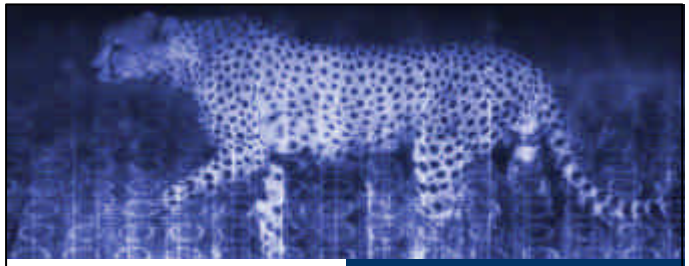


Finmatica
Expanding World

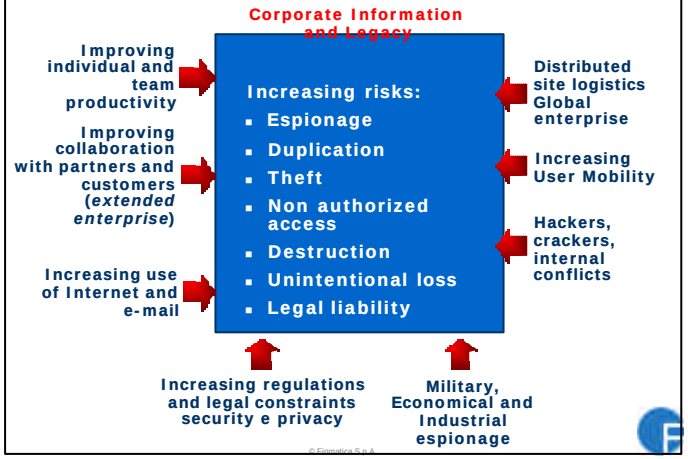
Safeguarding Corporate Information Assets and Legacy

Mario Sforza
Global Forum 2003
Rome, 6-7 November 2003

Summary

- Threats for corporate information assets
- Information security awareness
- Computer crime: myths and realities
- Security of email communications
- Security on PCs and mobile devices
- Security of IT infrastructures
- Finmatica solution to safeguard critical corporate information

Corporate information: current needs and threats



Information security awareness (1)

In the last three decades, the growing needs to increase enterprise efficiency and market global presence have triggered a massive increase in the use of IT tools with two main consequences :

- The corporate information legacy (projects, reports, price lists, deals, HR data, etc.) is available in 'any' types of electronic formats and on 'any' kinds of logical and physical devices (file, email, database, desktop, laptop, pda, mail server, file server, etc.);
- The need to transmit/share/access information is paramount

Information security awareness (2)

Additional “obvious” considerations…….

- The corporate messaging network infrastructure represents the *‘de facto’* repository of the entire corporate knowledge base;

- PCs (desktop or laptop) can have actual value of a few thousands of Euro but potentially are worth millions of Euro in terms of critical information stocked;

- IT system administrators (network, email, application SW, back up, etc.) have access to the entire corporate information assets;

- The email database of your PC contains the majority of your *personal* and *professional* legacy.

Information security awareness (3)

But…

1. US companies claim that **theft** of strategic and critical corporate information represents the main cause of their financial loss due to computer crimes (2,5 times more than virus attacks);
2. 50% of US companies (71% of respondents) don’t report computer crime incidents to law enforcement agencies due to:
   - Negative publicity
   - Competitors would use to advantage
3. Only 62% of US companies is able to quantify the number of computer crime incidents occurred in the last 12 months, and 33% can’t say how many came from the inside;
4. 75% claim financial losses, but only 47% is able to quantify them.

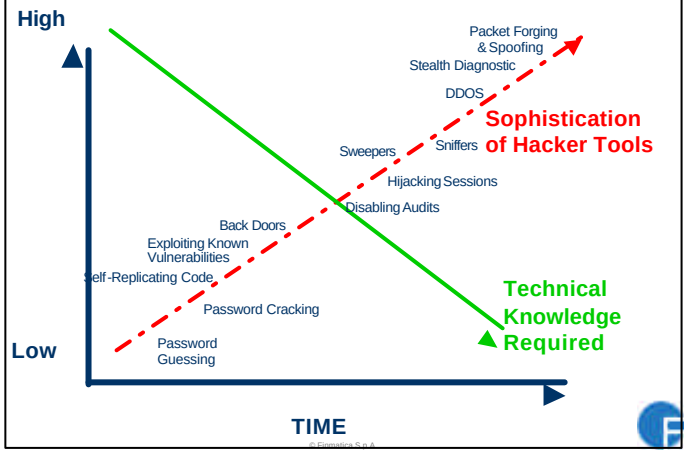
Source CSI/FBI 2003 Computer Crime and Security Survey

Information security awareness (4)

…so awareness on key IT security issues is essential but still low. Meanwhile, our view……..

1. damages reported as internal attacks tend to *underestimate* the real relevance of the problem (estimates provided by companies “attacked” are usually very conservative);
2. too many organizations do not take *appropriate* steps to safeguard their corporate information assets from the inside, while they massively invest in border security solutions;
3. information security is still seen as a cost to bear, after an incident has occurred, rather than a *preventive* positive action or a business opportunity.

