FIDA INFORM

Incontro ClubTI Milano: "Attacchi Informatici"
Assolombarda - Milano
25 gennaio 2010

Gli attacchi informatici ed i dati per l'Italia del Rapporto OAI 2009

Marco Bozzetti

VP FidaInform, Past President ClubTI

Malabo Srl (www.malaboadvisoring.it), GeaLab Srl (www.gea.it)

ClubTI
Club per le tecnologie dell'informazione

OAI, Osservatorio Attacchi Informatici in Italia

- **Che cosa è**
  - **Indagine annuale sugli attacchi ai Sistemi Informativi di Aziende e Pubbliche Amministrazioni in Italia condotta attraverso un questionario on-line indirizzo a CIO, CISO, CSO ed ai consulenti che si occupano di sicurezza informatica**
- **Chi lo attua**

FIDA INFORM

Club TI – Club per le tecnologie dell'informazione

SOIEL INTERNATIONAL – Eventi e riviste per l'organizzazione aziendale

- **Con la collaborazione di**

polizia delle comunicazioni

- **I patrocinatori**

aipsa – Associazione Italiana Professionisti Security Aziendale

aipsi

ASSOLOMBARDA

FTI – FORUM per la TECNOLOGIA della INFORMAZIONE

Inforav – Istituto per lo sviluppo e la gestione avanzata dell'informazione

Obiettivi OAI

- Avere cadenza periodica annuale
- Coinvolgere tutte le Associazioni e gli Enti coinvolti e/o interessati nella sicurezza informatica
- Divenire uno strumento di ausilio nell'Analisi del Rischio ed il punto di riferimento nazionale sulla sicurezza ICT, analogamente a quanto avviene con il Rapporto CSI statunitense
- Far conoscere e sensibilizzare i vertici delle Aziende/Enti sui problemi della sicurezza ICT

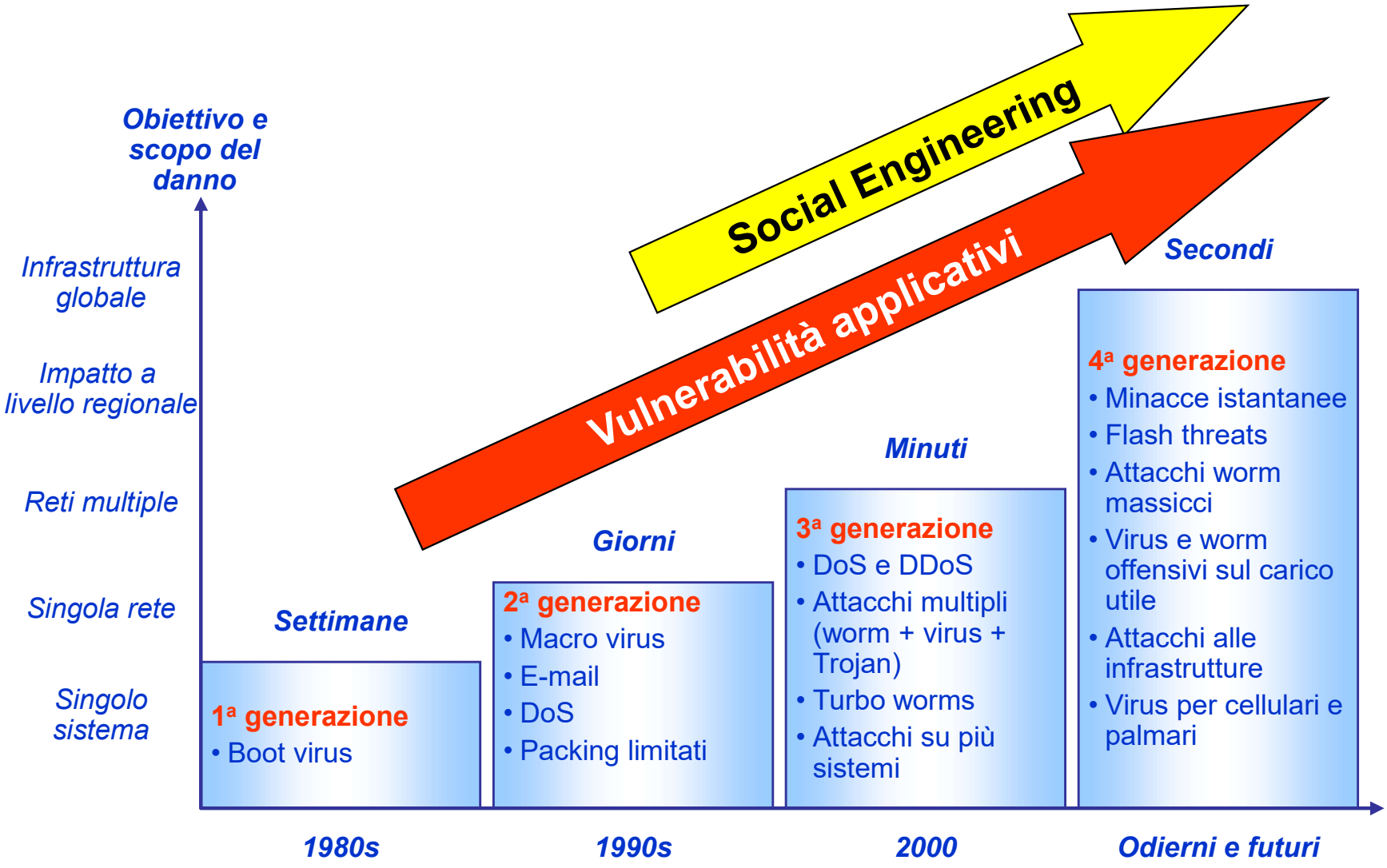
- Che cosa non è e non vuole essere OAI :
  - Un'indagine criminologica estesa a tutti i crimini informatici (es. pornografia e pedofilia elettronica, pirateria prodotti software, ecc.)
  - Uno studio accademico
  - Un'indagine di mercato

Sicurezza informatica … solo un problema tecnico?

- La pervasività dell'ICT ed il suo ruolo di tecnologia abilitante per ogni processo ed attività all'interno di qualsiasi organizzazione rende la sicurezza dell'ICT un elemento chiave per **garantire la continuità operativa** dell'Aziende o dell'Ente stesso

- Un elemento così determinante per il funzionamento di qualsiasi Azienda/Ente non può essere relegato a solo problema tecnico, ma dovrebbe essere **considerato ed indirizzato-guidato dallo stesso imprenditore e/o dai responsabili di più alto livello** della struttura organizzativa
  - troppo spesso vengono considerati un costo da ridurre quanto più possibile, un male necessario di difficile comprensione
  - delegato a figure tecniche senza adeguato commitment e budget
  - falsa sicurezza

Passato, presente e futuro di minacce ICT

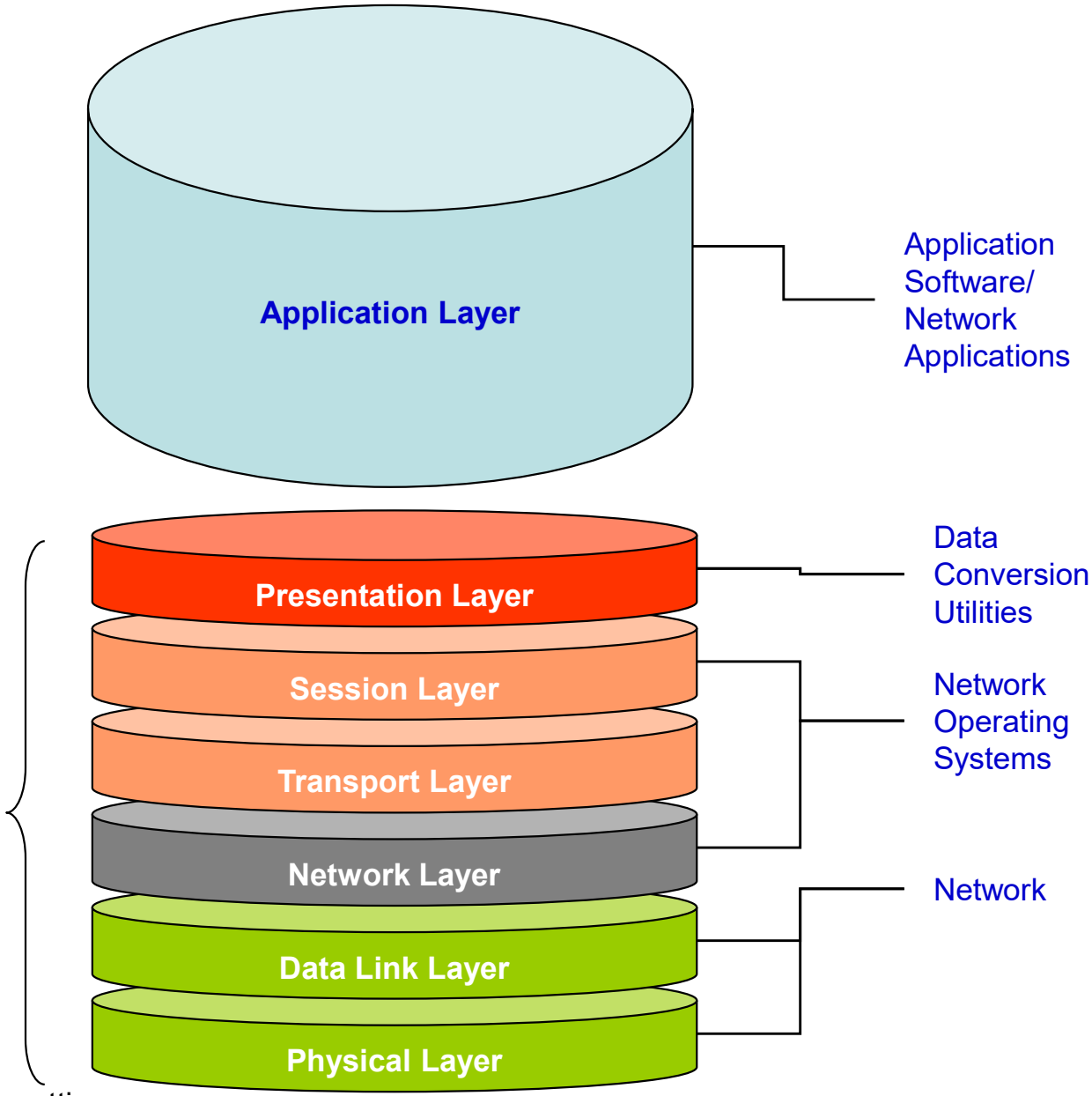


Fonte: dal volume “Sicurezza Digitale” di Marco Bozzetti

Vulnerabilità applicative: il gigante dai piedi d'argilla

Ma chi e come è in grado di verificare le vulnerabilità di un applicativo?
- OO e componentware
- web services/SOA

A questi livelli esistono soluzioni diffuse ed affidabili, anche proattive.



