Kroll

GLOBAL FRAUD & RISK REPORT

Essere resilienti in un mondo instabile

EDIZIONE ANNUALE **2016/17**

FORRESTER®

Ricerca condotta su commissione da Forrester Consulting.

Informazioni sulla metodologia di ricerca

Per la preparazione del Global Fraud and Risk Report 2016/2017, Kroll ha incaricato Forrester Consulting di eseguire 10 interviste approfondite e un sondaggio online integrativo con 545 alti dirigenti operanti in tutto il mondo, in diversi settori e aree geografiche. Il sondaggio è stato condotto tra il luglio e agosto 2016.

Oltre ad affrontare il tema delle frodi, già oggetto di precedenti lavori di Kroll, l'ambito della ricerca di questa edizione è stato ampliato al fine di includere percezioni ed esperienze relative ai rischi di natura informatica e di sicurezza. Come visto nelle precedenti edizioni, il campione degli intervistati comprende un'ampia gamma di settori di attività, tra cui Tecnologia, media e telecomunicazioni; Servizi professionali; Industria manifatturiera; Risorse naturali; Costruzione, ingegneria e infrastrutture; Beni di consumo; Servizi finanziari; Vendita al dettaglio, all'ingrosso e distribuzione; Turismo, tempo libero e trasporti; Sanità, farmaceutica e biotecnologie.

Gli intervistati ricoprivano posizioni di rilievo nelle loro aziende; tra questi, il 70% è rappresentato da manager di primo livello. Il 61% delle imprese faceva registrare un fatturato annuo di 500 milioni di dollari o superiore.

Gli intervistati rappresentano tutte le principali aree geografiche mondiali; il 25% opera in Europa, il 20% nell'area Asia-Pacifico, il 20% in Nord America, 19% in Medio Oriente / Africa e il 16% in America Latina.

Tutti i valori monetari sono espressi in dollari statunitensi.

Prefazione

Da quest'anno il nostro Report si chiama Kroll Fraud and Risk Report, in quanto la sua portata è stata ampliata per includere l'analisi delle minacce informatiche e alla sicurezza: due sfide sempre più impegnative che i nostri clienti si trovano ad affrontare in tutto il mondo.

Un altro aspetto che non è più possibile ignorare è l'importanza di prevedere e affrontare le minacce provenienti dall'interno dell'azienda. Questa conclusione è corroborata e ampiamente dimostrata dai risultati della nostra indagine. Che si tratti di frode, minacce informatiche o rischi in materia di sicurezza; che le imprese operino in Asia, in Europa o nelle Americhe, o nei settori dei servizi, finanza, vendita al dettaglio o industria manifatturiera, le cifre dimostrano che a mettere le aziende in pericolo sono in massima parte dipendenti, ex dipendenti, freelance e dipendenti a termine.

Con due implicazioni, una buona e una cattiva. Quella buona è che le imprese, una volta individuata e soppesata la minaccia, hanno maggiori possibilità di gestire la propria esposizione al rischio se questo proviene dall'interno dell'azienda piuttosto che dall'esterno. Avendo pieno accesso e controllo sugli indizi, le aziende hanno maggiori possibilità di concludere positivamente le indagini.

D'altra parte, se una minaccia o un incidente interno non sono gestiti con la dovuta attenzione, l'impatto negativo sulla reputazione, sia all'interno sia all'esterno dell'azienda, può rivelarsi ancora più grave. La nostra indagine dimostra infatti che una delle conseguenze più gravi di un evento di questo genere è rappresentato dall'impatto sul morale dei dipendenti. Nel caso di settori regolamentati, le autorità competenti in materia si interesseranno quasi certamente al vostro caso: Se si trascurano i controlli in un dato settore, le autorità potrebbero essere spinte ad avviare indagini più approfondite, anche qualora il problema non attenga per nulla alla sicurezza, ai dati dei clienti o ai fondi.

La preoccupazione per il morale del personale da un lato e l'attenzione per le attività degli organi di controllo dall'altro possono portare a due diversi approcci investigativi. I timori per la reputazione e le reazioni dei dipendenti potrebbero suggerire l'adozione di una risposta poco invasiva che miri a non agitare troppo le acque e a limitare i danni. D'altra parte, il contenimento del rischio normativo (e il conseguente rischio di contenziosi) richiede uno sforzo tempestivo e rigoroso nell'indagare a fondo sul problema, determinarne le cause e risolverlo: Gli organi di controllo in genere non danno grande peso alle vostre preoccupazioni per i danni all'immagine e al morale del personale. Arrivare a una soluzione di compromesso tra queste due esigenze è un compito che richiede esperienza: bisogna comprendere la natura del problema, valutare le diverse tecniche di indagine e le strategie applicabili, ed essere consapevoli della rilevanza dei risultati.

E' inoltre imprescindibile conoscere a fondo la cultura e le leggi locali, in particolare quando si tratta di attività all'estero. Le leggi in materia di privacy, lavoro e segreto professionale – che possono essere determinanti

per tutelare i risultati di un'indagine – variano in base alla giurisdizione. Se non si valutano a dovere queste regole di base, si rischia di rendere inutile un'indagine e finanche di peggiorare il problema.

Esistono poi dei fattori intangibili, quali le differenze culturali tra i vari paesi e talvolta tra regioni di uno stesso paese, che possono rivelarsi critici per un esito positivo: il rispetto per le gerarchie, la fedeltà a un manager locale piuttosto che all'azienda, la volontà di parlare con un soggetto esterno, la propensione a comunicare a un inquirente le informazioni che sta cercando oppure, in alternativa, l'omertà totale. Comprendere queste differenze richiede conoscenza del contesto locale ed esperienza: potrebbe non essere possibile fare affidamento sul management locale, in quanto potrebbe essere esso stesso coinvolto.

Il "fattore umano" è importante sia in fase di prevenzione sia nel corso dell'indagine. In materia di cyber security, per esempio, potrebbe sembrare opportuno adottare un approccio puramente tecnico: Checché se ne dica, la bontà di un approccio di questo tipo dipende da chi lo pone in essere e in che modo. Sistemi sofisticati di cyber security possono aiutare a limitare e mitigare il danno se e quando si riscontri un problema. Ma prima bisogna fare i conti col comportamento umano.

Per le imprese che operano in un contesto multinazionale, politiche e procedure standardizzate possono essere altrettanto disfunzionali. Una determinata politica può essere fraintesa in un paese, totalmente ignorata in un altro e finanche contraria alle consuetudini e alle leggi locali in un altro ancora. Ad ogni modo, anche le società che operano all'estero attraverso joint venture, agenti o distributori devono attrezzarsi a dovere. Per esempio, oggi le leggi anticorruzione di molti paesi rendono le imprese potenzialmente responsabili per le azioni poste in essere dai loro partner e agenti, mentre la cattiva condotta di un distributore, nel migliore dei casi, comprometterà la vostra reputazione.

Il mondo sta diventando sempre più rischioso. Ecco perché abbiamo aggiunto la parola "risk" al titolo di questo Report: come sempre saremo lieti di offrire la nostra esperienza a livello internazionale per aiutarvi a navigare in uno scenario globale così complesso.

TOMMY HELSBY
Co-Presidente, divisione Investigations and Disputes di Kroll

Sintesi della Ricerca

Introduzione

Da un decennio il Kroll Global Fraud Report e' una pubblicazione di riferimento per la comprensione del fenomeno delle frodi a livello mondiale, grazie alla raccolta di opinioni ed interviste ad alti dirigenti nelle varie parti del mondo e operanti in una vasta gamma di settori e posizioni. Quest'anno Kroll ha deciso di estendere l'ambito dell'indagine su una gamma più ampia di rischi, andando a includere quelli legati a frodi, attacchi informatici e sicurezza. Questa edizione del Kroll Global Fraud & Risk Report include statistiche e trend sull'incidenza delle frodi e nuove serie di dati concernenti i rischi informatici e di sicurezza. Il Report è articolato in quattro sezioni: Sintesi della Ricerca, Considerazioni, Contributi per Area Geografica, Contributi per Settore.

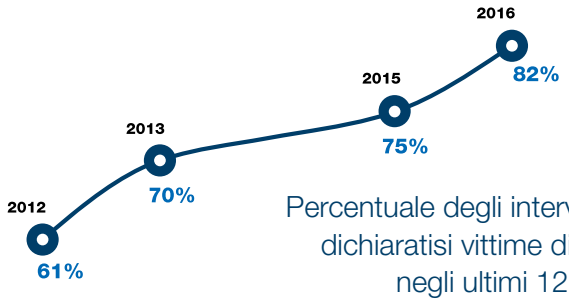
I risultati dell'indagine di quest'anno descrivono un contesto economico globale caratterizzato da rischi e relative ripercussioni in forte crescita; tipologie di rischio, di autori e di modalità di attacco più complesse; l'adozione di politiche e procedure di contenimento del rischio per rinforzare la capacità di recupero (resilienza) aziendale. Di seguito riportiamo alcune conclusioni fondamentali.

1 Incidenza elevata e ripercussioni diffuse

Incidenza

FRODI

Dai risultati dell'indagine di quest'anno emerge che l'incidenza delle frodi ha continuato ad aumentare. Nel complesso, l'82% dei dirigenti intervistati ha riferito di esser stato vittima di almeno un caso di frode nel corso dell'ultimo anno, rispetto al 75% registrato nel 2015. Questo dato riflette le tendenze individuate nelle edizioni precedenti del Global Fraud Report, quando l'incidenza delle frodi riportata dai dirigenti si attestava al 61% nel 2012 e al 70% nel 2013.



Percentuale degli intervistati dichiaratisi vittime di frodi negli ultimi 12 mesi

CYBER SECURITY

Un dato che colpisce: l'85% dei dirigenti intervistati ha dichiarato che la propria azienda ha subito un attacco informatico o un furto, perdita o attacco alle informazioni negli ultimi 12 mesi.

SICUREZZA

Più di due terzi (68%) degli intervistati hanno riferito il verificarsi di almeno un incidente in materia di sicurezza nel corso dell'ultimo anno.

Ripercussioni

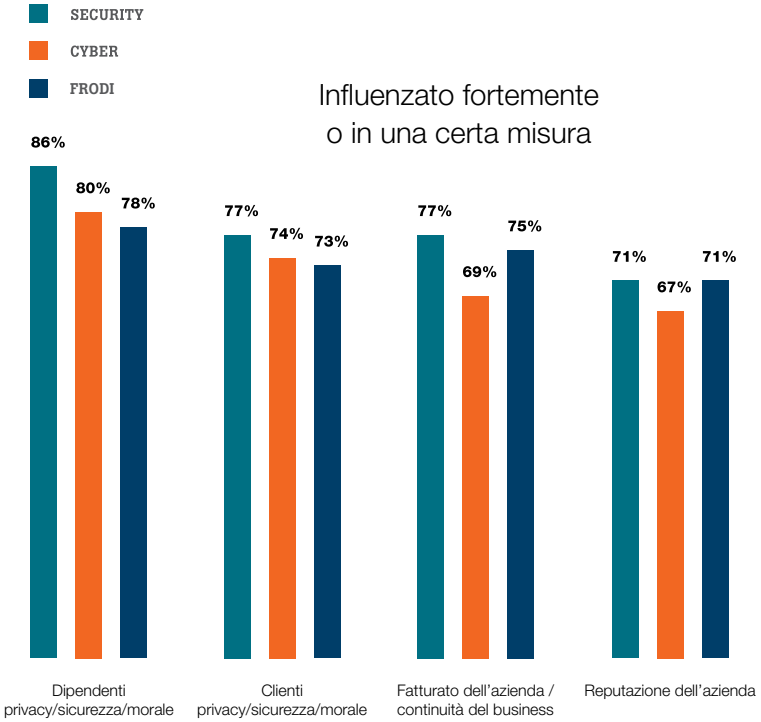
L'indagine indica che gli eventi come frodi, attacchi informatici o violazioni della sicurezza ha ripercussioni diffuse sui dipendenti e sulla clientela di un'azienda, oltre ai danni a livello economico e reputazionale.

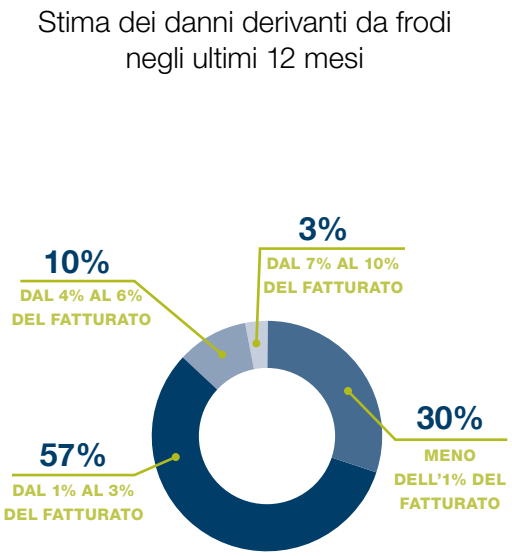
- La ripercussione osservata più di frequente è stata l'impatto sui dipendenti: l'86% degli intervistati vittime di un incidente in materia di sicurezza sostiene che la privacy, la sicurezza o il morale dei dipendenti sono risultati compromessi in misura più o meno grave. Questo livello di impatto sui dipendenti è stato segnalato dall'80% degli intervistati che ha menzionato un attacco informatico e dal 78% di coloro che hanno segnalato un episodio di frode.

- Anche se la prevalenza complessiva degli incidenti in materia di sicurezza è inferiore alle frodi o alle violazioni informatiche, l'impatto è in qualche misura più ampio. In aggiunta all'impatto sui dipendenti, il 77% degli intervistati che hanno subito un incidente in materia di sicurezza ha sostenuto che la clientela e i ricavi sono stati compromessi a livelli più o meno gravi, mentre la percentuale di chi lamenta un danno forte o moderato alla reputazione ammonta al 71%.

- Tra coloro che hanno subito un attacco informatico, quasi i tre quarti (74%) hanno fatto notare che la privacy, la sicurezza o la soddisfazione dei clienti ha subito un danno più o meno grave. L'esperto di Kroll Brian Lapidus scrive nel suo approfondimento a pagina 37 che, in seguito a una violazione dei sistemi, è fondamentale concentrarsi sulle esigenze della clientela. L'articolo tratteggia alcune linee guida che possono essere d'aiuto per ricostruire la fiducia dei clienti.

- Gli intervistati hanno dichiarato di aver subito danni economici significativi a causa delle frodi. La maggioranza (57%) dei dirigenti ha stimato che le perdite riconducibili alle frodi oscillano tra l'1% e il 3% dei ricavi, mentre una impresa su dieci ha registrato una perdita pari al 4% - 6% del fatturato.

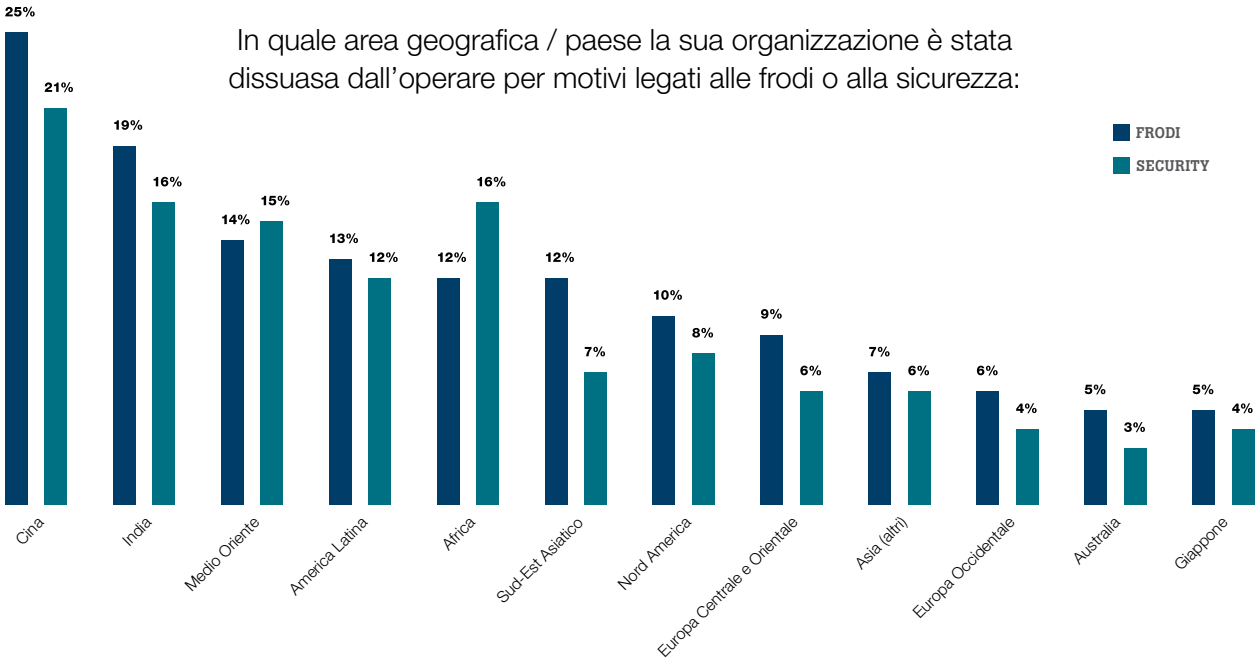




Rischi per area geografica

La globalizzazione, oltre alle opportunità strategiche di espansione, porta con sé una vasta gamma di rischi in molte aree geografiche. Lo scorso anno, il 69% dei dirigenti ha dichiarato di esser stato dissuaso dall'operare in una data nazione o area geografica a causa della maggior esposizione alle frodi. Inoltre il 63% degli intervistati sostiene di essersi allontanato da alcune aree geografiche per questioni di sicurezza.

Le preoccupazioni sono più consistenti quando si tratta di andare ad operare in Cina e in India. Gli esperti di Kroll Violet Ho e Reshmi Khurana, basati rispettivamente in Cina e India, descrivono nei loro articoli a pagina 57 e 61 le possibilità di contenere i rischi in questi paesi.



I dati raccolti dagli intervistati del settore manifatturiero indicano che si tratta di uno dei settori più colpiti dalle frodi (l'89% ha segnalato un episodio nel corso dell'ultimo anno). Oltre la metà degli intervistati del settore (51%) ha concluso che l'entrata in nuovi mercati a rischio più elevato è stato un fattore chiave dell'aumento del rischio di frode. Tuttavia, come evidenziato dagli esperti Brian Weihs, Nicole Lamb-Hale e Brian Sperling nel loro articolo a pagina 79, le aziende manifatturiere, così come quelle di altri settori, possono compiere alcune mosse per ridurre i rischi operativi in mercati emergenti.

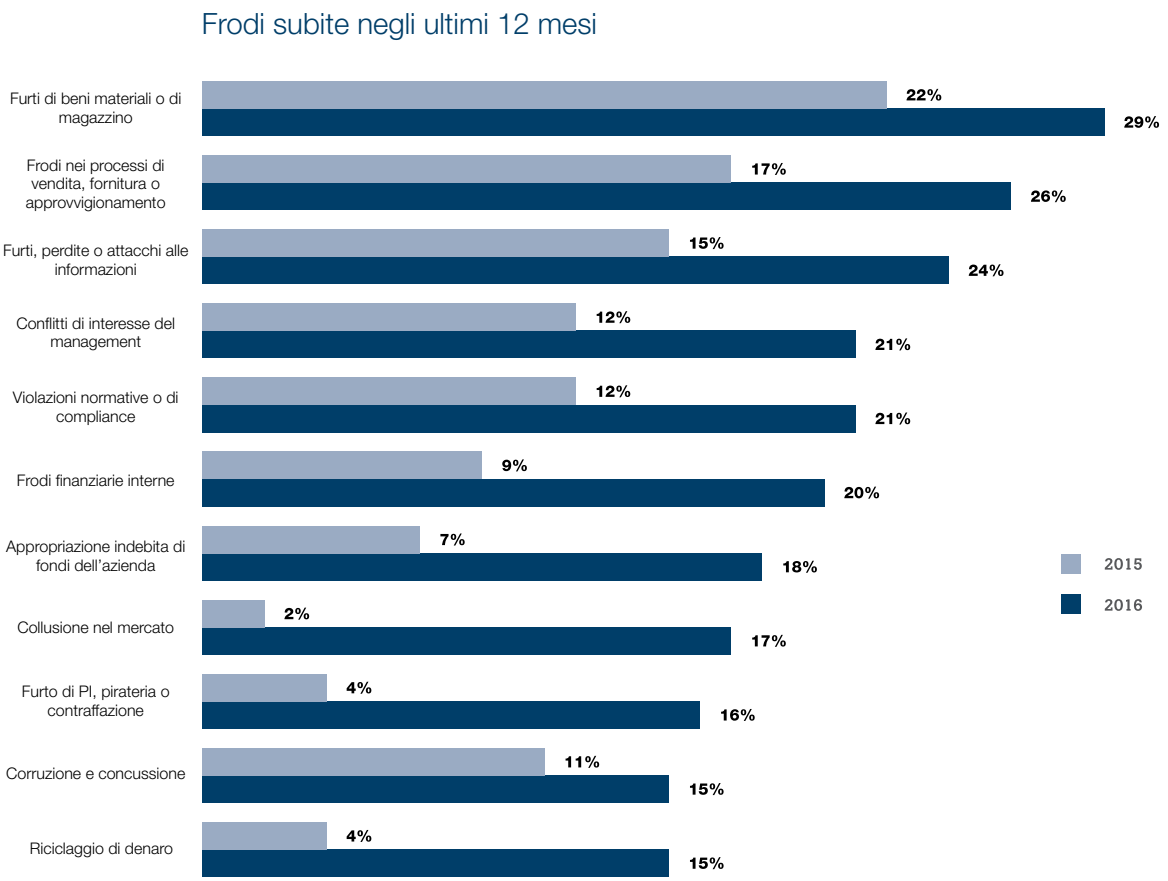
2 La complessità della minaccia

La varietà di episodi, responsabili e mezzi di attacco testimoniano un ambiente sempre più complesso in termini di gestione del rischio per le imprese. Va notato che continuano a prevalere le minacce interne, rappresentate da dipendenti, freelance o ex dipendenti.

