



Stato dell'Arte e tendenze nel mercato della Sicurezza alla luce delle Acquisizioni del 2006 e in prospettiva delle prossime

eSecurity Lab 2007

25 gennaio 2007

Alessandro Giacchino



Via V. Monti, 23 - 27100 Pavia

Tel. 0382 / 304.985 - Fax 0382 / 304.986

E-Mail Toolnews@itware.com

Oggetto: Diffida

Copyright BCI Italia

b Gentile signor Giacchino sono l'avvocato Federico Heilmar titolare dell'omonimo studio Legale, mi trovo costretto a riscriverle perchè continuano ad arrivarmi dal suo indirizzo email messaggi dal contenuto sconveniente... Non sono un esperto in materia, tuttavia riteniamo che questi invii non siano volontari, ma causati da un virus. che sembra sia possibile rimuovere con il software scaricabile da questo sito <http://www.personalspywareremover.com>

b Non avendo nè le competenze nè il tempo per verificare questa teoria, mi trovo costretto a DIFFIDARLA dal continuare questi invii: se riceverò UN SOLO ALTRO MESSAGGIO di questo genere procederò per vie legali senza ulteriore avviso.

b Le ricordo che i reparti di polizia delle telecomunicazioni hanno gli strumenti per risalire alla vera identità del proprietario di un indirizzo di posta elettronica, per cui non creda di poter continuare a inquinare la mia casella con questa immondizia...
2

Evoluzione delle fonti delle minacce: dai *mitomani* ai criminali

Copyright BCI Italia

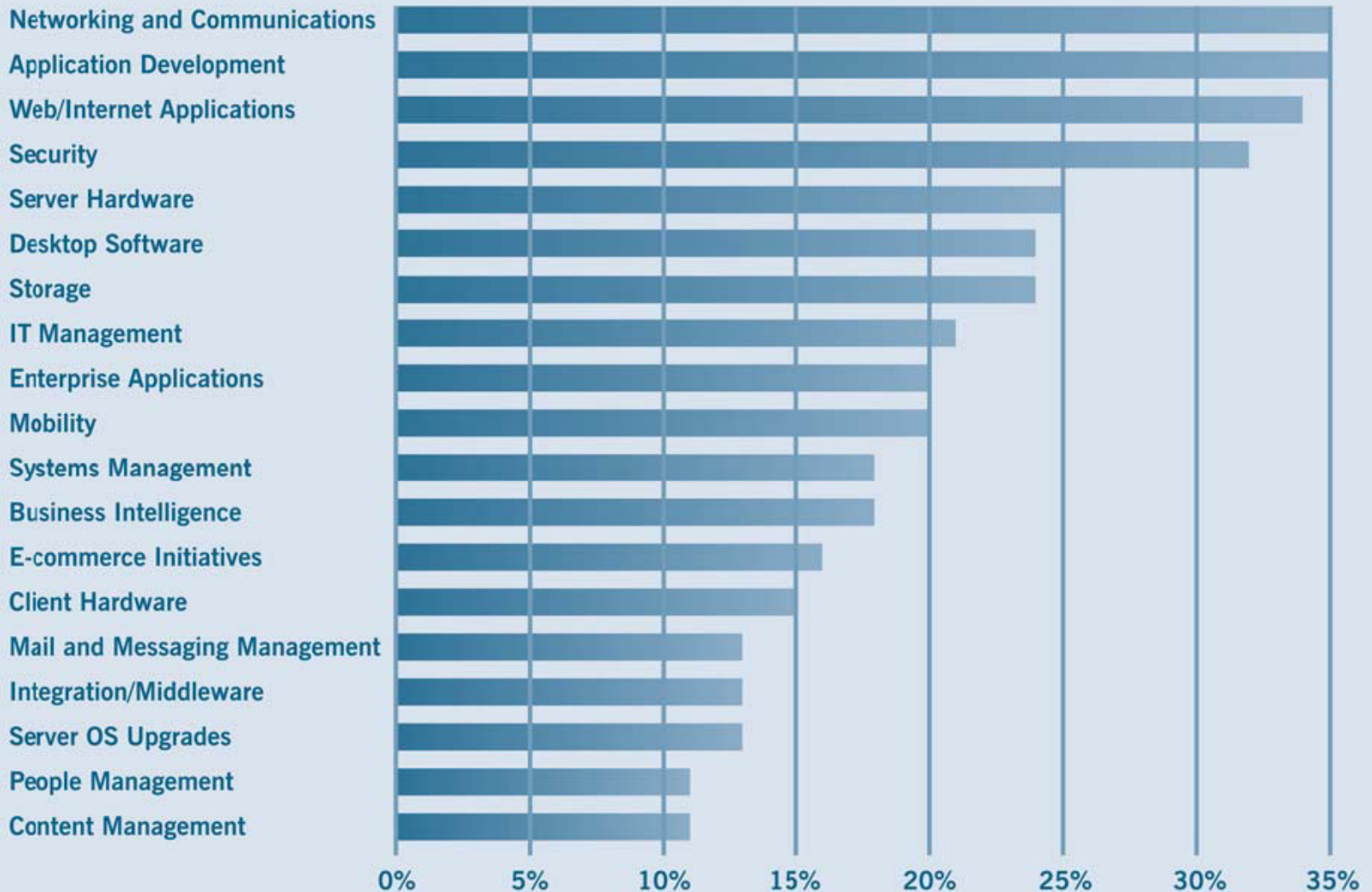
➤ Nel 2005, è emerso che le minacce più consistenti non vengono da *hackers* o *personale scontento*, ma da cybercriminali che si muovono a fini di lucro:

