

# Il ruolo della sicurezza ICT nell'e-government

Danilo Bruschi  
Dipartimento di Informatica e Comunicazione  
Università degli Studi di Milano  
bruschi@ dico.unimi.it



UNIVERSITÀ DEGLI STUDI DI MILANO/ *DICo*

## L'evoluzione di Internet

- Dal punto di vista delle applicazioni lo sviluppo di Internet può essere suddiviso in tre diverse fasi:
  - la fase della ricerca in cui i principali fruitori di Internet erano gli enti di ricerca e le università
  - la fase delle applicazioni corporate in cui le potenzialità di Internet sono state sfruttate dalle aziende per attività di business
  - la fase dell'e-government. Questa fase in tutti i paesi è succeduta a quelle precedenti e coincide con la presa di coscienza delle potenzialità di Internet come mezzo di comunicazione di massa



UNIVERSITÀ DEGLI STUDI DI MILANO/ *DICo*

Danilo Bruschi

## e-government

- Attraverso le applicazioni di e-government lo Stato tenta
  - un riavvicinamento ai cittadini attraverso l'abbattimento di barriere innalzate da burocrazie non sempre giustificate
  - di riavvicinare i cittadini alla vita politica del paese con le applicazioni di e-democracy (ad es. Internet voting)
  - di dare al cittadino un'immagine di efficienza



## e-government

- Con e-government lo stato quindi vuole fornire ai propri cittadini una nuova immagine di se, imperniata sull'efficienza e sulla disponibilità
- Lo fa affidandosi alle nuove tecnologie dell'informazione e della comunicazione in particolare a Internet



## E-government vs. Informatizzazione

- Informatizzazione: processo mirato al miglioramento dell'efficienza interna di una amministrazione attraverso il ricorso a ICT.  
**Focus primario la PA.**
- E-Gov: processo mirato alla smaterializzazione e delocalizzazione del rapporto cittadino-PA, e a ad un maggior coinvolgimento del cittadino nella vita pubblica. **Focus: il cittadino.**




## Internet

- La storia ci insegna però che l'uso di Internet non è solo fonte di vantaggi, ma porta con sé molti rischi legati all'insicurezza dei sistemi ICT
- Dal 1987 in poi sistemi appartenenti alle più disparate organizzazioni (governative, banche, aziende private) sono stati vittime di attacchi informatici che:
  - possono ridicolizzare i siti visitati (CIA, [DoJ](#), Pentagono)
  - bloccare l'utilizzo per qualche ora o per intere giornate i servizi offerti
  - rubare informazioni sensibili
  - distruggerne il contenuto informativo




**1020 757**




United States  
Department of  
Injustice

This page is in violation of the Communications Decency Act!

Special words from our Forefather George Washington



Move my grave  
to a free country!  
This rolling is making



UNIVERSITÀ DEGLI STUDI DI MILANO/ **DICo**

Danilo Bruschi

### La sicurezza e Internet

**Online Shopping Usage (X)**  
**Creating Awareness (Y)**

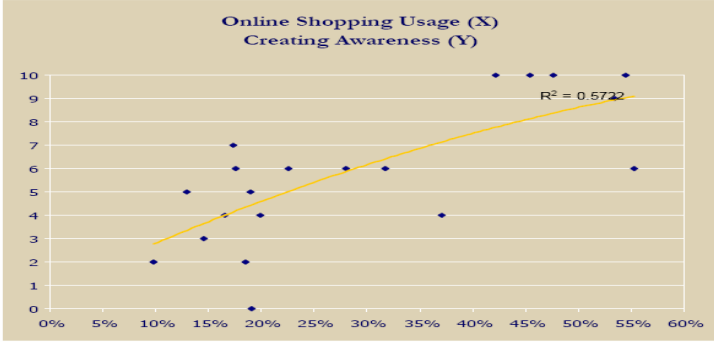



Figure 17. Online shopping usage versus the awareness scores of the EU countries



Fonte Deloitte  
UNIVERSITÀ DEGLI STUDI DI MILANO/ **DICo**

Danilo Bruschi

## e-government (criticità)

- Ovviamente un governo che decide di ricostruire il proprio rapporto con il cittadino attraverso Internet deve prestare molta attenzione a non cadere vittima della stessa
- L'effetto potrebbe essere assolutamente controproducente, verrebbe meno la fiducia degli utenti e si darebbe l'immagine di uno stato arretrato ed incapace di gestire le moderne tecnologie



## I beni da proteggere

- In un sistema di e-gov questi alcuni dei beni coinvolti:
  - Dati sanitari
  - Dati giudiziari
  - Dati Finanziari
  - Fiducia del cittadino verso le istituzioni
  - Compiacimento del cittadino verso gli amministratori
  - Stima del cittadino verso il governo



## Quale il rischio

- Il rischio viene calcolato come il prodotto:  
$$\text{Rischio} = \text{Danno} \times \text{Probabilità di Accadimento}$$
- Qual è il danno legato alla perdita di stima da parte dei cittadini?
- Quale governo è pronto ad accollarsi questo rischio?