Tipologia di episodi subiti dalle imprese

TIPOLOGIA DI FRODI

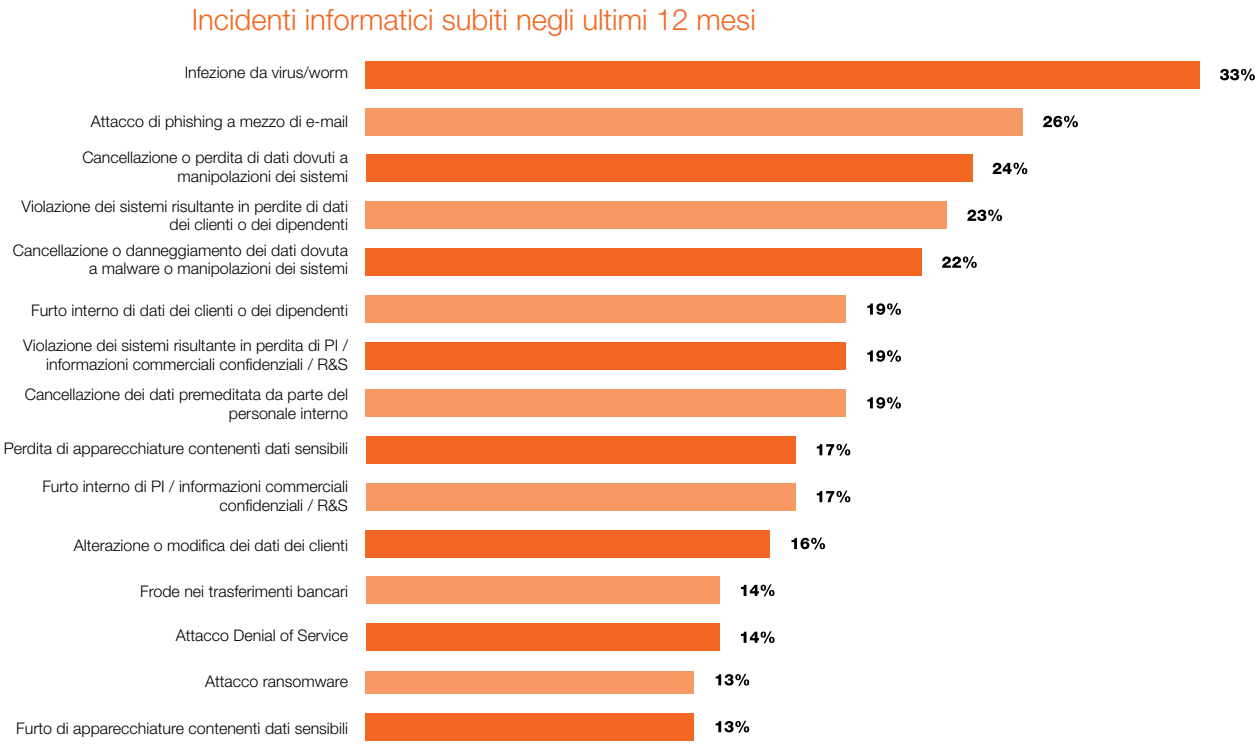
I dati raccolti dagli intervistati riportano un aumento di ogni singola tipologia di frode rispetto all'edizione precedente del 2015. Inoltre l'incidenza dichiarata ha ormai raggiunto livelli a due cifre per qualunque tipologia.



Il furto di beni materiali è ancora il tipo di frode più diffuso riscontrato nell'ultimo anno, riportato dal 29% degli intervistati: si tratta di 7 punti percentuali in più rispetto al 22% registrato nella precedente edizione. Le frodi nei processi di vendita, fornitura o approvvigionamento (26%) e i furti, le perdite e gli attacchi alle informazioni (24%) sono in seconda e terza posizione, con un aumento su base annua del 9%.

TIPOLOGIA DEGLI ATTACCHI INFORMATICI

L'indagine mostra che le imprese hanno dovuto fare i conti con una vasta gamma di attacchi informatici, articolati su diversi livelli di complessità.



Un terzo (33%) del totale dei dirigenti intervistati ha dichiarato di aver subito un'infezione da virus o worm: questo è il tipo di incidente informatico menzionato più di frequente nel Report di quest'anno. In seconda posizione troviamo l'attacco tramite phishing a mezzo e-mail, citato da poco più di un quarto (26%) del totale degli intervistati.

Nell'era dei big data, l'indagine mostra che le perdite o i furti di dati sono stati consistenti: gli incidenti informatici includono violazione dei sistemi, cancellazione dei dati e perdita di supporti contenenti dati sensibili.

- **Violazione dei sistemi:** Quasi un quarto (23%) degli intervistati ha dichiarato di aver subito violazioni dei sistemi risultanti in una perdita dei dati dei clienti o dei dipendenti, mentre nel 19% dei casi la violazione ha causato la perdita di segreti commerciali, proprietà intellettuali o studi di ricerca e sviluppo.

- **Cancellazione dei dati:** Il 24% dei dirigenti intervistati ha indicato di aver subito episodi di cancellazione dei dati dovuti a manipolazione dei sistemi; nel 22% dei casi la cancellazione o la corruzione dei dati sono stati causati da problemi di malware o problemi di sistema, mentre il 19% è stato imputabile ad azioni dolose da parte di risorse interne all'azienda.

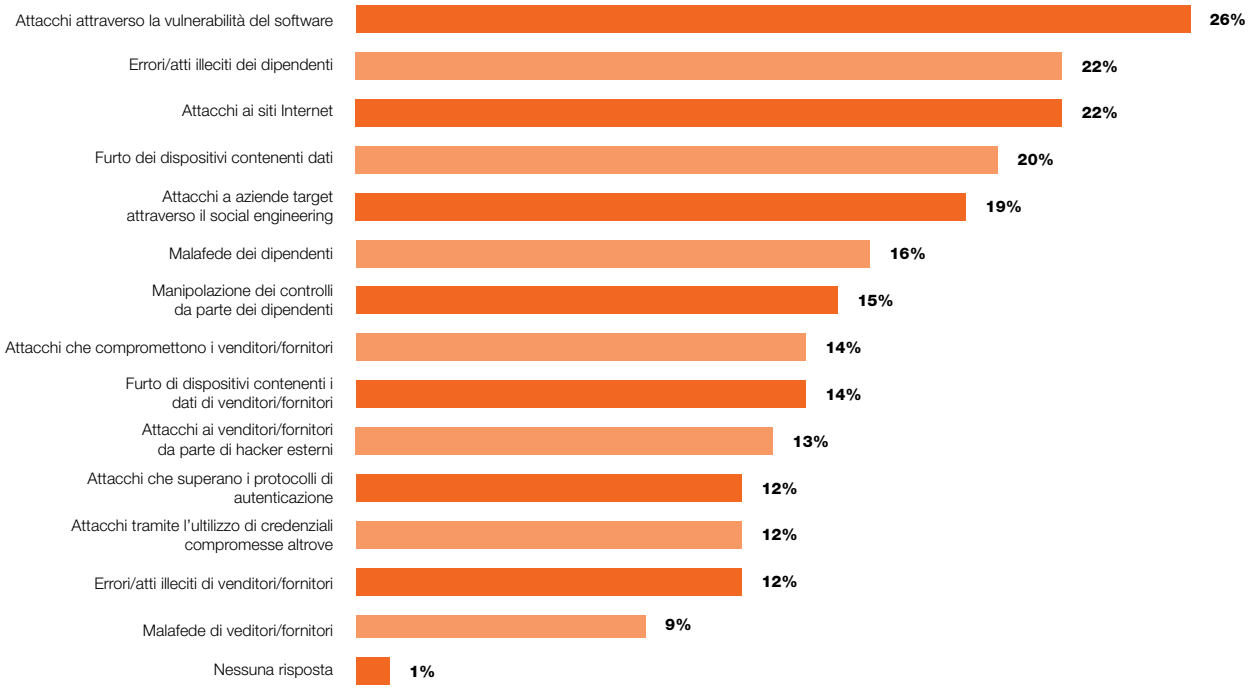
- **Perdita di apparecchiature:** Il 17% del campione ha riportato la perdita di supporti contenenti dati sensibili, mentre il furto è avvenuto nel 13% dei casi.

Come avvengono gli attacchi informatici

L'indagine rivela che la maggior parte degli attacchi informatici avvengono con diverse modalità di attacco. Queste risultano essere molteplici e interconnesse tra loro: attacchi diretti su software, sistemi e siti web; tramite terze parti mediante atti illeciti, attacchi contro i loro sistemi o per errore; errori o atti illeciti da parte dei dipendenti; infine, dal furto dei dispositivi.

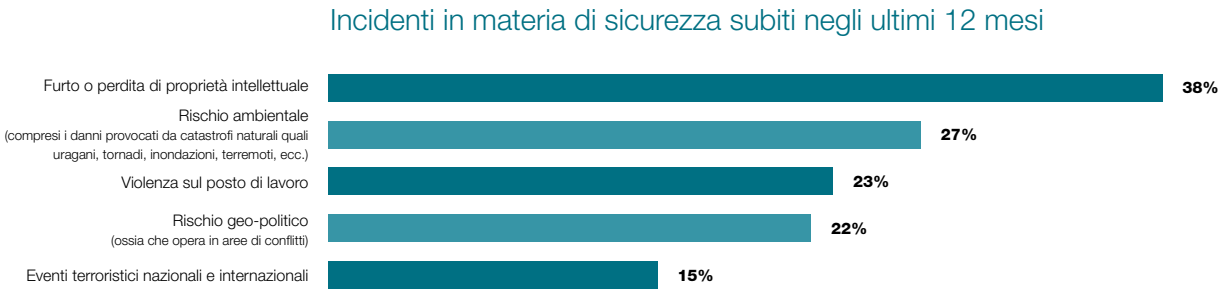
Il vettore di attacco più di frequente è la vulnerabilità del software, indicata da oltre un quarto degli intervistati (26%). Gli errori o gli atti illeciti dei dipendenti sono menzionati dal 22% degli intervistati. Gli attacchi a un sito Internet sono stati citati dal 22% degli intervistati.

Se la sua azienda ha subito un attacco informatico o la perdita, il furto o l'attacco alle informazioni negli ultimi 12 mesi, quale tra le seguenti situazioni si avvicina di più alla sua esperienza?
(Agli intervistati è stato chiesto di scegliere un massimo di tre risposte.)



TIPOLOGIE DI INCIDENTI IN MATERIA DI SICUREZZA

Il furto o la perdita di proprietà intellettuale è stata la voce più comune di incidente in materia di sicurezza, menzionato dal 38% di coloro che hanno subito un episodio negli ultimi 12 mesi. I rischi ambientali, come le catastrofi naturali, hanno avuto conseguenze sul 27% degli intervistati che hanno subito un incidente in materia di sicurezza, con particolare rilevanza in Canada (46%) e in Cina (45%). Quasi un quarto (23%) degli intervistati ha menzionato la violenza sul posto di lavoro. Il rischio geopolitico e il terrorismo presentano un'incidenza minore, rispettivamente del 22% e del 15%. A testimonianza della validità del concetto di instabilità, è importante riconoscere che entrambe queste fattispecie si attestano su valori a due cifre.



Gli autori

I risultati rivelano che le minacce provengono prevalentemente dall'interno. I dipendenti e gli ex dipendenti sono stati individuati come i maggiori responsabili dei casi di frode, incidenti informatici e di sicurezza nel corso degli ultimi 12 mesi. A prescindere da questa constatazione, anche i soggetti esterni sono stati identificati come autori attivi di illeciti.

AUTORI DELLE FRODI

Quasi 8 intervistati su 10 (79%) hanno puntato il dito contro una delle seguenti categorie di responsabili:

- Manager senior o di livello intermedio interni alla propria azienda
- Dipendenti junior interni all'azienda
- Ex dipendenti
- Dipendenti a termine / freelance

A testimonianza della complessità dei rischi di frode, la maggioranza (60%) dei dirigenti che hanno sostenuto di aver subito frodi ha identificato una combinazione di autori, tra cui dipendenti, ex-dipendenti e soggetti terzi. Quasi la metà (49%) degli intervistati ha menzionato contemporaneamente i tre gruppi. Quasi quattro intervistati su dieci (39%) sono stati vittime di frodi per mano di un dipendente junior, il 30% dai manager, il 27% dagli ex-dipendenti e il 27% da freelance e dipendenti temporanei. Anche gli agenti e / o gli intermediari, che a volte sono considerati quasi alla stessa stregua dei dipendenti, sono stati indicati dal 27% degli intervistati come coinvolti in attività fraudolente.

Anche se le risorse interne sono indicate come i principali responsabili delle frodi, spetta anche a loro il merito di averle scoperte. Quasi la metà (44%) degli intervistati ha dichiarato che la scoperta delle frodi era merito del sistema di whistleblowing interno, mentre il 39% menziona l'indagine interna come metodo più rilevante.

Gli esperti di Kroll Alex Volcic e Yaser Dajani, nel loro articolo a pagina 33, sostengono che è importante fare una cernita accurata delle segnalazioni dei whistleblower e testare un sistema di assegnazione delle priorità per garantire l'efficacia del sistema di segnalazione.

AUTORI DEGLI ATTACCHI INFORMATICI

Nel complesso, il 44% degli intervistati ha riferito che le risorse interne sono state i principali responsabili di un attacco informatico, menzionando ex-dipendenti (20%), freelance / dipendenti a termine (14%) e dipendenti a tempo indeterminato (10%). Se consideriamo anche gli agenti / intermediari alla stregua dei dipendenti, come fatto notare dal 13% degli intervistati, la percentuale delle risorse interne additate come principali responsabili sale fino ad avere uno quota maggioritaria (57%). Quasi un dirigente su tre (29%) ha dichiarato che i responsabili principali sono stati esterni all'azienda.

AUTORI DI INCIDENTI IN MATERIA DI SICUREZZA

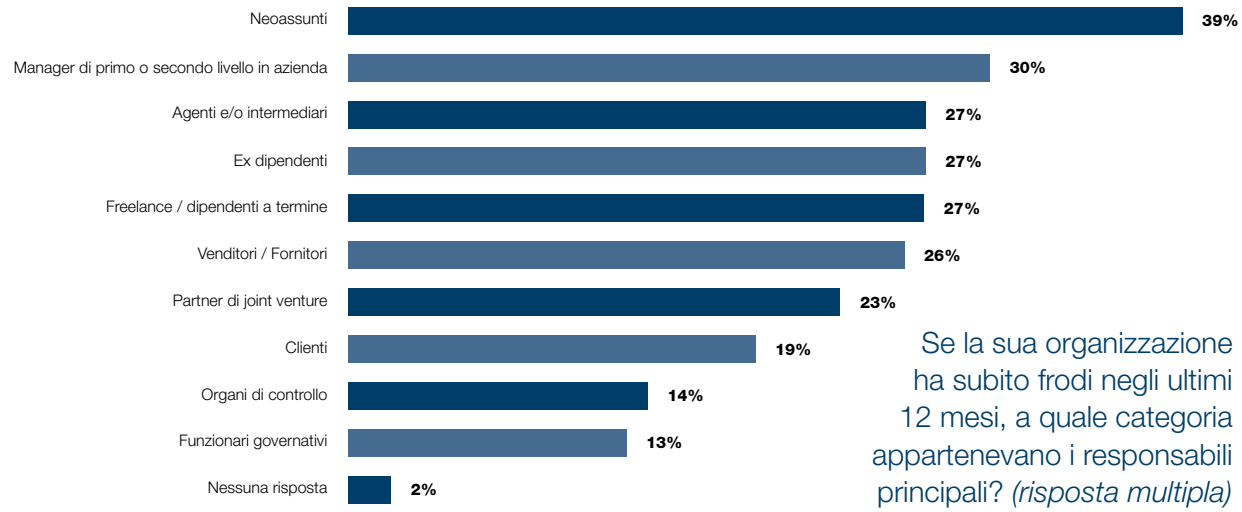
Nel complesso, il 56% dei dirigenti intervistati ha riferito che le risorse interne sono state i principali autori di incidenti in materia di sicurezza, menzionando ex-dipendenti (23%), dipendenti a tempo indeterminato (17%) e freelance / dipendenti a termine (16%).

È interessante notare che, tra gli autori esterni, più di un dirigente su dieci (12%) ha dichiarato che i concorrenti sono stati gli autori più frequenti, mentre il 10% punta il dito contro i cani sciolti. Gli attivisti politici, i governi di altre nazioni e i terroristi raggiungono un dato combinato del 20%.

GESTIRE LA MINACCIA RAPPRESENTATA DAGLI EX DIPENDENTI

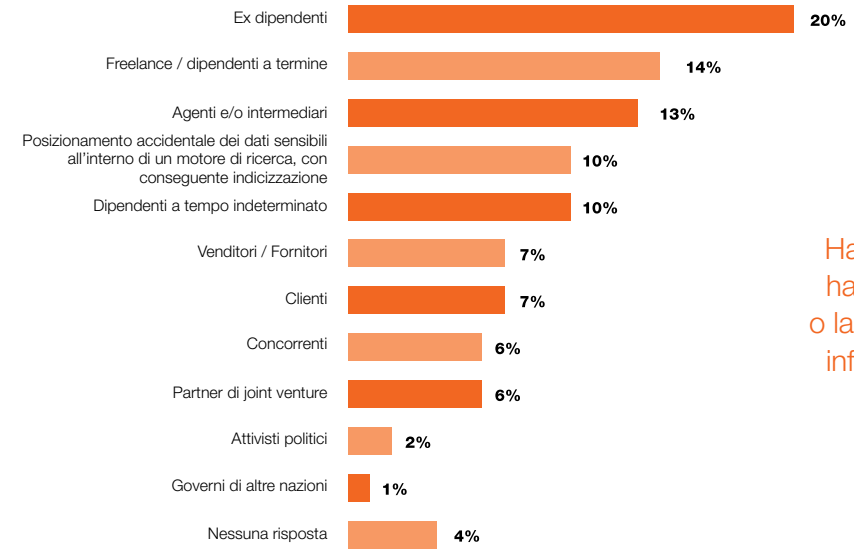
L'indagine ha mostrato che una percentuale notevolmente elevata degli intervistati ha individuato negli ex dipendenti gli autori principali di frodi (27%), attacchi informatici (20%) e incidenti in materia di sicurezza(23%). Gli esperti di Kroll Marianna Vintiadis e Tadashi Kageyama, nel loro articolo a pagina 25, trattano proprio questo argomento, illustrando quali sono le strategie impiegabili dalle imprese per gestire con attenzione l'allontanamento dei dipendenti.

Autori delle frodi



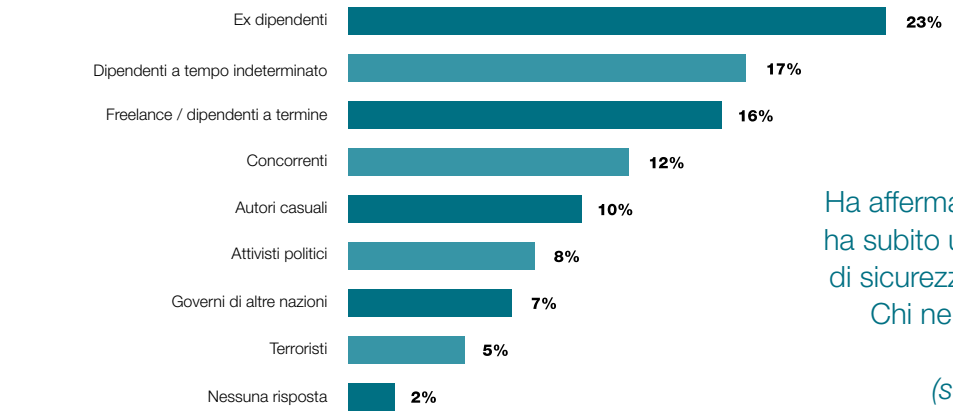
Se la sua organizzazione ha subito frodi negli ultimi 12 mesi, a quale categoria appartenevano i responsabili principali? *(risposta multipla)*

Autori di attacchi informatici o volti a furti, perdite e sottrazioni di informazioni



Ha affermato che la sua impresa ha subito un attacco informatico o la perdita, il furto o l'attacco alle informazioni negli ultimi 12 mesi. Chi ne è stato il responsabile principale? *(selezionare un'opzione)*

Autori dI incidenti in materia di sicurezza



Ha affermato che la sua impresa ha subito un incidente in materia di sicurezza negli ultimi 12 mesi. Chi ne è stato il responsabile principale? *(selezionare un'opzione)*

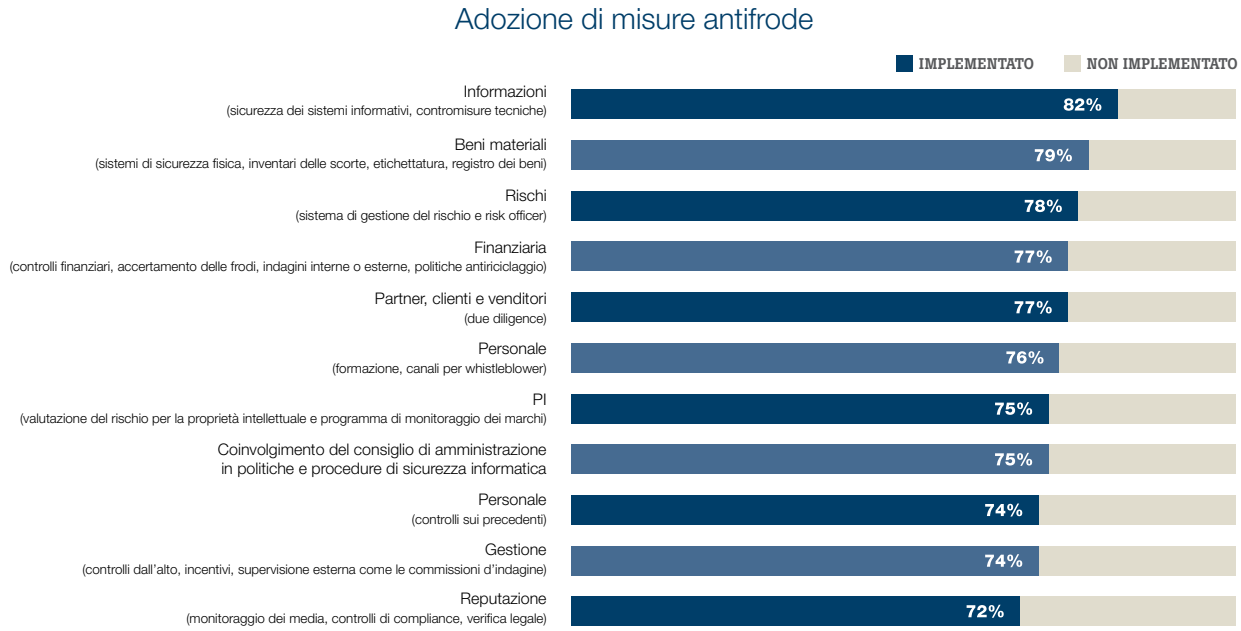
3 Verso la resilienza

Di fronte a un rischio d'impresa sempre crescente, ai costi significativi e all'impatto generalizzato sui rapporti con gli interlocutori e sulla propria reputazione, le imprese hanno fatto registrare un'adozione ampia delle misure di contenimento del rischio. Tuttavia, è superfluo dire che è necessario uno sforzo più consistente e continuativo per costruire e sostenere la resilienza aziendale.