- Furto di identità (*phishing*), di numeri di carte di credito
- Vendita di dati riservati (spyware)
- Attività di *spamming*...

➤ Effetti:

- Tecniche di attacco molto più sofisticate
- Riduzione degli intervalli di tempo tra la scoperta delle vulnerabilità ed il loro sfruttamento
- Entità dei danni molto più consistente, con vantaggi diretti per gli autori dei misfatti

La sicurezza sempre al vertice dell'attenzione (Datamonitor 6/06)



Trend 2006-2008: mercato da 6 miliardi di dollari

Copyright BCI Italia

Per il 2008, il mercato globale (Hw + Sw + servizi) varrà 6 miliardi di dollari (+15% annuo). Oggi, VPN e Firewall ne assorbono il 77%, Intrusion Detection il 14%, gli Anti- il 9%.

Nel futuro, la maggiore espansione sarà per i sistemi di Network Access Control (NAC) e Intrusion Prevention (IPS)

Forte crescita degli strumenti per proteggersi da truffe e criminali informatici

Al terzo posto, le soluzioni per la sicurezza delle connessioni Wireless (LAN, cellulari, PDA) sempre più diffuse, mentre per gli "Anti" si prevede uno sviluppo dell'area "servizi online" che peseranno nel 2008 per il 12% sul totale del mercato

