

# Sicurezza Informatica in Italia



*DICo*

---

Danilo Bruschi  
Dip. di Informatica e Comunicazione  
Università degli Studi di Milano

# Sicurezza Informatica: cos'è



*DICo*

- Una patologia che colpisce, in forme più o meno gravi, tutti i sistemi informatici e per la quale ad oggi non sono noti rimedi definitivi
- La patologia si diffonde con maggiore virulenza in ambienti con un livello elevato di informatizzazione

## Gli effetti



- Furto di informazioni sensibili
- Modifica di informazioni critiche
- Disservizi nelle attività di rete
- Blocco di attività critiche
- Danneggiamento degli asset

# Le conseguenze



- Perdita d'immagine verso l'opinione pubblica
- Perdita d'immagine verso i propri clienti
- Perdita del competitive advantage
- Mancato rispetto di regole contrattuali
- Mancato rispetto delle leggi
- Coinvolgimento in procedimenti processuali



*DICo*

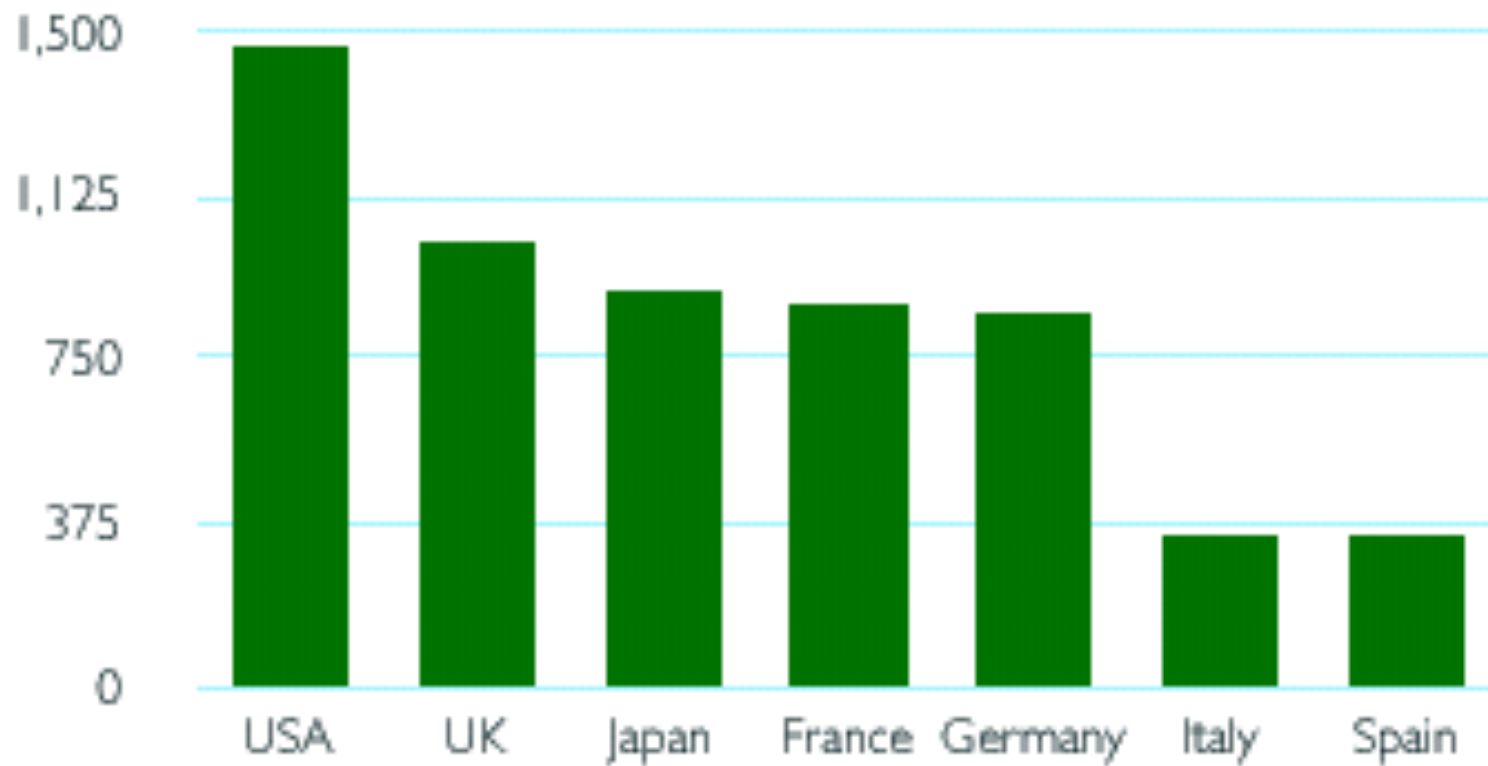
---

Una prima visione macroscopica del  
fenomeno

# IT in Italia (1)



■ IT spesa pro capite (Euro) - Fonte Assinform 2008

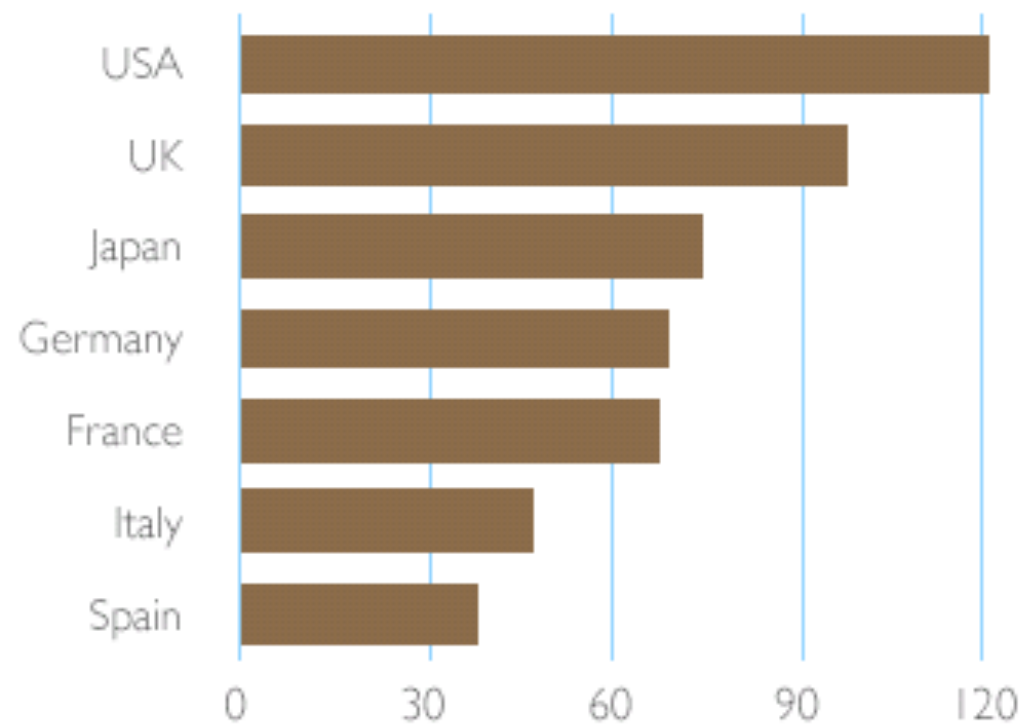


# IT in Italia



*DICo*

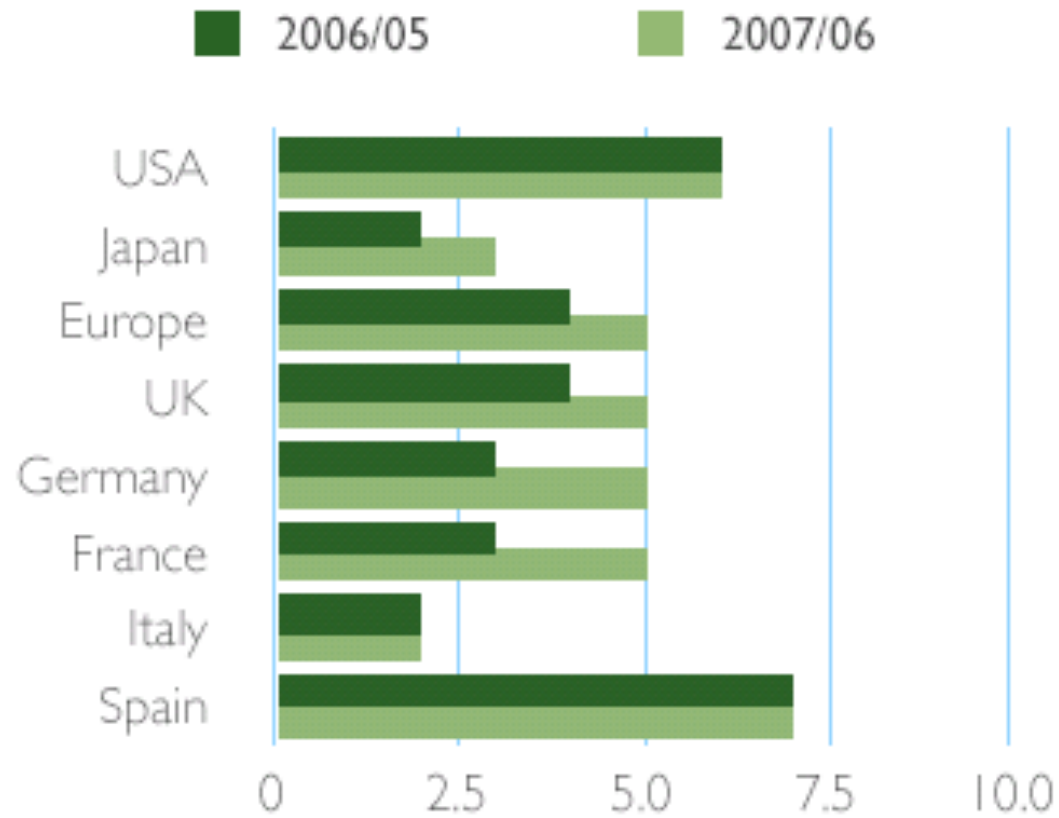
■ N° PC per 100 abitanti, Fonte Assinform 2008