Qui di seguito riportiamo una sintesi delle misure già adottate da molte aziende, spesso insieme a un piano per il loro potenziamento futuro.

Misure di contenimento del rischio adottate

MISURE DI CONTENIMENTO DEL RISCHIO DI FRODE

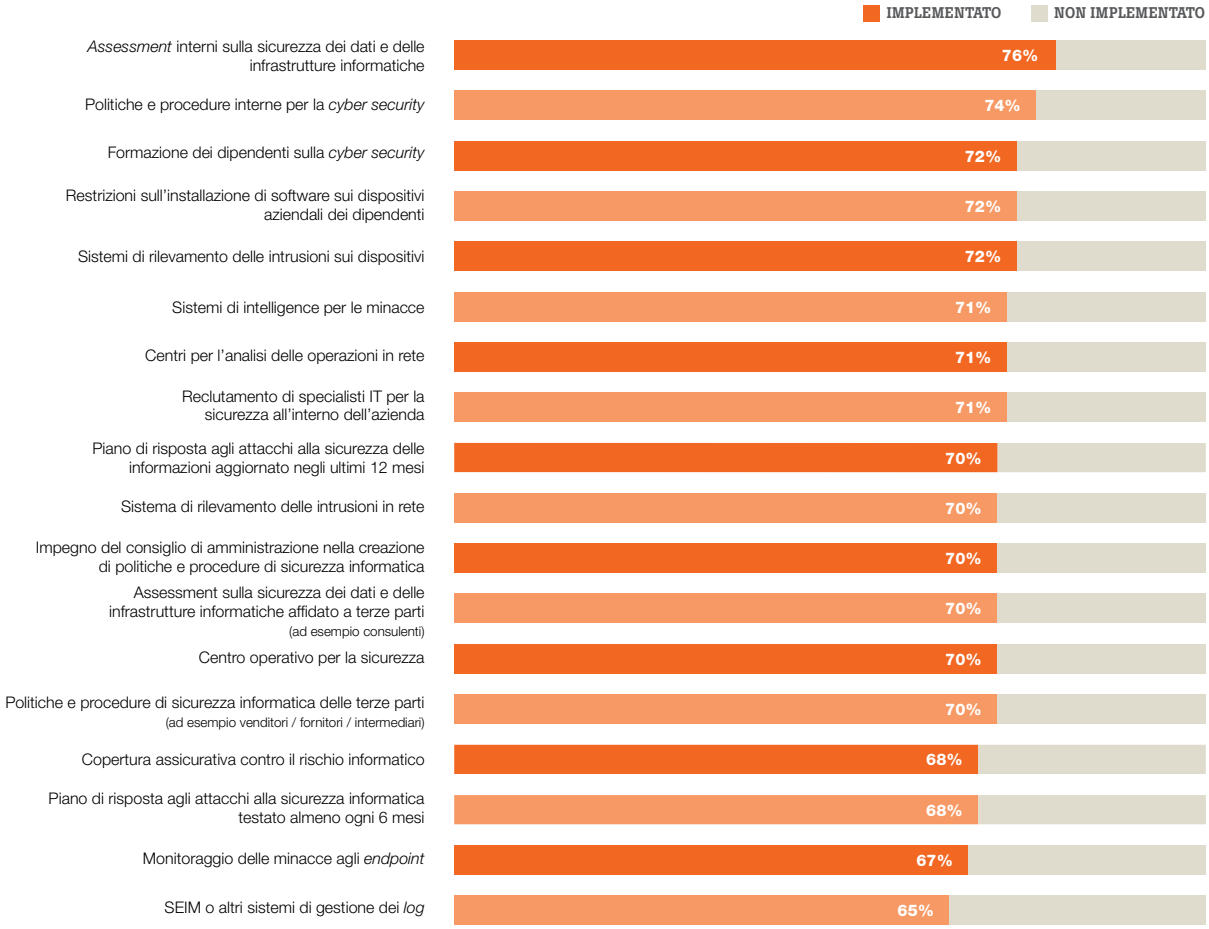


Tra le misure antifrode, quella adottata con maggior frequenza - riportata dall'82% dei dirigenti intervistati dirigenti - si concentra sulle informazioni, come il potenziamento della sicurezza informatica e delle contromisure tecniche. Se si legge questo dato dal punto di vista opposto, siamo di fronte a una situazione preoccupante: quasi un quinto degli intervistati (18%) non ha adottato le protezioni in questione. Come già osservato in precedenza, il furto di beni materiali o di scorte è stato il tipo più frequente di frodi riscontrate (29% dei dirigenti intervistati); di conseguenza, al secondo posto nella classifica delle misure antifrode figurano le iniziative sui beni materiali, per esempio, la distribuzione di sistemi di sicurezza fisica e l'etichettatura dei prodotti. È interessante notare che la terza misura più diffusa è stata la nomina di un risk manager e la disposizione di un sistema di gestione dei rischi formalizzato. La conduzione di controlli finanziari segue nella posizione successiva (77%), a pari merito con l'adozione di procedure di due diligence su terze parti.

L'enorme quantità di dati interni detenuta dalle imprese può essere preziosa per il contrasto alle frodi. Per esempio, gli strumenti di data analytics, quando interpretati da analisti esperti, spesso rivelano operazioni sospette e anomalie nell'ambito di indagini su corruzione e concussione, come illustrato dagli esperti di Kroll Zoë Newman, John Slavek e Peter Glanville nel loro articolo a pagina 29.

MISURE DI CONTENIMENTO DEL RISCHIO INFORMATICO

Adozione di misure di contenimento del rischio informatico



L'azione più frequente per il contenimento del rischio informatico è la conduzione di assessment interni sulla sicurezza dei dati e delle infrastrutture informatiche, menzionata dal 76% dei dirigenti intervistati. Va notato che il 70% degli intervistati ha citato anche l'implementazione di assessment sulla sicurezza dei dati e delle infrastrutture informatiche affidata a *terze parti o consulenti*. Quasi i tre quarti (74%) degli intervistati sostengono che la loro azienda ha implementato politiche e procedure interne per la cyber security.

Come già riportato in precedenza, il 44% degli attacchi informatici sono imputabili al personale interno (dipendenti, freelance / dipendenti a termine, ex-dipendenti) e questa realtà si riflette nell'adozione di politiche e corsi formativi in azienda: il 72% dei dirigenti ha introdotto la formazione dei dipendenti alla cyber security, mentre una percentuale equivalente ha imposto ai dipendenti delle restrizioni sull'installazione di software su dispositivi aziendali.

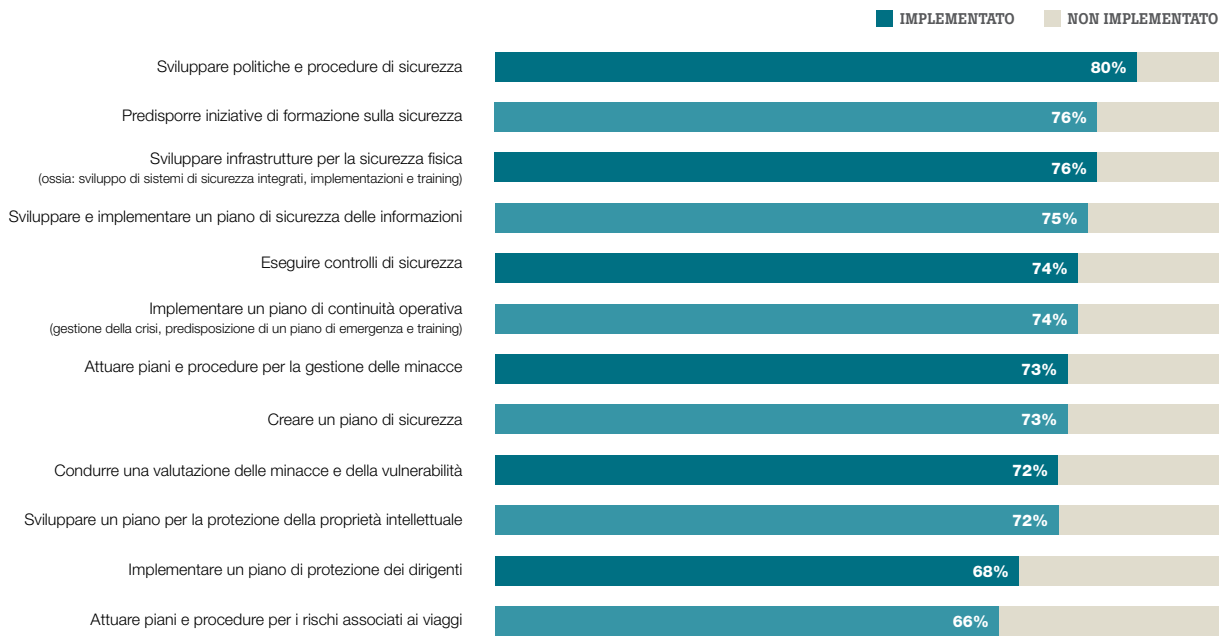
I metodi di rilevamento si posizionano nella parte alta della classifica, seguiti dai sistemi di rilevamento delle intrusioni, dai sistemi di intelligence per le minacce e dai centri per l'analisi delle operazioni in rete.

Considerando la prevalenza pari all'85% degli attacchi informatici negli ultimi 12 mesi, risulta preoccupante che solo il 70% degli intervistati abbia riferito che la propria azienda ha aggiornato il proprio piano di risposta agli attacchi alla sicurezza delle informazioni negli ultimi 12 mesi, mentre solo il 68% ha testato il proprio piano di risposta agli incidenti con cadenza semestrale. Gli esperti di Kroll Andrew Beckett, Michael Quinn, e Lucie Hayward testimoniano l'importanza di dotarsi di un piano di risposta agli incidenti collaudato e solido nel loro articolo a pagina 35.

Un dato di rilievo, che riflette l'importanza delle questioni legate alla governance informatica, è che il 70% degli intervistati sostiene che il proprio consiglio di amministrazione è impegnato nella creazione di politiche e procedure di sicurezza informatica.

MISURE DI CONTENIMENTO DEI RISCHI IN MATERIA DI SICUREZZA

Adozione di misure di contenimento del rischio di sicurezza



Nel complesso, l'80% dei dirigenti intervistati ha dichiarato che la propria azienda ha sviluppato politiche e le procedure di sicurezza, il 76% ha organizzato iniziative di formazione sulla sicurezza e il 76% riporta che la propria azienda ha sviluppato le infrastrutture per la sicurezza fisica. Tuttavia, c'è ancora molto da fare; per esempio, dato che il furto o la perdita di proprietà intellettuale è stato il tipo più frequente di incidente (38%), risulta preoccupante che il 28% degli intervistati indichi di non aver messo a punto un piano per tutelare la proprietà intellettuale. In un contesto economico globale come quello di oggi, più di un terzo (34%) dei dirigenti intervistati dichiara di non aver implementato piani e procedure per affrontare i rischi associati ai viaggi e spostamenti all'estero.

Secondo gli esperti di Kroll Nick Doyle e Rafael Lopez, nel loro articolo a pagina 27 sui rischi in materia di sicurezza nei mercati emergenti, una strategia concentrata sulla gestione del rischio in azienda può identificare, valutare e gestire le vulnerabilità in modo più efficace ed efficiente. Il vero punto di forza di questo approccio è la capacità di analizzare il rischio nel suo contesto e in tutte le attività dell'impresa.

Conclusioni

I rischi sono sempre in agguato, la complessità aumenta, i malfattori fanno rete, le metodologie di attacco si trasformano e le tecniche per occultare le proprie malefatte sono sempre più sofisticate. Nel frattempo, le aziende sono sempre più sotto i riflettori per la loro condotta in termini di gestione del rischio e risposta agli incidenti. Spinte dalla necessità sia di adeguarsi alla situazione, sia di giungere preparate ad affrontare episodi concreti, le imprese hanno fatto passi significativi verso lo sviluppo della business resilience. Bisogna fare di più.

L'esperto di Kroll Jordan Strauss scrive nel suo articolo a pagina 23 che l'agilità e la flessibilità di un'organizzazione, quando messa di fronte a eventi imprevedibili, può dipendere in larga misura dalla lungimiranza dei propri dirigenti nel voler rendere la resilienza uno dei valori fondamentali dell'impresa.

Il cammino per raggiungere la resilienza richiede infatti risorse, analisi, creatività, comprensione del comportamento umano e una vigilanza attenta per migliorare continuamente la capacità di un'impresa di prevenire, prepararsi, rispondere, indagare e risolvere i casi di frode e i rischi. In un contesto di rischio in evoluzione costante, è comprensibile il ricorso sempre maggiore ad esperti esterni, sia per ottenere una comprensione profonda dei fatti, sia per farsi suggerire le soluzioni migliori da mettere in campo.

Mappa globale del rischio

La mappa mostra la percentuale degli intervistati operanti in un dato paese o area geografica le cui società hanno subito frodi, attacchi informatici o incidenti in materia di sicurezza negli ultimi 12 mesi.

CANADA

La maggiore disponibilità al pubblico di punti di contatto digitali è la causa principale dell'aumento dell'esposizione al rischio di frode (riportato dal 54% degli intervistati)

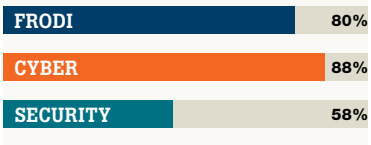
93%
Ritengono che l'esposizione alle frodi sia aumentata

REGNO UNITO

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 47% degli intervistati)

92%
Ritengono che l'esposizione alle frodi sia aumentata

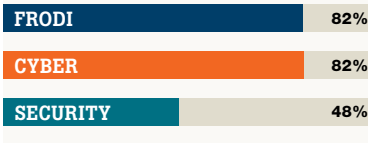
STATI UNITI



La complessità delle infrastrutture informatiche è la causa principale dell'aumento del rischio di frode (riportata dal 50% degli intervistati)

94%
Ritengono che l'esposizione alle frodi sia aumentata

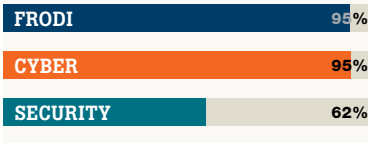
MESSICO



Il ricorso crescente all'outsourcing e alle società offshore è la causa principale dell'aumento del rischio di frode (riportato dal 45% degli intervistati)

94%
Ritengono che l'esposizione alle frodi sia aumentata

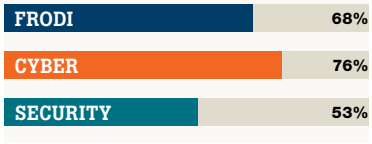
COLOMBIA



L'ingresso in nuovi mercati più rischiosi e la complessità delle infrastrutture informatiche sono i fattori principali alla base delle frodi (entrambi riportati dal 29% degli intervistati)

100%
Ritengono che l'esposizione alle frodi sia aumentata

BRASILE

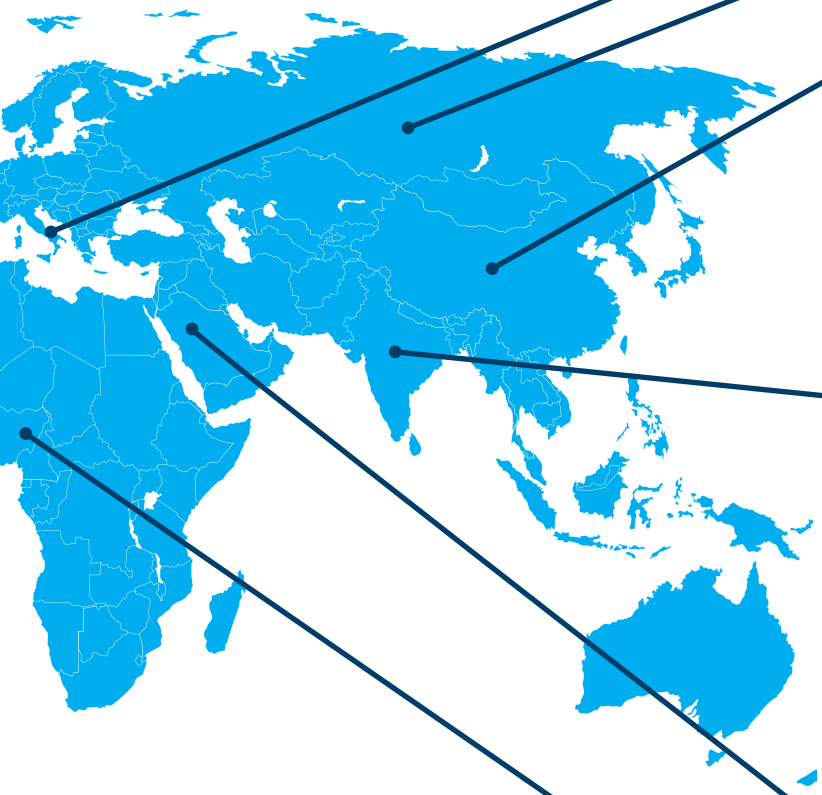


L'ingresso in nuovi mercati più rischiosi e la complessità delle infrastrutture informatiche sono i fattori principali alla base delle frodi (entrambi riportati dal 29% degli intervistati)

94%
Ritengono che l'esposizione alle frodi sia aumentata

Base: 545 decisori di livello dirigenziale che influenzano o sono responsabili delle strategie di contrasto al rischio e alle frodi della propria impresa

Fonte: Studio condotto su commissione da Forrester Consulting per conto di Kroll, agosto 2016



ITALIA

FRODI	77%
CYBER	79%
SECURITY	68%

91%
Ritengono che l'esposizione alle frodi sia aumentata

L'ingresso in nuovi mercati a rischio più elevato è la causa principale dell'aumento del rischio di frode (riportato dal 36% degli intervistati)

RUSSIA

FRODI	82%
CYBER	82%
SECURITY	59%

85%
Ritengono che l'esposizione alle frodi sia aumentata

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 31% degli intervistati)

CINA

FRODI	86%
CYBER	86%
SECURITY	75%

92%
Ritengono che l'esposizione alle frodi sia aumentata

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 55% degli intervistati)

INDIA

FRODI	68%
CYBER	73%
SECURITY	72%

78%
Ritengono che l'esposizione alle frodi sia aumentata

L'ingresso in nuovi mercati a rischio più elevato è la causa principale dell'aumento del rischio di frode (riportato dal 45% degli intervistati)

AFRICA SUB-SAHARIANA

FRODI	89%
CYBER	91%
SECURITY	74%

93%
Ritengono che l'esposizione alle frodi sia aumentata

La maggiore disponibilità al pubblico di punti di contatto digitali è la causa principale dell'aumento dell'esposizione al rischio di frode (riportato dal 33% degli intervistati)

MEDIO ORIENTE

FRODI	88%
CYBER	90%
SECURITY	82%

94%
Ritengono che l'esposizione alle frodi sia aumentata

La complessità dell'infrastruttura informatica e la mancanza di budget / risorse per la conformità delle infrastrutture sono le cause principali dell'aumento del rischio di frode (ambedue nominate dal 34% degli intervistati)

Mappa del rischio per settore

La mappa mostra la percentuale degli intervistati operanti in un dato settore di attività le cui società hanno subito frodi, incidenti informatici o incidenti di sicurezza negli ultimi 12 mesi.