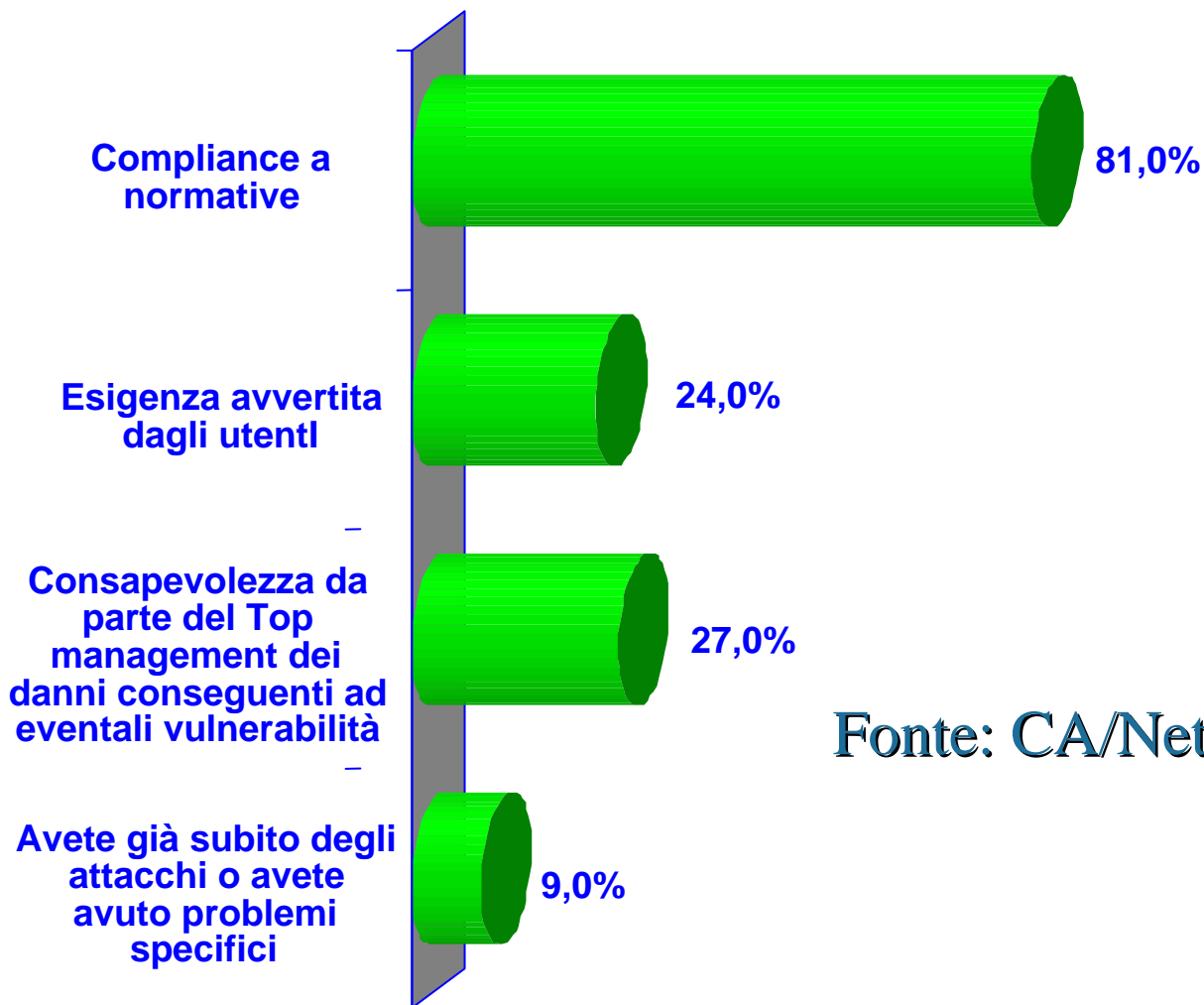
Stato dell'arte: i punti chiave per il Butler Group – I Driver

Copyright BCI Italia

- **Uno dei maggiori Driver nelle scelte diviene l'obbligo di rispettare nuove leggi e normative:**
 - **ISO-17799 / BS 7799-2 / Cobit**
 - **Il Codice di Protezione dei Dati Personali**
 - **Il Documento programmatico della sicurezza**
 - **Basilea II – SOX (Sarbanes-Oxley Act)**
- **Protezione del patrimonio aziendale**
- **Riduzione dei costi di allestimento/gestione e incremento qualità/efficacia dei controlli**

Anche in Italia, si fa sicurezza perché obbligati!

