



DFLabs Business Security BluePrint.

A premier on IT Security Governance

La Security Governance: Nuova indagine di Carnegie Mellon

Dario Forte

La generazione tecnica cresciuta e sviluppatasi ormai un decennio fa è quella che ormai ha la responsabilità della security governance delle aziende. Un recente survey effettuato dalla Carnegie Mellon University ha analizzato le tendenze di security governance, stimolando tutti ad una seria riflessione.

Una situazione complessa

Tagli di budget, crisi finanziaria, compliance, protezione delle informazioni. Sono tematiche che in questo momento storico sono in continuo conflitto tra di loro, pur avendo, a seconda delle prospettive, la stessa importanza strategica. Al momento in cui scriviamo, queste priorità vengono gestite, a vario titolo, da numerose funzioni all'interno delle Aziende, le quali hanno, evidentemente, differenti priorità e budget. Le funzioni sicurezza IT, per esempio, stanno avendo generalmente un commitment di tipo tattico, orientato in questo periodo al mantenimento delle piattaforme già esistenti, con un relativo sguardo (attendista) alle problematiche ritenute di emergenza (per esempio: Data Loss Prevention). A livello più alto, invece, si sta prestando una certa attenzione ad attività di monitoraggio interno (sia per prevenzione frodi sia per illeciti/incidenti di sicurezza aziendali in genere) il cui costo è sicuramente elevato ma al contempo giustificato da esigenze di governance.

Proprio su quest'ultimo fattore si è concentrata una recente iniziativa dell'Università di Carnegie Mellon negli Stati Uniti.

All'interno di questa struttura è inquadrato il Cylab, un gruppo di ricercatori specializzati provenienti da tutto il mondo, tra i quali vi è Richard Power, già noto per essere l'ideatore del Csi FBI Computer Crime Survey. Carnegie Mellon CyLab ha quindi intrapreso uno studio finalizzato a misurare il grado di governance supportato dai board aziendali e dal senior management. Questa indagine, denominata CyLab 2008 report on its Governance of Enterprise Security Survey ("Governance Survey"), è stata stilata su un campione di 703 manager presso aziende americane quotate. I due terzi degli intervistati sono componenti esterni del Board, mentre i rimanenti sono costituiti da personale interno e da cosiddetti "non-voting board attendees", che includono senior management, general counsels (responsabili affari legali), e responsabili affari generali.

I risultati

Dal punto di vista generale, il survey ha rivelato che i Board prendono in maniera estremamente seria il risk management, ma sussiste ancora un notevole gap nella comprensione del collegamento tra IT ed enterprise risk management. Molte delle domande che sono state poste agli intervistati, hanno ricevuto la conferma che sia il Board sia molti senior executives non sono adeguatamente coinvolti nelle cosiddette "key areas" inerenti la governance della enterprise security. Nella fattispecie, sull'intera base degli intervistati, solo il 36% di essi ha indicato che il board ha avuto un ruolo diretto nella definizione dell'information security. Vi è poi un numero consistente di best practices relative al coinvolgimento del board su ruoli di IT governance, ma i risultati del survey hanno indicato che i Consigli di Amministrazione sono interessati soltanto occasionalmente alle attività indicate in queste best practices.

