

## Il ruolo della Sicurezza Informatica nelle aziende italiane

La diffusione di nuove tecnologie in grado di rendere dati e informazioni fruibili in formato digitale ha reso più veloce e agevole la loro reperibilità, ma nello stesso tempo ha aumentato in misura considerevole la vulnerabilità delle aziende, che sono quotidianamente esposte al rischio di furti o attacchi non solo da parte di malintenzionati, ma molto più spesso dagli stessi dipendenti.

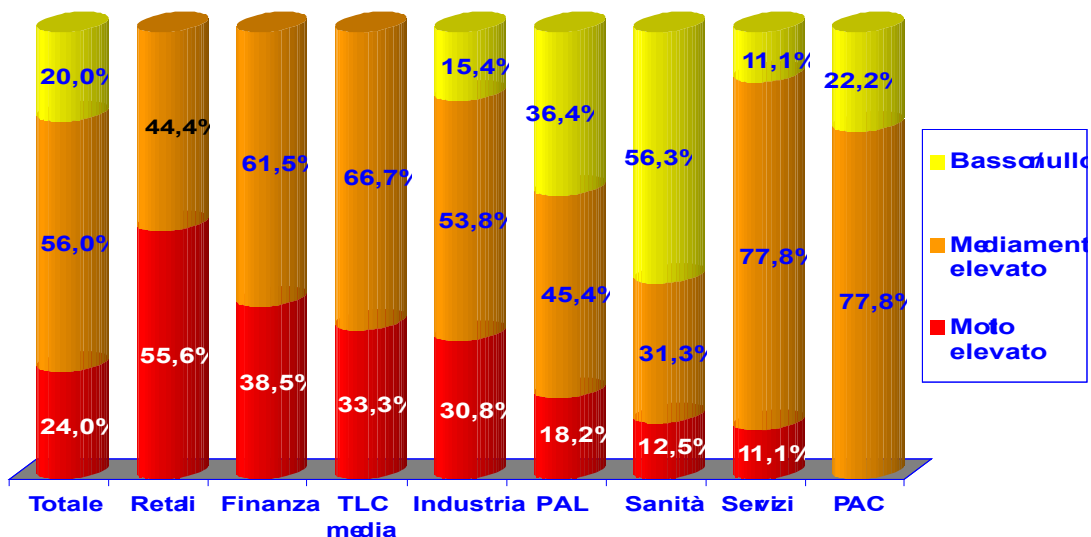
La sicurezza dei dati e delle informazioni diventa, in tale contesto, il presupposto fondamentale per lo sviluppo e la continuità del business.

Partendo da queste considerazioni, NetConsulting ha condotto un'indagine, promossa da CA, sul ruolo della sicurezza nelle aziende italiane, intervistando Security Manager e CIO di 108 aziende di dimensioni medio-grandi appartenenti a diversi settori merceologici. Dall'indagine è possibile estrapolare una fotografia dell'attuale livello di dotazione delle aziende in tema di sicurezza informatica, ma soprattutto della strategicità che tale tematica assume.

Un primo indicatore a riguardo è rappresentato dal dato relativo alla presenza di un'unità organizzativa con responsabilità nell'ambito della sicurezza informatica, rilevata presso il 64% delle aziende intervistate, con picchi elevati nel Finance, pari al 92%, e di contro una minor presenza nella PAL dove questo tipo di unità esiste solo presso il 36% degli enti.

Anche dal punto di vista del Commitment che il Top Management attribuisce alla sicurezza, a fronte di un dato medio abbastanza elevato, si riscontrano differenze rilevanti tra i settori che si traducono in un commitment molto elevato nel Retail e nel Finance, cui si contrappone un commitment molto basso nella Sanità e nella PAL (fig. 1)

