIs, some facts
- ☞Insurance/Business Incentives
- ☞Some preventions means and tools
- ☞CLUSIF, a non profit association

A wider concern than "Telecom Package"

We live in a (more and more) digitalized society

- Any size (including SME-SMI)
- Any sector of activity

Various equipments at stake

- Storage media (historically), laptop, CD, DVD, USB stick, Hard Disk disposal…

Wherever the data

- Database (File Server)
- Data Flow (communication)
- "Broadcast" (through social networks)
- Outsourced, clouded…

A wider concern than "Telecom Package"

Nature of content

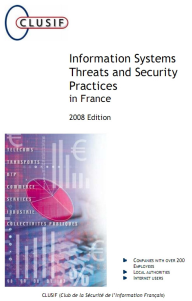
- Financial records (historically)
- ID
- Trade secrets (business espionage)
- …

TWO victims… most of time

- Data "owner" (aka end-user or citizen)
- Enterprise or Local Authority who have been hacked or accidentally disclosed information
  - ☞Indirect or collateral damages

French SME-SMIs, some 2008 facts

Source:



Information Systems
Threats and Security
Practices
in France

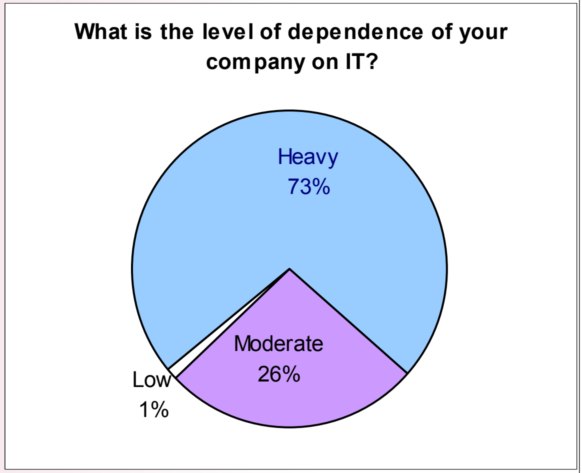
2008 Edition

- Companies with over 200 Employees
- Local authorities
- Internet users

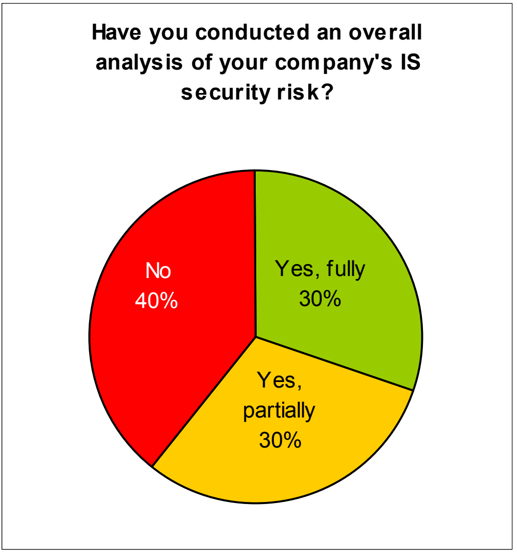
CLUSIF (*Club de la Sécurité de l'Information Français*)

Lack of Risks Assessment

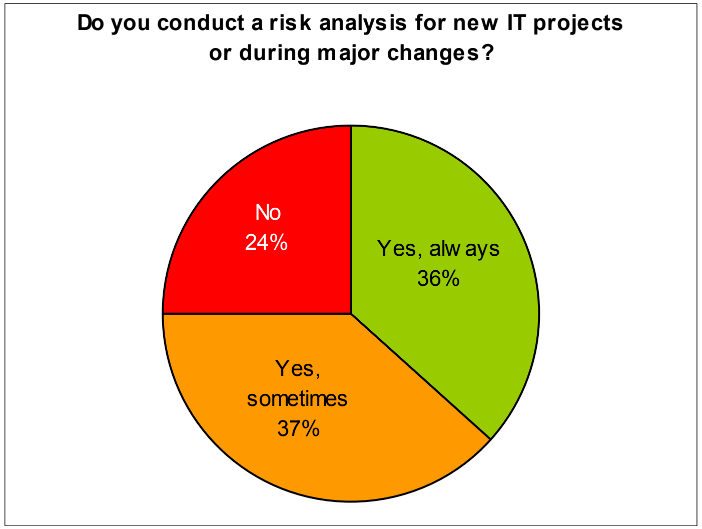
A paradox: Very dependant… very unaware!