Fonte: dal volume "Sicurezza Digitale" di Marco Bozzetti

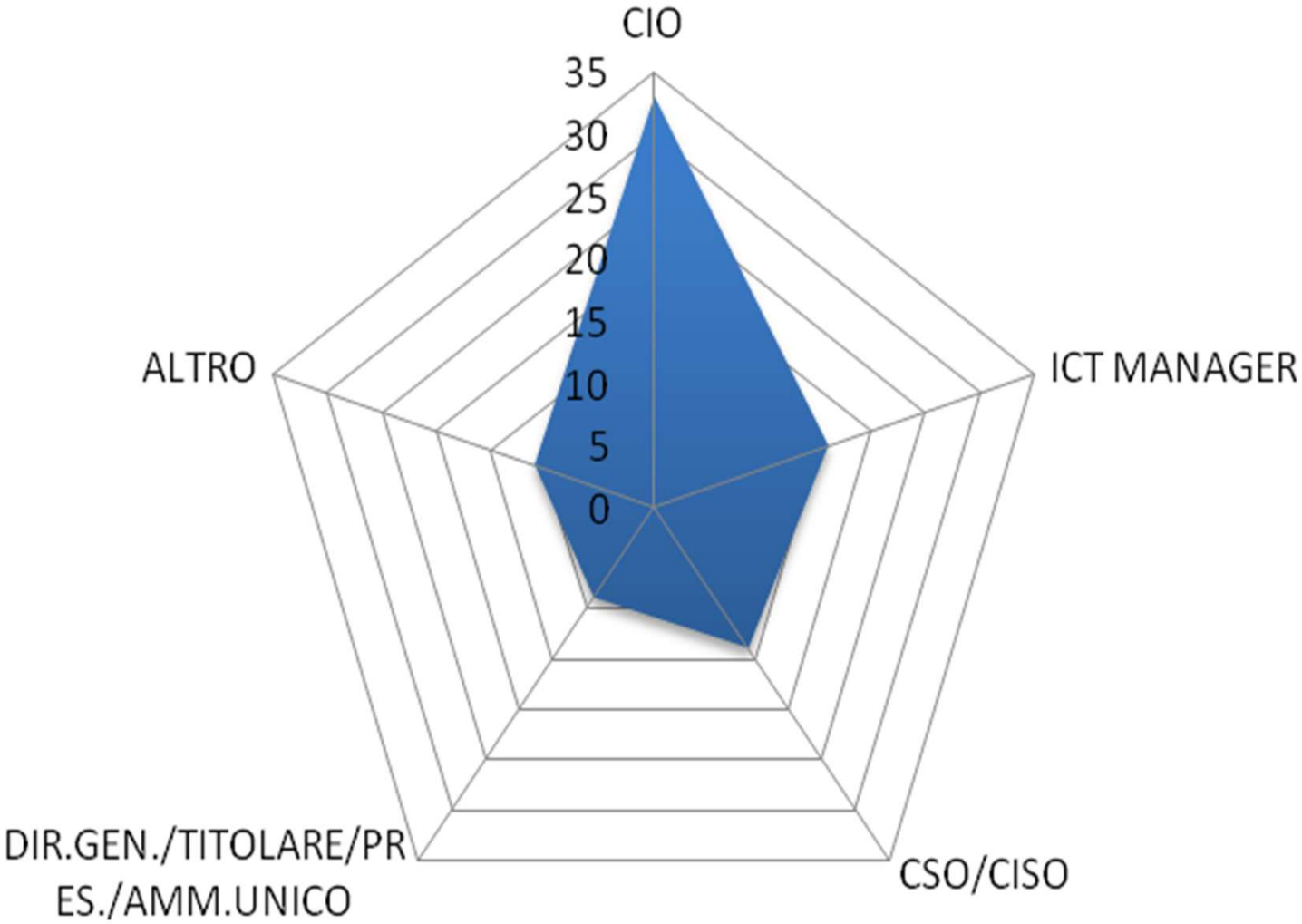
Il questionario per il Rapporto OAI 2009

- Il questionario fa riferimento sia agli attacchi subiti nel 2007 che nel 2008.
- Il questionario è breve e non richiede dettagli sulle infrastrutture informatiche e sulle modalità di attacco e di difesa, sia per renderlo il più possibile anonimo sia per non appesantire la sua compilazione.
- Struttura del questionario
  - La “Sezione 1” richiede informazioni atte a rilevare le caratteristiche dell’organizzazione interessata dagli eventi descritti, in termini di dimensioni (n° di addetti), settore di attività, area geografica di copertura e sistemi informativi e di comunicazione disponibili.
  - La “Sezione 2” è volta a rilevare gli attacchi informatici subiti nel corso del 2007 e del 2008.
  - La “Sezione 3” è volta a rilevare la tipologia e la frequenza con cui si sono verificate le tipologie di attacco di maggior rilievo.
  - La “Sezione 4” è volta a rilevare quali siano gli attacchi potenziali maggiormente temuti, indipendentemente da quelli effettivamente subiti e riscontrati.
  - La “Sezione 5” è volta a rilevare quali misure e politiche di sicurezza siano state pianificate o realizzate per tutelare le informazioni e i sistemi.

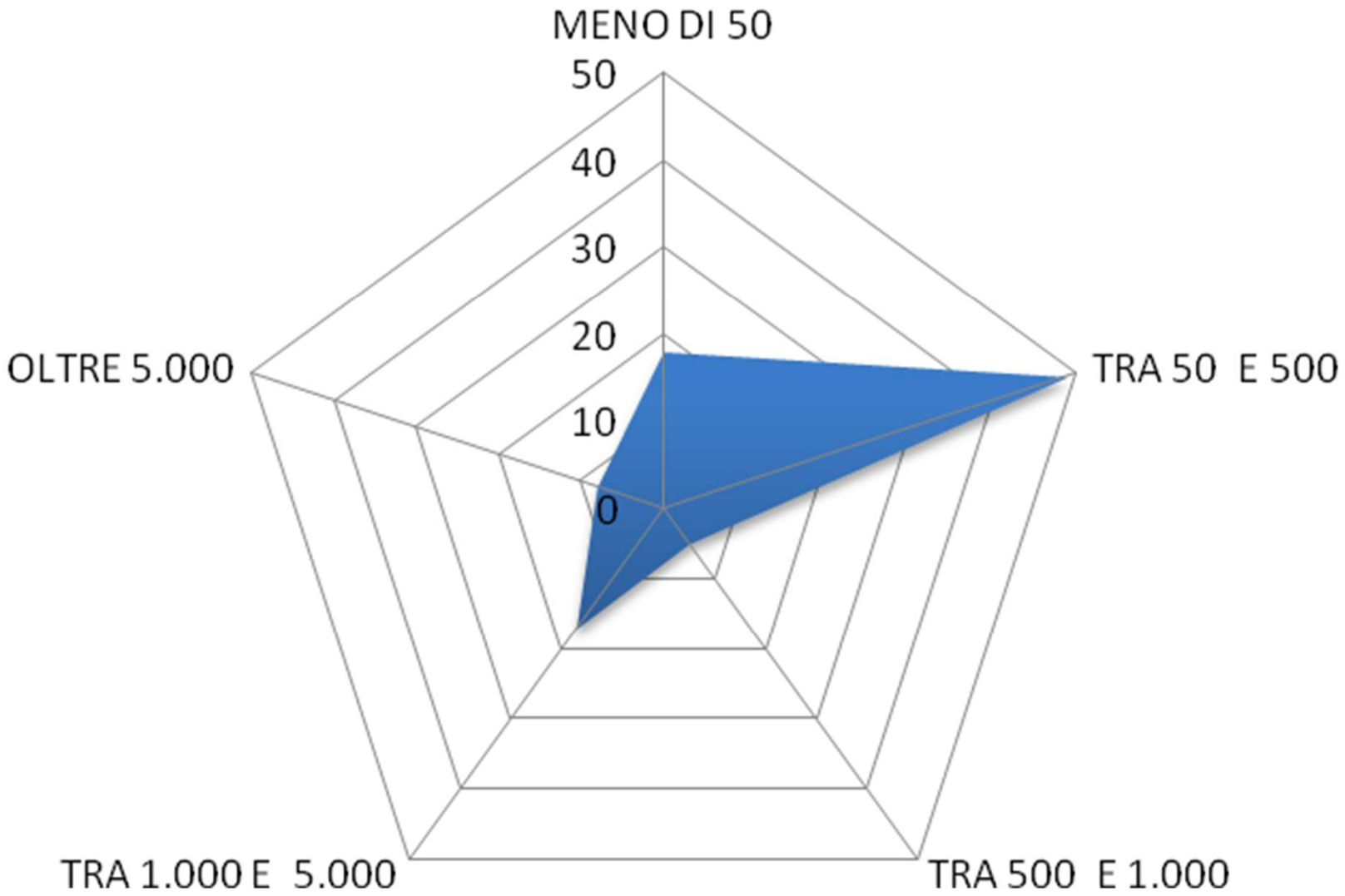
La tassonomia degli attacchi considerata

1) **Accesso e uso non autorizzato** degli elaboratori, delle applicazioni supportate e delle relative informazioni
2) **Modifiche non autorizzate ai programmi** applicativi e di sistema, alle configurazioni ecc.
3) **Modifiche non autorizzate ai dati e alle informazioni**
4) Utilizzo **codici maligni** (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server
5) Utilizzo **vulnerabilità del codice software**, sia a livello di posto di lavoro che di server: tipici esempi back-door aperte, SQL injection, buffer overflow ecc.
6) **Saturazione risorse** informatiche e di telecomunicazione: oltre a DoS (Denial of Service) e DDoS (Distributed Denial of Service), si includono in questa classe anche mail bombing, catene di S. Antonio informatiche, spamming ecc.
7) **Furto di apparati** informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette USB ecc.)
8) **Furto di informazioni o uso illegale** di informazioni
    a) da dispostivi mobili (palmari, cellulari, laptop)
    b) da tutte le altre risorse
9) Attacchi alle **reti**, fisse o wireless, e ai **DNS**, Domain Name System
10) **Frodi** tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni ecc.)
11) Attacchi di **Social Engineering** e di **Phishing** per tentare di ottenere con l'inganno (via telefono, e-mail, chat ecc.) informazioni riservate quali credenziali di accesso e il furto d'identità digitale
12) **Ricatti** sulla continuità operativa e sull'integrità dei dati del sistema informativo (ad esempio se non paghi attacco il sistema e ti procuro danni, magari con dimostrazione delle capacità di attacco e di danno conseguente…)
13) Altri tipi di attacco, quali ad esempio **attacchi di tipo misto** (Blended threat), **sabotaggi**, **vandalismi** con distruzione di risorse informatiche.

