Global Economic Crime and Fraud Survey 2018

Summary Italia

pwc

www.pwc.com/it

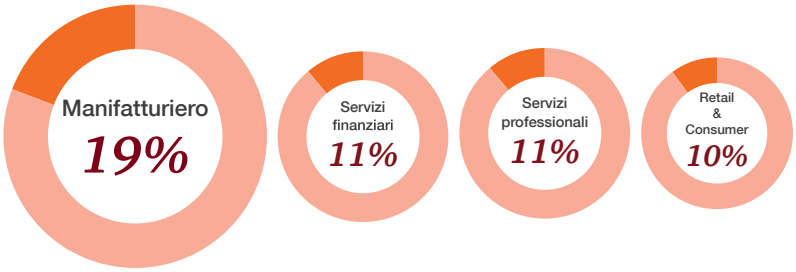
L'adesione delle organizzazioni

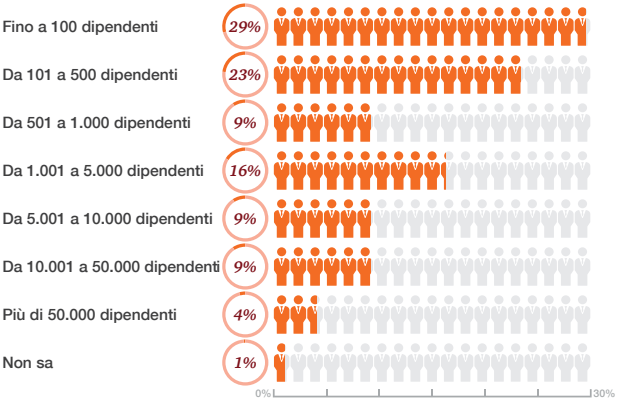
Quest'anno hanno aderito alla Global Economic Crime and Fraud Survey **164 organizzazioni italiane**, con un aumento del 15% rispetto alla precedente edizione. Gli intervistati appartengono prevalentemente alle funzioni Finance (40%), Internal Audit (18%) e all'Executive Management (16%). I settori più rappresentati: manifatturiero (19%), servizi finanziari (11%), servizi professionali (11%), Retail & Consumer (10%).

7.228 Partecipanti totali

123 Paesi coinvolti

Adesione Italia per settore merceologico

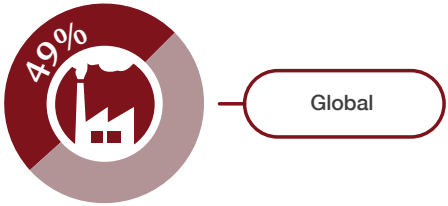


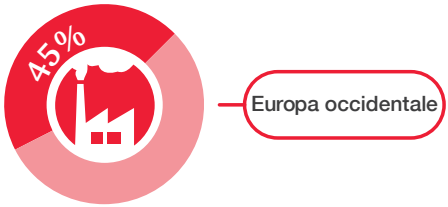


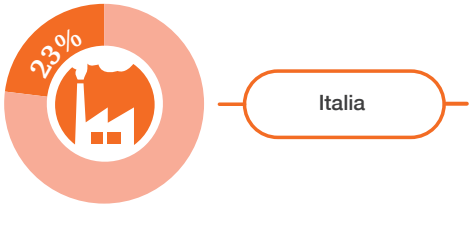
Partecipazione Survey 2018 Italia - Nr. dipendenti organizzazioni

Dimensioni del fenomeno: Italia vs Global

In Italia il 23% degli intervistati ha dichiarato che la propria organizzazione è stata vittima di reati economico-finanziari negli ultimi 24 mesi, contro il 49% registrato a livello Global e il 45% a livello di Europa Occidentale.



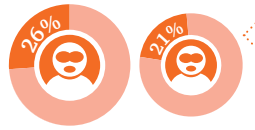




Mentre in Italia il fenomeno sembrerebbe stabile rispetto all'edizione 2016 della Survey (nella quale il 21% delle organizzazioni dichiarava di aver subito almeno una frode nei precedenti 24 mesi), a livello Global si registra un aumento di oltre il 30% rispetto al dato 2016.

