TOLLERANZA DEL CAMBIAMENTO

La gestione del cambiamento IT è l'ultimo fattore da prendere in considerazione per capire in che modo le aziende riusciranno a sopravvivere in questo contesto caratterizzato da un elevato livello di rischio. Come indicato nella prima parte del documento, gli approcci alla sicurezza informatica basati su best practice rappresentano un cambiamento rispetto alle metodologie utilizzate da anni. Per cambiare la mentalità e la filosofia delle aziende in termini di sicurezza occorre integrare il cambiamento nell'IT a sostegno di questi processi.

In questo caso, l'elemento chiave è costituito dalla trasformazione digitale, uno dei motivi principali a spingere le aziende a gestire livelli di rischio di queste dimensioni. Le metodologie standard utilizzate dai professionisti della sicurezza potrebbero limitare l'adozione di tecnologie come social business, mobilità, Big Data/analytics e cloud, tecnologie che potrebbero aumentare l'esposizione al rischio. Tuttavia, si tratta di un approccio poco maturo: invece di arrestare la trasformazione digitale, le aziende più avanzate dovranno aumentare i mezzi a disposizione degli utenti fornendo strumenti utili per attuare la trasformazione digitale in maniera sicura.

Come indicato nella figura 4 riportata di seguito, la maturità di un'organizzazione, come definito nella ricerca, è direttamente proporzionale alla capacità di gestione del cambiamento IT. Le aziende meno mature, indicate nella parte bassa della scala, non riescono a gestire i cambiamenti IT in maniera ottimale, soprattutto per quanto riguarda l'implementazione di elementi che vadano oltre le modifiche di base apportate ad applicazioni e servizi. Al contrario, le aziende più evolute, presenti nella parte alta della scala di maturità, ritengono di gestire questo tipo di cambiamenti in maniera quantomeno ottimale.

In base ai risultati, uno degli elementi chiave per diventare un'azienda dinamica e di successo nell'attuale ambiente relativo alla sicurezza consiste nell'adottare un approccio maturo nei confronti della sicurezza e nel gestire i cambiamenti IT in maniera audace e coraggiosa, anziché temerli. Si tratta di un fattore bidirezionale caratterizzato da una forte associazione tra questi elementi. capacità di cambiare L'IT richiede una gestione matura delle implicazioni relative alla sicurezza. Allo stesso tempo, per adottare un atteggiamento maturo nei confronti della sicurezza, occorre la capacità di cambiare ed evolvere l'IT aziendale.

Capacità di gestire il cambiamento in base ai livelli di maturità dei rischi informatici

Q2. In caso di richieste da parte di aziende per applicazioni o servizi nuovi o avanzati, quale affermazione riflette meglio le capacità del reparto IT della Sua organizzazione?