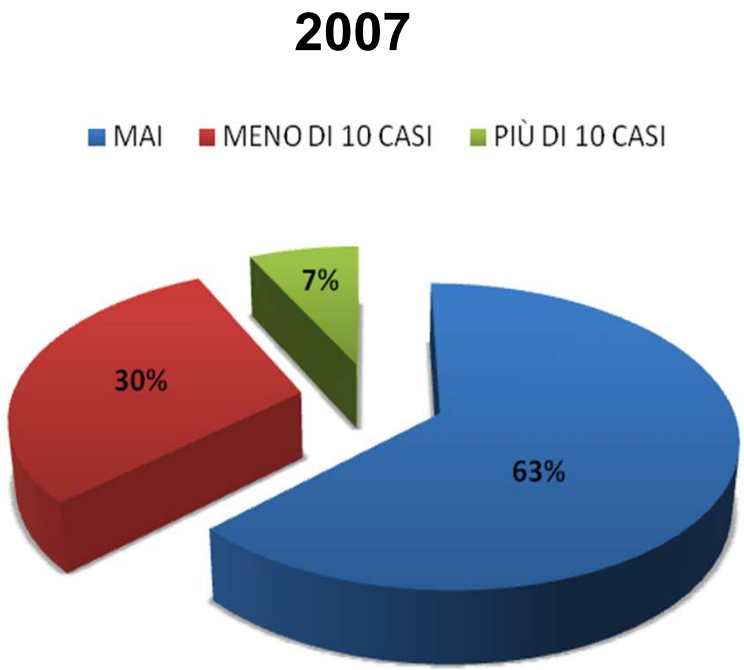
OAI 2009: chi ha risposto al questionario (in %)

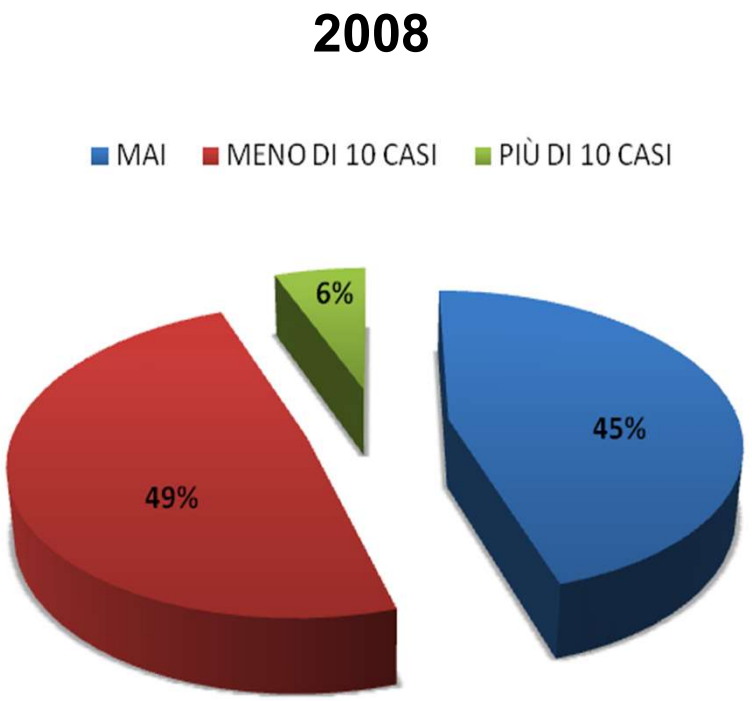


OAI 2009: le dimensioni delle Aziende/Enti



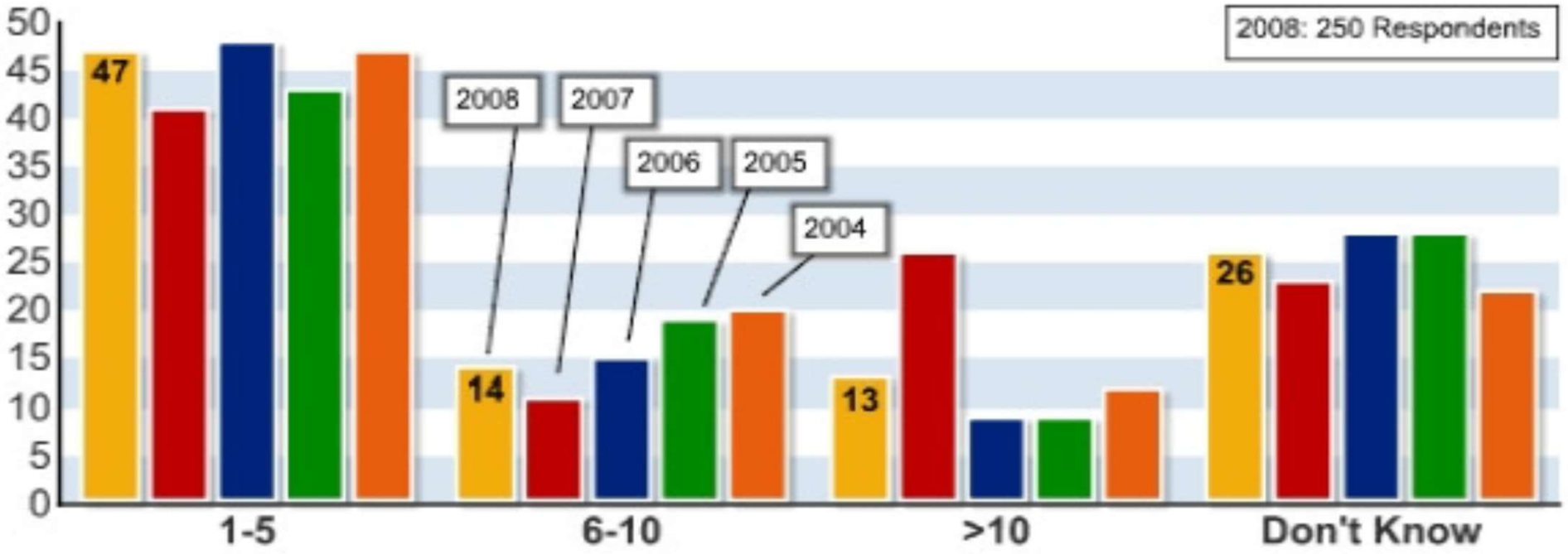
OAI 2009: % numero attacchi rilevati nel 2007 e nel 2008





CSI 2008: l'analoga analisi negli USA

Il macro-trend è simile

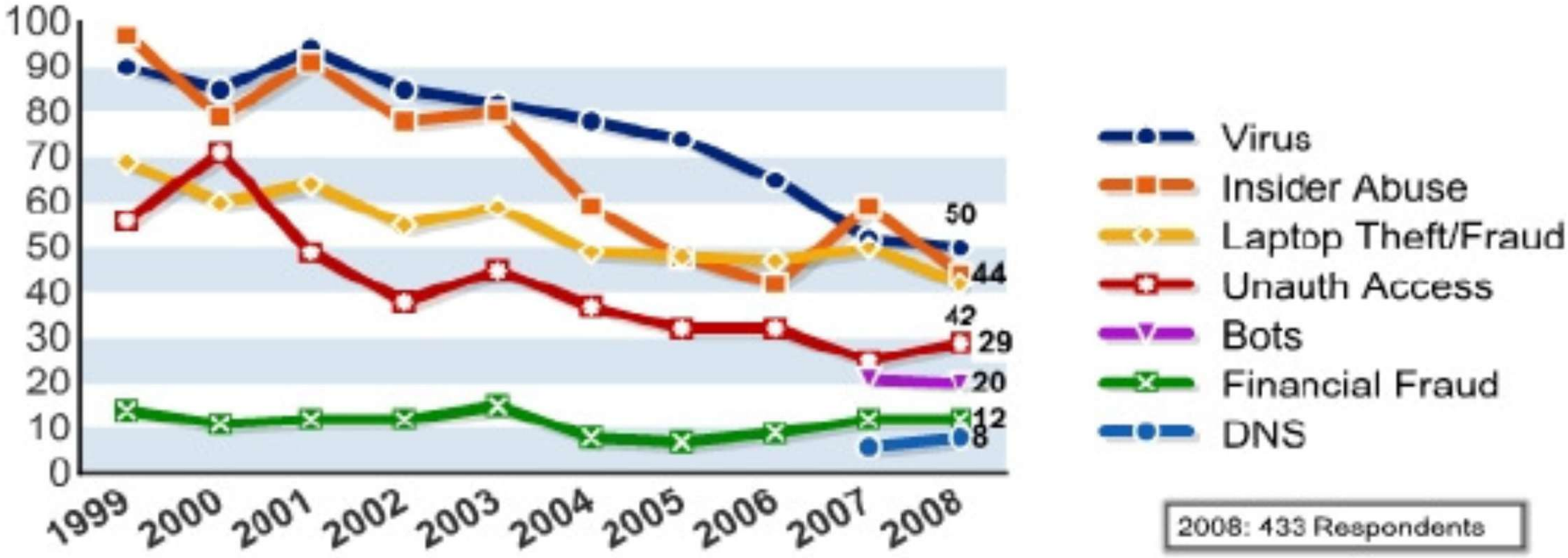


Dal Rapporto CSI 2008 (www.gocsi.com)