In realtà sappiamo che i dati conosciuti sono una sottostima di un fenomeno molto più ampio. I risultati a livello italiano, più che mostrare una minor diffusione delle frodi nel nostro Paese rispetto alla media internazionale, potrebbero evidenziare una minor consapevolezza da parte delle organizzazioni. In altri termini: le aziende italiane sono meno esposte alle frodi o non riescono ad intercettarle?

Inoltre, come abbiamo già avuto modo di osservare nelle diverse edizioni della Global Economic Crime & Fraud Survey, le aziende non sono sempre propense a dichiarare di aver subito frodi, quindi è possibile che una parte di frodi intercettate non sia stata comunicata.

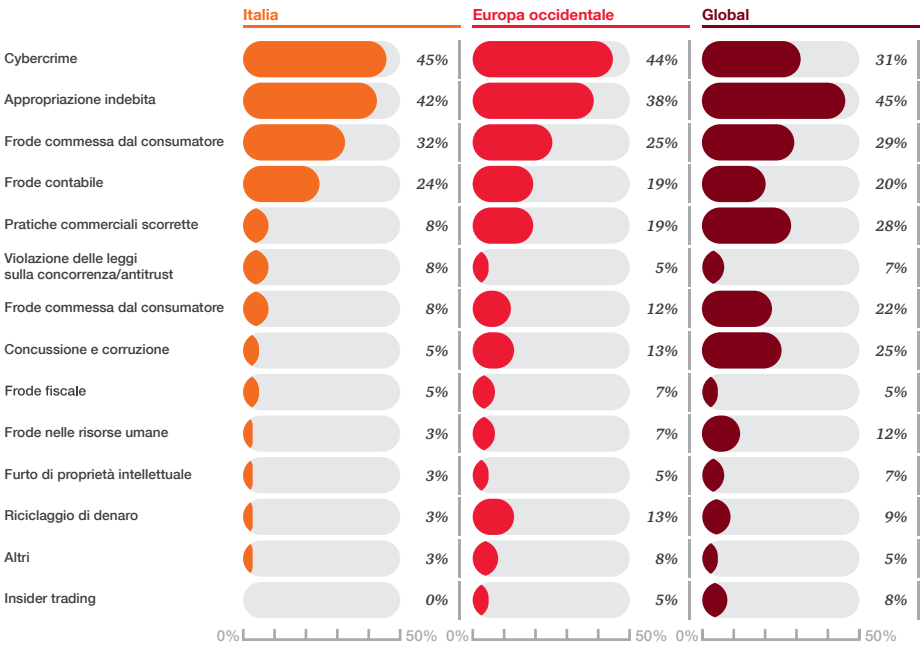


I settori merceologici maggiormente impattati dalle frodi negli ultimi 24 mesi sono il settore manifatturiero (26%) e servizi finanziari (21%)

Tipologia di frodi dichiarate

L'edizione 2018 della Global Economic Crime & Fraud Survey vede l'inserimento di due «nuove» categorie di illecito: 1) frodi commesse dai consumatori e 2) pratiche commerciali scorrette. Osservando la distribuzione delle frodi subite negli ultimi 24 mesi, si evince che le frodi commesse dai consumatori sono fra le tre tipologie più dichiarate (32%). Nelle edizioni passate questa categoria era inclusa nell'appropriazione indebita, che infatti quest'anno registra un calo del 35% rispetto al 2016.

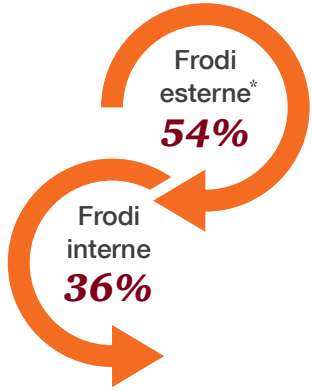
Tipologia di frodi dichiarate dalle organizzazioni negli ultimi 24 mesi



Il Cybercrime è la categoria di frode più diffusa in Italia (45%), seguita dall'appropriazione indebita (42%), dalle frodi commesse dai consumatori (32%) e dalle frodi contabili(24%).