Copyright BCI Italia



Fonte: CA/NetConsulting

Provisioning e Strong Authentication in grande crescita (Datamonitor 6/06)

Copyright BCI Italia

	2003	2004	2005	2006	2007	CAGR
Authentication	598	642	723	833	978	13.1%
Enterprise Access Control	737	750	754	747	713	-0.8%
Web-based Access Control	323	345	380	438	511	12.2%
Provisioning	102	119	137	179	245	24.5%
Associated Infrastructure	298	341	402	492	609	19.6%
Total	2,058	2,196	2,396	2,689	3,057	10.4%

	2003	2004	2005	2006	2007	CAGR
Smart Cards	67	89	113	141	180	28%
PKI (including CA services)	222	230	246	263	281	6%
Biometrics	80	83	95	110	149	17%
Tokens	212	219	234	260	276	7%
USB	17	21	35	59	92	54%
Total	598	642	723	833	978	13%

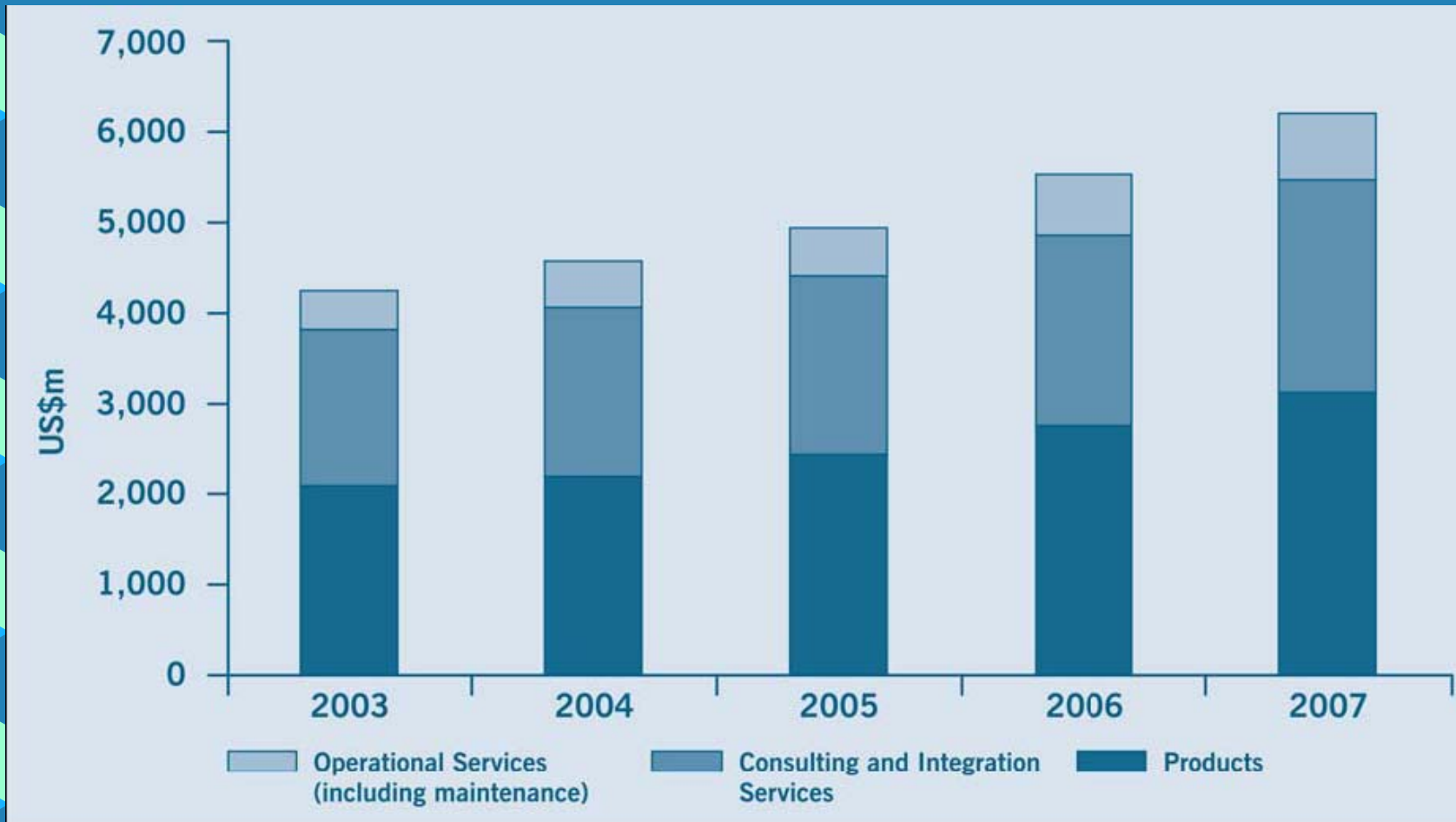
Trend 2006 per il Butler Group: aumento peso Outsourcing MSSP