OAI 2009: quali attacchi

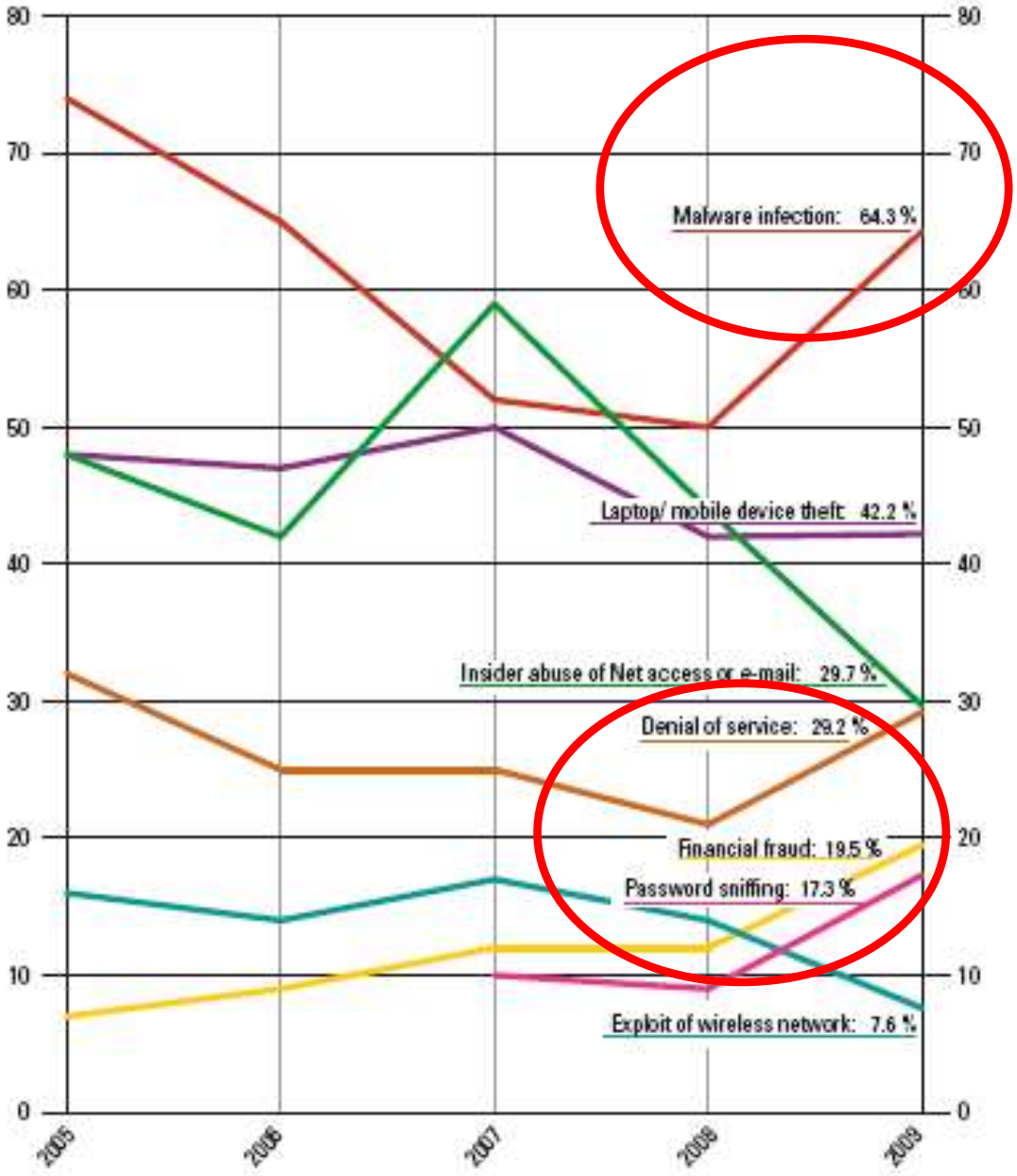
	NESSUNO		DA 1 A 5		DA 6 A 10		OLTRE 10	
TEMI	**2007**	**2008**	**2007**	**2008**	**2007**	**2008**	**2007**	**2008**
Accesso a ed uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni	70%	66%	20%	24%	6%	6%	4%	4%
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.	72%	71,50%	24%	24,50 %	4%	2%	0%	2%
Modifiche non autorizzate ai dati e alle informazioni	93,90%	86%	6,10%	10%	2%	4%	0%	0%
Utilizzo codici maligni (malware)	23,50%	15,70%	54,90 %	60,80 %	11,80%	7,80%	9,80%	15,70%
Furto di apparati informatici contenenti dati	56%	50%	34%	34%	6%	12%	4%	4%
Furto di informazioni o uso illegale di informazioni da dispositivi mobili (palmari, cellulari, laptop)	90%	91,80%	8%	4,10%	2%	4,10%	0%	0%
Furto di informazioni o uso illegale	88%	86%	6%	10%	6%	4%	0%	0%
Attacchi alle reti, fisse o wireless, e ai DNS	60%	58%	34%	34%	4%	2%	2%	6%
Frodi tramite uso improprio o manipolazioni	78%	78%	18%	16%	2%	6%	2%	0%
Attacchi di Social Engineering e di Phishing	56%	42%	16%	30%	14%	6%	14%	22%
Ricatti sulla continuità operativa e sull'integrità dei dati	94%	94%	2%	2%	4%	2%	0%	2%
Altri tipi di attacco,	87,80%	91,40%	8,20%	4,30%	4%	4,30%	0%	0%

CSI 2008: i principali attacchi rilevati

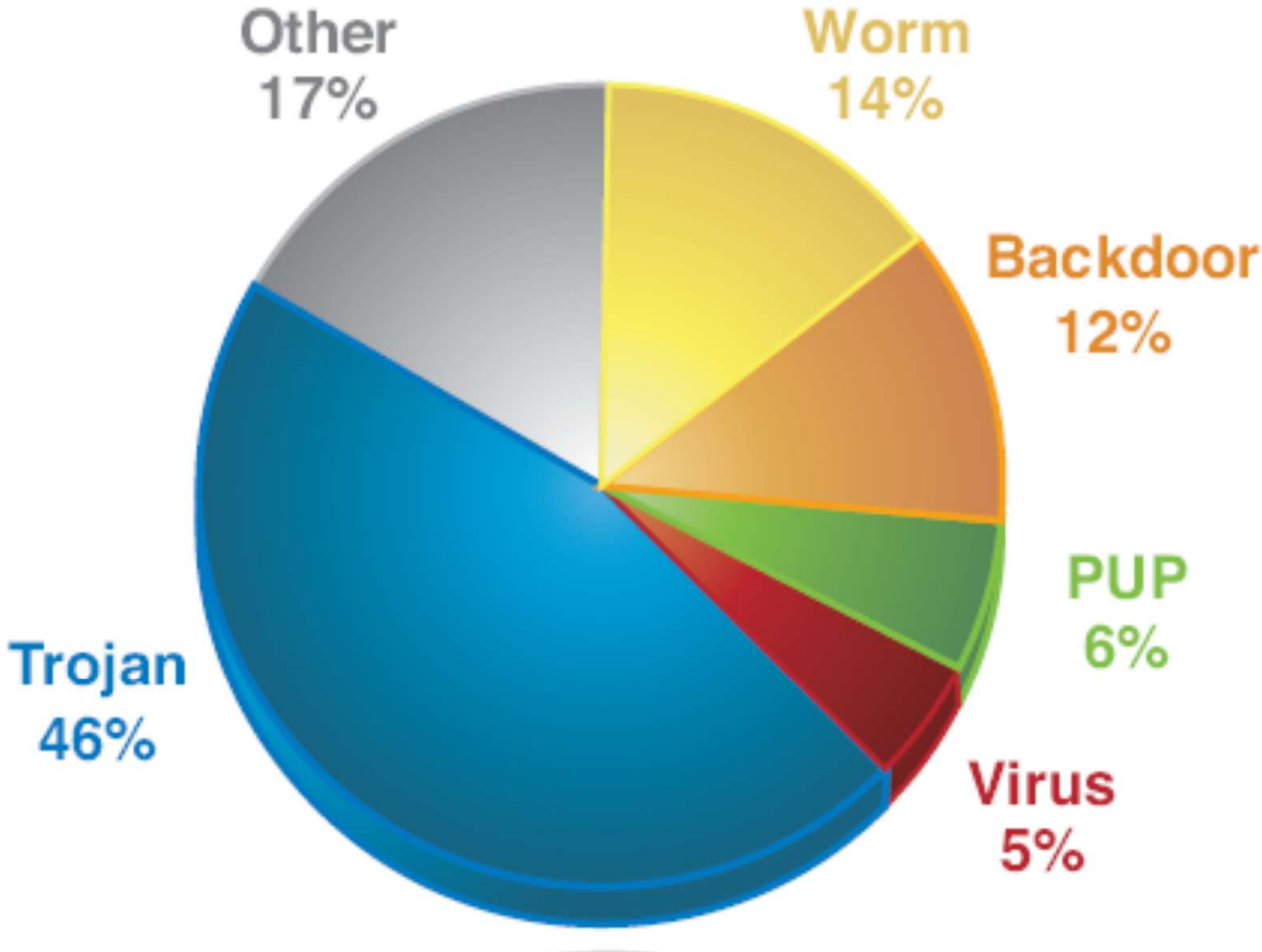


Dal Rapporto CSI 2008 (www.gocsi.com)