In crescita le frodi esterne

Mentre a livello Global prevalgono le frodi realizzate da soggetti interni all'organizzazione (52%), in Italia quest'anno si registra un aumento delle frodi esterne, che passano dal 30% del 2016 al 54%. L'aumento è in linea con la crescita della minaccia cyber e con la diffusione delle frodi realizzate dai consumatori. Se guardiamo chi sono i soggetti esterni autori della frode effettivamente quasi la metà rientrano nella categoria «cliente» (47%) e circa un terzo nella categoria «hacker». Tuttavia, è significativo che il 20% dei casi di frode esterna intervengano nelle relazioni che normalmente si basano su rapporti continuativi e di fiducia professionale, ossia intermediari, agenti e fornitori.
Inoltre, va sottolineato che nel 27% dei casi la frode esterna non è opera di un singolo, ma di organizzazioni criminali.
Osservando le frodi interne, gli autori sono per lo più appartenenti al junior management.



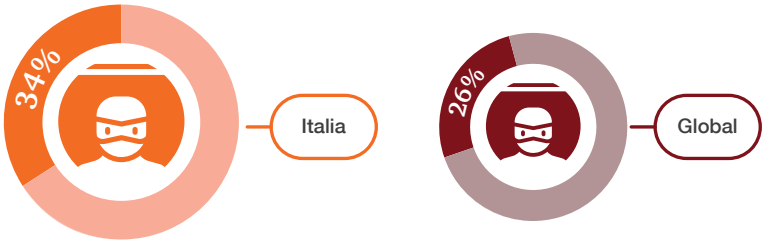
*Il 10% degli intervistati non sa o preferisce non dichiarare chi è stato l'autore della frode

Il cybercrime: un fenomeno in continua espansione

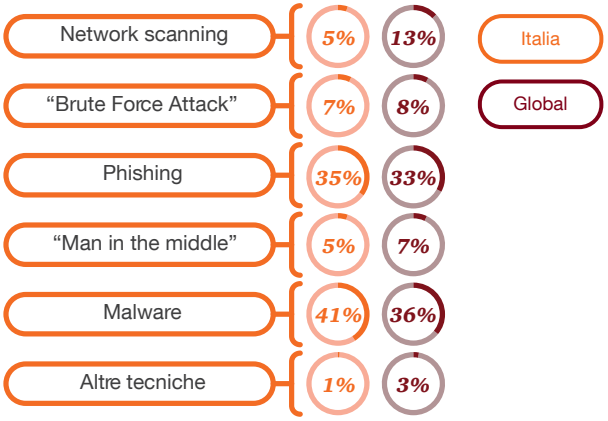
La crescita del cybercrime è sicuramente uno dei temi più significativi di questa edizione: in due anni le frodi dichiarate sono passate dal 20% al 45%. Probabilmente il dato riflette sia una effettiva espansione del fenomeno, sia una maggior consapevolezza delle organizzazioni: le minacce diventano sempre più pervasive e le tecniche sono più raffinate, di conseguenza le organizzazioni stanno anche imparando ad attrezzarsi.
Il cybercrime è al momento il principale timore delle organizzazioni anche per il futuro: tra tutte le categorie di frode, il cybercrime è stato indicato sia in Italia (34% degli intervistati) sia a livello Global (26%) come la minaccia più seria dei prossimi due anni.

È importante capire dove e cosa colpisce il cybercrime. Le aziende sono spesso vittime di attacchi informatici e stanno investendo nell'implementazione di strumenti di prevenzione: questa maggior sensibilità facilita anche una visione più ampia sull'obiettivo finale dell'attacco informatico. Abbiamo indagato quest'aspetto chiedendo ai partecipanti di indicare qual è stata la frode subita tramite un attacco informatico. Le risposte evidenziano che nella maggioranza dei casi l'obiettivo è interrompere o danneggiare i processi di business (31%), sottrarre asset all'azienda (29%) o mettere in atto forme di estorsione (25%).