Figura 1 Commitment del Top management alle problematiche della sicurezza



Fonte: NetConsulting 2006

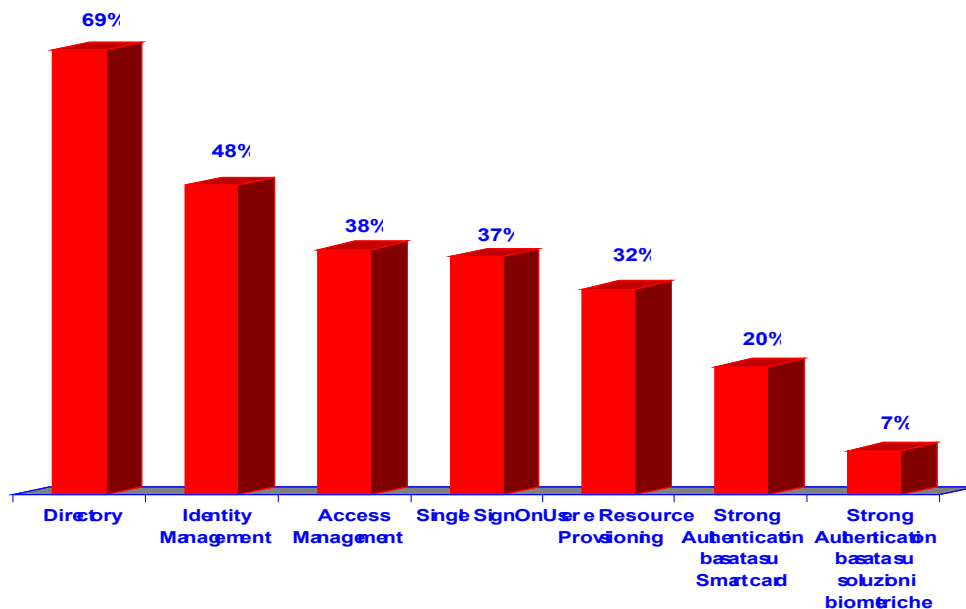
Completa questo quadro la presenza di strumenti per la pianificazione di interventi e per stabilire le norme e le procedure da seguire per garantire la sicurezza aziendale. La diffusione di norme e procedure formalizzate è abbastanza elevata, così come l'adozione di un piano di sicurezza completo. Meno elevata è invece l'adozione di un Business Continuity Plan, che viene utilizzato in misura rilevante solo nel Finance, dove, peraltro, ha influito la pressione esercitata dalle direttive a riguardo introdotte da Banca d'Italia.

Il quadro relativo all'adozione delle diverse tipologie di strumenti di sicurezza informatica appare molto disomogeneo, con aree ancora in gran parte scoperte. Nell'area del Threat Management, ovvero delle soluzioni che consentono di individuare e prevenire attacchi informatici come virus, intrusioni e abusi della rete, le aziende hanno raggiunto un grado copertura molto elevato, seppure anche qui con delle differenze tra i diversi strumenti considerati: sono soprattutto Antivirus e Firewall ad avere la maggiore diffusione, con una penetrazione pari rispettivamente al 100% e al 99% del campione. Si tratta di soluzioni di cui qualsiasi azienda che abbia il proprio sistema informativo collegato a Internet non può più fare a meno. Subito dopo, con una presenza presso l'81% delle aziende, arriva l'antispam. Meno diffuse le tecnologie di antispyware e di Intrusion Detection, adottate rispettivamente dal 64% e dal 56% delle aziende, probabilmente a causa dell'approccio superficiale di alcune aziende che ritengono di essere sufficientemente protette una

volta installato un firewall e un antivirus, sebbene si tratti di strumenti non sufficienti per attuare una politica preventiva a 360 gradi.

Meno diffuse, inoltre, risultano le soluzioni per la gestione delle autenticazioni e degli accessi, ovvero l'Identity & Access Management. Si rileva, infatti, una presenza piuttosto cospicua solo di soluzioni di Directory (69%), ovvero il repository in cui risiedono le identità aziendali e le relative password, anche se queste rappresentano solo una piccola parte di una gestione degli accessi più completa, integrata, automatizzata e centralizzata di tutti gli utenti aziendali, che garantisce un accesso sicuro alle applicazioni. A tale funzionalità rispondono le soluzioni di Identity & Access Management, che, con una penetrazione rispettivamente del 48% e del 38%, risultano però ancora poco diffuse; le User e Resource Provisioning, a loro volta, sono presenti solo presso il 32% delle aziende. Una presenza ancora più limitata è raggiunta da soluzioni di Strong Authentication, che possono basarsi su Smart Card o, qualora si voglia garantire una sicurezza ancora più elevata, su tecnologie biometriche, che consentono l'autenticazione dell'utente attraverso alcuni valori quali impronte digitali o retina oculare (fig. 2).