CSI 2009: i principali attacchi rilevati

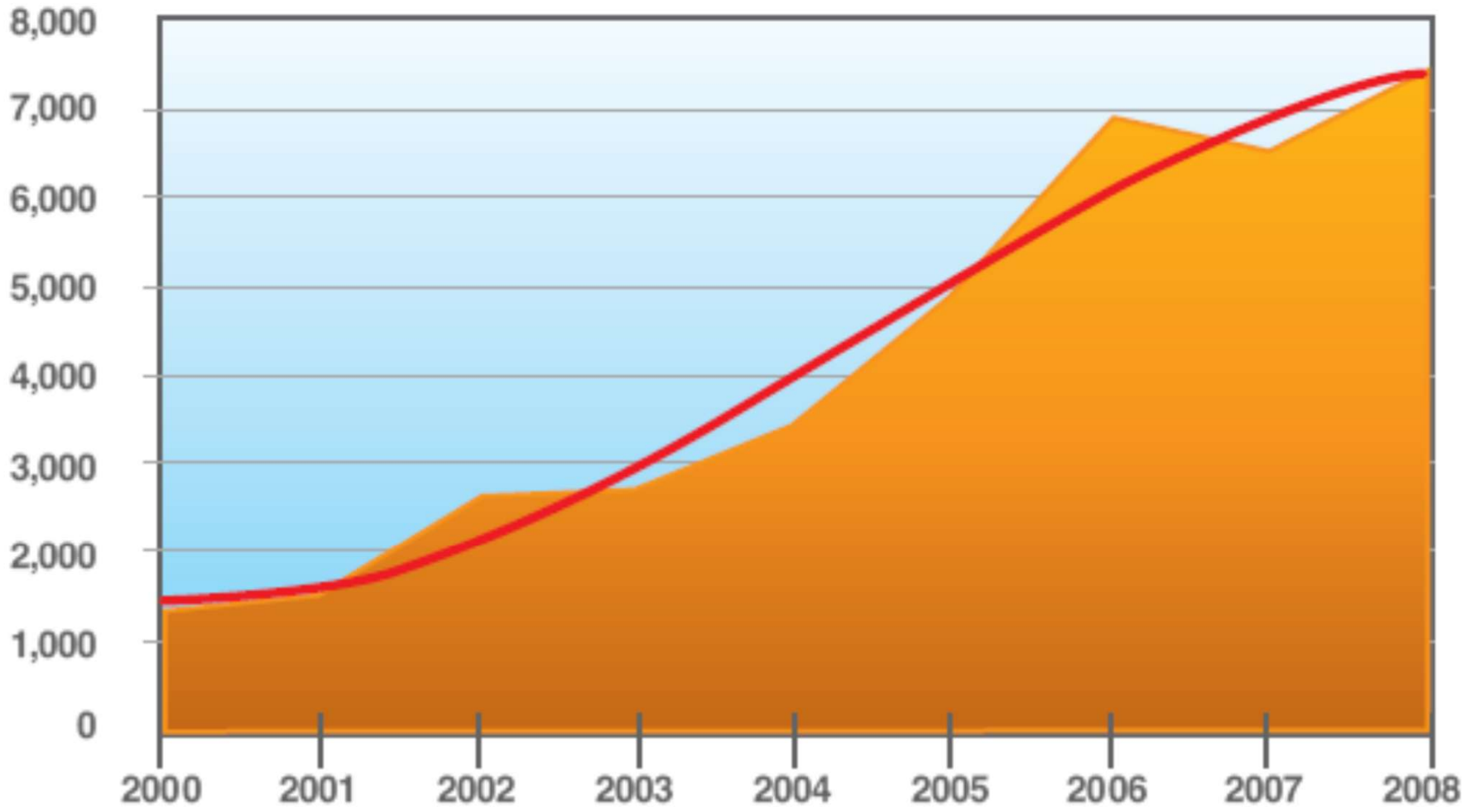


Tipologia “Malware” nel 2008 (IBM – xForce)

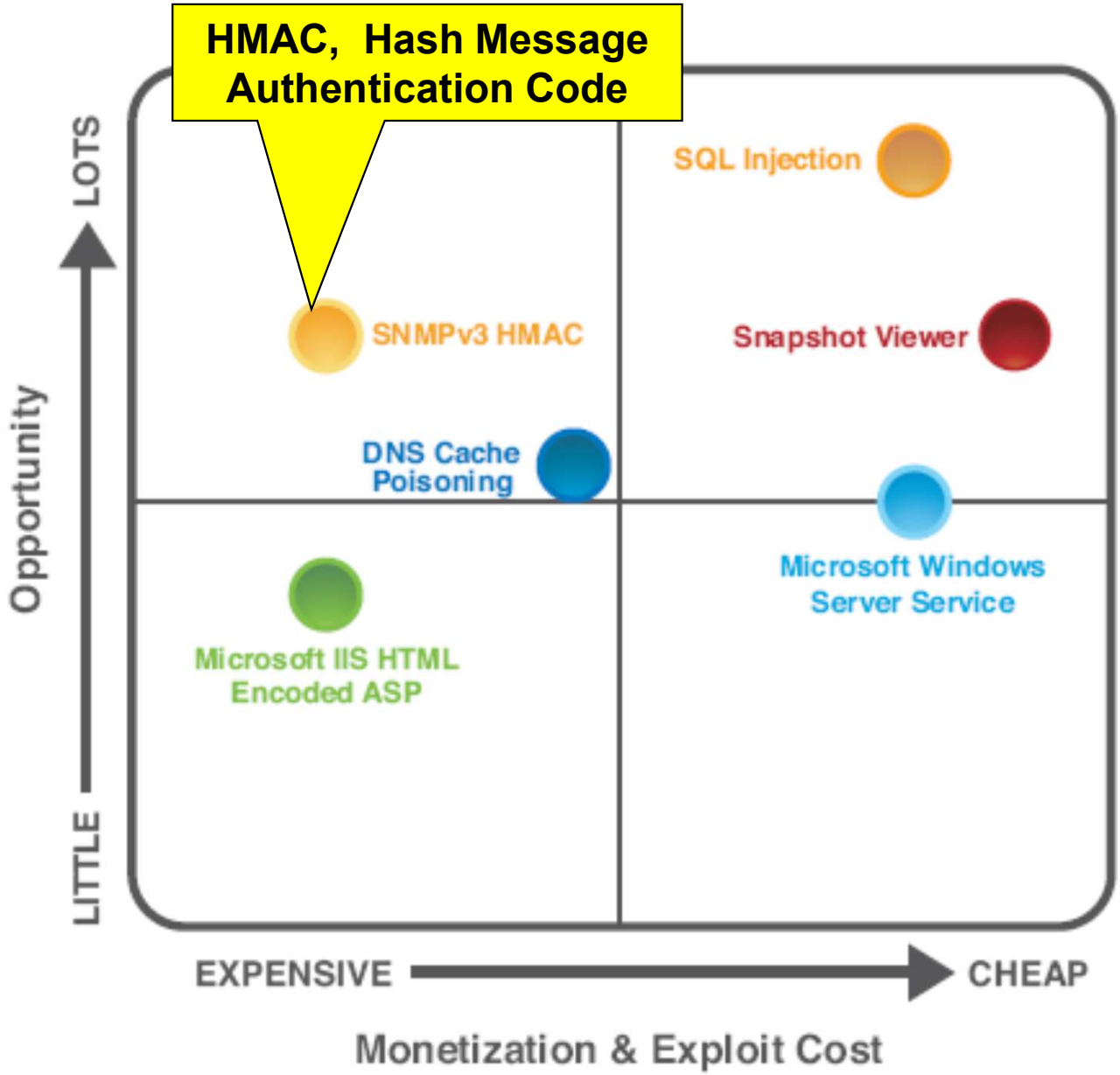


PUP, Potentially Unwanted Programs

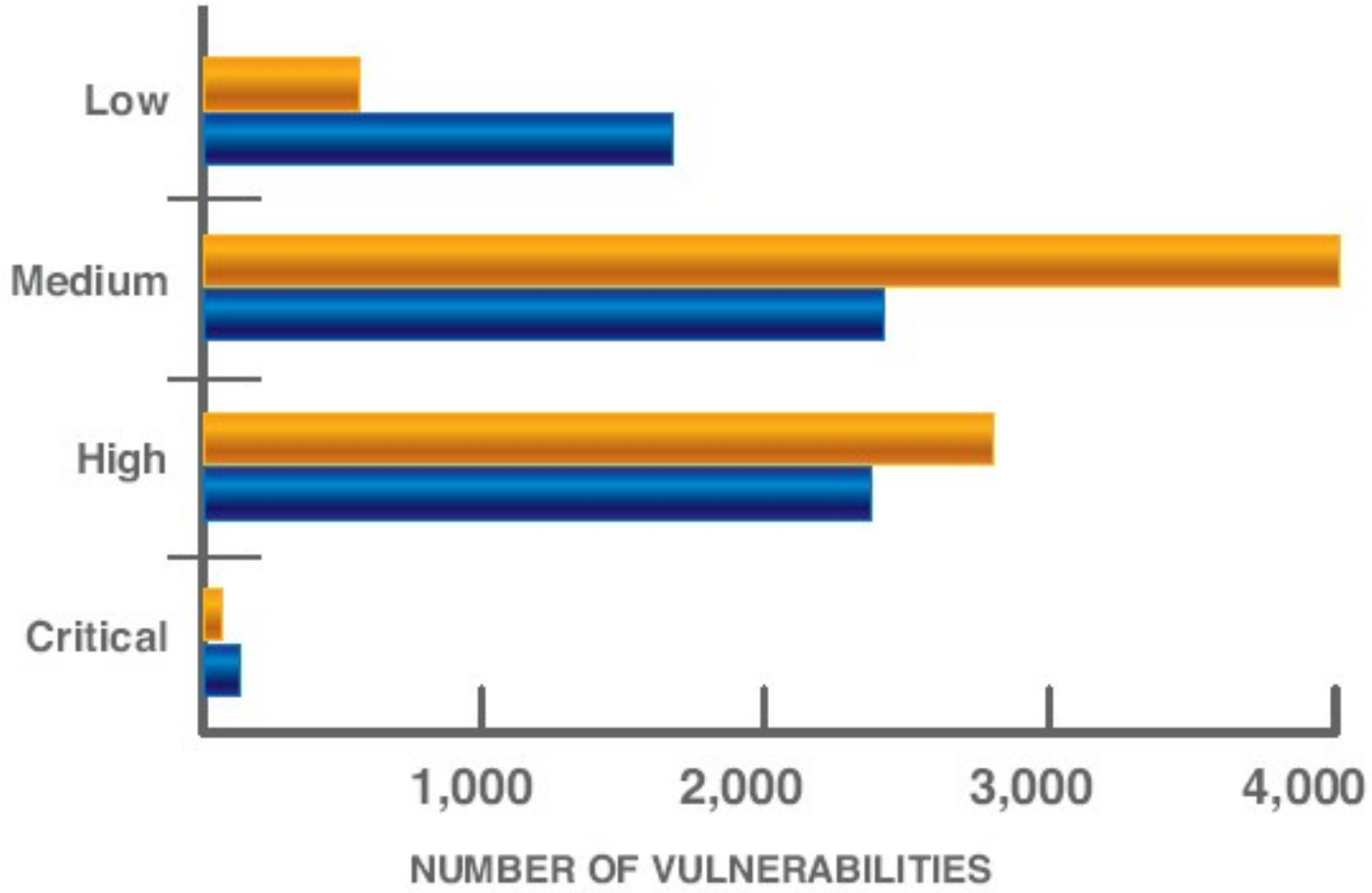
Vulnerabilità sistemi 2000-2008 (IBM – xForce)