COSTRUZIONI, INGEGNERIA E INFRASTRUTTURE

FRODI	70%
CYBER	77%
SECURITY	63%

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 40% degli intervistati)

86%
Ritengono che l'esposizione alle frodi sia aumentata

BENI DI CONSUMO

FRODI	82%
CYBER	83%
SECURITY	65%

L'ingresso in nuovi mercati a rischio più elevato è la causa principale dell'aumento del rischio di frode (riportato dal 40% degli intervistati)

92%
Ritengono che l'esposizione alle frodi sia aumentata

SERVIZI FINANZIARI

FRODI	89%
CYBER	89%
SECURITY	57%

L'ingresso in nuovi mercati a rischio più elevato è la causa principale dell'aumento del rischio di frode (riportato dal 34% degli intervistati)

91%
Ritengono che l'esposizione alle frodi sia aumentata

SANITÀ, FARMACEUTICA E BIOTECNOLOGIE

FRODI	80%
CYBER	86%
SECURITY	65%

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 41% degli intervistati)

88%
Ritengono che l'esposizione alle frodi sia aumentata

PRODUZIONE

FRODI	89%
CYBER	91%
SECURITY	81%

L'ingresso in nuovi mercati a rischio più elevato è la causa principale dell'aumento del rischio di frode (riportato dal 51% degli intervistati)

96%
Ritengono che l'esposizione alle frodi sia aumentata

VENDITA AL DETTAGLIO, ALL'INGROSSO E DISTRIBUZIONE

FRODI	83%
CYBER	87%
SECURITY	79%

La maggiore disponibilità al pubblico di punti di contatto digitali è la causa principale dell'aumento dell'esposizione al rischio di frode (riportato dal 33% degli intervistati)

87%
Ritengono che l'esposizione alle frodi sia aumentata

RISORSE NATURALI

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 40% degli intervistati)

92%

Ritengono che l'esposizione alle frodi sia aumentata

VIAGGI, TEMPO LIBERO E TRASPORTI

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 43% degli intervistati)

96%

Ritengono che l'esposizione alle frodi sia aumentata

SERVIZI PROFESSIONALI

Il frequente ricambio del personale è la causa principale dell'aumento del rischio di frode (riportato dal 47% degli intervistati)

96%

Ritengono che l'esposizione alle frodi sia aumentata

TECNOLOGIA, MEDIA E TELECOMUNICAZIONI

La complessità delle infrastrutture informatiche è la causa principale dell'aumento del rischio di frode (riportata dal 39% degli intervistati)

86%

Ritengono che l'esposizione alle frodi sia aumentata

Base: 545 decisori di livello dirigenziale che influenzano o sono responsabili delle strategie di contrasto al rischio e alle frodi della propria impresa

Fonte: Studio condotto su commissione da Forrester Consulting per conto di Kroll, agosto 2016

Raggiungere la Resilienza

DI JORDAN STRAUSS

Nel marzo del 2011 il Giappone è stato colpito da un potente terremoto e dal successivo tsunami , che hanno innescato una serie di eventi a catena artefici della peggiore crisi radioattiva dai tempi di Chernobyl. Al di là del Pacifico, al riparo da sguardi indiscreti, un gruppo di alti funzionari del governo degli Stati Uniti e i loro collaboratori erano radunati per una serie di riunioni estenuanti. Le responsabilità quotidiane di molti di questi leader non avevano nulla a che vedere con la risposta alle crisi. Tra loro si annoveravano avvocati, medici, meteorologi e specialisti di politiche ambientali. Molti si conoscevano già tra di loro, dato che solo pochi mesi prima avevano partecipato a un'esercitazione trimestrale per affrontare un'ipotetica situazione di emergenza nucleare negli Stati Uniti. Molti avevano lavorato insieme anche durante il disastro della Deepwater Horizon (British Petroleum); in questo modo, quando si è verificata la crisi non è stato perso del tempo nel costruire relazioni già createsi.

Anche se il beneficio di una pianificazione anticipata sembra evidente, un quarto di tutti gli intervistati dell'indagine Kroll Global Fraud and Risk 2016 ha dichiarato di non aver implementato o pianificato misure di preparazione ad eventuali minacce come catastrofi naturali, attentati terroristici, violazioni dei sistemi o interruzioni della continuità operativa.

In casi del genere, chi opera nel settore privato dovrebbe prendere esempio dagli enti governativi. Nella pianificazione volta a garantire la capacità di recupero (*resilienza)* in caso di crisi, esistono tre principi da prendere in considerazione:

1 Pensare alla preparazione come un processo, non come uno stato, e impegnarsi a migliorare di continuo.
Sforzarsi di essere più preparati domani rispetto a quanto lo si è oggi. Riflettere attentamente sui soggetti di riferimento ai quali rivolgersi durante un evento di crisi, prima che questo accada. Poiché le ore immediatamente successive a una crisi sono le più importanti, è fondamentale pianificare l'impatto di un evento del genere sulla propria reputazione e sui propri

La pianificazione della risposta alle crisi è fondamentale per ogni organizzazione e per qualsiasi settore di attività.

JORDAN STRAUSS
Jordan Strauss è Associate Managing Director per la sezione Investigations and Disputes di Kroll. Jordan ha svolto la funzione di Direttore presso il National Security Council della Casa Bianca, di Deputy Justice Attaché e Senior Legal Advisor in forza al Dipartimento di Giustizia degli Stati Uniti a Kabul, in Afghanistan, e come procuratore federale e avvocato presso il Dipartimento di Giustizia. Grazie alle conoscenze maturate nelle aule di tribunale, è stato l'avvocato specializzato in crisi ed emergenze di maggior esperienza del Dipartimento di Giustizia. Autore di numerose pubblicazioni e dotato di indiscussa abilità oratoria, Jordan ha offerto le sue testimonianze sotto giuramento, dirigendo e partecipando a innumerevoli esercitazioni, sia su larga scala sia riservate al management, sulla preparazione ai disastri e agli attacchi informatici.

dipendenti. Prendere in considerazione l'organizzazione di esercitazioni con una selezione multidisciplinare dei propri dirigenti. Studiare attentamente le conseguenze di un incidente grave accaduto a un concorrente. Chi è interessato alla solidità della propria impresa dovrebbe chiedersi sempre: "cosa faremmo se capitasse anche a noi?" Ci sono molti modi di condurre esercitazioni per valutare la propria reattività, sia con costi esigui per la società, sia totalmente senza costi. La prossima volta che si intende comunicare un evento, per esempio un allarme meteo, si può verificare se il sistema di notifica ai dipendenti funziona (se è già stato implementato): tutto sommato è lo stesso sistema di notifica da usare in presenza di un kamikaze in azienda. La costruzione di una cultura della resilienza all'interno di un'organizzazione inizia dall'alto. L'impegno di un amministratore delegato nel potenziare la resilienza e la reattività di un'impresa dovrebbe essere evidente per tutti i dipendenti: uno dei modi per raggiungere quest'obiettivo è dimostrare l'interesse dei dirigenti di alto livello per il successo di iniziative come la messa in stato d'allerta dei dipendenti e i programmi di comunicazione interna.

2 Il problema più evidente non sempre corrisponde al rischio più grande: bisogna sempre pensare al rischio in funzione sia delle probabilità, sia delle conseguenze.
La determinazione della probabilità di un dato evento è di tipo attuariale e si basa sull'intelligence: Non si tratta di preoccuparsi per l'ultima notizia tragica ascoltata in TV. Il "Risk" è calcolato come la probabilità moltiplicata per le conseguenze, pertanto una conoscenza approfondita delle possibili conseguenze è fondamentale per prendere decisioni informate in base al rischio. Questo richiede un impegno sostanziale da parte di una selezione multidisciplinare di alti dirigenti.

Per esempio, oltre a compromettere il morale dei dipendenti, le violazioni dei sistemi possono anche comportare responsabilità giuridiche, problemi di natura normativa e danni alla reputazione consistenti e persistenti. Nel valutare le conseguenze di un evento, si dovrebbe tener conto di tutti questi aspetti, insieme ai costi (consulenza, spese legali, contenziosi e pubbliche relazioni) legati alla loro risoluzione. Anche la stima dei costi associati alla fuoriuscita dalla crisi è fondamentale: spese legali, spese di pubbliche relazioni e servizi esterni di gestione delle crisi sono voci di bilancio consistenti. Allo stesso modo, un episodio di violenza sessuale in un campus universitario colpisce nel profondo la comunità, ha conseguenze devastanti su una persona giovane e comporta una serie di problemi in termini di reputazione, responsabilità e moralità. Una pianificazione anticipata che tenga conto in pieno dell'impatto di questi problemi, comprese le spese legali e quelle legate alle pubbliche relazioni, può contribuire a contenere gli effetti negativi.

Le esercitazioni per i dirigenti sono un ottimo strumento per la pianificazione anticipata, come lo sono le discussioni orientate e le sessioni di brainstorming. Inoltre è fondamentale fare tesoro delle esperienze passate e osservare cosa accade nelle altre imprese.

3 Garantire che i rischi effettivi siano tenuti in considerazione durante l'allocazione delle risorse.
Durante il disastro avvenuto in Giappone, i funzionari governativi degli Stati Uniti si sono occupati per prima cosa delle vite in pericolo e in seconda battuta delle conseguenze collaterali. Hanno preso una decisione giustificabile e ponderata sui rischi su come impiegare il loro tempo, che in ultima analisi è la loro risorsa più preziosa.

I funzionari governativi di alto livello hanno avuto accesso ai dati necessari per prendere decisioni cruciali con la dovuta attenzione. Sono stati aiutati da diversi team di risposta interdipartimentali che avevano imparato la lezione impartita dalla crisi della Deepwater Horizon. I rapporti creatisi nel corso delle esercitazioni e del disastro reale hanno reso la risposta molto più tempestiva. Non vi è alcun motivo per cui le imprese debbano essere impreparate di fronte a un futuro incerto.

La pianificazione della risposta alle crisi è fondamentale per ogni organizzazione e per qualsiasi settore di attività. Ecco perché sia il gestore di uno stadio sia di un club sportivo professionale con un budget limitato dovrebbero valutare la probabilità e le conseguenze di eventi come attacchi terroristici o emergenze mediche. Le loro risorse devono concentrarsi sull'evento a maggior rischio, non necessariamente sull'evento di più alto profilo. Un processo decisionale che tiene il rischio nella giusta considerazione offre ai dirigenti una maniera logica e giustificabile di allocare le risorse e deve essere preparato in anticipo, non durante una crisi.

Ricambio del personale: Contenere le perdite di informazioni riservate e di proprietà intellettuale

DI MARIANNA VINTIADIS E TADASHI KAGEYAMA

Il direttore di una fabbrica di alta tecnologia in Asia stava cenando e facendo zapping col telecomando, quando all'improvviso apparve in TV un servizio che rischiò di farlo soffocare. Era il volto di uno dei suoi ex ingegneri, che ora prestava servizio per uno dei suoi principali concorrenti. L'ingegnere gli aveva detto di voler tornare nella sua città natale per aiutare i suoi anziani genitori a gestire la loro piccola attività di pesca. Il manager andò a dormire piuttosto preoccupato. E ne aveva ben donde: la mattina seguente andò al lavoro e scoprì che altri ingegneri avevano lasciato l'azienda per essere assunti presso lo stesso concorrente.

Così si è rivolto a Kroll per chiedere aiuto. Abbiamo scoperto che un totale di 25 ingegneri impiegati in attività di progettazione, produzione e controllo qualità erano stati sistematicamente reclutati dal concorrente attraverso il network dei dipendenti e dei cacciatori di teste. Questi dipendenti portavano via con loro un prezioso know-how, informazioni riservate sull'ingegneria, gli elenchi dei fornitori e i manuali di processo.

Molte aziende stanno prendendo atto del rischio di furto o di perdita di informazioni commerciali confidenziali e di tecnologie preziose per mano dei propri dipendenti. Questo rischio si sta decisamente acutizzando nei paesi asiatici in rapida crescita. Una strada sempre più battuta per l'acquisizione di informazioni commerciali o industriali confidenziali di un concorrente è l'assunzione del loro personale.

Tuttavia, nella nostra esperienza, i manager spesso ci rivolgono la domanda sbagliata. Ci chiedono: "Come posso impedire ai miei validi dipendenti di passare alla concorrenza?" La loro domanda, in realtà, dovrebbe concentrarsi su riflessioni come: "Stiamo facendo abbastanza per farli restare?"

Il modo migliore per preservare le informazioni riservate e il know-how è trattare bene i dipendenti, per assicurarsi che anche in caso di abbandono, questo avvenga nel migliore dei modi. Qualsiasi iniziativa in grado di ridurre l'avvicendamento dei dipendenti migliorerà l'integrità dell'azienda - nel vero senso della parola. Questa conclusione trova conferma nell'indagine condotta da Kroll, dalla quale emerge che il fattore principale individuato per l'aumento del rischio di frode è il turnover elevato del personale, menzionato dal 37% degli intervistati.

Tuttavia, anche se le imprese possono aver preso provvedimenti rigorosi per creare una cultura aziendale positiva, altri eventi possono ancora generare insoddisfazione dei dipendenti. In Europa, per esempio, molte imprese sono a conduzione familiare. Quando avviene un trasferimento di proprietà o un passaggio generazionale, l'atmosfera lavorativa può cambiare dal giorno alla notte. Anche le operazioni di fusione e acquisizione sono causa di malcontento nei dipendenti, dato che le posizioni lavorative sono accorpate o scompaiono del tutto.

MARIANNA VINTIADIS
Marianna Vintiadis è Country Manager di Kroll in Italia ed è inoltre responsabile delle operazioni Kroll in Austria e Grecia. Da quando ha assunto la direzione della sede italiana di Kroll, Marianna ha ampliato con successo il portafoglio clienti locale, che oggi include le più grandi imprese e gli istituti finanziari italiani di maggior rilievo, oltre agli studi legali più prestigiosi. Ha inoltre aperto i servizi di Kroll al mercato italiano delle PMI, colonna portante dell'economia nazionale.

TADASHI KAGEYAMA
Tadashi Kageyama è Regional Managing Director e responsabile delle operazioni di Kroll nel continente asiatico. Tadashi offre il suo contributo ai clienti per contenere il rischio di frode, rispondere alle violazioni normative e di compliance e risolvere le controversie e i contenziosi. Inoltre aiuta i clienti a gestire la loro proprietà intellettuale, fornendo servizi investigativi e di consulenza sulle azioni di contrasto a livello globale. Tadashi ha oltre 15 anni di esperienza nella conduzione di attività di business intelligence delicate e complesse relative agiurisdizioni diverse.

Di seguito elenchiamo sette errori commessi di frequente dalle aziende in merito ai rischi di fuga delle informazioni legati ai dipendenti:

1 Sottovalutare le motivazioni fornite nel colloquio di fine rapporto.

Il colloquio di fine rapporto ha diverse finalità. Quando un dipendente si allontana, il datore di lavoro dovrebbe utilizzare l'intervista per valutare il rischio di furto di informazioni o di proprietà intellettuale (PI). È un'opportunità per valutare lo stato d'animo dei dipendenti e per ribadire loro le prescrizioni sulla sicurezza delle informazioni e della proprietà intellettuale, nonché i patti di non concorrenza o non sollecitazione. Il basso morale di un dipendente può rivelare la presenza di un malessere più profondo e la possibilità di ulteriori allontanamenti in azienda. Troppo spesso le imprese sottovalutano il malcontento dei loro dipendenti.

2 Distruggere le informazioni a rischio.

Quando i dipendenti vanno via, le imprese tendono a riutilizzare i loro computer, a cancellare gli account di posta elettronica e a non archiviare i registri telefonici. In Asia ci troviamo spesso di fronte a casi in cui i dipendenti in uscita sono autorizzati a mantenere i loro computer e cellulari come parte dei benefit per le dimissioni. Tutti i dati e i dispositivi, inclusi i registri di accesso aziendali e le registrazioni video di sicurezza (ove consentito dalla legge), devono essere conservati per un dato periodo di tempo, visto che spesso la scoperta di un'infrazione può richiedere mesi. Se ai dipendenti è permesso trattenere i dispositivi, questi devono essere accuratamente formattati o puliti per garantire che nessuna informazione riservata sia ancora nelle loro mani, in quanto queste potrebbero essere messe a disposizione dei concorrenti.

3 Restringere eccessivamente le responsabilità.

Spesso le aziende affidano la valutazione delle minacce e la stesura di piani e politiche esclusivamente ai reparti Risorse Umane e Sicurezza dei Dati. Tuttavia, il rischio deve essere affrontato da più interlocutori, tra cui i reparti Affari Legali, Proprietà Intellettuale, Marketing, l'azienda stessa e finanche l'amministratore delegato nel caso in cui la potenziale perdita potenziale sia di rilevanza strategica, di grande entità o possa comportare una pubblicità negativa.

4 Consentire ai dipendenti di utilizzare i propri dispositivi per il lavoro in azienda.

Con l'aumento degli straordinari, del lavoro da casa e della flessibilità, stabilire regole chiare sui dispositivi dei dipendenti ricopre un'importanza sempre maggiore. Raramente, per non dire mai, risulta possibile compiere indagini su personal computer e telefoni cellulari che appartengono ai dipendenti. Consigliamo ai nostri clienti di permettere ai dipendenti di lavorare solo sui beni aziendali e non sui dispositivi personali. Inoltre i programmi e i documenti di lavoro dovrebbero essere sempre memorizzati sul server aziendale, mai in locale. Senza dimenticare che è importante evitare che il dipendente abusi del suo potere decisionale, contrastando questo rischio con politiche e procedure ben congegnate. Per esempio, un tipo di deterrente può essere la proibizione di usare le chiavette USB. Tuttavia, se tutti i dispositivi assegnati al personale avranno le porte USB disattivate, l'uso improprio - sia per errore, sia di proposito - diventerà molto più difficile.

5 Fare attenzione al furto digitale.

Troppo spesso le aziende si concentrano sul furto di informazioni digitali, ma anche i registri fisici possono essere veicoli di perdite notevoli.

6 Gratificare le condotte scorrette.

Le aziende potrebbero assumere un dipendente che porta con sé informazioni raccolte dalla sua posizione lavorativa precedente, come gli elenchi dei clienti o le informazioni sul prodotto. Quello che non tengono in considerazione è che le persone che si sono comportate male, in tutta probabilità, lo faranno nuovamente. Kroll ha lavorato di recente con una società di ingegneria nella quale l'ingegnere capo aveva lasciato il posto e messo a disposizione dei concorrenti alcuni progetti importanti. Durante l'indagine, abbiamo scoperto che il dipendente aveva fatto lo stesso con il suo datore di lavoro precedente.

7 Sottovalutare l'impatto di un'indagine.

Quando un dipendente è allontanato a causa di un sospetto di furto di informazioni, l'indagine conseguente può compromettere il morale degli altri dipendenti. È importante assicurarsi che tutte le misure prese dall'azienda per proteggere legittimamente il proprio patrimonio non appaiano come una ritorsione. Le persone non amano finire sotto inchiesta o partecipare alle indagini sui propri colleghi. Le imprese spesso si affidano a investigatori esterni per evitare che i dipendenti indaghino sui loro colleghi, con tutte le complicazioni del caso, e per assicurarsi che l'indagine sia condotta nel modo più efficiente possibile. Inoltre non va dimenticato che le indagini interne devono essere condotte in conformità alle leggi in vigore, quali le normative (a titolo indicativo e non limitativo) sul lavoro, la riservatezza dei dati e il whistleblowing, se quest'ultimo è regolamentato, e che le normative differiscono da paese a paese. Un investigatore esterno può lavorare affiancato da un consulente interno o esterno per garantire che l'indagine sia condotta nel rispetto di tutte le leggi vigenti e che le prove ottenute non siano compromesse.
Come sempre, prevenire è meglio che curare. Favorire una cultura positiva e stabilire procedure adeguate contribuirà a proteggere gli asset più preziosi della vostra azienda.

Rischi in materia di sicurezza nei mercati emergenti

DI NICK DOYLE E RAFAEL LOPEZ

Al giorno d'oggi le aziende che operano su scala globale si trovano di fronte a molte sfide legate al loro ingresso nei mercati emergenti: i rischi per la sicurezza quali il terrorismo, la debolezza delle istituzioni e della pubblica sicurezza, i disordini sociali e la corruzione, che devono essere fronteggiati facendo affidamento a risorse locali sempre più scarse.

Queste sfide impongono alle imprese che operano su scala globale o locale di prendersi cura dei i loro dipendenti, proteggere il valore degli asset per gli azionisti e far fede ai loro obblighi di natura giuridica e sociale verso la comunità locale.

Sussistono anche rischi notevoli per la reputazione di un'azienda e la sua indipendenza da soggetti esterni. La società civile e la comunità internazionale restano vigili su eventuali violazioni dei diritti umani o minacce per le comunità locali. Le imprese potrebbero decidere di sottovalutare l'entità dei rischi identificabili e non porvi rimedio, prestando il fianco alle critiche dei media, del settore o degli investitori.

Per fare un esempio, una società mineraria canadese si è vista accusare del fatto che il suo personale di sicurezza aveva ucciso un attivista locale contrario alle attività di una miniera in Guatemala e ne aveva reso permanentemente invalido un altro nel 2009. La società ha smentito le accuse e a tutt'oggi sta combattendo in tribunale (anche se non possiede più la miniera).

Un altro caso riguarda una società che gestiva un centro di distribuzione nelle periferie di Città del Messico, entrata in contatto con Kroll dopo esser stata vittima di una rapina a mano armata. Due camion, in pieno giorno, hanno portato via gli stock più preziosi della società. Tra i banditi sono stati identificati in prima battuta molte ex guardie giurate che avevano lavorato per l'azienda. Conoscevano bene li deposito e sapevano esattamente cosa prendere. Dopo il rifiuto della polizia locale di indagare, si è scoperto che i responsabili erano i proprietari dell'istituto di vigilanza.

NICK DOYLE
Nick Doyle è Managing Director e Responsabile della gestione dei rischi in materia di sicurezza presso la divisione Indagini e contenziosi di Kroll presso la sede di Londra. Nick coordina l'offerta di soluzioni per la sicurezza di Kroll in Europa, Medio Oriente e Africa. Dal suo arrivo in Kroll nel 2008, dopo aver brillantemente prestato servizio nell'esercito e nelle forze dell'ordine, Nick ha gestito oltre 350 progetti in 50 paesi.