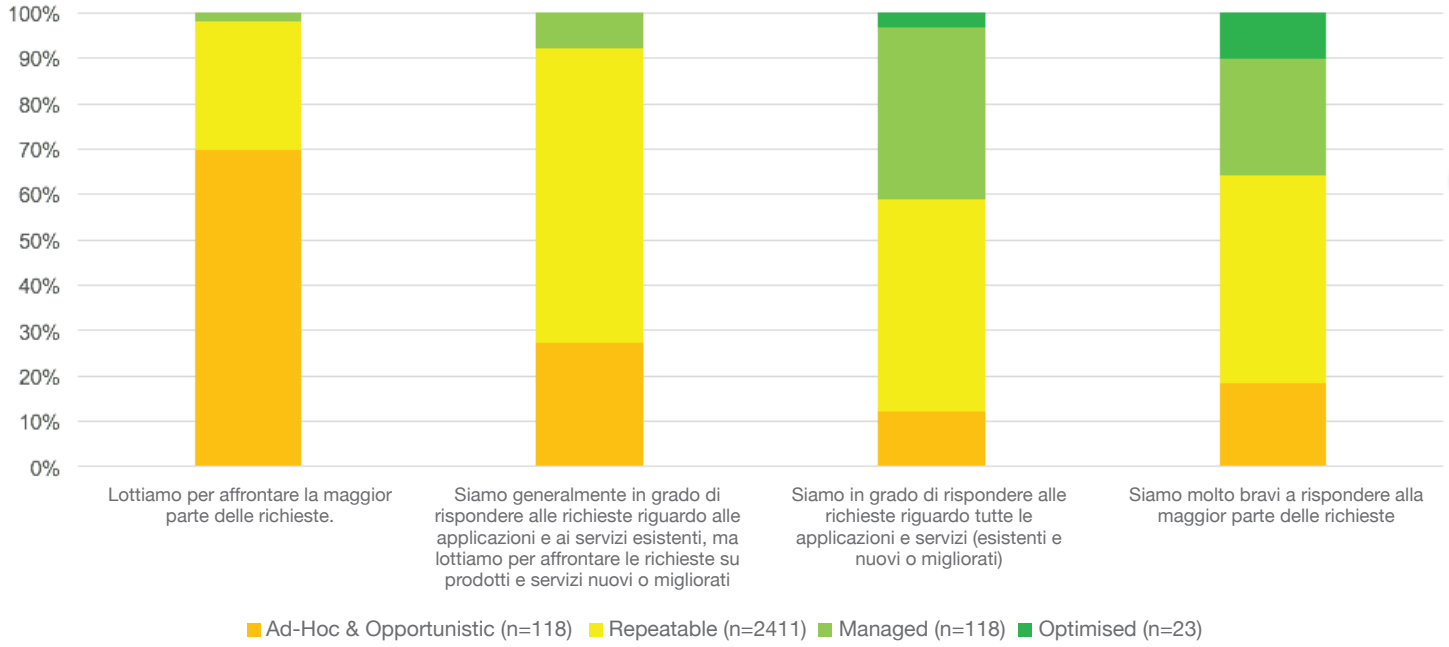

Figura 4 *Source: IDC, 2016*

10 SUGGERIMENTI PER LA VOSTRA ORGANIZZAZIONE

Seguono 10 suggerimenti che costituiscono un quadro generale per migliorare il livello di maturità relativo alla sicurezza dell'azienda:

- **Confrontare la vostra posizione con quella dei concorrenti più simili in termini di settore, dimensioni e localizzazione geografica.**
- **Definire una strategia relativa alla maturità attuale e a quella desiderata.**
- **Individuare le lacune del vostro approccio attuale sulla sicurezza rispetto allo stato desiderato.**
- **Valutare l'impiego di specialisti di sicurezza di terze parti per la progettazione e l'implementazione dei cambiamenti necessari per raggiungere il vostro obiettivo.**
- **Identificare i processi e le attività di sicurezza essenziali e quelli ripetitivi e di minor valore.**
- **Individuare le attività di minor valore da automatizzare per ridurre l'utilizzo delle risorse.**
- **Individuare i punti in cui ottimizzare i risultati collaborando con i MSSP. È possibile iniziare individuando le attività di minor valore in modo da sfruttare modelli di erogazione industrializzati e globali.**
- **Tuttavia, quando i MSS diventeranno una consuetudine comunea livello aziendale, sarà possibile avvalersi delle competenze specialistiche per ottimizzare i risultati desiderati in termini di costi e qualità.**
- **Adottare un approccio basato sulla valutazione dei rischiche gravano sull'intera impresa. Ogni utente potrebbe rappresentare una potenziale "minaccia interna", per cui è consigliabile una strategia e una cultura di tipo olistico a livello di sicurezza.**
- **Coinvolgere sin dall'inizio i responsabili della sicurezza nelle nuove iniziative aziendali. Verificare che le nuove iniziative siano progettate considerando la sicurezza in modo da semplificare il lavoro successivo.**