**Figura 2 La diffusione di soluzioni per la gestione delle autenticazioni e degli accessi alle applicazioni aziendali**

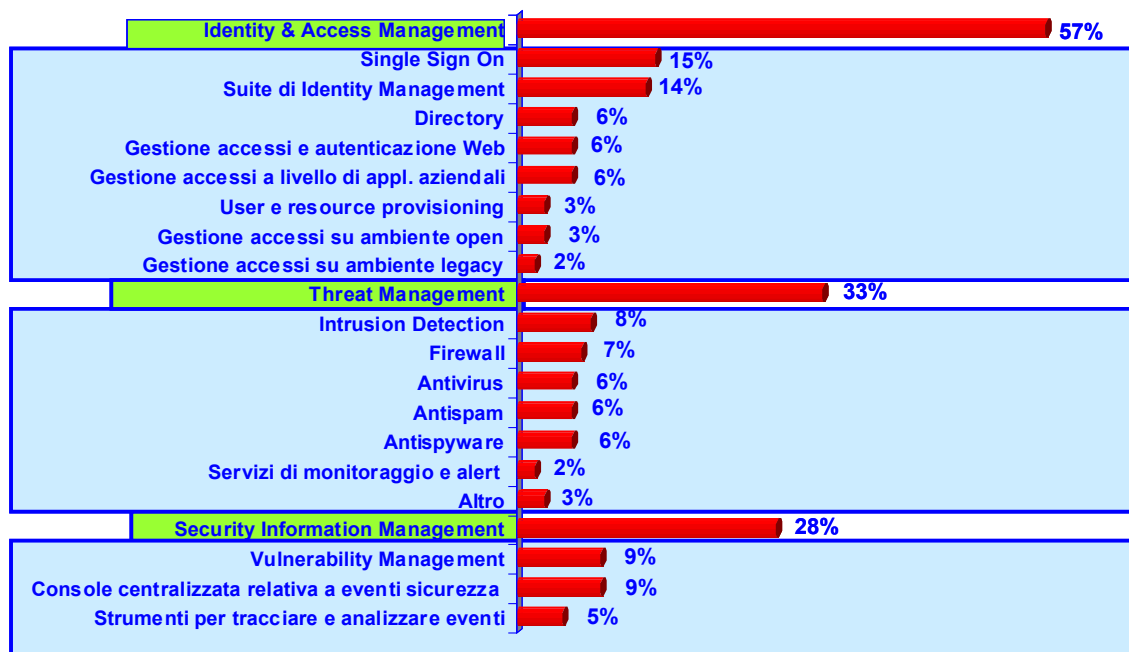


Fonte: NetConsulting, 2006

Ancora meno diffusi, ma in forte ascesa se si guarda al medio lungo periodo, sono i cruscotti per il monitoraggio di eventi legati alla sicurezza al fine di individuare eventuali anomalie, generare alert e prevenire in questo modo eventuali danni da attacchi, su cui solo il settore delle Telecomunicazioni ha già raggiunto un discreto grado di adozione.

Le prospettive di investimento per il 2007 sono orientate proprio a colmare i gap rilevati sull'area dell'Identity & Access management, su cui il 57% delle aziende intervistate prevedono di investire, con un focus particolare sul Single Sign on, ovvero sulle soluzioni che consentono di accedere alle applicazioni aziendali attraverso la digitazione di un'unica password e ID al momento dell'accesso al sistema. Sul Threat management si continuerà ad investire, soprattutto per sostituire o aggiornare soluzioni già esistenti. Si rileva, infine, un discreto interesse già nel 2007 sull'area del Security Information management, che rientra nei piani di investimenti del 28% delle aziende (fig. 3).

