

I reati informatici

Governance, Risk & Compliance



I reati informatici

Dal 5 Aprile 2008 è in vigore la legge 48/08 di ratifica della Convenzione del Consiglio d'Europa sulla Criminalità Informatica siglata a Budapest il 23 Novembre 2001. La legge estende l'ambito di applicazione del D.Lgs 231/2001 (responsabilità amministrativa delle persone giuridiche) introducendo, tra i reati presupposto per l'applicabilità del decreto, i cosiddetti "Reati Informatici".

Alcuni esempi di attività illecite condotte nell'interesse o vantaggio dell'Ente

- Accesso a sistemi informatici di aziende competitors allo scopo di copiare informazioni utili per battere la concorrenza;
- Accesso a sistemi informatici afferenti ad Enti Pubblici allo scopo di modificare dei dati a vantaggio dell'ente;
- Intercettazione di telecomunicazioni allo scopo di veicolare false informazioni a vantaggio dell'ente;
- Diffusione di programmi appositamente modificati (virus) che alterano sistemi target allo scopo di danneggiare l'immagine di un competitor;
- Alterazione di documenti elettronici pubblici e/o privati aventi efficacia probatoria, a vantaggio dell'ente;
- Detenzione abusiva di credenziali di accesso ai sistemi informatici (es. siti web) di enti pubblici o privati;

Le sfide per le imprese

Per far fronte al mutato scenario le aziende devono predisporre preventive ed idonee misure di sicurezza e di controllo volte a evitare la commissione dei Reati Informatici al loro interno e individuare sistemi per l'identificazione di eventuali comportamenti illeciti e dell'autore degli stessi.

Le domande chiave da porsi possono essere sintetizzate in:

- Il modello 231/2001 implementato recepisce tutti i cambiamenti normativi?
- I rischi sottesi all'uso estensivo di Information and Communication Technology, sono stati correttamente valutati?
- Il crescente impatto della frode elettronica e della Criminalità Informatica sulle aziende è pienamente compreso?
- I Controlli indirizzano in maniera adeguata i rischi individuati?
- Sono in linea con le Best Practice internazionali?

Perché PwC

PwC ha maturato un'esperienza pluriennale al fianco di aziende di rilevanza nazionale ed internazionale nonché di enti di piccole e medie dimensioni nella definizione di modelli di compliance al D.Lgs 231/2001.

Gli specialisti PwC in ambito Information and Communication Technology hanno conseguito specifiche certificazioni (CISA e ISO27001) e sono in grado di applicare specifiche competenze, tecniche e metodologiche, per individuare le modalità di realizzazione dei reati e le migliori pratiche di controllo in risposta dei rischi individuati.

PwC è l'autore del CoSO report, che rappresenta a tutt'oggi il modello fondamentale di riferimento per progettare e realizzare un efficace sistema di controllo interno. Gli esperti PwC partecipano ai gruppi di lavoro delle associazioni di categoria finalizzati alla predisposizione delle linee guida per la definizione/aggiornamento dei modelli.

PwC ha svolto attività di supporto agli Organismi di Vigilanza nell'attività di monitoraggio del modello, ha assistito aziende indagate a supporto del Collegio di Difesa nonché come consulenti tecnici di parte.

L'attività di consulenza è supportata da strumenti informatici e da un repository che raccoglie le più significative Linee guida, gli orientamenti giurisprudenziali disponibili, la dottrina prevalente e le modalità applicative delle più rilevanti aziende in materia di D.Lgs 231/01.

L'approccio PwC

L'approccio alle attività di adeguamento/integrazione del modello ex D.Lgs 231/2001 si basa sulla metodologia PwC di analisi e valutazione dei rischi.

Tale metodologia è in linea con quanto previsto dalle linee guida delle principali associazioni di categoria tra cui Confindustria, ed è applicabile a qualsiasi realtà organizzativa.

Data la metodologia di riferimento il processo di adeguamento del modello ai recenti aggiornamenti normativi consiste nelle fasi di seguito elencate:

1. Identificazione delle aree/sistemi nell'ambito delle quali o per mezzo dei quali potrebbero essere realizzate condotte illecite;
2. Identificazione dei punti di controllo atti a prevenire la commissione di reati. Tali punti di controllo sono basati su framework internazionalmente riconosciuti in tema di IT Governance & Security, quali COBIT (Control Objectives for Information and related Technology) e ISO 27001:2005 (norma internazionale che fornisce i requisiti per un sistema di gestione della sicurezza delle informazioni);
3. Integrazione, nell'ambito delle altre componenti del Modello, dei vari aspetti connessi ai reati informatici;
4. Monitoraggio del Modello, supporto nella pianificazione e definizione di test di operatività dei controlli.

Le attività descritte, così come impostate nella metodologia PwC, consentono di rispondere a quanto previsto dal D. Lgs 231/01, ma al tempo stesso consentono di implementare/migliorare i controlli sulla sicurezza delle informazioni, imprescindibili per un buon sistema di controllo interno sui sistemi informatici.

Contatti

Alfredo Gallistru
Partner PwC
Tel. +39 02 7785 458
alfredo.gallistru@it.pwc.com

Nicola Monti
Partner PwC
Tel. +39 02 6672 0566
nicola.monti@it.pwc.com

© 2011 PricewaterhouseCoopers. All rights reserved.

"PricewaterhouseCoopers" and "PwC" refer to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL). Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.