RAFAEL LOPEZ
Rafael Lopez è Direttore del reparto Indagini e contenziosi della filiale messicana di Kroll. Rafael ha organizzato programmi di sicurezza personalizzati e gestito i trasferimenti all'estero del personale, coordinando le squadre per la protezione dei dirigenti in Messico, Cile e Venezuela. Ha inoltre tenuto seminari sulla sensibilizzazione alla sicurezza e workshop sulla gestione del rischio in materia di estorsioni, sequestri di persona e andamenti nel mondo criminale. Ha diretto i controlli di sicurezza di siti in Messico, Stati Uniti, Panama, Guatemala, Colombia, Ecuador e Venezuela.

Vista la difficoltà di operare in mercati non conosciuti, le imprese si rivolgono spesso a consulenti per la sicurezza operanti su scala globale per gestire meglio questi "rischi d'impresa." Possono avere subito un evento grave e improvviso di notevole impatto e hanno urgente necessità di consulenza, assistenza e supporto. Oppure potrebbero aver individuato rischi e minacce potenziali nei nuovi mercati o presso le filiali già stabilite, ma non dispongono di risorse interne, esperienza, conoscenze o capacità per affrontarle.

Adottando una strategia basata sulla gestione del rischio di sicurezza aziendale, le imprese possono identificare, valutare e contenere i loro punti di vulnerabilità in maniera strutturata e onnicomprensiva. Il vero punto di forza di questo approccio è la capacità di analizzare il rischio nel suo contesto e in tutte le attività dell'impresa. La strategia coinvolge sia il mondo fisico, che quello informatico, un aspetto essenziale per assicurare che il rischio sia affrontato in modo equilibrato e calibrato, evitando le sottovalutazioni o le spese superflue.

La gestione dei rischi in materia di sicurezza in azienda, nella sua forma più semplice, è un mezzo per individuare, comunicare e classificare i rischi per favorire l'allocazione ottimale delle risorse. Alcuni rischi, quando compresi a fondo, saranno accettati. Altri richiederanno un investimento bilanciato di competenze, risorse e controlli di gestione. I sistemi o le misure di gestione del rischio in un'impresa devono essere rispettati, applicati e sottoposti a revisione costante.

In ultima analisi, i clienti detengono l'expertise in materia di attività, obiettivi e capacità della propria organizzazione. I consulenti esterni possono apportare le loro conoscenze e l'esperienza per identificare e contenere le vulnerabilità. Il risultato di questi sforzi combinati è un modo più efficace e diversificato di allocare le risorse. Le imprese che adottano un approccio olistico alla gestione del rischio in azienda spesso sono in grado di identificare e interrompere le attività inefficaci e dispendiose, risparmiando così tempo e denaro.

Caso studio - Risposta alle crisi

Kroll è stata contattata da società di consulenza e ristrutturazione aziendale per ottenere assistenza sul caso di una banca finita in bancarotta a causa di una frode di grande entità. Abbiamo valutato dinamicamente i rischi della banca, i suoi dipendenti e il team di consulenti e avvocati dell'impresa. Abbiamo stabilito un quadro di gestione dei rischi in materia di sicurezza che ha coinvolto specialisti in crisi aziendali, agenti di sorveglianza e personale per la protezione dei dirigenti durante le varie fasi del progetto. Il lavoro ha previsto la valutazione di:

- Gestione delle strutture
- Sicurezza di movimento per il personale
- Supervisione dei trasferimenti di denaro dagli sportelli alla banca centrale e distruzione delle carte di credito
- Sicurezza degli edifici
- Sicurezza operativa dei beni
- Sicurezza delle informazioni
- Cyber Security
- Notifica delle ordinanze giudiziarie
- Pianificazione e gestione della sicurezza per le grandi riunioni dei creditori

Grazie ai nostri servizi, i consulenti aziendali sono stati in grado di lavorare efficacemente con la garanzia di poter operare in un ambiente sicuro.

Data Analytics: Trovare l'ago nel pagliaio non è sempre così difficile

DI ZOE NEWMAN, PETER GLANVILLE E JOHN SLAVEK

L'indagine Global Fraud and Risk condotta da Kroll ha rilevato che il 44% delle frodi in azienda è stato scoperto da un whistleblower, a fronte del 39% accertato dalle indagini interne e del 32% dal management. Rilevare e affrontare i problemi prima che un whistleblower decida di denunciarli o che si passi all'intervento delle autorità comporta dei chiari benefici in materia di finanze, reputazione e risorse. In che modo le aziende possono essere in prima linea nel contrasto alle frodi, alla corruzione e alla concussione?

Sfruttando i dati raccolti in azienda per individuare le frodi, la concussione e la corruzione

'L'espressione *''Data Analytics"* è stata ripetuta all'infinito dai consulenti in questi ultimi anni. Eppure, sulle sue applicazioni pratiche per le imprese, di parole ne sono state profuse poche. In poche parole, data analytics significa semplicemente consultare i dati grezzi raccolti dai sistemi gestionali e finanziari di una società e analizzarli per trarre delle conclusioni. La maggior parte di noi ha svolto quest'attività per anni.

L'elemento fondamentale è saper analizzare i dati in modo efficiente ed efficace per individuare gli andamenti e le anomalie per conto dell'utente finale, utilizzando i migliori strumenti disponibili.

ZOE NEWMAN
Zoë Newman ricopre il ruolo di Managing Director nella sezione Investigations and Disputes presso la sede londinese di Kroll. Zoë è responsabile delle indagini finanziarie per l'area geografica Europa, Medio Oriente e Africa. Ha accumulato una vasta esperienza nella conduzione di indagini forensi transnazionali complesse in materia di frode, corruzione e potenziali violazioni della legge, comprese le indagini ai sensi di normative come il Foreign Corrupt Practices Act (FCPA) e lo UK Bribery Act. Inoltre offre ai clienti i suoi servizi di consulenza per ottimizzare l'implementazione dei controlli per ridurre i rischi in questione.

PETER GLANVILLE
Peter Glanville ricopre la posizione di Managing Director nella sezione Investigations and Disputes di Kroll presso la sede di Hong Kong. È specializzato nella consulenza alla clientela sulla contabilità forense e la criminalità finanziaria. Peter è un commercialista con oltre 15 anni di esperienza nelle questioni finanziarie delicate, come indagini su frodi, corruzione e concussione, audit contrattuali, revisione dei controlli, valutazione dei programmi per la lotta alla criminalità finanziaria e la compliance, offrendo inoltre consulenza contabile di alto livello. Peter ha offerto i suoi servizi a imprese operanti in diversi settori nel Regno Unito, Europa, Asia e Australia.

JOHN SLAVEK
John Slavek ricopre la posizione di CPA e Managing Director presso la sede Kroll di Philadelphia. Fin dall'inizio della sua collaborazione con Kroll nel 1998, John ha aiutato i clienti ad affrontare un ampio raggio di questioni finanziarie e contabili, tra cui indagini sulle società straniere operanti negli Stati Uniti ai sensi del Foreign Corrupt Practices Act, appropriazione indebita, bancarotta, controversie contrattuali e valutazione dei controlli interni. Possiede inoltre una notevole esperienza sul campo in progetti di due diligence, indagini sulla manipolazione dei rendiconti finanziari e quantificazione delle potenziali perdite di profitto nei contenziosi commerciali.

Storicamente, le indagini su frodi, corruzione e concussione sono state condotte seguendo un metodo di controllo a campione sulle transazioni e la documentazione di supporto. Tuttavia, l'analisi dei dati oggi può essere applicata per scandagliare i registri finanziari di una società alla ricerca di transazioni ad alto rischio, così da poter condurre attività investigative mirate.

La chiave dell'analisi dei dati raccolti sta nell'individuare i rischi di corruzione e concussione e nel definire quali transazioni sono da considerare sospette.

Per condurre un'analisi del genere, è richiesto l'intervento di analisti altamente qualificati. Per esempio, se si devono analizzare milioni di transazioni nei sistemi contabili di una società, questo tipo di analisi non sarebbe possibile con strumenti di base come Excel. Gli esperti impiegherebbero strumenti di data anlytics più sofisticati, per esempio SQL, per individuare le transazioni che corrispondono ai modelli tipici delle frodi.

In che modo si può usare l'analisi dei dati per individuare le frodi, la concussione e la corruzione in azienda?

Nelle imprese sta crescendo la consapevolezza che la grande quantità di documenti finanziari e operativi storici presenti in archivio può essere una preziosa fonte di dati supplementari per l'implementazione di un programma anticorruzione più strutturato.

La difficoltà dell'analisi dei dati raccolti sta nell'individuare i rischi di corruzione e concussione e nel definire quali transazioni sono da considerare sospette.

Kroll scende in campo operando una selezione dei dati contabili (o in alcuni casi esaminando l'intera contabilità generale) ed elaborando questi dati (a volte combinandoli con dati esterni all'organizzazione) per individuare le operazioni sospette.

Questo processo è affidato ad analisti di dati altamente qualificati, ma soprattutto indicizziamo per rendere consultabili agli archivi attraverso interrogazioni puntali con liste di parole chiave perfezionate nel tempo grazie alla nostra esperienza pluriennale in questo tipo di indagini. Queste procedure sono concepite per identificare rapidamente le operazioni e le relazioni dalle quali emergono gli elementi tipici di pagamenti fraudolenti o finalizzati alla corruzione. Le procedure interrogative sono integrate con modelli di ricerca specifici per settore o creati su misura per la società, al fine di individuare altre transazioni potenzialmente sospette.

Non tutte le operazioni sospette corrispondono a violazioni. Lo scopo della procedura è evidenziare i modelli di comportamento e le relazioni anomale con clienti e fornitori, oppure individuare i singoli pagamenti da sottoporre a ulteriori indagini. Mentre alcuni di questi possono risultare giustificati, altri rappresentano un motivo di preoccupazione.

Questa strategia basata sul rischio garantisce risparmi di tempo e denaro, consentendo alla società di gestire autonomamente i processi e i risultati. Una volta individuata un'anomalia, l'azienda può svolgere le indagini e fare le valutazioni del caso, richiedere consulenza e prendere il controllo della situazione in maniera proattiva; una soluzione di gran lunga preferibile alla ricezione improvvisa di una lettera inviata da un whistleblower o da un autorità giudiziaria.

Quali sono le tendenze attuali e le buone prassi? Come si sta evolvendo il panorama?

Il rischio di corruzione e concussione resta uno dei maggiori fattori di preoccupazione per le imprese. Dall'indagine condotta da Kroll emerge che il 23% degli intervistati è stato dissuaso dall'operare nei mercati esteri a causa del rischio percepito di corruzione. Tuttavia, se si sceglie di tenersi alla larga dai mercati esteri, si possono perdere opportunità di sviluppo potenzialmente elevate.

Il rischio di corruzione può essere gestito dispiegando i controlli appropriati e un programma di compliance efficace. I reparti aziendali specializzati stanno migliorando le loro strategie per individuare e gestire i rischi in questione. L'uso di valutazione del rischio e i programmi di due diligence su terze parti sono in crescendo, permettendo quindi di acquisire conoscenze approfondite sulla storia delle relazioni tra le società esterne e l'impresa.

Gli autori delle frodi stanno diventando sempre più sofisticati nell'occultare le loro tracce?

Le aziende diventano più intelligenti nel gestire il rischio di concussione e corruzione, ma i disonesti non stanno a guardare. Sono consapevoli che agenti e terze parti sono tenuti al rispetto della due diligence e devono trovare soluzioni creative per accettare tangenti e altri pagamenti irregolari.

Fino a cinque anni fa, le operazioni sospette erano relativamente facili da individuare. Tra queste figuravano:

- Fornitori registrati come società off-shore
- Conti bancari in giurisdizioni sospette
- Pagamenti una tantum a cifra tonda
- Operazioni registrate come contabilità generale per le consulenze

I disonesti sono coscienti del fatto che queste transazioni sono subito identificate come sospette. Oggi Kroll riscontra maniere molto più creative di mascherare i pagamenti, tra cui:

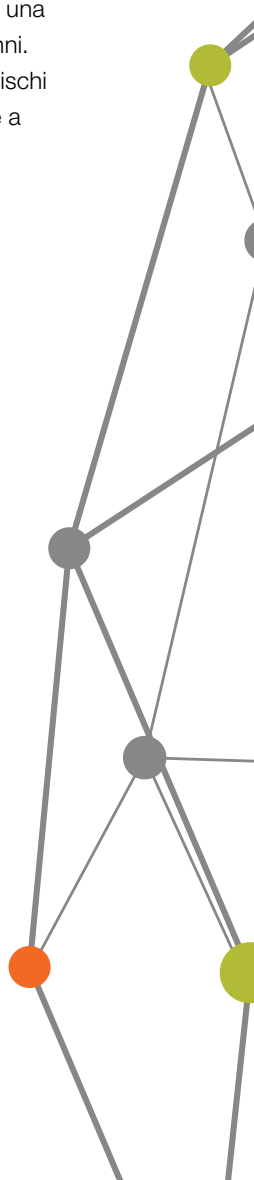
- False fatturazioni verso soggetti terzi noti finalizzate alla creazione di fondi neri
- Sconti troppo consistenti a clienti e distributori
- Concessioni di sconti derivanti dalla fatturazione di quantità eccessive di merci
- I collaboratori di fiducia e ben noti in azienda, come gli agenti di viaggio, sono stati spinti a fare da intermediari

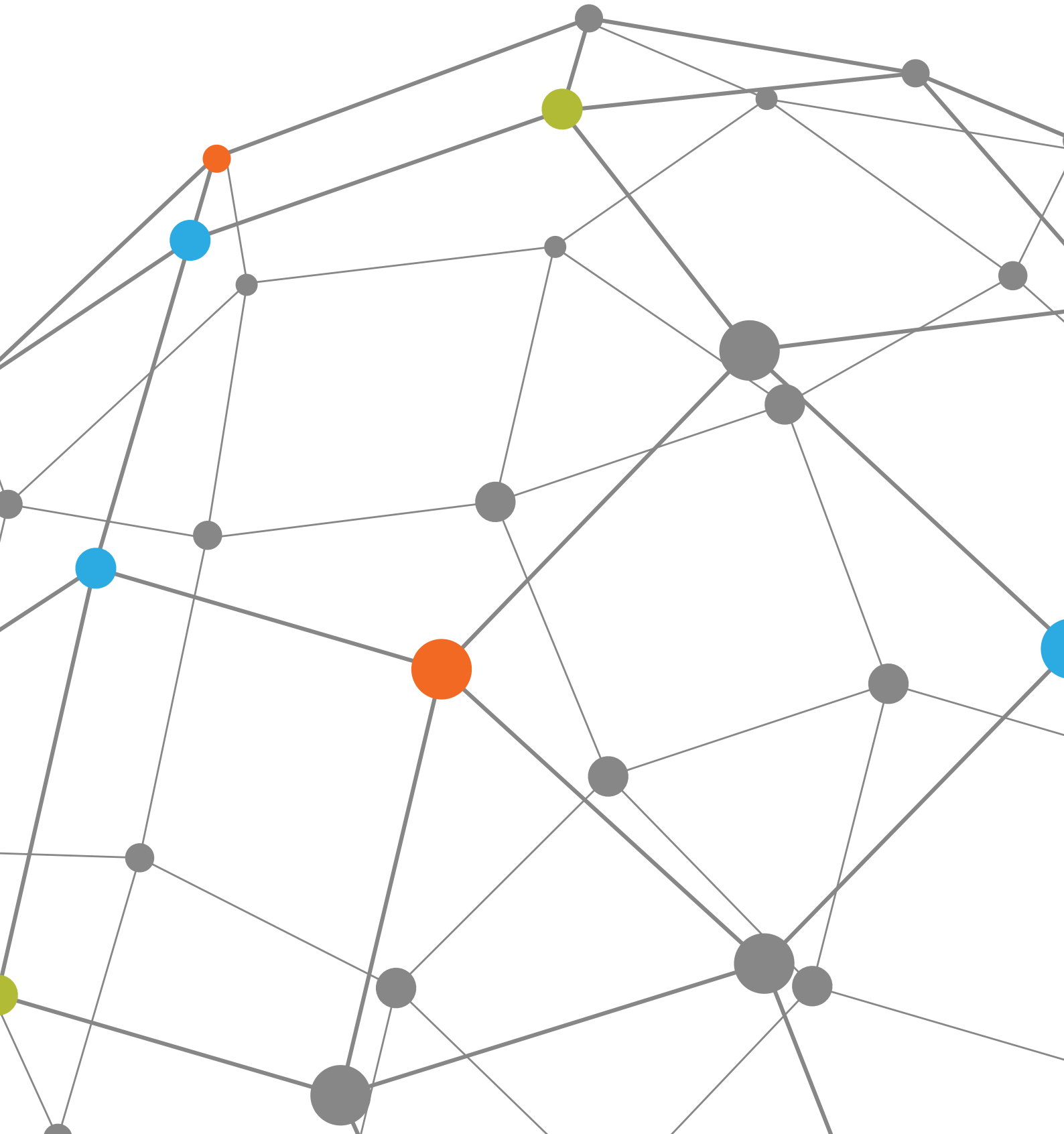
La buona notizia è che le tecniche di data analytics consentono di smascherare questi imbrogli.

Prendiamo come esempio una controllata che si occupa di forniture da dieci anni, il cui fatturato aumenta improvvisamente di 20 volte negli ultimi due anni. Le revisioni interne e le verifiche di compliance e di bilancio condotte nella sede centrale non sempre notano questi trend durante le loro attività quotidiane. Ma un'anomalia del genere può essere facilmente individuata quando si applicano tecniche di data analytics contabili dell'intero gruppo.

Solo il 15% degli intervistati da Kroll ha dichiarato di esser stato vittima di corruzione e di frodi connesse alla corruzione negli ultimi 12 mesi. Tuttavia, a differenza di quanto accade con altre tipologie di frode, il problema è che la maggior parte delle imprese non si rendono immediatamente conto dello sblocco di questi pagamenti, e quando queste transazioni vengono identificate, ormai è troppo tardi.

Nella maggior parte delle indagini condotte da Kroll, i pagamenti in questione spesso sono riconducibili a una controllata acquisita o sono avvenuti già da molti anni. Un approccio dinamico all'individuazione di questi rischi mediante l'analisi dei dati dà l'opportunità di riuscire a scovare l'ago nel pagliaio.





Rispondere alle denunce dei whistleblower

DI ALEX VOLCIC E YASER DAJANI

Le imprese fanno molto affidamento sulle informazioni provenienti dai whistleblower per scoprire le frodi interne. L'ultima edizione dell'indagine Kroll Global Fraud and Risk ha mostrato che il 44% delle frodi individuate è stato scoperto grazie a un whistleblower interno all'azienda. Dato che il 79% delle frodi coinvolge dipendenti, ex dipendenti o dipendenti a termine, il personale interno è una risorsa fondamentale per contrastare le frodi. Risulta dunque sorprendente che un numero consistente di intervistati che ha già in atto programmi ad hoc per i whistleblower (36%) non intenda riesaminarli, modificarli o ampliarli nei prossimi 12 mesi.

Il *Princeton Dictionary* definisce il "whistleblower" (letteralmente, pifferaio) come "un informatore che denuncia condotte illecite all'interno di un'organizzazione, nella speranza di fermarle." Tuttavia, nel mondo delle aziende non si è ancora arrivati a una definizione univoca del termine. A seconda della definizione di "whistleblower" contenuta nelle politiche aziendali, un whistleblower all'interno di una organizzazione può non essere considerato come tale in un'altra organizzazione. Di conseguenza, è importante che le aziende ne diano una definizione chiara nelle loro politiche.

Le imprese sono inondate da consigli su come predisporre un canale privilegiato per i whistleblower, mentre le loro reazioni alle accuse di condotta illecita si differenziano di molto. In molte aziende si discute vivacemente su quale reparto debba gestire le segnalazioni dei whistleblower. Purtroppo non esistono degli standard uniformi per valutare queste accuse, per cui la fase di cernita iniziale - un aspetto cruciale - non sempre è gestita nel modo più efficace.

La risposta a caldo alle denunce dei whistleblower riveste un'importanza enorme e in questa fase molte cose possono andar male (e lo fanno). Per esempio, nel corso di un'indagine Kroll condotta di recente negli Emirati Arabi Uniti, un amministratore delegato ha voluto interrogare immediatamente e di persona il presunto malfattore dopo essere stato messo al corrente di un'accusa. Fortunatamente, dopo aver discusso con il team di Kroll, il cliente ha accolto il nostro consiglio e ha cambiato questa strategia. Intervistare un sospetto prima che tutti i fatti siano accertati può rovinare il lavoro d'indagine e, in molti casi, generare alienazione in un dipendente potenzialmente leale e innocente.

Le prime 24 ore successive alle segnalazioni di un whistleblower sono fondamentali. Dovrebbe essere costituito un team di intervento, composto da dirigenti di alto livello che non abbiano rapporti diretti con il dipendente la

ALEX VOLCIC
Alex Volcic è Managing Director e capo della filiale moscovita di Kroll. Alex è al comando del team operante in Russia e nella CSI e si occupa dei clienti in Europa Centrale, nell'Est Europa e in Scandinavia. Coordina una vasta gamma di indagini per imprese e istituzioni finanziarie e di consulenza, tra cui analisi di due diligence preliminari, investigazioni, indagini di mercato sui paesi emergenti, indagini su corruzione e tangenti interne, contabilità forense, controlli sulla legalità dei soggetti terzi e indagini patrimoniali.