**Figura 3 Investimenti previsti o in corso in ambito sicurezza informatica**

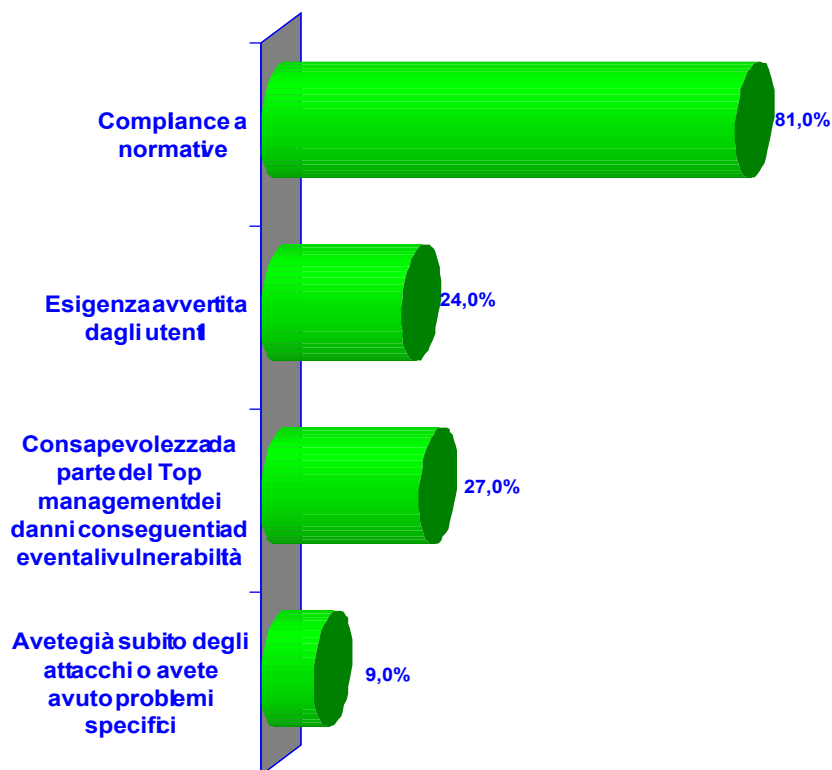


Fonte: NetConsulting, 2006

Tra i principali stimoli ad effettuare investimenti in sicurezza, al primo posto si pone l'adeguamento normativo, citato dall'81% delle aziende intervistate. In particolare, emerge dall'indagine l'esigenza

di rispondere al Testo Unico sulla Privacy, che impone il rispetto di una serie di norme di comportamento, seguito dalla Sarbanes-Oxley, che riguarda però le sole aziende con azioni quotate nelle Borse USA, in particolare nel settore Finance, e da Basilea 2, limitatamente alle Banche (fig.4).

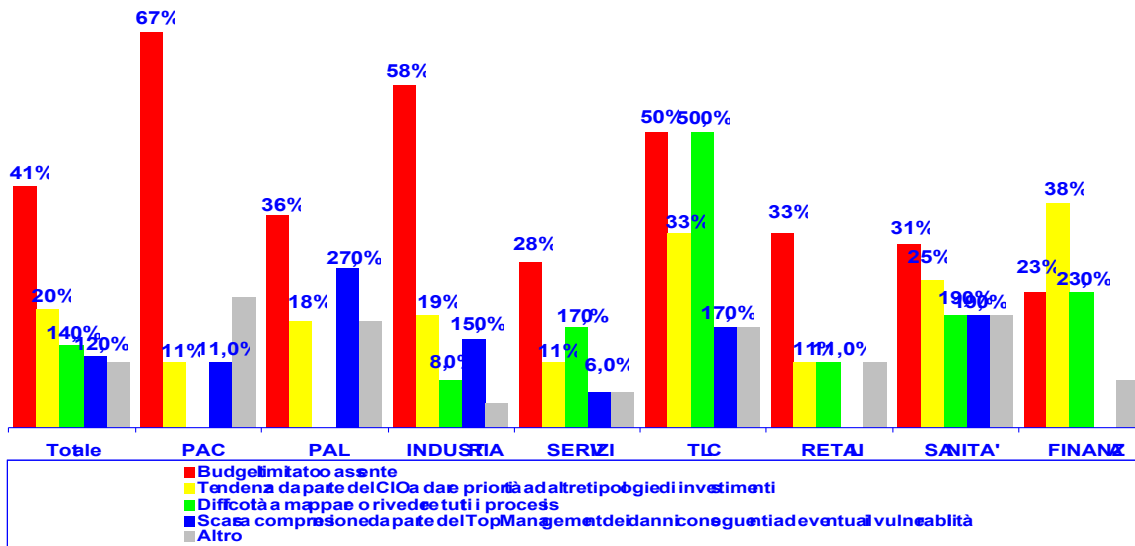
**Figura 4 I driver degli investimenti in sicurezza**



Fonte: NetConsulting 2006

Meno rilevanti in termini di intensità di risposte i fattori che frenano gli investimenti, quasi a conferma dell'evidente necessità rappresentata dall'adozione di soluzioni di sicurezza informatica. Il principale freno è rappresentato dai vincoli di budget, rilevato presso il 41% degli intervistati, mentre a seguire troviamo la tendenza da parte del CIO a dare priorità ad altri investimenti, che però evidenzia una percentuale di risposte molto bassa, pari al 20% (fig. 5).