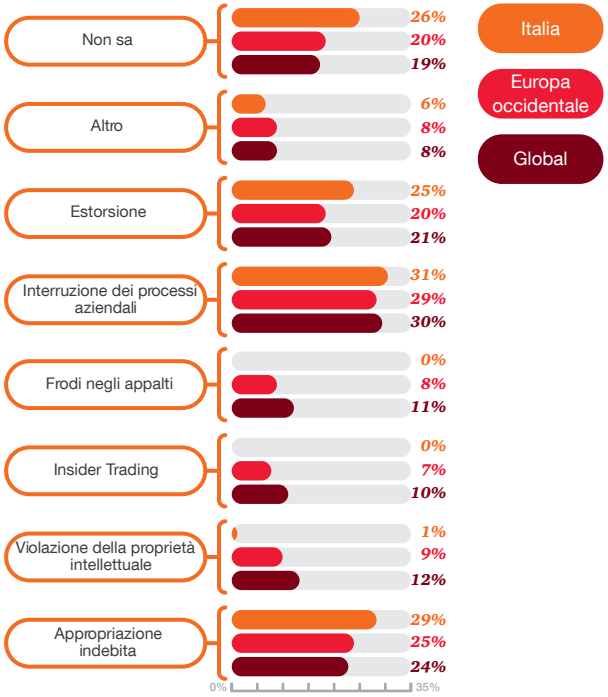
Cybercrime: la minaccia più seria per i prossimi due anni (Italia 34% degli intervistati, Global 26%)



Tecniche utilizzate nei cyber-attack



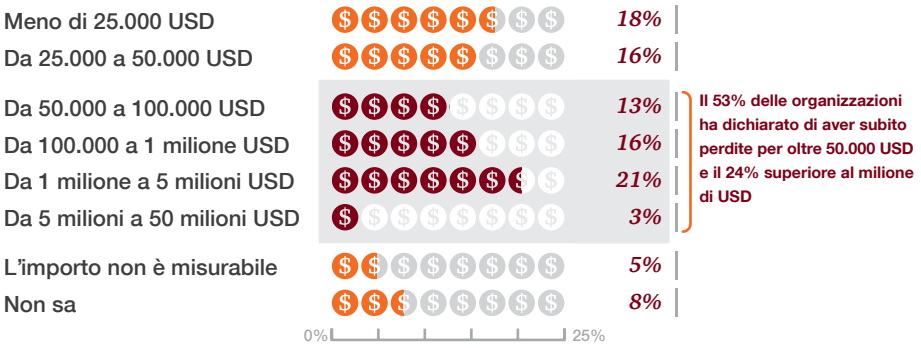
Frodi/reati economici commessi attraverso il cyber-attack



Il costo delle frodi

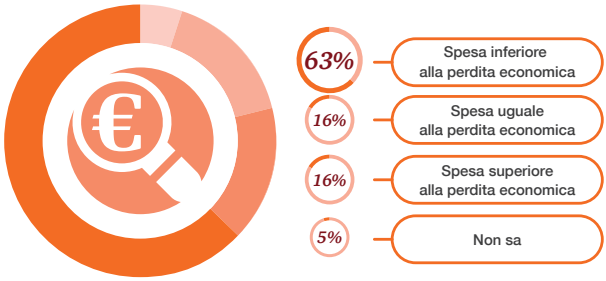
Abbiamo chiesto ai partecipanti di stimare le perdite economiche derivanti dalle frodi subite negli ultimi 24 mesi. In Italia più della metà delle aziende che hanno subito frodi dichiara che la perdita è stata superiore ai 50 mila USD, e il 24% addirittura, superiori al milione di dollari. In realtà per stimare correttamente quanto costano le frodi è necessario guardare oltre le perdite dirette ed esaminare anche i costi di gestione e investigazione della frode, eventuali sanzioni inflitte dalle autorità (pensiamo ai reati 231), i possibili contenziosi, ma soprattutto gli effetti reputazionali, che a cascata possono impattare sul business e sulla fiducia stessa del mercato.