YASER DAJANI
Yaser Dajani è Managing Director presso la sede Kroll di Dubai e Responsabile per l'area geografica mediorientale. Gestisce indagini per conto di società locali e internazionali e di enti governativi, oltre a coordinare un team di investigatori forensi e specialisti di business intelligence presso la sede di Dubai. Yaser è specializzato in business intelligence complessa, indagini interne, consulenza e assistenza legale, tracciabilità dei beni, supporto anticontraffazione e valutazione dei rischi di corruzione.

cui condotta è stata messa sotto accusa. Le imprese devono dotarsi di politiche e procedure per rispondere alle accuse attraverso meccanismi prestabiliti. Questi ultimi dovrebbero essere sufficientemente flessibili per individuare rapidamente la priorità da assegnare alle questioni puramente materiali. Una risposta tempestiva può anche contribuire a limitare i danni economici e reputazionali e, talvolta, contenere o evitare perdite.

La valutazione iniziale dovrà verificare la credibilità e la gravità delle presunte condotte illecite. Questi fattori devono essere chiariti prima di predisporre un'indagine a tutto campo.

Spesso le accuse sono difficili da verificare se il whistleblower non dà informazioni sufficienti. Per esempio, un whistleblower può sostenere che un manager dell'ufficio appalti abbia accettato una tangente da parte di un fornitore, ma può essere difficile provare che la "bustarella" sia finita fisicamente in tasca al dirigente. In uno di questi casi, l'analisi delle mail ha mostrato tracce della condotta illecita, ma non è stata sufficiente a sostenere l'accusa specifica di tangenti. Il caso è stato complicato ulteriormente da un altro aspetto riscontrato di frequente: il whistleblower non si impegnava sul lavoro e non era un testimone credibile o ben intenzionato.

A volte le accuse mosse da un whistleblower sono semplicemente indimostrabili, il che rende molto difficile accertare la buona fede del whistleblower. Kroll ha di recente indagato su un whistleblower considerato una fonte credibile e molto rispettata dagli alti dirigenti. Questa persona era convinta che un responsabile delle vendite fosse colluso con un importante distributore. Tuttavia, un'analisi approfondita condotta sulle abitudini del presunto malfattore non ha rivelato nulla di straordinario e da un'indagine forense sui suoi messaggi di posta elettronica non è emersa alcuna traccia di condotta illecita.

È importante porsi le seguenti domande durante la cernita o la valutazione delle accuse:

- Qual è il livello di dettaglio del contenuto delle accuse?
- Qual è la gravità delle conseguenze, se le accuse risultano veritiere?
- Qual è il livello di affidabilità e completezza delle accuse del whistleblower?
- Sarebbe utile far esaminare la questione a terze parti per valutarne la credibilità?
- Queste accuse possono essere comprovate dalle denunce di altri whistleblower?

Se si ritiene necessario procedere con l'indagine, questa dovrà essere assolutamente articolata in diverse fasi e, se possibile, effettuando in prima battuta una valutazione della credibilità con la massima discrezione. Una volta portata a termine l'analisi dei dati, il personale adeguatamente qualificato potrà iniziare a condurre interviste di accertamento con gli individui che potrebbero essere a conoscenza dei fatti incriminati. In genere il colloquio diretto con il sospettato avviene solo al termine delle altre fasi.

In molti casi, fare luce sulle accuse di un whistleblower è un compito complesso; è innanzitutto fondamentale esaminare la credibilità del whistleblower, dato che le sue denunce potrebbero essere immotivate.

A complicare ulteriormente le indagini, anche nelle aziende che hanno investito risorse per incoraggiare il personale a parlare e utilizzare i canali dedicati ai whistleblower, concorre il fatto che in alcune culture il whistleblowing è giudicato negativamente. Per esempio, i dipendenti in Russia e in altri paesi potrebbero non esser disposti a metterci la faccia.

I whistleblower in molti casi optano per una segnalazione anonima per motivi culturali, per paura di ritorsioni da parte dei loro colleghi o dalla società e per molti altri motivi. Nonostante le protezioni previste dalla legge, in alcune giurisdizioni le conseguenze per i whistleblower sinceri sono spesso gravi e durature. Anche se le imprese devono tutelare il diritto dei whistleblower di mantenere l'anonimato, questo in genere rende le indagini più difficili.

La cultura aziendale è una delle componenti fondamentali di un ambiente lavorativo che incoraggi i dipendenti a fare luce su un problema senza timore di ritorsioni. Le aziende dovrebbero citare espressamente la loro contrarietà alle ritorsioni nelle loro politiche e informare i propri dipendenti che nessuna forma di ritorsione sarà tollerata per qualsiasi segnalazione trasmessa in buona fede. Le nostre indagini hanno rivelato più volte che i dipendenti, nel momento in cui si trovano a decidere se farsi avanti o meno, danno grande importanza alla fiducia che nutrono nel processo di gestione dei whistleblower interno all'azienda.

Predisporre un piano di risposta agli incidenti (IRP): Come reagireste a un attacco informatico?

DI ANDREW BECKETT, MICHAEL QUINN E LUCIE HAYWARD

L'ultima edizione del Global Fraud and Risk Report di Kroll ha rivelato che, se pure l'85% degli intervistati ha dichiarato di aver subito un attacco informatico nel corso dell'ultimo anno, l'adozione di politiche e procedure interne per ridurre i rischi legati alla cyber security resta su livelli incredibilmente bassi. Solo il 36% dei dirigenti intervistati ha dichiarato che la propria azienda ha implementato politiche e procedure interne e ha in programma il loro ampliamento. Un ulteriore 38% ha implementato le politiche e le procedure in questione, ma non prevede il loro ampliamento. Il 25% non ha implementato alcuna politica o procedura interna.

Le politiche e le procedure sono importanti perché definiscono, in maniera articolata all'interno di un'organizzazione, le azioni che i dipendenti sono tenuti a compiere. La loro implementazione mette a disposizione dei dipendenti delle linee guida relative a ciò che dovrebbero e non dovrebbero fare. Ad esempio, quali informazioni si possono condividere sui social media? Cosa si dovrebbe fare se riceve un' email di phishing o si notano attività telematiche sospette?

ANDREW BECKETT
Andrew Beckett ricopre il ruolo di Managing Director nella divisione Cyber Security e Indagini Informatiche presso la sede londinese di Kroll. Con alle spalle una carriera brillante al servizio sia di enti governativi sia di imprese private, Andrew ha raggiunto l'eccellenza nello sviluppo e nell'implementazione di soluzioni per la sicurezza informatica, la protezione delle informazioni e la risposta agli incidenti per le realtà più complesse. Le sue solide conoscenze in campi come la gestione aziendale, l'analisi, la gestione della conoscenza e la gestione dei progetti completano il quadro delle sue competenze tecniche, permettendogli di sviluppare un approccio pragmatico alle sfide di natura informatica, sempre più impegnative, che le aziende di oggi devono affrontare giorno dopo giorno.

MICHAEL QUINN
Michael Quinn è Associate Managing Director nella divisione Sicurezza e Indagini Informatiche di Kroll. Ha lavorato per l'FBI, dove ha ricoperto la posizione di Supervisory Special Agent nella divisione Informatica. Michael ha gestito numerosi casi di intrusione sia da parte di criminali sia di potenze straniere presso diverse sedi dell'FBI: grazie al suo lavoro sono state inflitte le prime condanne della storia per attacchi informatici commissionate dai governi di altre nazioni.

MICHAEL QUINN
Michael Quinn è Associate Managing Director nella divisione Sicurezza e Indagini Informatiche di Kroll. Ha lavorato per l'FBI, dove ha ricoperto la posizione di Supervisory Special Agent nella divisione Informatica. Michael ha gestito numerosi casi di intrusione sia da parte di criminali sia di potenze straniere presso diverse sedi dell'FBI: grazie al suo lavoro sono state inflitte le prime condanne della storia per attacchi informatici commissionate dai governi di altre nazioni.

I risultati dell'indagine svolta da Kroll sono confermati da un rapporto pubblicato nel settembre 2016 dai Lloyds di Londra sul rischio informatico [1], nel quale si riporta che il 92% delle imprese europee ha subito violazioni informatiche nel corso degli ultimi cinque anni, ma solo il 42% si è detta preoccupata che l'evento si possa ripetere. All'inizio dell'anno in corso, un'indagine del governo britannico sulle violazioni alla cyber security[2] ha rilevato che il 69% delle imprese del Regno Unito reputa la cyber security una priorità, ma la percezione della fattibilità è molto più bassa. Solo il 29% aveva politiche di cyber security scritte e solo il 10% aveva creato un piano di risposta agli incidenti (Incident Response Plan, qui di seguito IRP).

Gli IRP sono una componente essenziale della lotta contro la criminalità informatica. Sono il primo punto di riferimento per una società in caso di attacco. La buona notizia è che la creazione di un IRP, che includa attori sia interni sia esterni e stabilisca il ruolo di ciascuno, non è un compito così arduo.

Un IRP dovrebbe includere sette fasi:

1 Stabilire chi abbia l'autorità di dichiarare un incidente. Nominare una persona autorizzata a dichiarare un incidente, sollecitare l'attuazione dell'IRP e convocare il team di risposta.

2 Assegnare le responsabilità di squadra. Definire con chiarezza tutti i ruoli di squadra nel piano per velocizzare il processo decisionale a fronte di un incidente. Scegliere con il dovuto anticipo i consulenti esterni e includerli nel piano. Fare scelte di questo tipo nel corso di una crisi, infatti, non è certo ideale.

3 Evitare di assegnare livelli di gravità. L'uso di diversi livelli di gravità può sembrare utile in fase iniziale, ma il rischio di una valutazione errata è troppo elevato. In questo modo, le aziende sono indotte a considerare ogni incidente come una priorità assoluta.

4 Stabilire le procedure e le responsabilità per la comunicazione. Stabilire chi si occuperà di informare gli interlocutori esterni e interni e come saranno trasmesse le informazioni. Per esempio, quale sarà il luogo d'incontro del team? Nel caso di una violazione dei sistemi, è importante stabilire la tempistica dell'incidente e conoscere la portata della violazione prima di comunicare l'attuazione del piano di risposta. Sopravvalutare la portata dei danni potrebbe generare panico immotivato. Sottovalutarla potrebbe causare ulteriori danni, ad esempio se non si cambiano le password prima che i gli autori dell'attacco riescano ad accedere agli account. In entrambi i casi, la fretta può tradursi in valutazioni inesatte e portare a gravi ripercussioni.

5 Raccogliere le necessarie informazioni col dovuto anticipo. Quando possibile, la raccolta di informazioni critiche prima di un incidente può rivelarsi molto utile. Dettagli quali i numeri di telefono di tutti i membri del team di risposta agli incidenti sono di primaria importanza, poiché gli incidenti avvengono spesso al di fuori dell'orario di lavoro.

6 Definire le fasi del processo. È naturale che i team vogliano risolvere il problema immediatamente. Tuttavia, se in questa fase si perde tempo, l'efficacia del processo può essere compromessa, con conseguenti danni per l'organizzazione. È opportuno che tutte le fasi del processo, a partire dalla convocazione della squadra nel punto di raccolta , siano delineate con chiarezza. È importante che le divisioni aziendali deputate alla sicurezza e ai sistemi informatici conoscano il processo a memoria.

7 Riesaminare e testare il piano. Consigliamo di condurre revisioni su base trimestrale e di apportare gli aggiornamenti che si rendessero necessari. In questo modo avremo l'opportunità di aggiornare i numeri di telefono ed esaminare eventuali cambiamenti nelle tecnologie o nelle procedure che potrebbero avere un impatto sull'IRP.

Dotarsi di un IRP in cui tutti gli interlocutori siano in grado di comprendere il ciclo di vita di un incidente e abbiano compiuto le dovute simulazioni a tutti i livelli dell'organizzazione, incluso il consiglio d'amministrazione, permette di prepararsi a mitigare i danni causati da un attacco.

1 Indagine "Facing the Cyber Risk Challenge" condotto da Lloyd's, http://bit.ly/2cPV5jo
2 Cyber Security Breaches Survey 2016, http://bit.ly/1T4MveX

Risposta in caso di violazione dei dati: Sette linee guida per riconquistare la fiducia dei clienti a seguito di una violazione

DI BRIAN LAPIDUS

La vostra azienda lavora duramente per offrire un prodotto o un servizio d'eccellenza. Fate ogni sforzo possibile per rendere entusiasti i vostri clienti. Non smettete mai di pensare che si possa migliorare ancora. E poi si verifica una violazione dei sistemi. Qualcuno nella vostra squadra perde un computer portatile o un dispositivo contenente i dati dei clienti. Tutto ciò che siete riusciti a costruire con la buona volontà, insieme alla vostra buona reputazione, rischia di volatilizzarsi davanti ai vostri occhi.

Non sareste i soli. Oltre l'85% degli intervistati nel corso dell'indagine Global Fraud and Risk condotta da Kroll nel 2016 ha dichiarato di aver subito un attacco informatico negli ultimi 12 mesi. Altrettanto preoccupante è che il 67% degli intervistati abbia dichiarato che tale attacco abbia influito negativamente e in modo significativo sulla reputazione della propria azienda.

Forse non c'è un momento in cui le esigenze dei clienti hanno una priorità più elevata come all'indomani di una violazione dei sistemi. La risposta migliore a questo tipo di eventi sono le sette linee guida elencate di seguito che, se applicate con attenzione, vi aiuteranno a ritrovare la stima dei clienti, riconquistare la loro fiducia e finanche rafforzare il rapporto professionale.

1 Informare il cliente tempestivamente ma, al tempo stesso, con cognizione di causa. Se siete assolutamente sicuri della portata e della natura dei dati compromessi, bisognerà agire in fretta. I clienti si aspettano di essere informati non appena venite a conoscenza della violazione. D'altra parte, sarebbe controproducente minimizzare l'accaduto per dover poi fornire ulteriori informazioni in un secondo tempo , così come è controproducente diffondere falsi allarmi. Sarebbe preferibile indagare con urgenza sull'accaduto e in seguito notificare solo le informazioni opportune. Per esempio, un cliente di Kroll, in seguito al furto di 35 computer portatili, aveva inizialmente stimato la compromissione dei dati di 2 milioni di persone. Le nostre indagini hanno dimostrato che erano stati sottratti i dati di soli 1.500 clienti.

BRIAN LAPIDUS
Brian Lapidus ricopre il ruolo di Managing Director e dirige la divisione di Kroll che si occupa di Furti d'identità e Notifica delle violazioni. Oltre ad aiutare le imprese a risolvere i problemi derivanti dalla violazione dei sistemi, Brian offre servizi di assistenza e contenimento dei danni. Ha contribuito all'ampliamento delle procedure di Kroll per rimediare ai furti di identità individuali nel 2007, data di lancio del programma in Canada. La sua divisione è specializzata nell'offerta di soluzioni nei settori della sanità, istruzione superiore, vendita al dettaglio e finanziario. Con oltre 15 anni di esperienza sul campo, Brian ha pubblicato una cospicua quantità di contenuti autorevoli, dagli articoli scientifici alle interviste concesse a riviste online e cartacee.

2 Rinforzare la credibilità. La pulizia dei vostri dati è fondamentale; l'invio di più notifiche a un singolo cliente può sminuire ai suoi occhi la vostra capacità di gestire i suoi dati. La vostra credibilità può essere messa a rischio in molti altri modi. Kroll ha lavorato per una società che ha impiegato diversi mesi per selezionare il fornitore che le proponesse l'offerta migliore per gestire una violazione di notevole entità. Anche se la risposta si è rivelata tutto sommato efficace e completa, l'azienda ha subito notevoli critiche per la lentezza nel prendere una decisione e alla fine si è ritrovata a fronteggiare una class action da parte dei suoi clienti. Il messaggio giunto ai suoi clienti è stato che per l'azienda risparmiare denaro era più importante che proteggere la propria clientela.

3 Personalizzare le comunicazioni in base alla categoria dei clienti colpiti. Anche se è forte la tentazione di scrivere un messaggio standard per tutti i soggetti colpiti dalla violazione , bisogna fare l'ulteriore sforzo di comprendere chi siano esattamente i soggetti colpiti e diversificare la comunicazione di conseguenza. Per esempio, Kroll ha lavorato ad un caso in cui alcuni dei soggetti colpiti erano coreani. Di conseguenza, non solo le notifiche sono state redatte in coreano, ma il personale dei call center messi a disposizione dei soggetti colpiti è stato affiancato da interpreti coreani.

4 Mostrare empatia. È opportuno personalizzare con attenzione il vostro messaggio in base alle caratteristiche o alle situazioni particolari dei gruppi colpiti. Questo approccio si rivela assolutamente fondamentale nel caso in cui la vostra azienda debba comunicare con individui che stanno affrontando momenti difficili o la perdita di persone care, per esempio i malati terminali e le loro famiglie, potenziali vittime di una violazione in una struttura di lungodegenza.

5 Offrire assistenza e servizi mirati e utili Il furto di identità costituisce una seria preoccupazione per i vostri clienti? Preparatevi a offrire servizi specifici che limitino questo rischio. Per esempio, di recente un cliente ha perso i numeri di carta di credito, i nomi utente e le password dei suoi clienti. Oltre ai servizi di monitoraggio del credito, il cliente ha offerto servizi di monitoraggio extra-bancari, come la ricerca dei codici venduti sui siti Internet dedicati alla pirateria, un indicatore che l'uso improprio di queste informazioni poteva mettere i consumatori in pericolo. In un altro caso un cliente aveva perso i numeri di previdenza sociale appartenenti a soggetti minorenni. Al fine di limitare il rischio di furto d'identità, Kroll ha mostrato ai genitori di questi soggetti come apporre un c.d. 'credit freeze' – ossia una limitazione all'accesso – agli account di previdenza sociale dei loro figli. Il rischio era che eventuali attività illegali condotte sugli account di previdenza sociale dei minori avrebbero potuto passare inosservate fino al compimento dei 18 anni, compromettendo così la possibilità per i titolari degli account di chiedere prestiti o di attivare una carta di credito.

6 Offrire alla clientela un'esperienza positiva Di recente uno dei nostri clienti ha divulgato inavvertitamente i dati sanitari personali dei pazienti, compresi i dati relativi alle diagnosi, le liste dei farmaci somministrati e le cartelle cliniche. L'incidente ha sollevato grandi preoccupazioni nell'amministratore delegato in quanto andava a violare proprio i valori fondamentali dell'organizzazione. Il cliente si è quindi impegnato a fornire la necessaria formazione ai call center gestiti da Kroll al fine di assicurare che fossero in grado di esprimre quei valori fondamentali ai soggetti colpiti. E' bene ricordare che mettere a disposizione la propria esperienza in seguito a una violazione è un fatto positivo che avrà ripercussioni sull'opinione dei vostri clienti per molti anni a venire.

7 Giocare d'anticipo sulle reazioni dei concorrenti. I vostri concorrenti sanno che, in caso di una violazione dei sistemi, sarete più vulnerabili al rischio di perdere clienti. Sarebbe opportuno organizzare dei team allo scopo di prevedere e monitorare le attività promozionali messe in atto dai vostri concorrenti in una situazione del genere e strutturare dei piani per prevenirle o contrastarle. Allo stesso modo, si può prendere in considerazione l'opportunità di offrire promozioni speciali ai vostri clienti, come servizi gratuiti, sconti o coupon per incoraggiarli a non abbandonarvi.

Il processo di ricostruzione della fiducia dei clienti all'indomani di una violazione dei sistemi è un impegno complesso e a lungo termine. Non aspettate che si verifichi un incidente prima di mettere in pratica i sette passaggi di cui abbiamo parlato. Gran parte del lavoro previsto da ciascuna linea guida può essere svolto in anticipo. Ciò vi metterà al riparo da conseguenze nefaste e vi aiuterà a riconquistare rapidamente la fiducia dei clienti.

Quadro Generale: Canada

FRODI

Nel corso dell'ultimo anno, il numero di intervistati in Canada che ha riferito di aver subito una frode è aumentato di quasi un quarto (23%) rispetto al 2015. Il numero di intervistati in Canada (88%) vittime di frodi è superiore alla media globale (82%) di 6 punti percentuali.

I responsabili dei casi di frode in Canada sono stati in massima parte soggetti all'interno delle aziende. In particolare, in Canada i manager di primo e secondo livello sono stati indicati come responsabili dei casi di frode in misura maggiore rispetto alle altre aree geografiche, con un dato superiore alla media globale (30%) di 17 punti percentuali. In Canada i neoassunti sono stati citati come principali responsabili nel 39% dei casi di frode, un valore in linea con la media mondiale. Dopo i manager di primo e secondo livello, si tratta della categoria di autori più diffusa.

Questa tendenza si rispecchia nella tipologia delle frodi perpetrate. Tra tutti i paesi presi in esame, solo gli intervistati canadesi hanno menzionato l'appropriazione indebita di fondi societari tra i primi cinque tipi di frodi subite negli ultimi 12 mesi. Gli intervistati canadesi hanno inoltre registrato valori superiori alla media per il furto fisico di scorte o beni (34%, 5 punti percentuali oltre la media globale del 29%), così come per il furto di dati (32%, 8 punti al di sopra della media globale del 24%).

Una grande maggioranza (90%) degli intervistati canadesi ha investito in un sistema di gestione del rischio incaricando un risk officer (12 punti percentuali in più rispetto alla media globale del 78%). Un ulteriore 88% ha investito in controlli di gestione (14% in più rispetto alla media globale del 74%). Nel complesso, gli intervistati canadesi hanno investito più risorse nelle misure antifrode rispetto alla media globale.

CYBER SECURITY

La maggior parte (85%) degli intervistati in Canada è stata vittima di un attacco informatico, in linea con l'incidenza media globale dell'85%. Gli attacchi con virus / worm sono risultati un problema significativo: Il 41% degli intervistati canadesi ha menzionato questo tipo di incidenti, 8 punti percentuali in più rispetto alla media globale del 33%. Anche la perdita di supporti contenenti dati sensibili si è rivelata problematica per i dirigenti canadesi, con un'incidenza più che raddoppiata (39%) rispetto alla media globale del 17%.