Figura 5 Fattori di freno agli investimenti in sicurezza

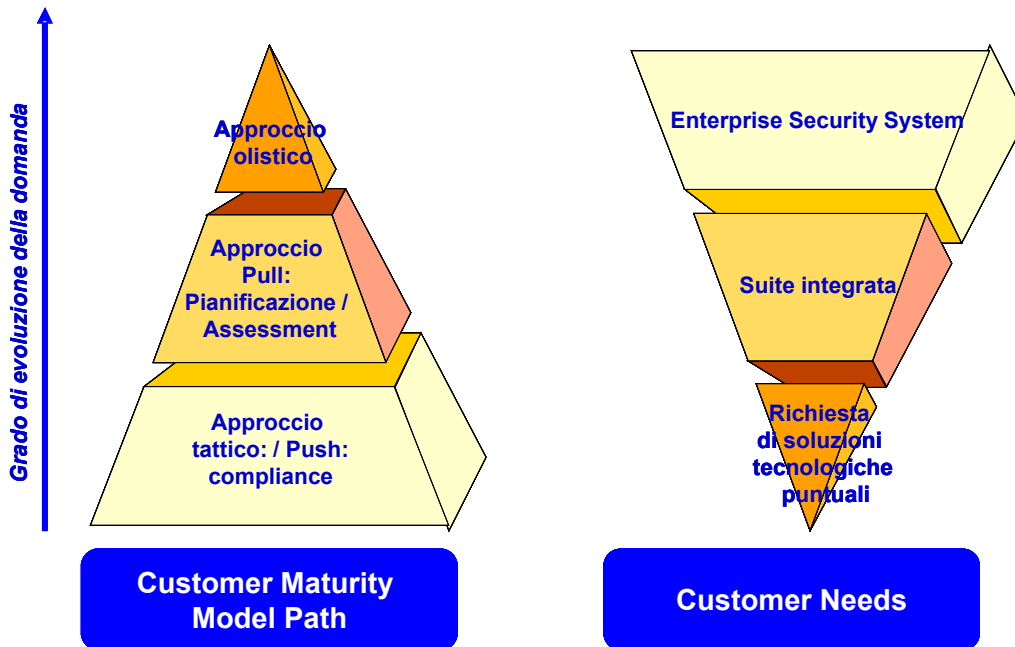


Fonte: NetConsulting, 2006

Il budget rappresenta senza dubbio un limite, soprattutto se si considera che le aziende hanno a disposizione mediamente una cifra di poco superiore a 1 milione di euro per gli investimenti in sicurezza, seppure con valori profondamente diversi tra i settori merceologici considerati.

Il quadro che emerge dall'indagine, pertanto, è molto eterogeneo: solo alcune aziende, soprattutto del settore Telecomunicazioni e Finance, hanno intrapreso un percorso evolutivo verso un approccio strategico alla problematica della sicurezza e solo in pochissimi casi si può parlare di un approccio olistico, in cui la sicurezza riguarda anche i processi, agendo in modo preventivo e adottando un programma di gestione dei rischi aziendali. La maggior parte delle aziende ha ancora un approccio tattico alla problematica, che si traduce nella domanda di soluzioni puntuali e nell'assenza di pianificazione (fig. 6).

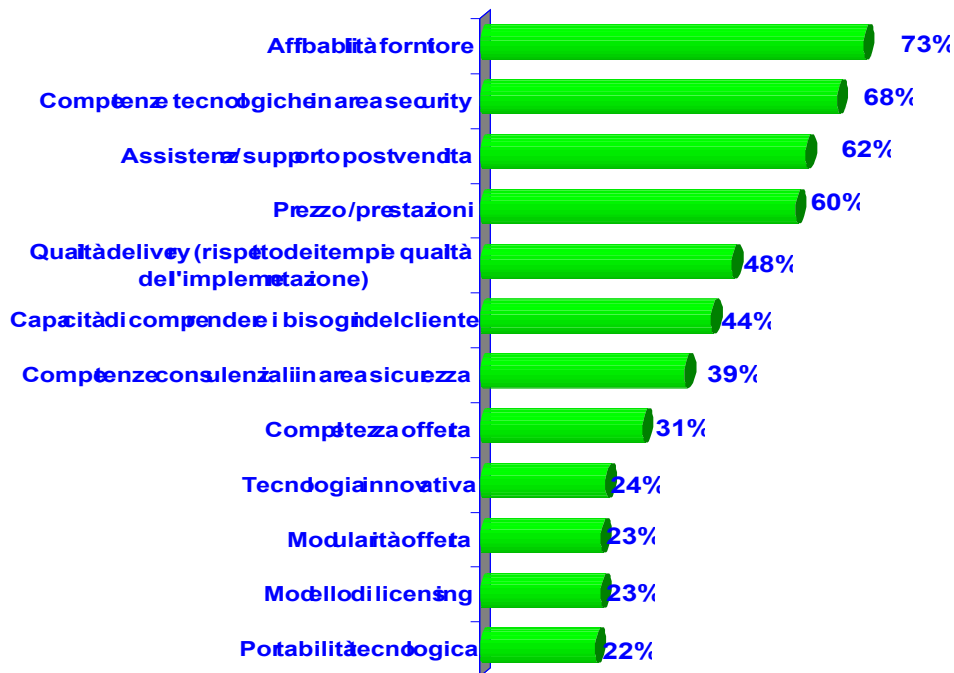
Figura 6 Il Customer Maturity Model Path verso la sicurezza