Perdite finanziarie dichiarate



Tra le aziende italiane che hanno subito frodi, 1 su 3 ha sostenuto costi per investigazione e gestione dell'evento, di importo pari o anche superiore alla perdita economica dovuta alla frode stessa. Se guardiamo i cosiddetti impatti indiretti della frode (molto difficili da quantificare) il più temuto riguarda le relazioni commerciali.

Rapporto tra spese sostenute per investigare la frode e importo della perdita economica



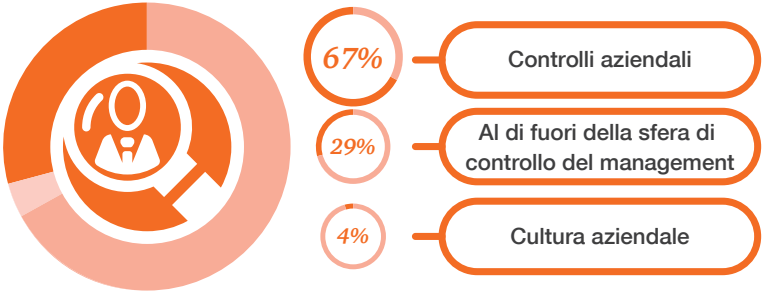
Gli impatti indiretti delle frodi

1. **Relazioni commerciali:** le frodi possono deteriorare le relazioni con clienti, partners, fornitori ecc.
2. **Morale dei dipendenti:** la frode può diffondere nell'organizzazione un clima di sfiducia e la percezione che certi comportamenti siano di fatto possibili o tollerati.
3. **Rapporti con le autorità di controllo:** ispezioni, sanzioni, indagini, provvedimenti restrittivi.
4. **Reputazione:** l'impatto reputazionale di una frode è spesso il più insidioso, perché può avere ricadute immediate sulla fiducia dei mercati e sulla continuità del business.
5. **Valore delle azioni:** è una conseguenza del danno d'immagine e del deterioramento della fiducia da parte dei mercati.

Come vengono scoperte le frodi: il ruolo del Sistema di controllo

Abbiamo chiesto alle organizzazioni di indicare come sono stati intercettati i casi di frode individuati negli ultimi due anni. Rispetto alle precedenti edizioni, la buona notizia è che il 67% delle frodi dichiarate è stato individuato grazie al sistema di controlli interni (contro il 47% di due anni fa). In particolare, nel 29% dei casi di frode è stata decisiva l'attività di monitoraggio di attività e operazioni a rischio, ma un ruolo centrale è occupato anche dalle attività di fraud risk management (18%) e dai controlli svolti dall'Internal Audit (11%).
Considerando però che quasi il 30% delle frodi è stato invece scoperto da canali esterni al sistema di controllo aziendale, riteniamo ci sia ancora un ampio margine di miglioramento nella capacità delle organizzazioni di individuare e gestire i rischi di frode cui sono esposte.
Inoltre, confrontando la più bassa percentuale delle frodi subite in Italia rispetto al dato Global, probabilmente i sistemi di controlli interno adottati dalle aziende italiane non sono ancora del tutto efficaci essendo basati su attività perlopiù manuali.