Gli attacchi informatici sono stati mirati principalmente ai dati dei clienti e a informazioni commerciali confidenziali e di ricerca e sviluppo delle imprese. Oltre la metà degli intervistati canadesi ha segnalato attacchi contro i dati dei clienti (57%), i beni materiali / denaro (57%) e le informazioni commerciali confidenziali (51%). Le categorie di autori più diffuse degli attacchi informatici in Canada sono stati identificate nei dipendenti a tempo indeterminato (20%), il doppio rispetto alla media globale del 10%.

In seguito a un attacco informatico, gli intervistati in Canada si sono rivolti il più delle volte a una azienda specializzata nella gestione degli attacchi informatici o a un fornitore di servizi IT.

SICUREZZA

Un dato sorprendente è che gli intervistati canadesi sono risultati più propensi a segnalare incidenti in materia di sicurezza, con un'incidenza superiore di 10 punti percentuali alla media globale (68%). Poco meno della metà (49%) degli intervistati canadesi ha dichiarato di aver subito un furto o una perdita di proprietà intellettuale. Gli ex dipendenti sono stati citati come le categorie di autori più diffuse secondo il 28% degli intervistati.

Gli intervistati canadesi hanno inoltre riferito un livello significativo di esposizione ai rischi ambientali (46%), un dato al di sopra della media globale (27%).

Per quanto riguarda gli incidenti in materia di sicurezza, chi opera in Canada si sente più vulnerabile alla violenza sul posto di lavoro e ai rischi ambientali, anche se la prima non figura nella top 3 degli incidenti riportati.

SCHEDA AREA GEOGRAFICA: CANADA

Risposte più frequenti date dagli intervistati

Frodi

88 — **Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.**

▲ 23% punti in più dal 2015

▲ 6% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	**34%**	29%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	**32%**	24%
	Violazioni delle norme o della compliance	**32%**	21%
	Frodi nei processi di vendita, fornitura o approvvigionamento	**32%**	26%
	Appropriazione indebita di fondi societari	**32%**	18%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Manager di primo o secondo livello in azienda	**47%**	30%
	Neoassunti in azienda	**39%**	39%
	Freelance / dipendenti a termine	**36%**	27%
	Ex dipendenti	**36%**	27%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	**36%**	27%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Rischio *(sistema di gestione del rischio e risk officer)*	**90%**	78%
	Gestione *(controlli dall'alto, incentivi, supervisione esterna come le commissioni d'indagine)*	**88%**	74%
	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	**86%**	82%
	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	**86%**	79%
	Partner, clienti e fornitori *(due diligence)*	**85%**	77%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	**44%**	44%

Cyber Security

85 — **Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.**

= pari alla media globale (85%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI INFORMATICI PIÙ COMUNI	Attacco con virus/worm	**41%**	33%
	Perdita di beni fisici contenenti dati sensibili	**39%**	17%
	Eliminazione o danneggiamento dei dati causato da malware o manipolazioni del sistema	**34%**	22%
	Violazione dei dati risultante in perdita di segreti commerciali / PI / R&S	**34%**	19%
AUTORI PIÙ COMUNI	Dipendenti a tempo indeterminato dell'impresa	**20%**	10%
OBIETTIVO PIÙ COMUNE	Dati dei clienti	**57%**	51%
	Beni materiali/denaro	**57%**	38%
	Segreti commerciali / R&S / PI	**51%**	40%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN INCIDENTE INFORMATICO	Società specializzata nella risposta agli incidenti	**20%**	14%
	Fornitore di servizi IT	**20%**	27%

Sicurezza

78 — **Percentuale degli intervistati vittime di incidenti di sicurezza negli ultimi 12 mesi.**

▲ 10% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**49%**	38%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	**46%**	27%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	**27%**	22%
AUTORI PIÙ COMUNI	Ex dipendenti	**28%**	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	**32%**	27%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	**29%**	20%
	Eventi terroristici nazionali e internazionali	**24%**	18%

Quadro Generale: Stati Uniti

FRODI

L’80% degli intervistati negli Stati Uniti è stato vittima di frodi negli ultimi 12 mesi, con un incremento di 5 punti percentuali rispetto all'anno precedente. Questo dato è inferiore di 2 punti percentuali rispetto alla media globale dell’82%.

Il furto di proprietà intellettuale (PI), che comprende pirateria o contraffazione, è una minaccia consistente per le imprese negli Stati Uniti secondo poco più di un quarto (27%) degli intervistati, quasi il doppio della media globale. Gli Stati Uniti sono stati l'unico paese in cui il furto di PI risulta essere il tipo più comune di frode riportata dai partecipanti. A questa tipologia di frode seguono il furto, la perdita o l’attacco alle informazioni, mentre in terza posizione troviamo i conflitti di interesse interni alla dirigenza delle imprese statunitensi.

I principali responsabili delle frodi sono interni all’azienda. Una volta scoperta la frode, il 36% dei dirigenti statunitensi indica come responsabili i neoassunti, mentre il 32% cita i manager di primo o secondo livello.

Gli intervistati statunitensi sono stati più propensi ad adottare misure di sicurezza dei sistemi informativi, seguiti dai controlli finanziari e dalla sicurezza dei beni materiali, per contenere il rischio di frode.

Negli Stati Uniti il metodo più comune di accertamento delle frodi non è stato ricorrendo al whistleblower, come è avvenuto nella maggior parte dei paesi presi in esame, bensì l’indagine interna. Quasi la metà (49%) degli intervistati degli Stati Uniti ha infatti indicato tale modalità di accertamento come la più comune.

CYBER SECURITY

Gli intervistati negli Stati Uniti sono stati particolarmente colpiti dagli attacchi informatici; la maggioranza (88%) riferisce di averne subiti negli ultimi 12 mesi.

I casi più comuni, con valori superiori alla media mondiale, risultano gli attacchi mediante virus o worm e la cancellazione o la perdita di dati dovuta a manipolazioni dei sistemi. In misura minore, un’azienda statunitense su cinque ha indicato gli attacchi di phishing tramite e-mail, un dato più basso rispetto alla media mondiale.

L'obiettivo più comune degli Stati Uniti, come avviene per altri paesi, sono stati i dati dei clienti, menzionati dal 57% degli intervistati. Anche le informazioni commerciali confidenziali e le identità delle imprese o dei dipendenti si sono trovati spesso nel mirino.

Le aziende negli Stati Uniti in seguito a un attacco sono state più propense rispetto a tutti gli altri paesi a rivolgersi direttamente al loro fornitore di servizi informativi (43% rispetto alla media globale del 27%).

SICUREZZA

Gli incidenti in materia di sicurezza negli Stati Uniti risultano meno diffusi rispetto agli altri paesi oggetto dell’indagine, fatta eccezione per il Brasile. La maggioranza dei dirigenti statunitensi ha dichiarato di aver subito almeno un incidente nel corso dell'ultimo anno (58%), un dato inferiore di 10 punti percentuali alla media globale del 68%. L'incidente in materia di sicurezza più comune riportato dagli intervistati statunitensi è stato il furto o la perdita di proprietà intellettuale, seguito dagli eventi ambientali e dalla violenza sul posto di lavoro.

Un dato peculiare registrato negli Stati Uniti è l’individuazione dei concorrenti e di aziende o individui esterni come i maggiori responsabili degli attacchi alla sicurezza. Gli Stati Uniti risultano essere l'unico paese in cui gli autori casuali sono stati indicati tra i maggiori responsabili, nonché l'unico paese insieme alla Cina dove i concorrenti figurano nelle prime due posizioni.

Un altro dato significativo è il minor numero di intervistati negli Stati Uniti che dichiara di sentirsi vulnerabile a tutti i principali tipi di rischi in materia di sicurezza, rispetto agli intervistati operanti altrove.

SCHEDA AREA GEOGRAFICA: STATI UNITI

Risposte più frequenti date dagli intervistati

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 5% punti in più dal 2015

▼ 2% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di PI *(es. di informazioni commerciali confidenziali)*, pirateria o contraffazione	27%	16%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	24%	24%
	Conflitto di interessi del management	24%	21%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti in azienda	36%	39%
	Manager di primo o secondo livello in azienda	32%	30%
	Ex dipendenti	30%	27%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	21%	26%
	Freelance / dipendenti a termine	17%	27%
	Clienti	17%	19%
MISURE ANTIFRODE PIÙ DIFFUSE	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	91%	82%
	Finanziaria *(controlli finanziari, accertamento delle frodi, indagini interne o esterne, politiche antiriciclaggio)*	86%	77%
	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	85%	79%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine interna	49%	39%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 3% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	42%	33%
	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	26%	24%
	Attacco di phishing a mezzo e-mail	21%	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	19%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	57%	51%
	Segreti commerciali / R&S / PI	38%	40%
	Identità aziendale o dei dipendenti	38%	36%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN INCIDENTE INFORMATICO	Fornitore di servizi IT	43%	27%

Sicurezza

Percentuale degli intervistati vittime di attacchi di sicurezza negli ultimi 12 mesi.

▼ 10% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	30%	38%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	21%	27%
	Violenza sul posto di lavoro	15%	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Concorrenti	21%	12%
	Autore esterno	21%	10%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	18%	27%
	Furto o perdita di PI	12%	19%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	9%	20%

Gli investimenti esteri negli Stati Uniti: Il modo migliore per ottenere l'approvazione da parte della CFIUS

DI DANIEL J. ROSENTHAL

Secondo dati ufficiali, nel mese di gennaio 2016 il piano messo a punto da Phillips per vendere le sue attività nel settore illuminazione ad acquirenti cinesi è stato vanificato dalla Commissione per gli investimenti esteri negli Stati Uniti (CFIUS), un ente governativo interdipartimentale che valuta gli investimenti stranieri nel paese volti ad acquisire il controllo di entità giuridiche negli Stati Uniti per determinare se sussistono implicazioni negative per la sicurezza nazionale[1]. La CFIUS detiene l'autorità per intraprendere diverse azioni che possono imporre costi significativi alle imprese. Per esempio, può bloccare processi di fusione e acquisizione sottoposti al suo vaglio, ordinare la cessione delle attività acquisite da società straniere nell'ambito di contratti che sono stati già firmati, nonché spingere le parti ad adottare ulteriori misure per contenere gli eventuali rischi legati all'evolversi della transazione.

Nel corso dell'ultimo anno, la CFIUS si è espressa su numerose proposte d'investimento internazionali di grandi dimensioni e di alto profilo negli Stati Uniti. Nel mese di agosto 2016, per esempio, ha dato il via libera all'acquisizione del gigante delle sementi Syngenta AG da parte della China National Chemical Corporation per un valore di 43 miliardi di dollari. Anche Il Congresso si è gettato nella mischia. Alcuni membri hanno chiesto pubblicamente leggi più stringenti per estendere il mandato della CFIUS e ampliare il quadro normativo per la valutazione dei rischi in materia di sicurezza nazionale: questo potrebbe rendere potenzialmente più difficile ottenere l'approvazione di un affare da parte della CFIUS.

Queste dinamiche hanno comportato un aumento del rischio di natura amministrativa per gli stranieri che intendono investire negli Stati Uniti. Tuttavia, riteniamo che le aziende non dovrebbero lasciarsi dissuadere dall'investire negli Stati Uniti, rispettando invece le procedure della CFIUS.

DANIEL J. ROSENTHAL
Daniel ("DJ") Rosenthal è Associate Managing Director della sezione Investigations and Disputes presso la sede di Washington D.C. di Kroll. La brillante carriera di DJ, che ha prestato servizio presso la Casa Bianca, il Dipartimento di Giustizia, la Intelligence Community, il sistema giudiziario degli Stati Uniti e l'avvocatura privata, è frutto di un'esperienza dal valore inestimabile che gli permette di assistere i clienti globali di Kroll su questioni complesse relative ai rischi, come le revisioni della CFIUS, la cyber security, le indagini interne e le questioni in materia di privacy.

1 Tutte le esposizioni dei fatti, le opinioni o le analisi espresse sono da intendersi dal punto di vista dell'autore e non riflettono necessariamente le posizioni o i punti di vista ufficiali del Dipartimento di Giustizia (DOJ) o di qualsiasi altro ente governativo degli Stati Uniti. Il presente articolo è stato rivisto dal DOJ per impedire la divulgazione di informazioni classificate come riservate o sensibili per altri motivi.

La nostra esperienza ci insegna che gli investitori possono attuare delle strategie per facilitare l'approvazione dalla CFIUS. Queste includono:

1 Essere proattivi. Anche se le parti non sempre possono prevedere le reazioni degli enti governativi, in molti casi le questioni di fondo sono ben note. Sia la società acquirente, sia la parte oggetto della vendita dovrebbero impegnarsi in un'analisi congiunta di due diligence, concentrandosi sulle tematiche di maggior interesse per la CFIUS, come per esempio la sensibilità della tecnologia impiegata nei prodotti e della base di conoscenza dell'impresa statunitense oggetto della cessione, nonché dei precedenti, della reputazione e degli eventuali legami con potenze straniere dell'acquirente. Essere proattivi aiuta tutte le parti in causa a individuare i potenziali problemi che potrebbero compromettere l'approvazione dell'accordo da parte della CFIUS. In questo modo le parti possono prendere una decisione più consapevole sulla conclusione dell'accordo e, in caso affermativo, se sottoporlo o meno alla CFIUS.

2 Essere trasparenti. Se si ha una buona comprensione degli aspetti che destano maggior preoccupazione nella CFIUS nel corso della revisione, le parti potranno presentarsi alla commissione insistendo sulla loro trasparenza in merito alle questioni più rilevanti. In questo modo le parti ottengono due vantaggi tangibili:

- Essere trasparenti equivale a inviare un messaggio chiaro alla CFIUS: il vero obiettivo delle imprese è perseguire un obiettivo commerciale e pertanto si impegnano con decisione a lavorare con la CFIUS, non contro di essa, durante l'esame delle conseguenze sulla sicurezza nazionale della transazione.
- Se si gioca in anticipo sulla trasparenza, le parti dell'operazione potranno discutere proattivamente con la commissione sulle misure da prendere per contenere le eventuali conseguenze negative. In molti, troppi casi, i negoziati con la commissione si svolgono in fretta e furia mentre la data stabilita per la decisione della CFIUS si avvicina. Mettere in campo la trasparenza sin dall'inizio offre alle aziende coinvolte e alla CFIUS molto tempo prezioso per negoziare e trovare una via d'uscita che possa mitigare le preoccupazioni della commissione e risulti accettabile dal punto di vista del business.

3 Essere collaborativi. Nel caso in cui le obiezioni della CFIUS riguardino lo scambio di informazioni sensibili o di know-how dei prodotti tra l'impresa statunitense e l'investitore straniero, la commissione può imporre (1) determinati protocolli e protezioni che essenzialmente isolano le informazioni detenute dalla parte americana e (2) la creazione di registri verificabili sulla compliance dei protocolli e delle misure protettive in questione.

Dato che la commissione non ha una conoscenza diretta delle operazioni commerciali delle parti, le condizioni di contenimento proposte potrebbero essere difficili da implementare in termini di efficienza e oneri da sopportare. Le parti capaci di prevedere le obiezioni della CFIUS e che offrono proattivamente alla commissione delle misure di contenimento ben strutturate e verificabili possono dimostrare la loro volontà di portare a termine la transazione e il loro desiderio di adottare misure capaci di rispondere alle esigenze di sicurezza nazionale degli Stati Uniti. Così facendo, e questo è l'aspetto più importante, le parti possono dotarsi di una buona base di partenza per iniziare le discussioni con la commissione. È meglio lavorare sulla propria bozza che su quella degli altri. E la CFIUS apprezzerà questo vantaggio iniziale.

Quadro Generale: Medio Oriente

FRODI

Gli intervistati che operano in Medio Oriente hanno riportato l'incremento più elevato delle frodi negli ultimi 12 mesi rispetto a tutte le aree geografiche esaminate. Oltre un quarto in più (26%) degli intervistati ha dichiarato di essere stato vittima di frodi rispetto al 2015. Nel complesso, l'incidenza delle frodi in Medio Oriente si attesta su valori più alti di 6 punti rispetto alla media globale dell'82%.

La frode finanziaria interna è menzionata come il tipo di frode più comune dagli intervistati mediorientali. Le tipologie a seguire includono il furto di beni materiali e di informazioni, la cui incidenza risulta essere approssimativamente in linea con le medie globali (rispettivamente del 29% e del 24%).

Le categorie di autori più diffuse sono state i manager di primo e secondo livello, essendo stati menzionati dal 36% degli intervistati in Medio Oriente, seguiti dai neoassunti (34%). Anche i soggetti terzi sono considerati coinvolti in maniera significativa nella maggior parte dei casi di frode, con circa un quarto dei partecipanti che menziona i partner di joint venture, i fornitori, i venditori e gli agenti.

I partecipanti in Medio Oriente hanno riferito di aver implementato perlopiù misure antifrode legate alle informazioni, come ad esempio la sicurezza dei sistemi informativi e le contromisure tecniche (80% dei partecipanti), seguita dalla formazione del personale (70%), dalla nomina di un risk officer e l'implementazione di un sistema di gestione del rischio (68%) e dagli accertamenti sui precedenti del personale (68%).

CYBER SECURITY

La maggioranza (90%) dei dirigenti operanti in Medio Oriente ha segnalato almeno un caso di attacco informatico, un valore superiore di 5 punti percentuali alla media globale dell'85%.

Gli attacchi da virus e worm, insieme alla cancellazione di dati causata da manipolazione dei sistemi, sono stati i tipi di attacchi informatici più comuni. Quest'area geografica è contraddistinta da livelli superiori alla media per la perdita di supporti contenenti dati sensibili: 28% rispetto alla media globale del 17%.

Gli attacchi informatici sono stati indirizzati perlopiù verso beni materiali e denaro (47% degli intervistati). Al terzo posto figurano i dati dei clienti. Come avviene in altre regioni, gli intervistati operanti in Medio Oriente hanno contattato i loro fornitori di servizi informativi in seguito a un incidente.

SICUREZZA

I dirigenti mediorientali hanno fatto registrare una percentuale di incidenti in materia di sicurezza subiti più elevata rispetto ad altre regioni. La maggior parte (82%) delle imprese ha riportato di aver subito un incidente, un dato superiore alla media globale di 14 punti percentuali. L'incidente più comune è risultato essere il furto o la perdita di PI, riportato dal 38% dei partecipanti.

Per quel che riguarda gli autori degli incidenti in materia di sicurezza subiti negli ultimi 12 mesi, il 24% dei partecipanti ha puntato il dito contro i dipendenti a tempo indeterminato (7 punti percentuali in più rispetto alla media globale del 17%).

Tra le cause degli incidenti, al secondo posto troviamo la violenza sul posto di lavoro: questo tipo di rischio, secondo gli intervistati, è quello che li fa sentire più vulnerabili.

SCHEDA AREA GEOGRAFICA: MEDIO ORIENTE

Risposte più frequenti date dai partecipanti al sondaggio.

Frodi

88 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 26% punti in più dal 2015

▲ 6% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Frode finanziaria interna *(manipolazione dei risultati aziendali)*	**30%**	20%
	Furto di beni materiali o scorte	**26%**	29%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	**24%**	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Manager di primo o secondo livello in azienda	**36%**	30%
	Neoassunti in azienda	**34%**	39%
	Partner di joint venture *(ossia un partner che fornisce servizi produttivi di altra natura, oppure un affiliato)*	**30%**	23%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	**27%**	27%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	**23%**	26%
MISURE ANTIFRODE PIÙ DIFFUSE	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	**80%**	82%
	Personale *(formazione, canali per whistleblower)*	**70%**	76%
	Personale *(controlli sui precedenti)*	**68%**	74%
	Rischio *(sistema di gestione del rischio e risk officer)*	**68%**	78%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	**50%**	44%

Cyber Security

90 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 5% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	**30%**	33%
	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	**30%**	24%
	Perdita di supporti contenenti dati sensibili	**28%**	17%
	Attacco di phishing a mezzo e-mail	**28%**	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Divulgazione accidentale di dati sensibili indicizzati da un motore di ricerca *(es. Google)*	**22%**	10%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Beni materiali/denaro	**47%**	38%
	Informazioni commerciali confidenziali / R&S / PI	**42%**	40%
	Dati dei clienti	**38%**	51%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN ATTACCO INFORMATICO	Fornitore di servizi IT	**24%**	27%

Sicurezza

82 Percentuale degli intervistati vittime di incidenti in materia di sicurezzanegli ultimi 12 mesi.

▲ 14% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**38%**	38%
	Violenza sul posto di lavoro	**32%**	23%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	**32%**	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Dipendenti a tempo indeterminato dell'impresa	**24%**	17%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	**28%**	27%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali come inondazioni)*	**24%**	20%
	Furto o perdita di PI	**22%**	19%

Quadro Generale: Italia

FRODI

Nonostante un aumento di 3 punti percentuali rispetto al 2015, l'incidenza delle frodi secondo gli intervistati italiani è inferiore alla media globale (77%).

I tre casi segnalati più di frequente sono il furto di beni materiali (34%) o di informazioni (26%), insieme alle violazioni delle norme e della compliance (26%).

Per quanto riguarda gli autori delle frodi, il panorama italiano è variegato. I neoassunti sono stati considerati i colpevoli principali dalla metà dei dirigenti intervistati in Italia, eppure il dato sorprendente è che anche i clienti fanno registrare un dato relativamente elevato, con poco più di un quinto dei casi (22%).