Quadrante “magico” Rapporto 2008 IBM – xForce



CVSS, Common Vulnerability Scoring System Base Score 2007-2008

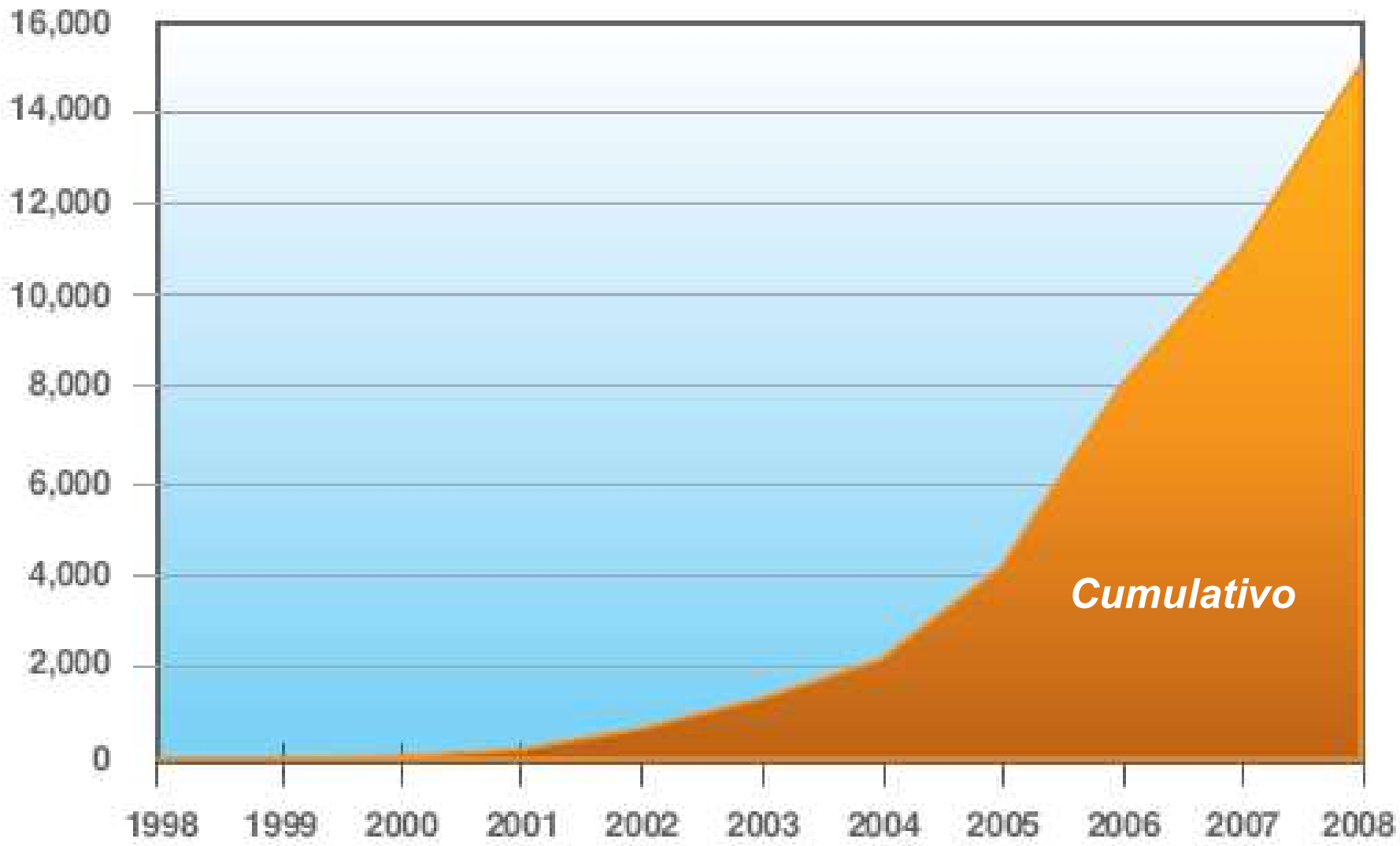


CVSS ScoreLevel	Severity Level
10	Critical
7.0–9.9	High
4.0–6.9	Medium
0.0–3.9	Low

Vulnerabilità sistemi operativi 2008 (IBM – xForce)

Operating System	Percentage
Apple Mac OS X Server	14.3%
Apple Mac OS X	14.3%
Linux Kernel	10.9%
Sun Solaris	7.3%
Microsoft Windows XP	5.5%
Microsoft Windows 2003 Server	5.2%
Microsoft Windows Vista	5.1%
Microsoft Windows 2000	4.8%
Microsoft Windows 2008	4.1%
IBM AIX	3.7%
Others	24.9%

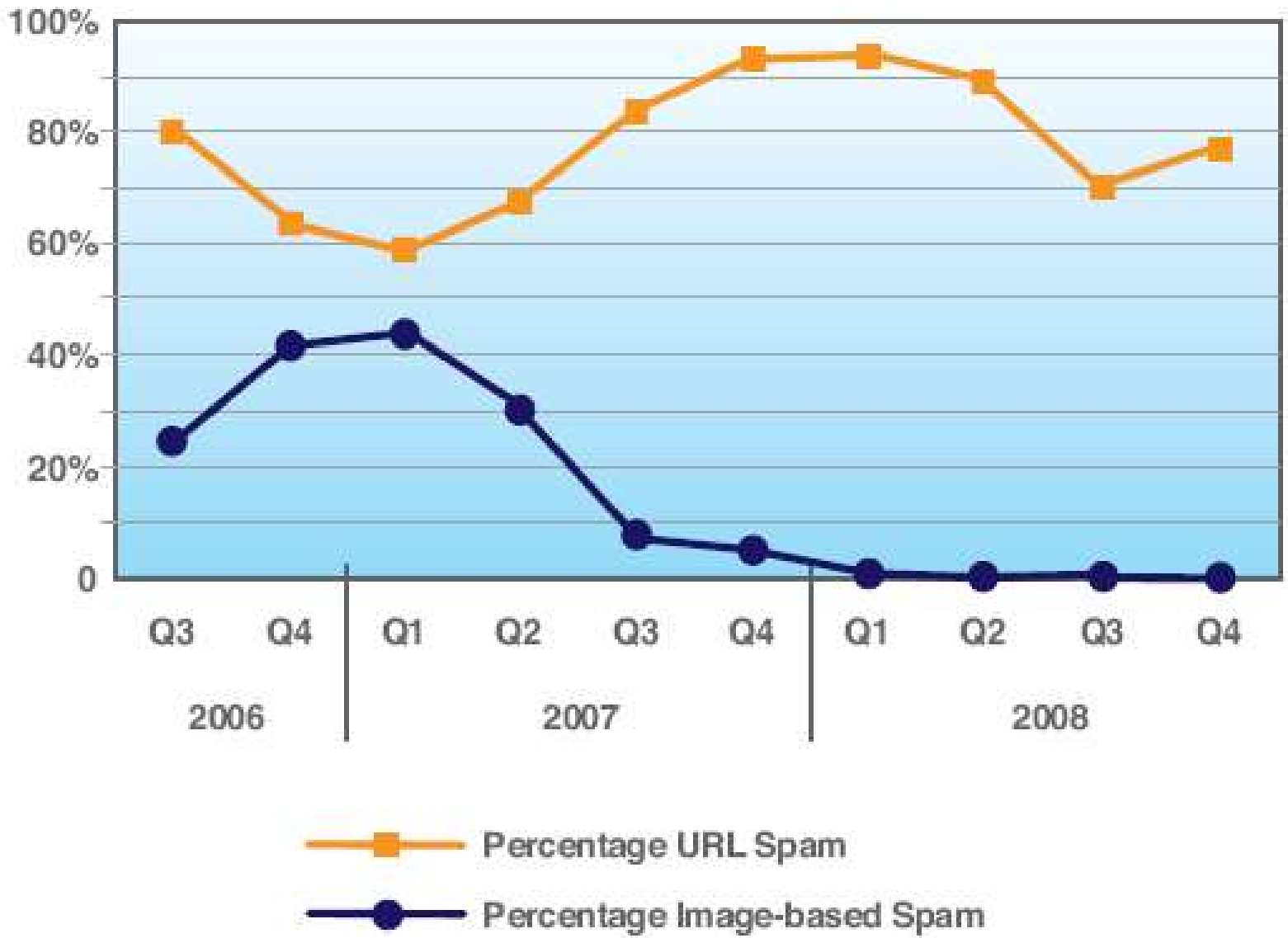
Principali vulnerabilità applicativi web nel 2008 (IBM – xForce)



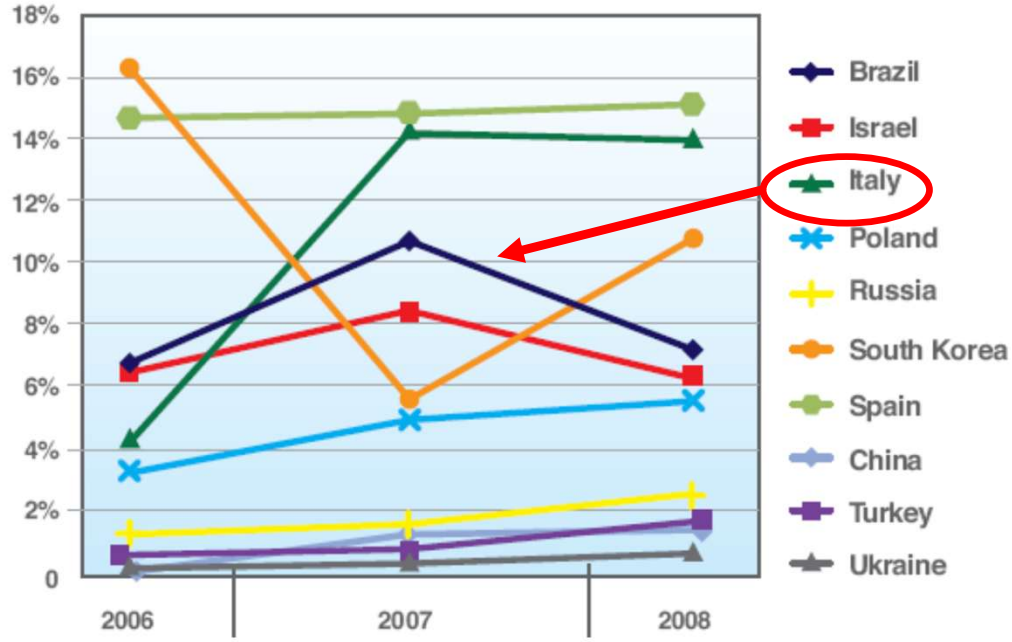
Principali Web Browser Exploits nel 2008 (IBM – xForce)