Does computer crime require an IT genius? (1)



Does computer crime require an IT genius? (2)

Q1: In order to steal your CEO's PC laptop, is it necessary to be an IT genius?

A1: Not so, as long as you got limited robbery skills and spare time to wait for him at the hotel or airport lounges !

Q2: And in order to crack your CEO's Windows password, is then again necessary to be an IT genius?

A2: Not really, an IT C level grade will do! Enjoy your Google surfing session entering "*password recovery for Windows*"!

The security of communications via email (1)

- E-mail is the most frequently used communication tool, especially for business purposes.
- Quantity and volume of information transported by e-mail is by far more relevant than any other communication platform

…….however…….

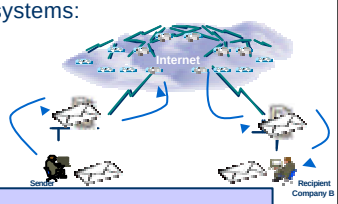
Did you ever consider the number of systems through which your emails are routed?

Did you ever count the number of systems where these emails could be buffered in, at the end of the communication flow?

The security of communications via email (2)

For example, User of Company A sends an email to an user of Company B. At the end of the communication flow, this email will probably stay on at least 4 systems:

- sender PC;
- recipient PC;
- sender mail server;
- recipient mail server.



Are you confident that you are able to control the security of this communication process?

If this email carries business critical information, it could be worth to evaluate solutions (available right now!) in order to be sure that this email will be only available for the sender and the intended recipient.

The security of communications via email (3)

A real (negative) case: on April the 28th the Security Exchange Commission has convicted several American finance research analysts, ordering to pay civil money penalties for millions of dollars.

They were found guilty of violating NASDAQ and NYSE Rules "by publishing misleading, exaggerated, unbalanced financial information" about several stocks on NASDAQ and NYSE.

The major and most significant proofs have been obtained by the investigators acquiring emails from their PCs!

Source:
http://www.sec.gov/litigation/complaints/comp18111b.htm

The security of information on PCs and mobile devices (1)

The current business scenario and the growing global and ubiquitous nature of an enterprise call for an increasing mobility of professionals.

At network level, laptops and PDAs meet such nomadic needs providing professionals and employees with powerful computing and access technologic solutions, thus enhancing individual and group productivity…

However this distributed and remote access pose greater risk for the enterprise information assets…

This **risk is** too often **underestimated**, even in

organizations with an advanced ICT infrastructure.

The security information on PCs and mobile devices (2)

A recent survey made in the UK by Infosecurity Europe and published on Computer Weekly, showed that 73% of Companies don't apply any security policy regarding mobile devices.

As for PDAs, 57% are completely non protected.

…..not to mention wifi security……

The security of information on the ICT infrastructure

The elements of an IT enterprise infrastructure which are particularly critical from an information security standpoint are:

- Local Area Network;
- Mail Delivery System;
- Back Up Infrastructure;
- Storage Area Network.

On any of these systems there are always relevant parts of the enterprise information assets and legacy, either archived or in transit.

The risk to have even minimal loss of strategic information and data from insiders fraudulent attacks is too high if security policies and technology countermeasures are not properly regulated, implemented and monitored.

Security begins with sound Security Policies

Organization must determine internal **procedures** and solid **standards** in order to define well thought out Security Policies

The defined **Security Policies** set the tone and legal precedent to design an effective security program. The security program should include and define internal standards and procedures as well as solutions and products that implement the security requirements

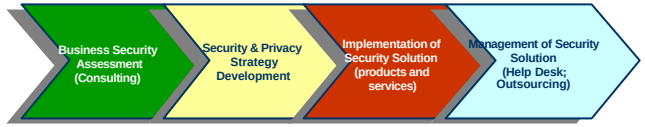
The overall **security program** can then be implemented and managed using the solid standards and proven procedures as a sound foundation

Finmatica Advanced Technologies and Information Security

Finmatica offers a complete and integrated solution for the protection of any enterprise corporate information assets and legacy:

- A suite of products with solutions for the protection, secure transmission and archiving of data, using advanced encryption, digital signature and strong authentication technologies;
- A Business Information Risk Management team: legal, business process engineering and consultancy, even for compliancy checks and monitoring with legal and regulatory requirements and international standards;

The e-security value chain



- **Business Consulting and Processes/Organisation**
- **Data/application, network and physical security**
- **Planned hack (penetratio test)**
- **Risk evaluation**
- Opportunity-cost evaluatior Third-party security

- **Privacy policy**
- Network architect
- Security product assessment
- Back-up/data-recovery process

- **Security products (Sw)**
- Sys Integration, **implementation Services**
- **Application/data security**
- **Education & training**
- Security products (Hw)
- Network security
- Physical security

- **Maintenance & Support**
- **Ongoing benchmarking**
- Network/firewall management
- Data management
- Intrusion/fraud detection
- Outsourcing (total; fleet; ASP; Help Desk..)
- Hosted Services

Source: **Gartner**

In **bold** Finmatica info security offer

Our approach to safeguard the Enterprise Information Legacy