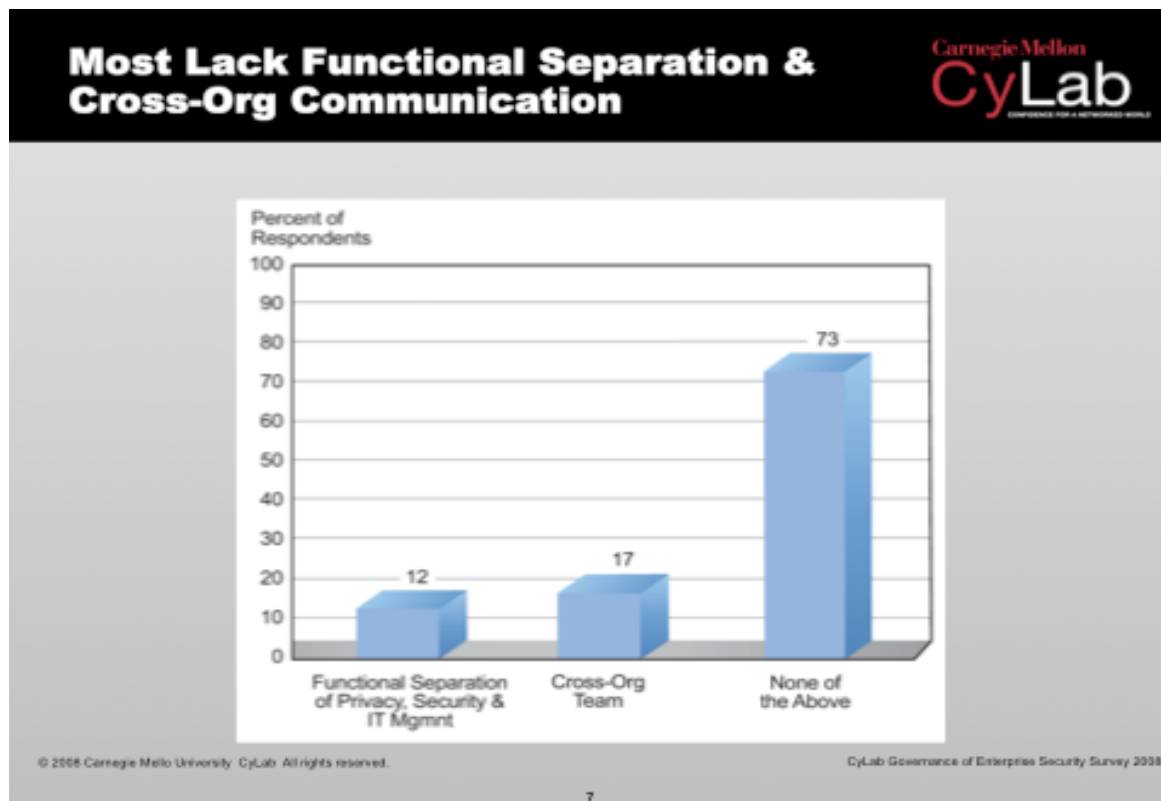
Una delle indicazioni, quindi, è quella di un maggior coinvolgimento del top management nelle attività di Governance. Cio' è ulteriormente confermato da alcuni intervistati che hanno riferito che molti Board of Directors coinvolti nella revisione delle politiche di sicurezza e privacy sono concentrati soltanto sul lato formale e non su alcuni controlli/indirizzi di tipo sostanziale che invece hanno un ruolo più importante, come per esempio il rischio reputazionale e le perdite derivanti da trattamento errato (illecito, per la legge italiana) di dati personali.

Il Governance Survey, inoltre, ha denotato che i Board rivestono un'estrema fiducia nell'operato dei comitati di controllo (Audit Committees), a volta sopravvalutandone i ruoli e le

responsabilità. Ciò di solito viene accertato principalmente in caso di incidente. L'inchiesta ha altresì denotato che molti board non separano la gestione del rischio dalle responsabilità di audit, mentre solo l' 8.5% degli intervistati ha dichiarato che il board ha al suo interno un Risk Committee e, di questi, solo il 54% si occupa direttamente di privacy e security. Questo viene definito in letteratura "The segregation of duties issue" e si verifica quando il board (o i suoi delegati) "governano" sia lo sviluppo dei programmi di sicurezza sia l'audit di questi ultimi.

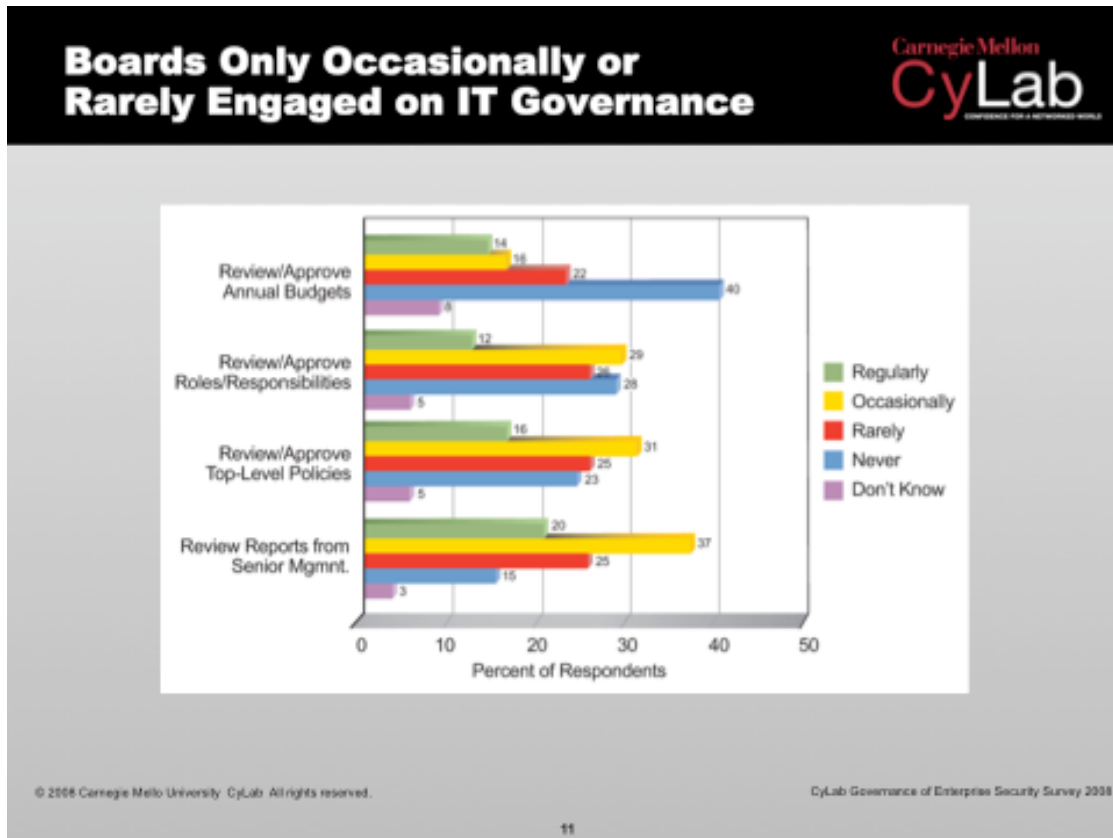
Continuano le problematiche organizzative.