What is the level of dependence of your company on IT?



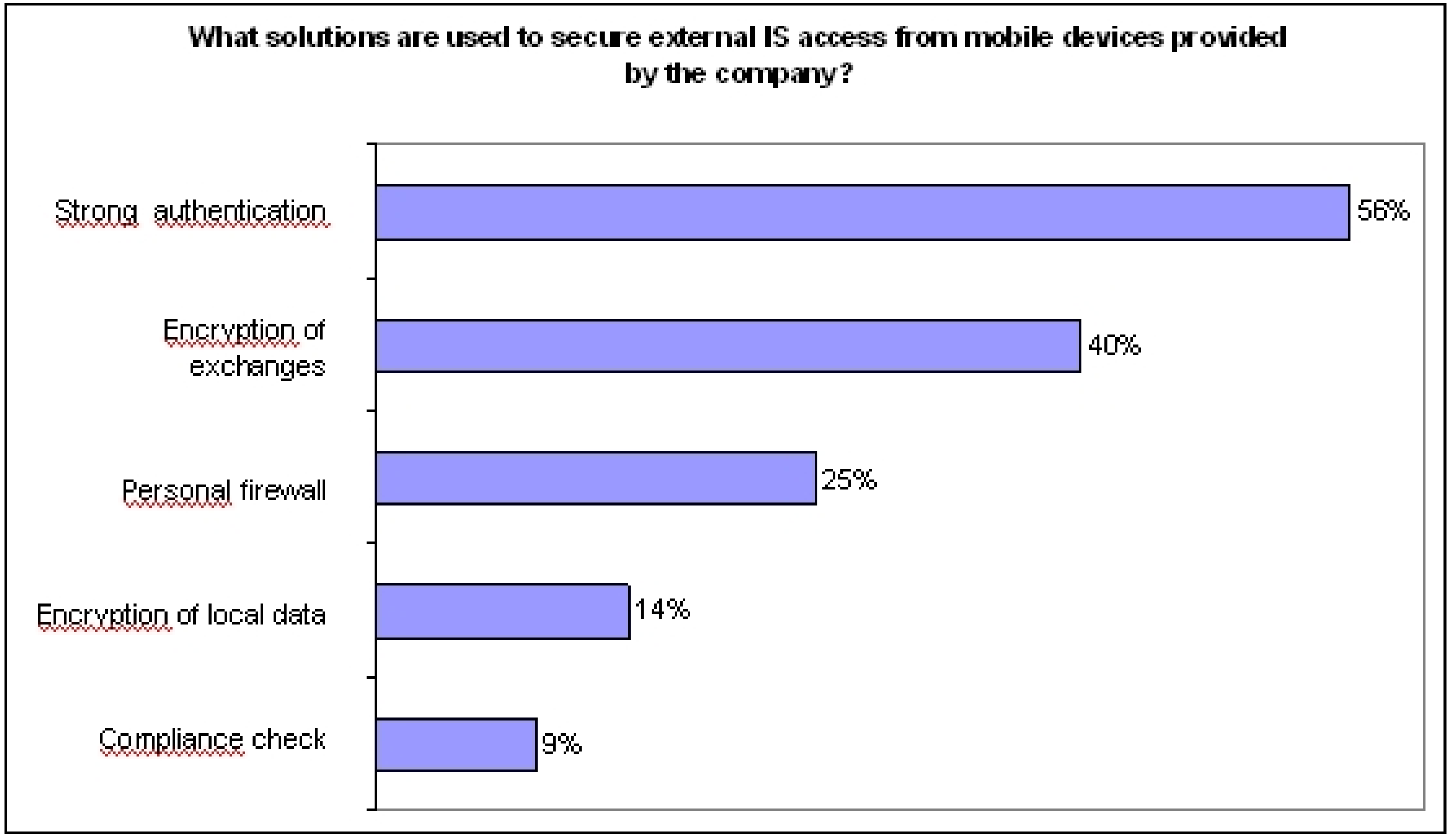
Have you conducted an overall analysis of your company's IS security risk?



Do you conduct a risk analysis for new IT projects or during major changes?