# IT in Italia



DICo



*Crescita del mercato IT  
(Fonte Assinform 2008)*

## Il in Italia: conclusioni



*DICo*

- In sostanza dal punto di vista dell'IT siamo un paese arretrato
- Secondo la Intelligence Unit dell'Economist in una classifica dei primi 66 paesi più competitivi in termini di uso dell'IT siamo al 25° posto, in Europa siamo davanti solo a Portogallo e Grecia

# Ma non tutto il male viene per nuocere?



- La patologia si diffonde con maggiore virulenza in ambienti con un livello elevato di informatizzazione



*DICo*

---

## Uno sguardo allo stato della Sicurezza Informatica in Italia

# ICT Security in Italia



DICo

Current Rank	Previous Rank	Country	Current Regional Percentage	Previous Regional Percentage	Current Global Percentage	Average Lifespan (days)	Command-and-Control Percentage
1	1	Germany	18%	23%	10%	1	22%
2	2	Spain	14%	15%	7%	3	3%
3	4	Italy	10%	9%	6%	3	6%
4	7	Poland	10%	6%	6%	3	2%
5	3	France	9%	11%	5%	3	6%
6	5	United Kingdom	7%	9%	4%	4	11%
7	9	Turkey	6%	2%	3%	2	5%
8	6	Israel	5%	6%	3%	3	2%
9	11	Russia	3%	2%	1%	7	5%
10	8	Portugal	3%	2%	1%	2	1%

**Table 4. Bot-infected computers by country, EMEA**

Source: Symantec Corporation

# ICT Security in Italia



Current Rank	Previous Rank	City	Country	Current Regional Percentage	Previous Regional Percentage
1	1	Madrid	Spain	7%	8%
2	7	Ankara	Turkey	6%	2%
3	20	Cagliari	Italy	3%	1%
4	9	Warsaw	Poland	3%	2%
5	12	Wroclaw	Poland	3%	2%
6	3	Rome	Italy	2%	3%
7	8	Lisbon	Portugal	2%	2%
8	4	Milan	Italy	2%	3%
9	13	Rabat	Morocco	2%	2%
10	11	Moscow	Russia	2%	2%

**Table 5. Bot-infected computers by city, EMEA**

Source: Symantec Corporation

# ICT security in Italia



DICo

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage	Bt Rank	Command and Control Server Rank	Phishing Web Sites Rank	Malicious Code Rank	Spam Messages Rank	Attack Origin Rank
1	1	Germany	18%	19%	1	1	1	3	1	1
2	2	United Kingdom	11%	11%	6	2	4	1	8	3
3	3	France	9%	9%	5	6	3	6	4	4
4	5	Spain	8%	8%	2	10	9	4	6	2
5	4	Italy	8%	8%	3	4	7	5	3	5
6	6	Poland	5%	5%	4	13	8	10	5	6
7	9	Turkey	5%	3%	7	8	20	12	2	7
8	8	Netherlands	5%	4%	15	5	2	9	19	10
9	10	Russia	4%	3%	9	9	5	17	7	14
10	11	Sweden	3%	2%	17	3	6	16	34	9

**Table 1. Malicious activity by country, EMEA**

Source: Symantec Corporation

# ICT Security in Italia: conclusioni



*DICo*

Il problema si è manifestato e in dimensioni non trascurabili.  
Qual è l'atteggiamento più diffuso per affrontarlo?