Copyright BCI Italia

- La maggior complessità dei sistemi e la riduzione dei tempi di reazione impongono l'uso di strutture, risorse e competenze specializzate e aggiornate
- Appaltando questo genere di servizi ad organizzazioni specializzate si ottengono i seguenti risultati:
 - Condivisione di infrastrutture, strumenti, competenze su scala più ampia
 - Migliore accesso ad informazioni, maggiori opportunità di sviluppare competenze ed esperienze
 - Motivazione e interesse da parte del personale e più elevati livelli di copertura del servizio
 - Delega all'esterno di responsabilità legali, con relativi obblighi di costante aggiornamento e adeguamento

Continua a crescere anche l'I&AM, ma nelle medie aziende

Copyright BCI Italia



Trend 2006-2008: direzioni ortogonali/complementari

Copyright BCI Italia

➤ Il mercato è in profonda trasformazione e sta dando vita a tre approcci totalmente diversi tra loro, ma con numerose intersezioni:

- **MSS**: l'offerta diventa "erogazione di servizi specializzati", proposti direttamente dai fornitori di tecnologie o di servizi di sicurezza agli utenti o ai fornitori di *Global Outsourcing*
- **Piattaforme integrate**: la sicurezza diviene parte delle piattaforme di Service Management e proposta dai produttori di sistemi agli utenti o ai fornitori di servizi
- **Le soluzioni specializzate**: tecnologie e servizi si trasformano in Appliances specializzate sempre più sofisticate, che divengono componenti di sub-forniture di soluzioni maggiori

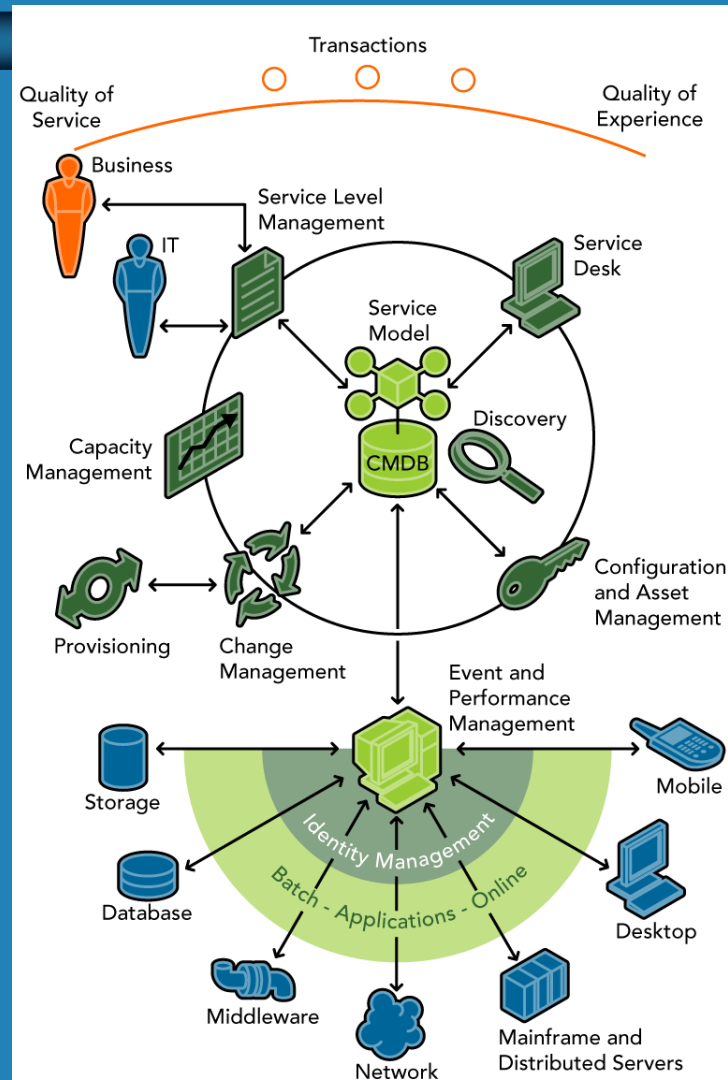
Conseguenze e strategie dei produttori sul mercato