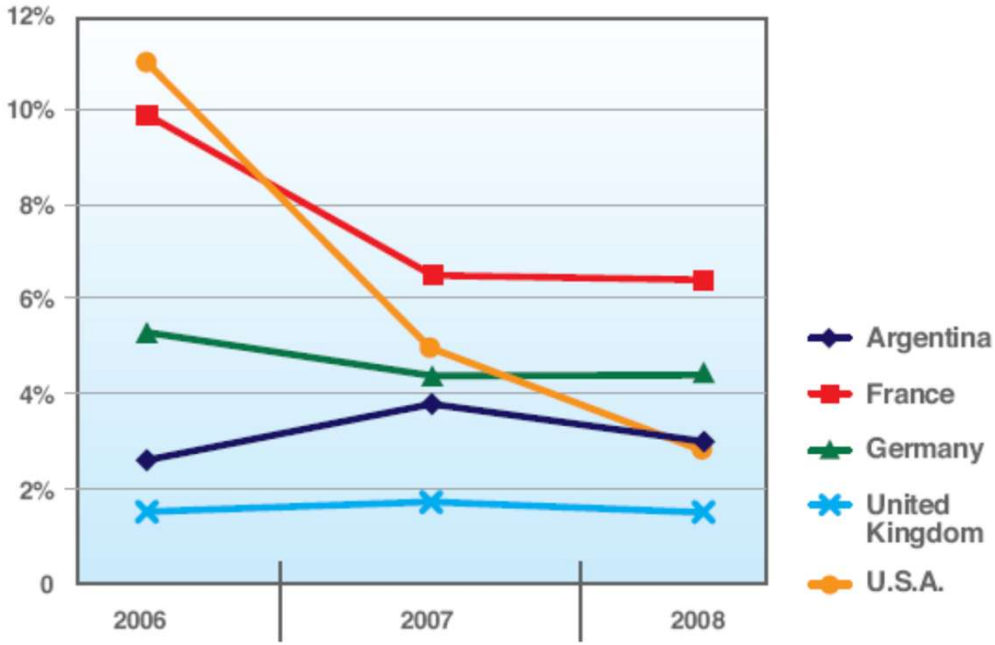
Rank	2008 (Full Year)
1.	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2.	RealPlayer IERPCtl ActiveX (CVE-2007-5601)
3.	Apple QuickTime RSTP URL (CVE-2007-0015)
4.	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)
5.	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)

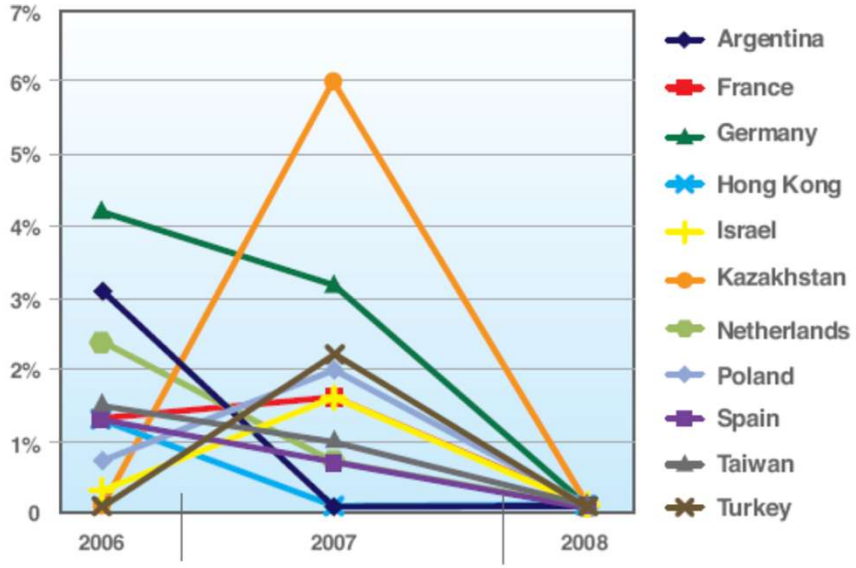
Spamming: andamento nel 2007- 2008 (IBM – xForce)



Phishing: andamento % provenienza nel 2006- 2008 (IBM – xForce)



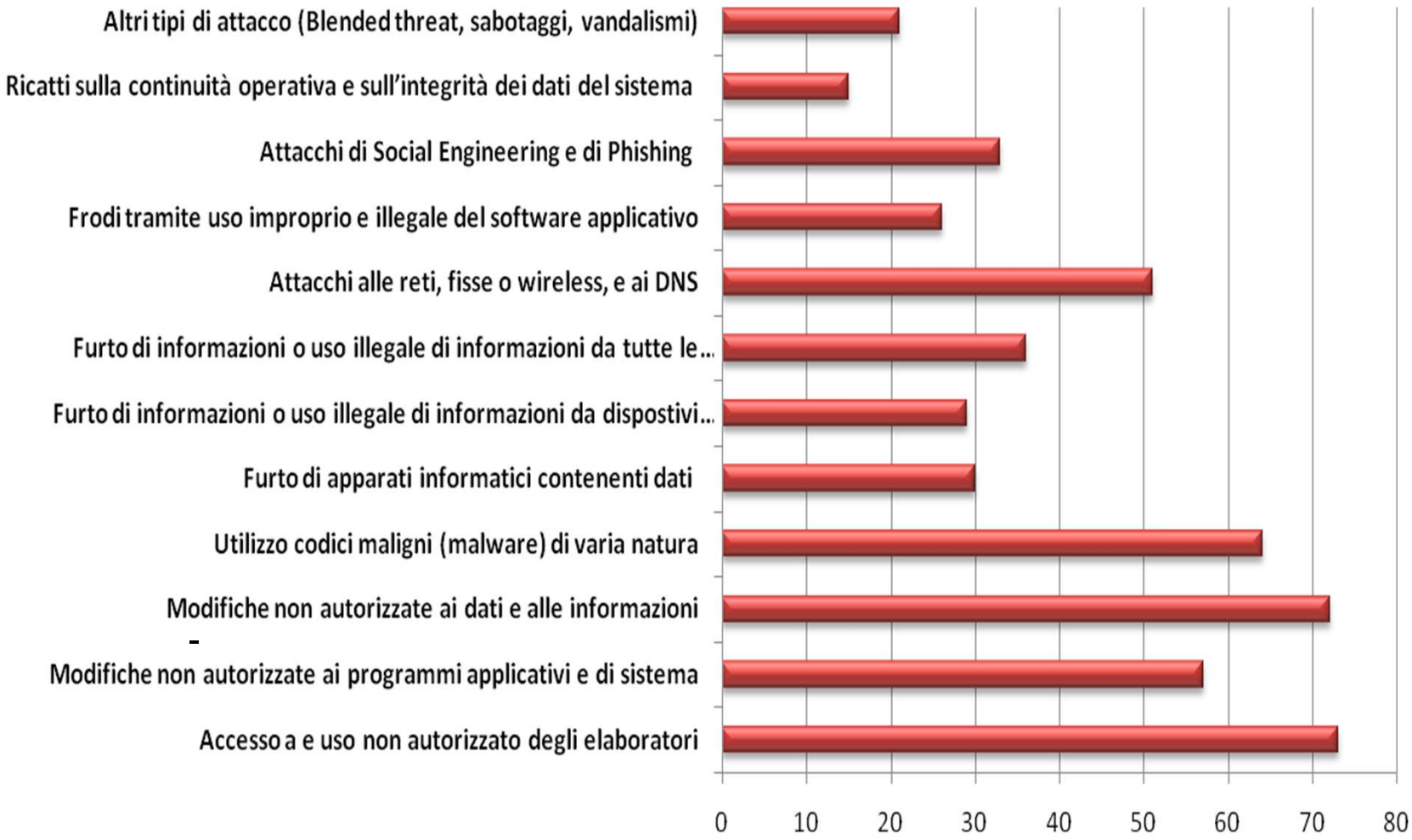




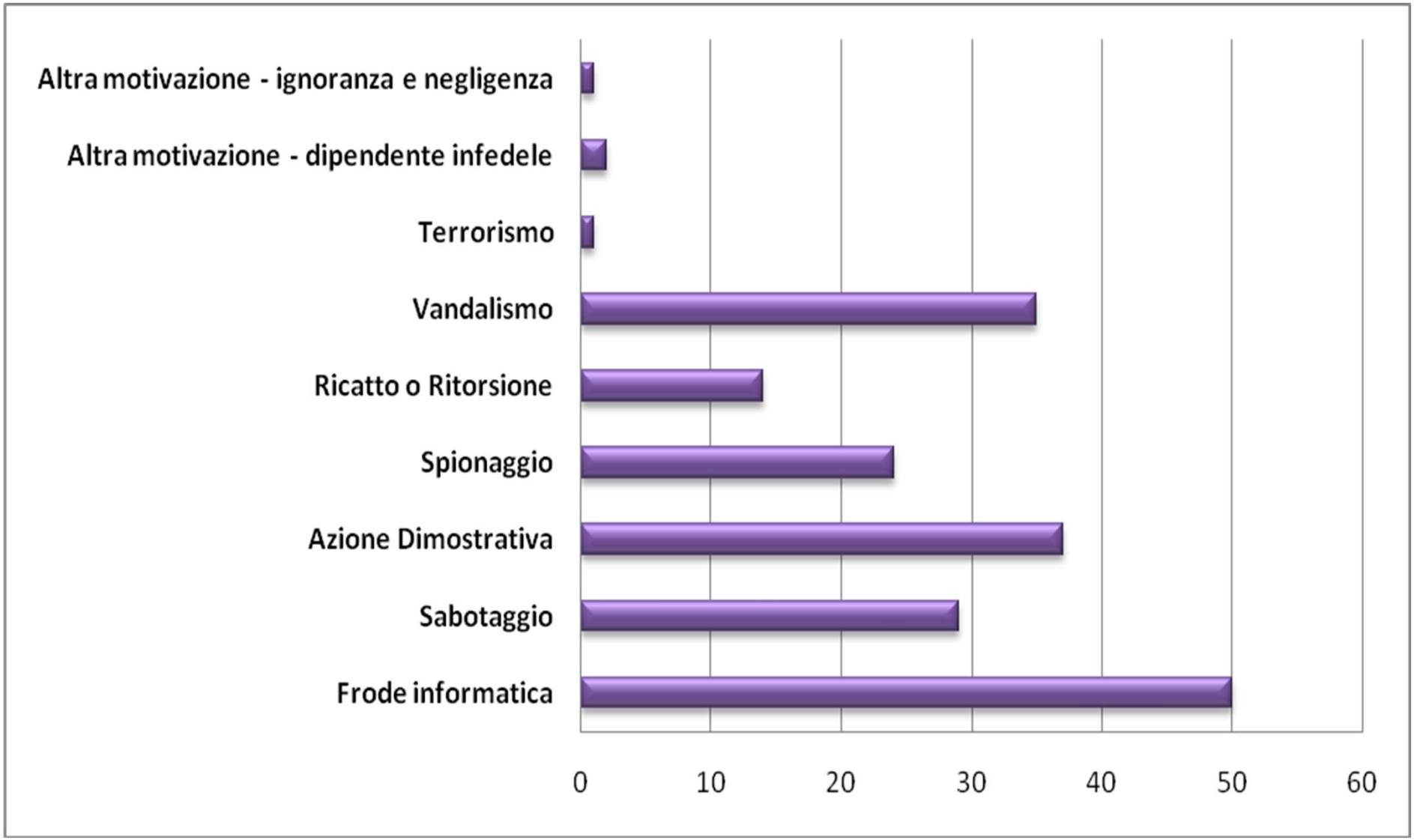
OAI 2009: % strumenti e metodologie in uso (di cui)

