Cybersecurity: una regolamentazione unica europea tra tutela della Privacy e sviluppo digitale

Nell'era digitale il tema della sicurezza dei dati e del rischio informatico è sempre più urgente.
La Confederazione Europea degli Istituti di Internal Auditing e la Federazione delle Associazioni dei Risk Manager Europei includono la questione della cybersecurity tra le competenze della corporate governance

Milano, 27 luglio 2017 - Un gruppo di lavoro congiunto, che rappresenta i Risk Manager e i revisori interni di 8 paesi dell'UE e di 6 diversi settori economici (banche, trasporti, difesa, IT, servizi alimentari e telecomunicazioni) ha sviluppato una serie di linee guida per le organizzazioni riguardo alle modalità innovative per organizzare internamente la gestione dei rischi informatici, presentandole presso la sede del parlamento Europeo di Bruxelles.

La digitalizzazione rappresenta un trend in accelerazione in tutto il mondo, costituendo un'opportunità chiave di business per le aziende europee e diventando cruciale per lo sviluppo di numerose organizzazioni, tanto quanto la sicurezza informatica. Di conseguenza oggi avere una strategia digitale è essenziale per la gestione di ogni tipo di impresa.

"*I dati delle imprese aprono opportunità per le organizzazioni europee, tuttavia, il bisogno di un ambiente sicuro si sta fondendo con le preoccupazioni dei consumatori in merito alla protezione dei dati personali.*" Dichiara **Alessandro De Felice, Presidente di ANRA** "Per le organizzazioni diventa così opportuno combinare in un unico processo i propri obblighi in tema di privacy e la pianificazione strategica delle attività delle norme sul trattamento dei dati, migliorando al contempo la qualità della gestione del progetto e riducendo i costi".

In questo contesto, la **European Confederation of Institutes of internal Auditors (ECIIA)** e la **European Federation of Risk Management Associations (FERMA)** hanno lavorato insieme allo sviluppo di una infrastruttura di gestione e governance del rischio informatico per il settore privato.

Una robusta infrastruttura per la governance del rischio informatico migliorerà i processi decisionali delle aziende, conducendo ad un migliore sviluppo dei prodotti e dei servizi, e allo stesso tempo fornendo una garanzia più forte e comprensiva che i rischi vengano identificati, quantificati, gestiti - in modo più efficiente e ad un costo inferiore - e mitigati.

ECIIA e FERMA sostengono che le organizzazioni debbano costituire un sistema di governance del rischio informatico, supportate da una infrastruttura di gestione dello stesso. È necessario dirigersi verso l'implementazione delle misure di IT, allo scopo di proteggere efficacemente le proprie attività e assicurarne la resistenza e continuità. Il modello è ancorato a due forti serie di principi: gli otto principi definiti nella

raccomandazione di OECD sul Digital Security Risk Management (2015) e le Three Lines of Defence model, riconosciute come standard dell'Enterprise Risk Management (ERM).
La prima linea di difesa ha il compito dell'implementazione delle polizze e degli standard tecnici, e ha la responsabilità di monitorare giorno per giorno le reti e le infrastrutture. La seconda linea è responsabile della maggior parte delle funzioni di governance relative alla sicurezza informatica. La terza e ultima è formata dall'Internal Audit, che supervisiona l'operato delle prime due linee e controlla la coerenza dell'intero processo di cyber risk governance, oltre a fornire un backup periodico al board.

"Fondamentalmente, una buona governance del rischio informatico consiste nel proteggere il valore all'interno dell'organizzazione." dichiara **Jo Willaert, Presidente di FERMA** *"I Consigli avranno sempre più bisogno di dimostrare agli investitori e al pubblico che i rischi informatici sono gestiti, non solo da un punto di vista tecnico, ma anche da una prospettiva finanziaria e gestionale. Gli stakeholder esterni richiederanno sempre di più la garanzia che le organizzazioni abbiano posto in essere un'efficiente gestione del rischio informatico".*

Il modello di gestione del rischio informatico proposto sostiene la creazione di un Cyber Risk Governance Group dedicato, la cui missione consiste nel determinare quali siano le esposizioni al rischio informatico in termini finanziari e delineare possibili piani di attenuazione.

"Questo modello costituisce un modo innovativo per approcciare la sicurezza informatica che consentirà al Consiglio Direttivo di dimostrare che la gestione dei rischi informatici è basata su un'analisi documentata e razionale dei rischi interni all'organizzazione." conclude **Jo Willaert, Presidente di FERMA** "FERMA e ECIIA, rappresentando le professioni di Risk Management e Internal Audit a livello europeo, giocano un ruolo chiave nell'apportare un contributo positivo alla modernizzazione di una buona governance per l'era informatica".

***

CHI È FERMA

FERMA - Federation of European Risk Management Associations, riunisce le 22 associazioni nazionali di risk management di 20 nazioni europee. Rappresenta oltre 4.200 professionisti che operano nei più svariati campi, dall'industria, al commercio, alla finanza presso le più importanti realtà imprenditoriali, organismi statali, privati o enti benefici. I membri rivestono un ruolo chiave nelle loro organizzazioni in quanto presidiano tutte le attività di gestione dei rischi assicurativi.

ferma.eu

CHI È ANRA

ANRA è l'associazione che dal 1972 raggruppa i risk manager e i responsabili delle assicurazioni aziendali. L'associazione opera attraverso la sede di Milano e vari corrispondenti regionali. ANRA è il punto di riferimento in Italia per diffondere la cultura d'impresa attraverso la gestione del rischio e delle assicurazioni in azienda. Si relaziona con le altre associazioni nazionali di risk manager in Ferma, a livello europeo, e in Ifrima a livello internazionale. ANRA è costituita da Risk Officer, Risk Manager ed Insurance Manager che operano quotidianamente nella professione e che trovano vantaggio nello scambio continuo delle proprie esperienze e nella condivisione di progetti a beneficio dello sviluppo del settore. Complessivamente, le aziende pubbliche e private di cui fanno parte i soci rappresentano un fatturato complessivo di oltre 600 miliardi (pari a circa il 39% del PIL). Nella piena convinzione che l'esperienza sia il miglior argomento per diffondere la cultura del risk management, ANRA organizza incontri aperti a professionisti ed aziende su tematiche inerenti al rischio aziendale, corsi di formazione per nuove figure e scambi di esperienze con colleghi stranieri. Nella sua attività di supporto a manager ed imprese, ANRA si appoggia a molti partner, come enti universitari,

società di consulenza, compagnie assicurative, broker, società di servizio nell'ambito del rischio d'impresa: con le loro competenze specifiche, tutti questi attori portano valore aggiunto ai membri dell'associazione e alle loro imprese. Dal giugno 2016 ANRA promuove "alp" - ANRA Learning Path - la nuova Accademia ANRA per la formazione dei professionisti della gestione del rischio, riconosciuta e certificata RIMAP a livello europeo.

Ufficio stampa ANRA:

Mirandola Comunicazione
www.mirandola.net | Tel +39 0524.574708
Simona Miele | simona.miele@mirandola.net + 39 348 2509895

Media Contacts FERMA:

Lee Coppack
Media coordinator, FERMA
T: +44 (0) 7843 089904 (3-11 October); +44 (0) 208 318 0330 (after 11 October)
lee@coppack.co.uk