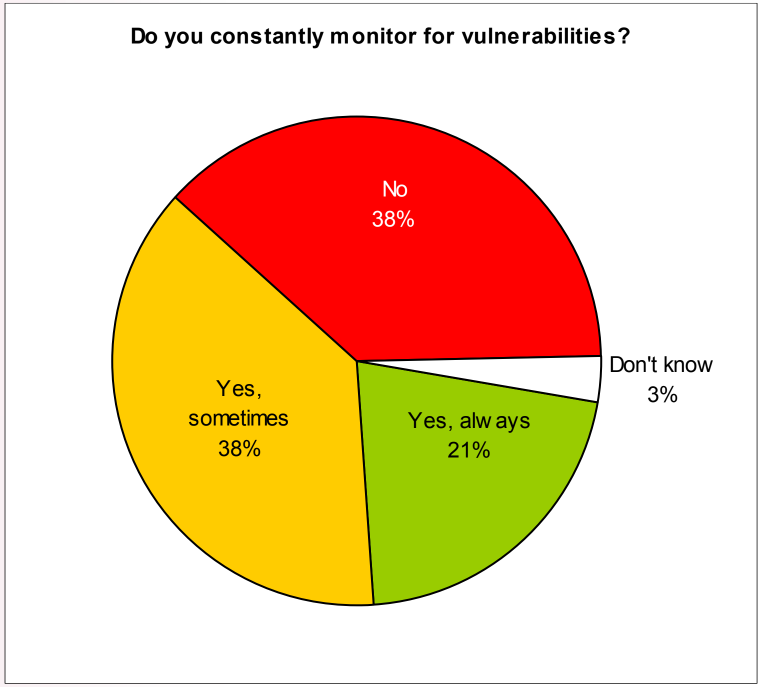
French SME-SMIs, some 2008 facts

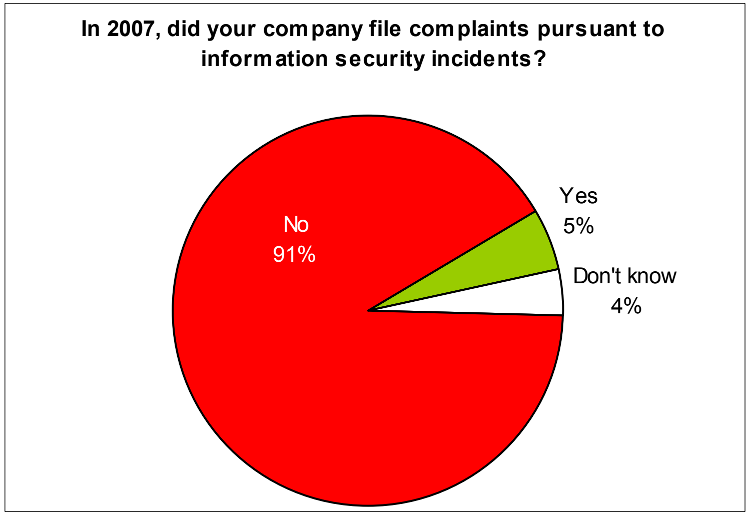
Lack of confidentiality

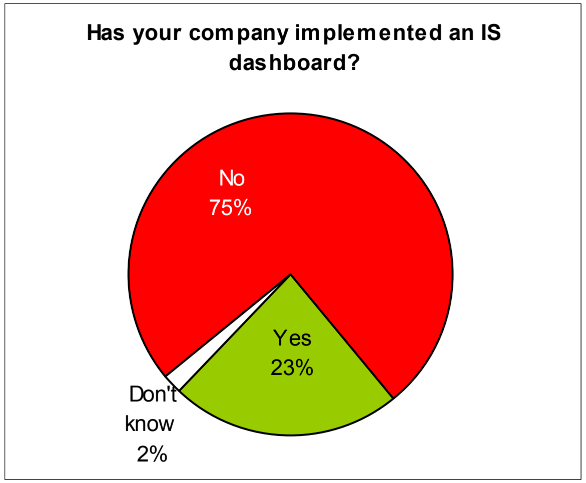


French SME-SMIs, some 2008 facts

Lack of dashboards and logs







- "only 28% of companies evaluate the financial impact of security incidents "

Insurance/Business incentives

Requirement to notify

- you will be much more "inclined" to implement security means if you are exposed to fines or could go to jail (without forgetting reputation)!