Fonte: NetConsulting, 2006

Per intraprendere un percorso evolutivo di questo tipo, bisogna riconosce un ruolo strategico al fornitore che deve essere in primo luogo affidabile e avere competenze tecnologiche molto forti sulla tematica della Security, oltre ad avere la capacità di fornire un'adeguata assistenza nella fase post vendita e un buon rapporto qualità/prezzo (fig. 7).

**Figura 7 Caratteristiche di un fornitore ottimale**



Fonte: NetConsulting, 2006

In sintesi, sono ancora elevate le barriere da superare per intraprendere un percorso consapevole verso l'adozione di un modello evoluto di Enterprise Security System e il budget limitato rappresenta per molte aziende un fattore vincolante. E' possibile però rimuovere questi ostacoli evidenziando al top management come una politica lungimirante sulla sicurezza dei sistemi, ma anche un'accurata gestione delle informazioni e delle infrastrutture su cui queste risiedono, contribuiscano in misura rilevante a preservare il patrimonio informativo aziendale.

L'indagine realizzata da Netconsulting evidenzia, fra le caratteristiche del fornitore ideale, requisiti in linea con le strategie di CA, relativamente all'area sicurezza IT.

CA è presente nel mercato dell'IT security dai primi anni ottanta con soluzioni per la protezione dei sistemi mainframe. Nel corso degli anni, ha modificato la sua offerta tecnologica e di servizi per rispondere alle esigenze del mercato che dal mainframe è passato a considerare i sistemi distribuiti e web.

Le competenze progettuali messe in campo dalla divisione Technology Services di CA, ove operano consulenti certificati secondo standard internazionali quali CISSP, CISA, CISM e hanno



superato esami di Lead Auditor BS7799/ISO 17799, sono una garanzia per il cliente. In aggiunta va sottolineata la ricca schiera di Partner con conoscenze tecnologiche, organizzative e legali rispetto a questo tema che colloca CA fra i fornitori in grado di soddisfare le molteplici esigenze in ambito sicurezza, nelle tre aree menzionate: Identity & Access Management, Security Information Management e Threat Management. Non va inoltre dimenticato che CA è riconosciuta fra i leader tecnologici sia nella prima che nella seconda area, oltre ad essere il vendor che da 6 anni ricopre la prima posizione a livello Worldwide (secondo indagini di IDC) relativamente al fatturato di Identity & Access Management. Nel 2007 CA prevede di consolidare ulteriormente la propria presenza nel mercato italiano della sicurezza IT, con l'acquisizione di nuovi clienti nell'ambito Identity and Access Management, dove anche secondo l'indagine di Netconsulting si assisterà ad un'ulteriore crescita.

Inoltre, CA punta a rafforzare la sua leadership anche nelle tecnologie di Security Information and Event Management, che consentono di realizzare una vera e propria IT Security Governance. Alcune aziende già hanno affrontato questo tema con le soluzioni CA, e altre sono in fase di valutazione. Relativamente all'area del Threat Management, a parte la riconosciuta tecnologia Antispyware di CA, è appena stata annunciata la nuova soluzione denominata CA HIPS (Host Intrusion Prevention System), che proviene dall'acquisizione di una nota azienda del settore: Tiny Software. Anche questa strategia è in linea con le esigenze dei clienti e i futuri sviluppi del mercato; in base al survey, infatti, la presenza di sistemi antiintrusione è ancora generalmente scarsa presso le aziende italiane.