## e-government (criticità)

- In ambito aziendale il problema della sicurezza informatica è alla fine un problema di gestione del rischio
- In ambito di e-government questa alternativa viene meno. **In ogni caso** il rischio va ridotto, pena la perdita di credibilità
- La sicurezza informatica diventa quindi un aspetto caratterizzante di ogni applicazione di e-gov, che deve prevederla come parte integrante



## Quali problemi

- La sicurezza nei servizi di e-gov è però la fine di un percorso non l'inizio
- Affinché ci possa essere sicurezza nell'e-gov è necessario che la stessa sia stata introdotta in tutti i processi di supporto all'e-gov
- La sicurezza dell'e-gov non può prescindere dalla sicurezza del gov quindi:
  - Degli organi di governo
  - Dell'intera PA



## Quali problemi

- In questo contesto la sicurezza dell'e-gov è solo un nuovo aspetto di un vecchio problema:
  - LA TUTELA DELLE INFORMAZIONI E L'EFFICIENZA DEI SERVIZI
- Non si può pensare di fare e-gov, senza rivedere i processi amministrativi e senza ridefinire ruoli e regole
- In questo senso fare e-gov coincide anche con modernizzazione della PA



## IL 1° Passo

- Devono essere emanate dal più alto livello di governo le strategie nazionali per la Sicurezza ICT
- L'implementazione delle stesse deve essere delegata a un organismo nell'ambito della Presidenza del Consiglio dei Ministri o alternativamente ad un ministro con delega specifica o a due/tre ministri



## ...e successivamente

- Definire un framework generale in cui siano specificati tutti i requisiti di sicurezza delle diverse componenti del sistema di e-gov in accordo con la strategia di sicurezza nazionale
- Devono essere definite politiche per vari sottosistemi:
  - Identificazione/autenticazione
  - Protezione delle Infrastrutture
  - Assurance
  - Confidenzialità delle Informazioni
  - Ecc. ecc.



... e successivamente

- In tutti i progetti per l'e-government devono essere inserite una serie di specifiche affinché gli stessi prevedano il soddisfacimento dei suddetti requisiti di sicurezza
- Tali requisiti dovranno essere definiti in funzione del tipo di applicazione considerata nell'ambito del progetto e dei dati su cui la stessa opera



Quanto siamo distanti da questo obiettivo?



		Awareness	Best practice	Alerts	Networking	Standards
<b>AT</b>	Austria	6	8			8
<b>BE</b>	Belgium	6	5	6		9
<b>CZ</b>	Czech Republic	6	5			1
<b>DE</b>	Germany	10	10	3		5
<b>DK</b>	Denmark	6	2	0	2	5
<b>ES</b>	Spain	4	8	9	9	8
<b>FI</b>	Finland		10	10	3	
<b>FR</b>	France	6	8	7	6	8
<b>GB</b>	United Kingdom	10	10	7	7	8
<b>GR</b>	Greece	2	0	5	0	7
<b>HU</b>	Hungary	3	2	2	4	2
<b>IE</b>	Ireland	10	8			8
<b>IS</b>	Iceland	1	1	5	5	0
<b>IT</b>	Italy	6	3	2	2	3
<b>LT</b>	Lithuania	2	0	2	2	3
<b>LU</b>	Luxembourg	4	6	2	2	
<b>LV</b>	Latvia	5				
<b>MT</b>	Malta	5	5			
<b>NL</b>	Netherlands	10	1	10	9	9
<b>NO</b>	Norway	3	7	7	8	5
<b>PL</b>	Poland	7	7	7	7	
<b>PT</b>	Portugal	4		5	5	
<b>SE</b>	Sweden	9	7	9	2	6
<b>SI</b>	Slovenia	5		2		
<b>SK</b>	Slovakia	2				



UNIVERSITÀ DEGLI STUDI DI MILANO/ **DICo**

Source: Deloitte

Danilo Bruschi

Grazie !!!



UNIVERSITÀ DEGLI STUDI DI MILANO/ **DICo**