Be prepared for an investigation

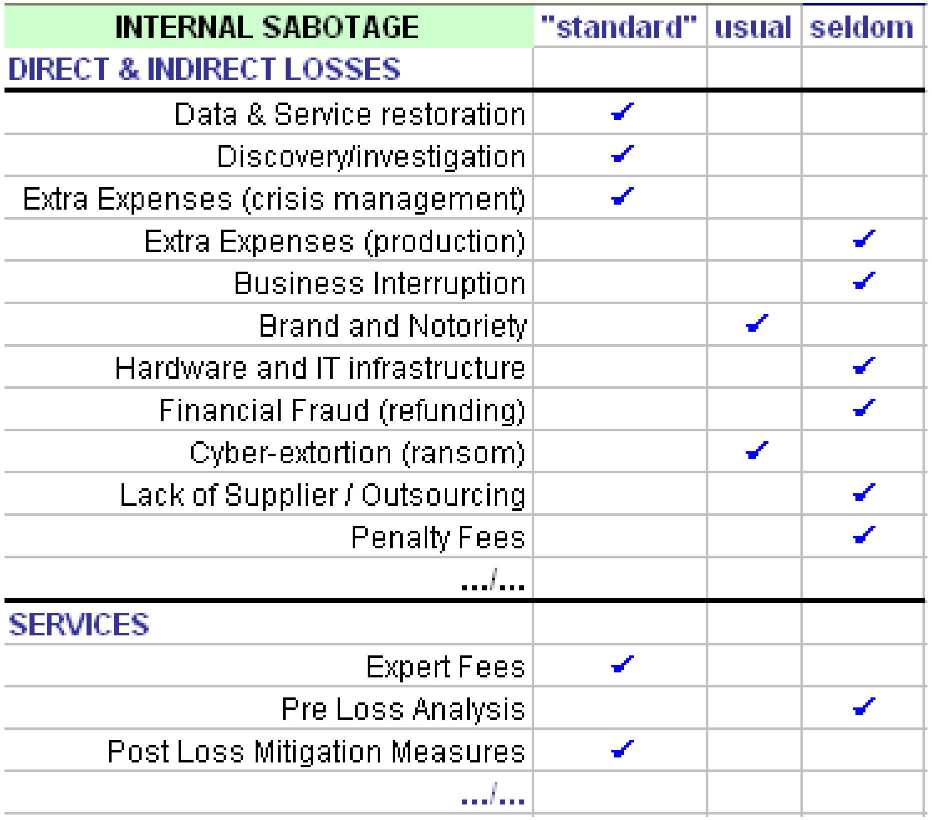
- Penal investigation (making the evidence to help the victimized enterprise)
- Insurance claims settlement
  - ☞Identify cause of loss
  - ☞Quantum of financial impact

Insurance/Business incentives

Think about indirect or collateral damages

- Restoration costs for data, resources, investigation, etc.
- Salaries (extra hours), expert fees, ransom, extra expenses to maintain activity, etc.
- Lack of profit, penalty fees, crisis communication, notoriety and reputation, loss of contracts…
- Possible legal and 3rd party damages, class action, etc.

Indicative matrix to identify possible costs for various scenarios (3 columns qualifying occurrence):



INTERNAL SABOTAGE	"standard"	usual	seldom
DIRECT & INDIRECT LOSSES			
Data & Service restoration	✓		
Discovery/investigation	✓		
Extra Expenses (crisis management)	✓		
Extra Expenses (production)			✓
Business Interruption			✓
Brand and Notoriety		✓	
Hardware and IT infrastructure			✓
Financial Fraud (refunding)			✓
Cyber-extortion (ransom)		✓	
Lack of Supplier / Outsourcing			✓
Penalty Fees			✓
.../...			
SERVICES			
Expert Fees	✓		
Pre Loss Analysis			✓
Post Loss Mitigation Measures	✓		
.../...			

Recent case: Payment Terminal Fraud

New England (USA), March 2008. Hannaford a grocery store chains discovers a credit card breach.
Around 4.2 million numbers were hacked (card number, expiry dat but not the cardholder name). The information obtained was sent overseas.
The breach began in December. 300 servers were affected, in stores in Florida (106), New England (165) and in franchises (24).

Consequences

- 1.800 proven cases of fraud over the course of March
- Re-issuing fees for approx. 100,000 cards
- $5 million class action suit led by a firm law
- Millions of dollars invested in security: encryption of data in transit, 24-hour monitoring system
- Hannaford compliant with the PCI-DSS standard… which was quickly modified to account for the operating mode!