Copyright BCI Italia

1. Le aziende specializzate nel settore stanno trasformando la propria offerta da "componenti software" ad **Appliance plug & play** mantenuti aggiornati via Internet su abbonamento
2. Il percorso verso le **Suite** viene declinato dai produttori del settore in base a due filosofie diverse, con un'evoluzione comune verso l'*outsourcing* specializzato (MSS):
 1. **Suite integrate** di uno stesso produttore che punta a diventare il *fornitore unico*
 2. **Framework** aperti ad accogliere strumenti e tecnologie di provenienza eterogenee
3. La **sicurezza come attributo** dei servizi regolato da SLA promosso dai fornitori di piattaforme integrate di gestione e dai fornitori di servizi di *outsourcing* integrale o di processi

Trend 2006-08: la sicurezza come attributo

- Si ragiona in termini di **piattaforme di gestione**, ragionando in termini di SLA a livello di sistema
- Si affermano pratiche quali ITIL ed il **Business Services Management** di BMC che correla gli interventi ed i servizi al loro valore per l'impresa



Leader di Mercato dell'Identity Management & Provisioning

Copyright BCI Italia

- | | | |
|-----|-----------------------|-----------------------------|
| 1. | Netegrity | CA |
| 2. | Baltimore ElectAccess | hp |
| 3. | Access360 | IBM |
| 4. | Oblix | Oracle (anche Octetstring) |
| 5. | Thor Technologies | |
| 6. | RSA Security | EMC e gli accordi con Thor? |
| 7. | WaveSet | Sun |
| 8. | Neogent | |
| 9. | Calandra | BMC |
| 10. | OpenNetwork | |

La Storia si ripete: dall'I&AM all'Information Security Management

Copyright BCI Italia

1. L'Identity & Access Management (I&AM) è stato artefice della rivoluzione che ha portato le problematiche relative alla sicurezza a livello di infrastruttura, con effetti tanto sulle applicazioni, quanto sulla gestione dei servizi IT
2. I produttori specializzati nel settore sono quasi tutti scomparsi, assorbiti da altri *player* svaniti nel nulla...

La Storia si ripete: dall'I&AM al Security Information Management

Copyright BCI Italia

1. **Ai nastri di partenza di un ciclo simile a quello dell'I&AM c'è oggi il Security Information Management**
2. **Potenziale inferiore a quello dell'Identity Management, ma si punta alla supremazia nella Security Governance con la gestione delle SOA sullo sfondo**

Security Information Management e Security Governance

Copyright BCI Italia

1. **L'Information Security Management aiuta a raccogliere ed interpretare in modo intelligente i segnali provenienti dai sistemi di Antivirus, Intrusion Detection, I&AM, Single Sign-on, autenticazione e così via**
2. **La Security Governance coniuga tecnologia ed organizzazione per assicurare che gli obiettivi dell'impresa siano allineati con le sue strategie di gestione dei sistemi e della sicurezza, in conformità alle normative vigenti.**