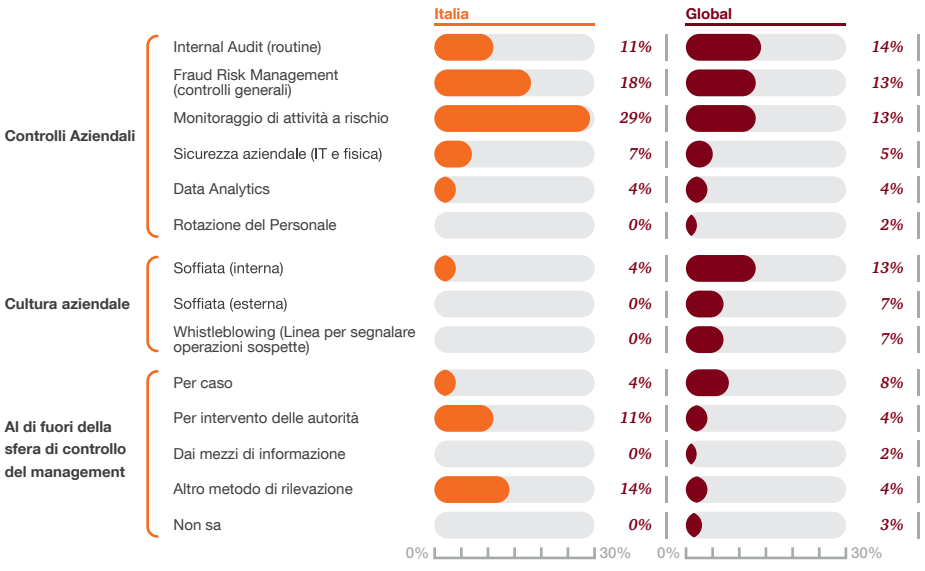
Tipologia dei metodi di intercettazione



È inoltre da sottolineare la totale assenza di frodi segnalate mediante canali ufficiali di whistleblowing. La scarsa diffusione della cultura del «whistlblowing» è nota da tempo ed è stata segnalata anche nelle edizioni passate della Survey, sia in Italia sia a livello Global. Quest'anno il dato Italia è particolarmente allarmante, perché molto sotto la media internazionale (7% dei casi). Considerando che alcune frodi sono state segnalate tramite «soffiate» interne, ancora una volta rileviamo un probabile tema di diffidenza verso uno strumento che non offre adeguate garanzie di tutela per il segnalante. Molto spesso il canale di whistleblowing non è altro che un indirizzo di posta elettronica e le modalità con cui vengono gestite le segnalazioni non sono sufficientemente regolate e comunicate al personale.

A questo proposito sarà interessante capire se la nuova legge sul whistlblowing entrata in vigore a dicembre 2017 – sul rafforzamento della tutela del segnalante – porterà le organizzazioni ad introdurre strumenti di segnalazione più strutturati.

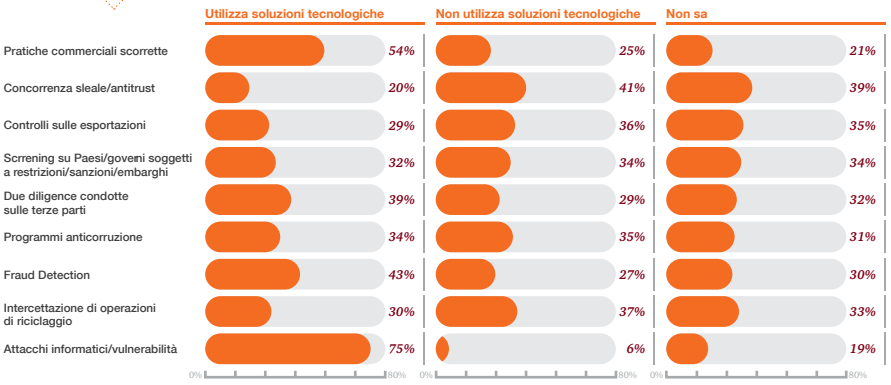
Metodi di intercettazione delle frodi



La tecnologia: elemento di vulnerabilità o risorsa contro la criminalità economico-finanziaria?

I dati sul cybercrime ci dicono che i sistemi informativi possono rappresentare un elemento di vulnerabilità per le organizzazioni. In realtà la tecnologia oggi ci permette anche di raccogliere, esaminare, elaborare e incrociare una mole inimmaginabile di dati e informazioni. Il patrimonio di dati (interni ed esterni) di cui l'organizzazione dispone è una risorsa che può facilitare l'intercettazione e la prevenzione di comportamenti fraudolenti. Abbiamo provato a capire qual è il livello di maturità delle aziende nell'uso della tecnologia come strumento di controllo e contrasto dei reati economico-finanziari, con particolare riferimento ad alcune tipiche aree di controllo (grafico sotto). Mentre è ovviamente elevata la percentuale di aziende che utilizza la tecnologia per la prevenzione di attacchi informatici (75%), in quasi tutte le altre aree di controllo sono meno della metà le aziende che utilizzano soluzioni o strumenti tecnologici. Fa eccezione il controllo sulle pratiche commerciali scorrette, ossia comportamenti che denotano una gestione del business contraria agli standard etici dell'organizzazione (ad esempio da parte della forza vendita o di broker, buyers, amministratori ecc.). In questo caso il 54% delle aziende utilizza anche soluzioni tecnologiche di monitoraggio.
Il dato più sorprendente è che molti non sanno se l'azienda si avvale o meno di soluzioni tecnologiche.