Recent case: Data theft and Ransom Demand

Saint-Louis (USA), November 2008. Express Scripts a company which manages medical prescription information is blackmailed via e-mail (threat to release 75 patient files, information on millions of patients is stored on database).

Ransom amount is not disclosed to the public but as some consequences

- Creation of a crisis website to inform patients and manage complaints
- Identity restoration service offered by consultant/security firm
- Commitment to pay any monetary losses
- Use of an investigation firm
- $1 million reward offered helped to catch the blackmail artists!

Summing-up, some preventions means and tools

☺ Requirement to notify

☺ Cipher tools implementation

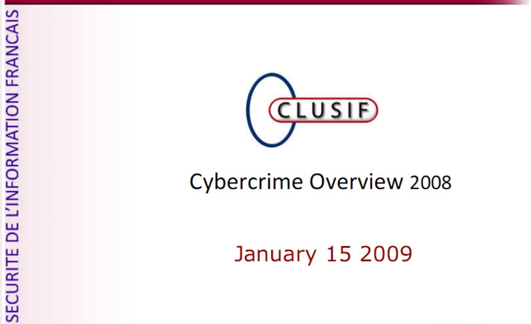
☺ Risks assessment promotion toward SME-SMI (Grundschutz, eBios, MEHARI, etc.)

- ISO checklist or « best practices » is not sufficient enough
- Compliance doesn't mean security (see numerous ISO 27001 hacked or damaged enterprise and defrauded PCI-DSS compliant enterprises)
- Security leads to compliancy

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

www.clusif.asso.fr a non profit computer security association

Free downloads…

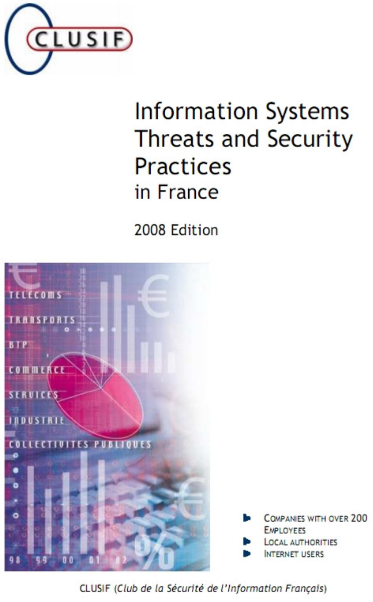


CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

CLUSIF

Cybercrime Overview 2008

January 15 2009



CLUSIF

Information Systems Threats and Security Practices in France

2008 Edition

- Companies with over 200 employees
- Local authorities
- Internet users

CLUSIF (*Club de la Sécurité de l'Information Français*)

CLUSIB (Club de la sécurité informatique belge)
8, Rue des Sols
1000 Bruxelles
Contact :
Tel : + 32 2 515 08 57
Fax : + 32 2 515 09 85
Secrétariat : Jan Steenlant
Web : http://www.clusib.be/.

CLUSSIL (Club de la sécurité des systèmes d'information Luxembourg)
c/o CRP Henri Tudor
29 rue John F. Kennedy
L-1855 Luxembourg - Kirchberg
Contact :
Tel : + 352 42 59 91 206
Fax : + 352 42 48 99
Secrétariat : Anne Gaspard
Web : http://www.clussil.lu/tiki-view_articles.php.

CLUSIS (Association suisse pour la sécurité des systèmes d'information)
Case postale 9
CH 1026 Lausanne
Contact :
Tel : + 41 21 636 32 39
Fax : + 41 21 636 32 38
Secrétariat : Patricia Probst.
Web : http://www.clusis.ch/.

CLUSIT (Associazione Italiana per la Sicurezza Informatica)
Università degli Studi di Milano
Dipartimento di Scienze dell' Informazione
Via Comelico 39, 20135 MILANO
Contact :
Tel : + 39 349 776 8882
Fax : + 39 02 700 440 566
Secrétariat.
Web : http://www.clusit.it/.

CLUSI Burkina Faso
Adresse Postale: 01 BP 521 Ouagadougou 01 Contact :
Tel : (226) 70 27 36 86 ou (226) 70 28 48 48
M. Youn SANFO.
Web : http://www.clusibf.org/.