*DICo*

---

# L'INDIFFERENZA

# Perché?



- Ritardo tecnologico mai compensato e scarso interesse alle innovazioni tecnologiche
  - in ambito aziendale il passaggio dal main frame alla rete non è stato ancora completamente assorbito!!!
  - arretratezza culturale nella domanda
  - arretratezza culturale nell'offerta

# Un'analisi del sistema



- Le componenti principali del sistema sono:
  - La domanda
    - Aziende
    - PA
    - Utenti
  - L'offerta
    - i costruttori di soluzioni tecnologiche
    - i venditori di soluzioni tecnologiche
    - le società di consulenza
  - Gli altri
    - l'università
    - i media
    - la società civile

# AZIENDE/PA



*DICo*

- Il management è principalmente costituito da persone che si sono formate negli anni '70/'80 quando la RETE era un concetto astratto
- “The computer is the network” non è solo uno slogan ma un concetto di non facile comprensione, le cui implicazioni in termini di sicurezza sono devastanti
- Di fatto il top management del sistema Italia (a partire dalle più alte sfere) ignora il problema
- Maggiore attenzione al problema da parte di PA, Banche e grandi aziende, grazie all'attività di quadri intermedi (solitamente più giovani)
- Nella PMI la situazione è molto critica

- Anche quando c'è consapevolezza l'atteggiamento più diffuso è comunque quello di ignorare il problema o nel migliore dei casi affrontarlo in maniera molto superficiale
- I costi per predisporre un piano di sicurezza non sono in genere trascurabili e si preferisce assumere il rischio
- Questa strategia in molti casi però può non essere praticabile !!!

## Utenti finali



*DICo*

- Sicura la fascia più debole del sistema, caratterizzati da una scarsa preparazione tecnologica e da diversi anni bersaglio principale di attacchi informatici
- Necessiterebbero di un maggiore supporto operativo
- La sicurezza di un sistema è quella dell'anello più debole della "catena"



*DICo*

---

L'offerta: vista la dimensione ridotta della domanda, l'offerta ne rispecchia le caratteristiche soprattutto in termini qualitativi

## I costruttori



*DICo*

- Esistono sul mercato una serie di soluzioni tecnologiche valide per far fronte al problema sicurezza informatica
- smart-card, network scanner, firewall, intrusion detection/prevention system, log analyzer, antivirus ecc. ecc.
- L'Italia è di fatto fuori da questo mercato

# I venditori



*DICo*

- Il numero di venditori di prodotti di sicurezza informatica è cresciuto a dismisura in questi ultimi anni
- Spesso sono chiamati a risolvere problemi non di loro competenza (disegno e progettazione di architetture di sicurezza)
- In molti casi le loro competenze si limitano a saper avviare in configurazione di default i prodotti che vendono

# Le società di consulenza



- Mercato egemonizzato oramai dai grossi player del settore
- In rari casi dispongono di personale all'altezza della situazione, anche loro devono recuperare un ritardo culturale nel settore
- Sfruttano l'incompetenza sul problema molto diffusa a livello di domanda



*DICo*

Gli altri

# Le Università



*DICo*

- Hanno la responsabilità di formare i nuovi quadri
- Da diversi anni erogano corsi di sicurezza informatica
- La sicurezza però non attira fondi di ricerca (sia pubblici che privati) e quindi è estremamente difficile attrarre docenti e ricercatori ad operare nel settore

## I media



*DICo*

- Potrebbero contribuire ad accrescere la consapevolezza sul problema
- Tecnicamente poco preparati
- Sempre in cerca dell'informazione d'effetto
- Poco interessati a fare informazione sul tema

# La società civile



*DICo*

- CERT-IT: tra le prime organizzazioni a occuparsi di sicurezza informatica nel nostro paese (1993)
- CLUSIT: fondato nel 2000, tra le più grosse associazioni europee che si occupano del tema
- Entrambi ben inseriti e rispettati nella comunità internazionale
- Meriterebbero una maggiore attenzione da parte delle istituzioni

# Conclusioni



*DICo*

- Nella società dell'informazione non esiste “competitive advantage” che prescindenda da una infrastruttura ICT sicura e affidabile
- In Italia il problema non si è sinora posto seriamente solo perché il paese è di fatto in termini di IT, sotto sviluppato
- Il ritardo culturale in termini di competenze nel settore dell'IT è la principale problematica che caratterizza il settore della sicurezza IT in Italia
- Dobbiamo avviare al più presto un nuovo piano di informatizzazione del paese che sia effettuato nel rispetto dei requisiti di sicurezza



*DICo*

---

GRAZIE DELL'ATTENZIONE!!