Pensando alle aree di controllo/monitoraggio sotto riportate, la sua organizzazione si avvale di strumenti o soluzioni tecnologiche?



Abbiamo quindi indicato alcuni strumenti, tecniche e modelli innovativi di monitoraggio, indagando il grado di conoscenza e utilizzo delle aziende (grafico a fianco). Mediamente, sono meno della metà le aziende che oggi utilizzano tecnologie innovative per il monitoraggio e il controllo delle frodi. In generale, siamo meno preparati rispetto alla media internazionale.

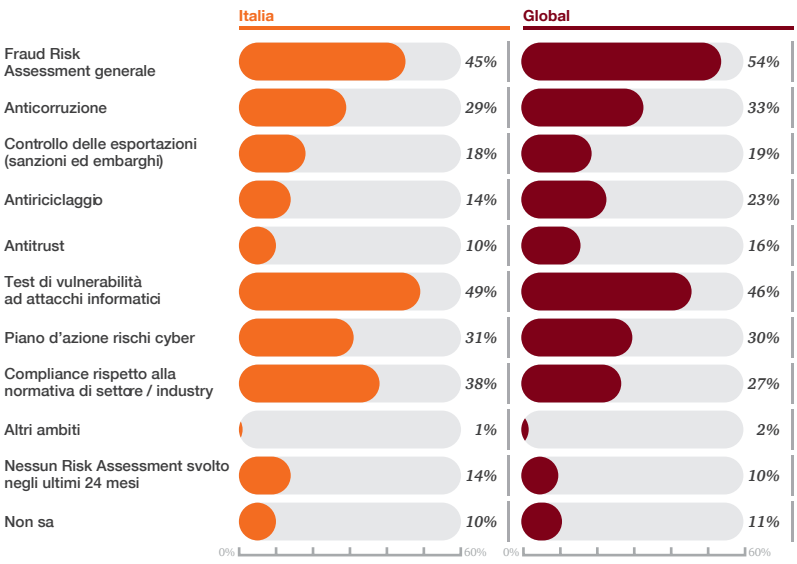
Tecnologia e strumenti innovativi di contrasto alla criminalità economico-finanziaria: l'esperienza delle aziende italiane

Se non sai cosa cercare, non troverai nulla: il fraud risk assessment

In effetti, non basta implementare dei controlli: bisogna innanzitutto capire cosa si sta controllando e perchè, quali priorità sono state fissate, e quanto il controllo è efficace rispetto ai rischi reali dell'organizzazione.
Il tema cruciale è che se non si sa cosa cercare probabilmente non si troverà nulla. Conoscere i propri rischi è il primo passo per un'efficace azione di contrasto, proporzionata rispetto alla dimensione del fenomeno e utile rispetto all'obiettivo.

In Italia circa il 75% degli intervistati ha dichiarato di aver svolto una o più attività di risk assessment negli ultimi 2 anni, su aree diverse. Tuttavia, meno della metà degli intervistati ha svolto un risk assessment generale sui rischi di frode e meno del 30% in ambito anticorruzione. Ancora una volta rileviamo che il tema più affrontato sembra essere la gestione dei rischi cyber, attraverso test preventivi di vulnerabilità (49% degli intervistati) o piani d'azione (31%).

Pensando alle aree sotto riportate, la sua organizzazione ha svolto attività di risk assessment negli ultimi 24 mesi?



Contatti

Alberto Beretta
Partner

+39 02 7785335
+39 348 8519831
alberto.beretta@pwc.com

Alessandro Colaci
Partner

+39 02 7785224
+39 348 1565395
alessandro.colaci@pwc.com

Sara Martocchia
Director

+39 02 7785376
+39 346 5074018
sara.martocchia@pwc.com