Il survey ha inoltre acquisito ulteriori interessanti particolari: Per esempio sono molte le organizzazioni intervistate che hanno fornito risposte circa le cosiddette deficienze organizzative. Molti intervistati, per esempio, hanno indicato di lavorare con mancanza effettiva di separazioni funzionali tra gli organi di privacy e sicurezza. In particolare, solo il 12% degli intervistati ha dichiarato che al loro interno è presente una separazione di ruoli e responsabilità in tal senso, con particolare riferimento a .privacy, security, e IT management. E' stata inoltre richiamata l'attenzione sulla comunicazione interna in temi di privacy, sicurezza ed aspetti correlati. Solo il 17% degli intervistati ha parlato esplicitamente di un'organizzazione ben definita di security management in grado di funzionare con efficacia.



Le raccomandazioni del survey

E non solo, verrebbe da dire. Molte di queste raccomandazioni sono consequenziali alle risposte ricevute, alcune delle quali sono forse preoccupanti. La priorità è sicuramente quella di separare il Risk Committee separate dall' Audit Committee, assegnando al primo responsabilità ben definite anche in ordine alle problematiche di rischio IT. Su questo non tutti sono d'accordo. Molti infatti ritengono che quest'ultimo fattore vada semplicemente "indirizzato" con un commitment ben definito ma comunque finalizzato alla tutela delle informazioni non degli asset IT. Un altro suggerimento che viene dato riguarda la creazione di un comitato stabile di sicurezza al cui interno vi siano collocati CIO, CFO, Legal e, ovviamente, i componenti la struttura di security. Il ruolo del comitato sarà sicuramente quello di indirizzo sia di livello alto sia di gestione crisi (ove necessario). Detto comitato, unitamente ad altre eventuali figure all'interno del board, dovrebbe altresì gestire una review annuale del cosiddetto "enterprise security program", a sua volta da sottoporre ad audit. Questi ultimi dovrebbero comunque essere effettuati almeno annualmente.



Conclusioni

Il survey è da una parte preoccupante, in quanto conferma il gap di conoscenza ed interesse manifestato dal top management delle aziende intervistate. La visione delle tabelle inserite in questo articolo, inoltre, conferma che vi è ancora molto da fare, sia in termini di organizzazione, sia di awareness in generale. Viviamo, inoltre, in un momento storico in cui i fondi per l'applicazione di un programma serio di sicurezza sono, in alcune realtà, limitati. Pertanto esiste anche un problema di carattere oggettivo causato dalla situazione contingente. Tuttavia, è pur vero che, dalle pagine del survey stesso, è possibile carpire che parte degli investimenti necessari non richiedono un impiego diretto di fondi, bensì una più efficace razionalizzazione di strategie e rispettive applicazioni.

*DFlabs Italy is a company specialized in Information Security Risk Management. With its three practices (Business Security, Compliance and Data Security), DFLabs is one of the most respected company at international level.
www.dflabs.com*

Per ulteriori approfondimenti DFLabs è lieta di organizzare un follow up, contattando info@dflabs.com