STRUMENTI E METODOLOGIE DI PROTEZIONE IN USO	%
Antivirus and antispyware	95%
Firewall e DMZ	85%
Identificazione dell'utente con identificativo d'utente e password	84%
VPN (Virtual Private Network)	79%
Strumenti di gestione delle autorizzazioni (Active Directory, Ldap, Access Control List, policy server)	77%
Uso di strumenti per la gestione delle patch, degli aggiornamenti, delle release	60%
Archiviazione e gestione dei log	52%
Politiche (policy) tecnico-organizzative di sicurezza ICT	52%
Uso sistemi ad alta affidabilità	47%
Disaster Recovery Planning	39%
Uso di procedure organizzative formalizzate nel supporto ai processi inerenti la sicurezza informatica	38%
Sistemi di PKI (Public Key Infrastructure)	20%
Identificazione dell'utente "forte" con certificati digitali	20%
Identificazione dell'utente biometrica	6%

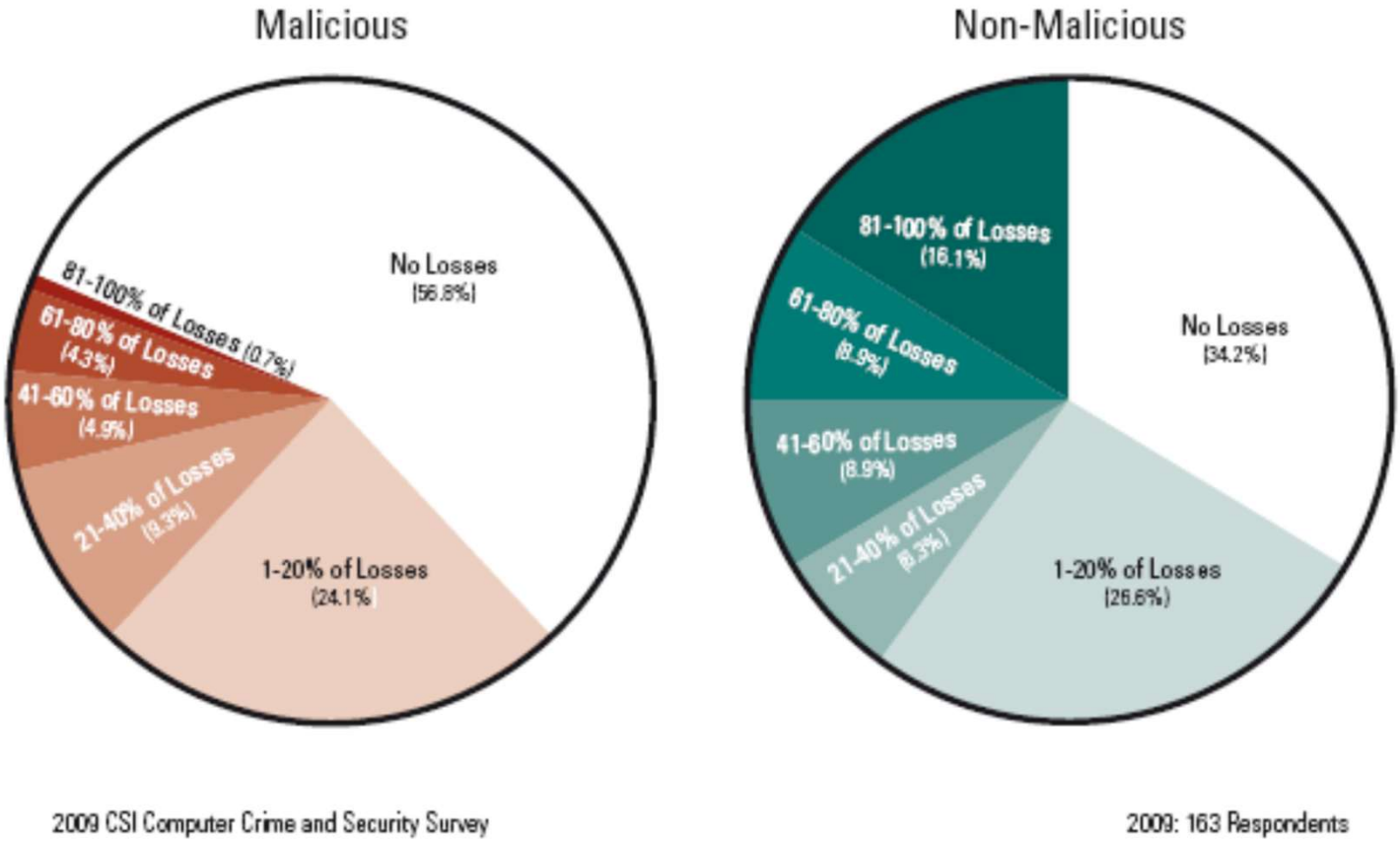
OAI 2009: % tipologia attacchi più temuti



OAI 2009: Ripartizione percentuale delle motivazioni per i potenziali attacchi

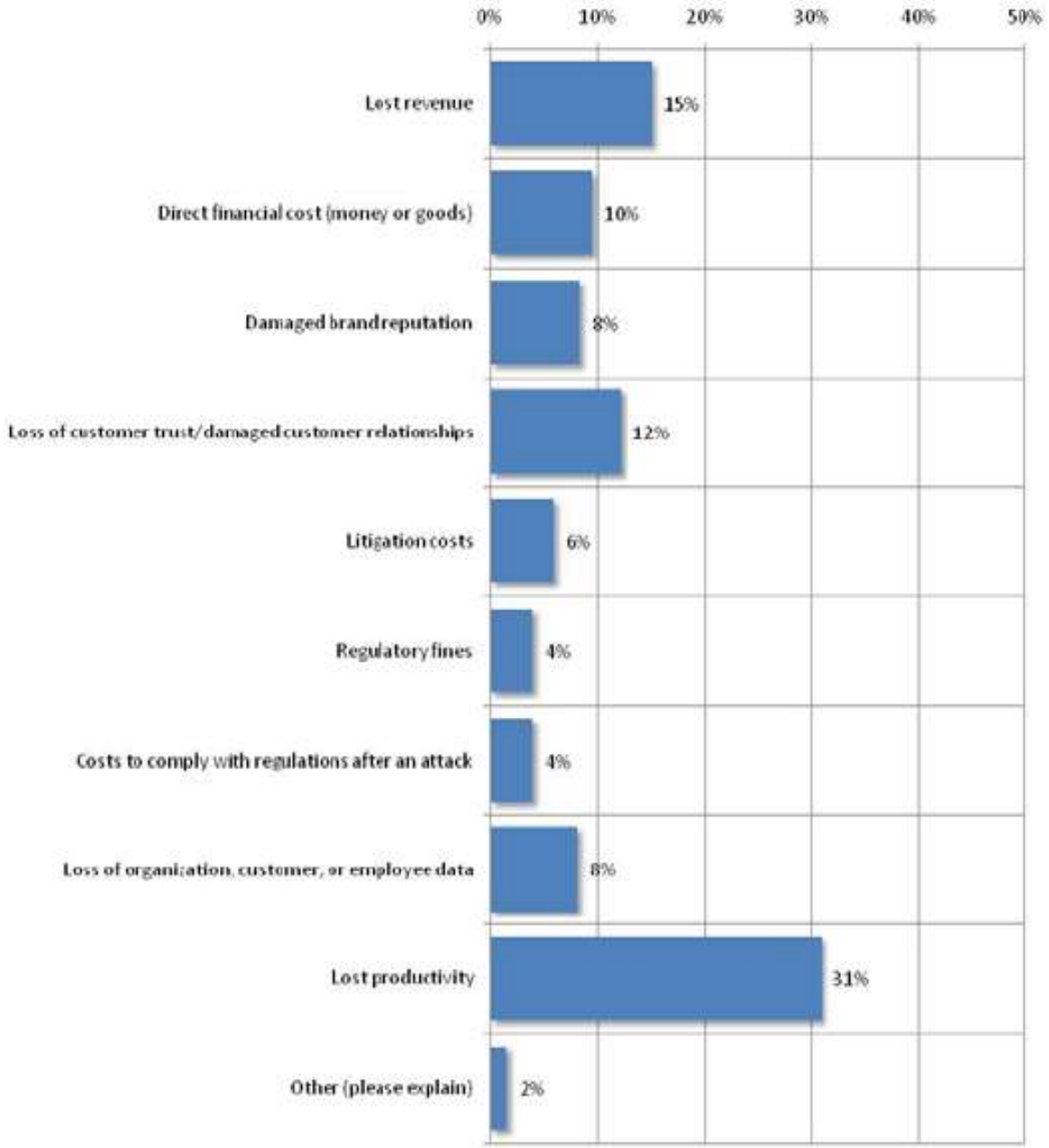


CSI 2009: % perdite economiche per attacchi dall'interno e dall'esterno



In OAI 2009 non sono state richieste stime delle perdite economiche (dirette, indirette, consequenziali) subite per la difficoltà nell'effettuare tali stime e la difficoltà o non volontà di rispondere a simili domande.

Principali perdite a seguito di attacchi (Symantec)



I prossimi passi

- Pubblicazione a breve del Rapporto OAI 2009 stampato

Si sta già impostando la raccolta on-line del prossimo Rapporto OAI 2010:

  - Migliorando il questionario
  - Coinvolgimento di altre Associazioni ed Istituzioni
  - Cercando di ampliare e di meglio bilanciare il numero di rispondenti per settore
- Sua disponibilità prevista entro ottobre 2010
- Partecipate numerosi alla compilazione del prossimo questionario che sarà accessibile da vari siti web, in particolare:
  - www.soiel.it
  - www.clubtimilano.net
  - www.aipsi.org
  - www.malaboadvisoring.it