Le misure antifrode più comuni attuate dagli intervistati in Italia sono state la messa in sicurezza dei beni materiali (83%), il coinvolgimento del consiglio di amministrazione nelle politiche e nelle procedure di cyber security (72%), la due diligence su partner e fornitori (70%) e la creazione di un sistema di monitoraggio più efficiente della PI (68%).

CYBER SECURITY

Gli intervistati operanti in Italia hanno subito attacchi informatici in misura minore rispetto alla media globale dell'85%, anche se l'incidenza è pur sempre elevata (79%).

Il problema menzionato più di frequente in Italia per gli attacchi informatici è stato la cancellazione dei dati premeditata da parte del personale interno, seguita dagli attacchi di phishing tramite e-mail e dagli attacchi mediante virus o worm. Gli intervistati italiani hanno indicato l'incidenza più elevata al mondo di casi di cancellazione dei dati premeditata da parte del personale interno (30%).

Un altro fattore di differenziazione dei dati raccolti in Italia mostra che gli obiettivi più frequenti degli attacchi informatici sono il denaro o i beni materiali, mentre i dati dei clienti risultano prevalenti in altre giurisdizioni. Gli intervistati italiani, in seguito all'attacco, dichiarano di preferire in prima battuta il contatto con il loro fornitore di servizi web. Similmente ad altre aree geografiche, le categorie più diffuse degli attacchi informatici risultano essere gli ex dipendenti, citati dal 24% degli intervistati.

SICUREZZA

I dirigenti italiani fanno registrare dati equivalenti alla media globale (68%) sugli incidenti in materia di sicurezza subiti nel corso degli ultimi 12 mesi. Il furto o la perdita di PI è stato l'incidente più comune, menzionato dal 43% degli intervistati, seguiti dagli incidenti di natura ambientale e dalla violenza sul posto di lavoro.

Gli intervistati in Italia individuano i fattori di vulnerabilità più rilevanti nella violenza sul posto di lavoro e nel furto o la perdita di PI.

SCHEDA AREA GEOGRAFICA: ITALIA

Risposte più frequenti date daigli intervistati.

Frodi

77 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 3% punti in più dal 2015

▼ 5% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	34%	29%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	26%	24%
	Violazioni delle norme o della compliance	26%	21%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti in azienda	50%	39%
	Ex dipendenti	36%	27%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	33%	26%
	Manager di primo o secondo livello in azienda	31%	30%
	Clienti	22%	19%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	83%	79%
	Coinvolgimento del consiglio di amministrazione in politiche e procedure di sicurezza informatica	72%	75%
	Partner, clienti e fornitori *(due diligence)*	70%	77%
	PI *(valutazione del rischio per la proprietà intellettuale e programma di monitoraggio dei marchi)*	68%	75%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	53%	44%

Cyber Security

79 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▼ 6% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI INFORMATICI PIÙ COMUNI	Cancellazione dei dati premeditata da parte di risorse interne	30%	19%
	Attacco di phishing a mezzo e-mail	21%	26%
	Infezione da virus / worm	21%	33%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	24%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Beni materiali/denaro	38%	38%
	Dati dei clienti	35%	51%
	Informazioni commerciali confidenziali/ R&S / PI	35%	40%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN ATTACCO INFORMATICO	Provider di spazi/siti web	16%	9%

Sicurezza

68 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

= pari alla media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	43%	38%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	21%	27%
	Violenza sul posto di lavoro	13%	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	31%	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI PER LA SICUREZZA	Violenza sul posto di lavoro	17%	27%
	Furto o perdita di PI	13%	19%
	Terrorismo *(compresi gli eventi nazionali e internazionali)*	9%	18%

Quadro generale: Russia

FRODI

Gli intervistati in Russia hanno riportato un aumento di 9 punti percentuali dei casi di frode negli ultimi 12 mesi (82%, pari alla media globale).

I tipi di frode più comuni sono stati il furto di beni materiali, il furto di dati e le frodi nelle forniture o negli approvvigionamenti. Il furto di beni si è attestato a un valore maggiore di 9 punti percentuali rispetto alla media globale del 29%. Nei casi in cui l'autore delle frodi è stato identificato, i maggiori responsabili sono stati i neoassunti, seguiti dai dipendenti a termine e dai freelance (rispettivamente citati dal 31% e dal 28% degli intervistati russi).

La misura di contenimento del rischio implementata più di frequente dagli intervistati in Russia è stata la messa in sicurezza delle informazioni, seguita dai controlli di gestione. Anche in questo caso, una percentuale significativa degli intervistati russi (77%) ritiene necessario coinvolgere i consigli di amministrazione nella creazione di politiche e procedure informatiche.

CYBER SECURITY

Gli attacchi informatici hanno fatto registrare un'incidenza minore in Russia rispetto ad altri paesi, con 3 punti percentuali in meno rispetto alla media globale dell'85%. In particolare, le infezioni da virus e worm si attestano su percentuali inferiori in Russia, essendo menzionati dal 18% degli intervistati rispetto a una media globale del 33%. Gli incidenti più comuni sono correlati al phishing e a malware o manipolazioni dei sistemi.

I dati di clienti e dipendenti risultano essere gli obiettivi primari, seguiti dagli attacchi a beni materiali o denaro. Il 56% degli intervistati menziona i dati dei clienti come obiettivo, un dato superiore di 5 punti percentuali alla media globale del 51%.

SICUREZZA

Gli intervistati in Russia hanno fatto registrare percentuali più basse rispetto ad altri paesi di incidenti in materia di sicurezza, 9 punti percentuali in meno rispetto alla media globale del 68%. Il tipo di incidente più comune è stato il furto e la perdita di proprietà intellettuale, a livelli equivalenti alla media mondiale.

Gli ex dipendenti sono stati identificati come responsabili di più di un terzo del totale degli incidenti, un valore doppio rispetto alla categoria in seconda posizione, ossia i dipendenti a tempo indeterminato.

Il divario tra la vulnerabilità percepita ai rischi in materia di sicurezza rispetto all'incidenza effettiva degli incidenti è risultato essere il più ampio dell'intera indagine. Per esempio, il 38% degli intervistati ha subito il furto o la perdita di PI, mentre solo l'8% ha dichiarato di sentirsi molto vulnerabile a questo tipo di rischio.

SCHEDA AREA GEOGRAFICA: RUSSIA

Risposte più frequenti date dai partecipanti al sondaggio.

Frodi

82 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 9% punti in più dal 2015

= pari alla media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	**38%**	29%
	Furto, perdita o attacco alle informazioni	**33%**	24%
	Frodi nei processi di vendita, fornitura o approvvigionamento	**26%**	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti in azienda	**31%**	39%
	Freelance / dipendenti a termine	**28%**	27%
	Manager di primo o secondo livello in azienda	**22%**	30%
	Ex dipendenti	**22%**	27%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	**19%**	26%
	Clienti	**19%**	19%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	**19%**	27%
MISURE ANTIFRODE PIÙ DIFFUSE	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	**90%**	82%
	Gestione *(controlli dall'alto, incentivi, supervisione esterna come le commissioni d'indagine)*	**79%**	74%
	Coinvolgimento del consiglio di amministrazione in politiche e procedure di sicurezza informatica	**77%**	75%
	Rischio *(sistema di gestione del rischio e risk officer)*	**77%**	78%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	**41%**	44%

Cyber Security

82 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▼ 3% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Attacco di phishing a mezzo e-mail	**33%**	26%
	Cancellazione o danneggiamento dei dati causato da malware o manipolazioni del sistema	**26%**	22%
	Furto interno di PI / informazioni commerciali confidenziali/ R&S	**18%**	17%
	Perdita di supporti contenenti dati sensibili	**18%**	17%
	Attacco Denial of Service (DoS)	**18%**	14%
	Infezione da virus / worm	**18%**	33%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**28%**	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	**56%**	51%
	Dati dei dipendenti	**34%**	40%
	Beni materiali/denaro	**28%**	38%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN ATTACCO INFORMATICO	Fornitore di servizi IT	**31%**	27%

Sicurezza

59 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 9% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**38%**	38%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	**21%**	22%
	Violenza sul posto di lavoro	**18%**	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**35%**	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	**18%**	27%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	**8%**	20%
	Furto o perdita di PI	**8%**	19%
	Rischio politico e geografico	**8%**	12%

Quadro generale: Africa sub-sahariana

FRODI

Gli intervistati che operano nell'Africa sub-sahariana hanno riportato il livello di incidenza delle frodi più elevato dell'intera indagine: l'89% ha subito almeno un tipo di frode nel corso dell'anno, un dato al di sopra della media mondiale di 7 punti percentuali, con un aumento di 5 punti rispetto al 2015.

I dirigenti africani hanno riportato l'incidenza più alta delle frodi finanziarie interne (31%), 11 punti percentuali al di sopra della media globale del 20%. Inoltre è emersa un'incidenza di furti o perdite di informazioni al di sopra della media.

I neoassunti sono stati citati come gli autori più comuni delle frodi, seguiti dai freelance e dai dipendenti a tempo indeterminato. Questa è l'unica regione dove gli intervistati hanno riportato che gli organi di controllo contribuiscono in modo significativo alle attività fraudolente, essendo stati citati in oltre un quinto (23%) di tutte le frodi riportate.

La misura antifrode citata con maggiore frequenza è il coinvolgimento del consiglio di amministrazione nello sviluppo di politiche e procedure per la cyber security. A seguire, le misure più comuni sono la messa in sicurezza delle informazioni e i controlli sul personale, entrambe adottate dal 70% degli intervistati nella regione. Tuttavia, queste strategie di contenimento sono state adottate in misura minore dagli intervistati nell'Africa sub-sahariana rispetto alla media mondiale.

CYBER SECURITY

Gli intervistati operanti nell'Africa sub-sahariana sono esposti in maniera molto elevata agli incidenti informatici (91%), il terzo valore più alto registrato al mondo. La cancellazione dei dati tramite manipolazione dei sistemi è stata segnalata come la forma di attacco più frequente da oltre un terzo degli intervistati nella regione.

Altre forme di attacco, come infezioni da virus e worm e attacchi di phishing a mezzo di posta elettronica, sono in linea con le medie globali. L'anomalia più notevole è stata riscontrata per frodi nei trasferimenti bancari, attestata ai livelli più elevati dell'intera indagine (26%), quasi il doppio della media mondiale del 14%.

Gli ex dipendenti sono risultati essere il gruppo maggiormente responsabile degli attacchi informatici secondo il 22% degli intervistati.

La violazione dei dati dei clienti e dei dipendenti risulta essere quasi a pari merito con le informazioni commerciali confidenziali per quel che riguarda l'obiettivo degli attacchi informatici.

Ad attacco avvenuto, solo il 22% degli intervistati ha dichiarato di voler richiedere in prima battuta l'assistenza dai propri fornitori di servizi informativi, mentre quasi altrettanti (16%) dichiarano di preferire un'azienda specializzata nella risposta agli incidenti.

SICUREZZA

Gli incidenti in materia di sicurezza registrano un'incidenza più elevata tra gli intervistati nella regione, 6 punti in più rispetto alla media globale del 68%. Gli incidenti più comuni riportati sono il furto o la perdita di proprietà intellettuale (PI) (43%) e la violenza sul posto di lavoro (26%).

Il furto o la perdita di PI destano grande preoccupazione e sono stati menzionati come un fattore di vulnerabilità da una percentuale di intervistati nella regione (28%) più alta rispetto a qualsiasi altra area geografica o paese.

I partecipanti citano gli ex dipendenti come gli autori più probabili degli incidenti in materia di sicurezza, in misura maggiore rispetto al mondo. (28% rispetto alla media globale del 23%).

SCHEDA AREA GEOGRAFICA: AFRICA SUB-SAHARIANA

Risposte più frequenti date dagli intervistati

Frodi

89 — **Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.**

▲ 5% punti in più dal 2015

▲ 7% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Frode finanziaria interna *(manipolazione dei risultati aziendali)*	**31%**	20%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	**30%**	24%
	Furto di beni materiali o scorte	**26%**	29%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti in azienda	**33%**	39%
	Freelance / dipendenti a termine	**27%**	27%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	**25%**	27%
	Manager di primo o secondo livello in azienda	**23%**	30%
	Organi di controllo	**23%**	14%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Coinvolgimento del consiglio di amministrazione in politiche e procedure di cyber security	**76%**	75%
	Personale*(controlli sui precedenti)*	**70%**	74%
	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	**70%**	82%
	Partner, clienti e fornitori *(due diligence)*	**70%**	77%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine interna	**60%**	39%

Cyber Security

91 — **Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.**

▲ 6% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI INFORMATICI PIÙ COMUNI	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	**35%**	24%
	Infezione da virus / worm	**31%**	33%
	Frode nei trasferimenti bancari	**26%**	14%
	Attacco di phishing a mezzo e-mail	**26%**	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**22%**	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	**49%**	51%
	Dati dei dipendenti	**47%**	40%
	Informazioni commerciali confidenziali	**47%**	40%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN ATTACCO INFORMATICO	Fornitore di servizi IT	**22%**	27%

Sicurezza

74 — **Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.**

▲ 6% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**43%**	38%
	Violenza sul posto di lavoro	**26%**	23%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	**19%**	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**28%**	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Furto o perdita di PI	**28%**	19%
	Violenza sul posto di lavoro	**19%**	27%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	**17%**	20%

Quadro generale: Regno Unito

FRODI

Gli intervistati del Regno Unito hanno riportato un'incidenza delle frodi più alta al mondo, ad eccezione della Colombia. La grande maggioranza (90%) degli intervistati ha dichiarato di esser stata vittima di frodi negli ultimi 12 mesi. Questo dato rappresenta un aumento di 16 punti percentuali rispetto allo scorso anno, superiore di 8 punti alla media globale dell'82%.

I due tipi più comuni di frode riportati dagli intervistati britannici sono il furto di beni materiali e l'appropriazione indebita di fondi societari. La diffusione di entrambe queste tipologie è più elevata nel Regno Unito che in qualsiasi altra area geografica oggetto d'indagine. Come per altre aree geografiche, nella maggior parte dei casi gli autori delle frodi sono interni all'impresa. I dirigenti britannici hanno indicato nei neoassunti la minaccia più grande, seguiti dai manager di primo e secondo livello (menzionati rispettivamente dal 41% e dal 32% degli intervistati).

Gli intervistati nel Regno Unito hanno implementato misure antifrode come la sicurezza dei sistemi informatici, i controlli di gestione e il controllo/monitoraggio della proprietà intellettuale.

CYBER SECURITY

I dirigenti britannici fanno registrare il tasso più alto al mondo di attacchi informatici dopo la Colombia. Quasi tutte le imprese (92%) hanno dichiarato di aver subito un attacco o una perdita di informazioni negli ultimi 12 mesi, un dato superiore di 7 punti percentuali alla media globale dell'85%.

Le infezioni da virus e worm sono state il tipo più comune di attacco, un dato in linea con la maggior parte dei paesi e delle aree geografiche. Il furto di dati dei clienti o dei dipendenti compiuto da risorse interne è risultato il secondo tipo più comune di attacco informatico nel Regno Unito, riportato dal 27% degli intervistati - un valore insolitamente elevato. Solo gli intervistati cinesi hanno riportato un'incidenza più elevata di questo tipo di furto di informazioni (33%).

Come per gli intervistati in altri paesi, nel Regno Unito i dati dei clienti sono stati il primo obiettivo di attacchi o di furto di informazioni e gli ex dipendenti indicati come la categoria di autori più comune.

SICUREZZA

Insieme agli intervistati in Medio Oriente, i dirigenti britannici hanno fatto registrare la percentuale di incidenti in materia di sicurezza più alta nel corso dell'anno passato. La maggior parte di loro (82%) ha dichiarato di essere stata vittima di un incidente, un dato che supera di 14 punti la media globale.

Il furto di proprietà intellettuale, gli eventi geopolitici e la violenza sul posto di lavoro si attestano a livelli superiori alla media globale.

I dirigenti operanti nel Regno Unito hanno dichiarato di sentirsi altamente vulnerabili a una gamma di rischi in materia di sicurezza più ampia rispetto a chi opera in altre aree geografiche.

SCHEDA AREA GEOGRAFICA: REGNO UNITO

Risposte più frequenti date dagli intervistati

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 16% punti in più dal 2015

▲ 8% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	**41%**	29%
	Appropriazione indebita di fondi societari	**37%**	18%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	**24%**	24%
	Collusione nel mercato *(es. cartello dei prezzi)*	**24%**	17%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti in azienda	**41%**	39%
	Manager di primo o secondo livello in azienda	**32%**	30%
	Ex dipendenti	**30%**	27%
	Freelance / dipendenti a termine	**27%**	27%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	**27%**	27%
	Clienti	**27%**	19%
MISURE ANTIFRODE PIÙ DIFFUSE	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	**84%**	82%
	Gestione *(controlli dall'alto, incentivi, supervisione esterna come le commissioni d'indagine)*	**80%**	74%
	PI *(valutazione del rischio per la proprietà intellettuale e programma di monitoraggio dei marchi)*	**76%**	75%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	**50%**	44%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 7% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	**33%**	33%
	Furto interno di dati dei clienti o dei dipendenti	**27%**	19%
	Violazione dei sistemi risultante in perdite di dati dei clienti o dei dipendenti	**22%**	23%
	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	**22%**	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**29%**	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	**42%**	51%
	Informazioni commerciali confidenziali / R&S / PI	**42%**	40%
	Identità aziendale o dei dipendenti	**40%**	36%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN ATTACCO INFORMATICO	Fornitore di servizi IT	**33%**	27%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 14% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**51%**	38%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	**39%**	22%
	Violenza sul posto di lavoro	**29%**	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**28%**	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	**31%**	27%
	Furto o perdita di PI	**24%**	19%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	**24%**	20%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	**24%**	12%
	Eventi terroristici nazionali e internazionali	**24%**	18%

Quadro Generale: Cina

FRODI

La maggior parte degli intervistati in Cina (86%) ha riferito di essere stata vittima di frodi negli ultimi 12 mesi, un dato superiore alla media globale dell'82% che fa registrare un aumento a doppia cifra (13 punti percentuali) rispetto al 2015.

Gli intervistati cinesi hanno registrato la diffusione più ampia dei vari tipi di frode. Tra tutte le regioni prese in esame, gli intervistati in Cina hanno menzionato le violazioni delle norme o della compliance, come la frode primaria (41%), un dato pari a quasi il doppio della media mondiale. La posizione successiva è occupata dalle frodi nella vendita, la fornitura e l'approvvigionamento, attestate a 11 punti percentuali al di sopra della media globale.

Le altre tipologie di frode menzionate includevano il furto di beni materiali o scorte, così come il furto di dati e informazioni. Gli intervistati in Cina sono stati inoltre vittime di corruzione e concussione con percentuali superiori alla media, di collusioni sul mercato e di appropriazione indebita di fondi societari.

Gli intervistati cinesi hanno identificato i partner delle joint venture come i principali responsabili delle frodi (52% dei casi), più del doppio rispetto alla media globale del 23% e significativamente superiore a quella riportata dagli intervistati in altre aree geografiche. Nel complesso, gli autori esterni all'azienda sono menzionati più frequentemente in Cina rispetto alle medie mondiali. Per esempio, gli agenti / intermediari sono stati identificati come i responsabili principali dal 43% dei dirigenti cinesi (16 punti in più della media globale del 27%) e i venditori / fornitori dal 36% degli intervistati (10 punti percentuali in più rispetto alla media globale del 26%).

Anche i dati sulle minacce interne fanno registrare livelli significativi. Quasi la metà (48%) degli intervistati ha identificato i neoassunti cinesi come responsabili delle frodi, mentre più di un terzo (34%) ha individuato i colpevoli nei manager di primo o secondo livello.

Gli intervistati cinesi hanno adottato diverse misure per combattere le frodi. Quasi tutti (90%) gli intervistati della regione hanno investito nella due diligence di partner, clienti o fornitori, un dato seguito dalla protezione dei beni materiali (86%) e dall'impegno della dirigenza nell'implementare politiche e procedure (86%) di sicurezza informatica.

In maniera simile alle altre regioni geografiche, gli intervistati in Cina riferiscono che la società è stata in grado di accertare le frodi attraverso informatori interni (55%), noti come whistleblower. La stessa percentuale ha citato le indagini esterne come metodo di rilevamento delle frodi, un dato superiore di 19 punti alla media globale del 36%.

CYBER SECURITY

Il numero di dirigenti in Cina che ha dichiarato di essere stata vittima di attacchi informatici è superiore di 1 punto percentuale alla media globale (85%). Tra gli incidenti più comuni, due casi hanno superato significativamente l'incidenza media globale: gli attacchi di phishing tramite e-mail (15 punti in più rispetto alla media globale del 26%) e la cancellazione dei dati dovuta a malware o manipolazioni dei sistemi (17 % in più rispetto alla media mondiale del 22%).

La maggior parte degli intervistati cinesi (82%) ha identificato i dati dei clienti come l'obiettivo preferito degli attacchi informatici. Questo dato risulta essere significativamente superiore alla media globale del 51%. Altri obiettivi frequenti sono stati le informazioni commerciali confidenziali e di ricerca e sviluppo o proprietà intellettuale (59%), nonché i dati e le identità dei dipendenti (41%).

Le categorie di autori più diffuse si individuano più frequentemente nei freelance e nei dipendenti a termine. In seguito alla scoperta dell'attacco, il 34% degli intervistati si è rivolto in prima istanza al fornitore di servizi informativi.

SICUREZZA

Tra gli incidenti in materia di sicurezza indicati in Cina, i rischi ambientali sono stati quelli segnalati più di frequente dagli intervistati, con quasi 20 punti percentuali in più rispetto all'incidenza media nel mondo del 27%.

Inoltre gli eventi geopolitici sono stati citati da un quarto degli intervistati, così come il furto o la perdita di proprietà intellettuale, riportata dal 41% degli intervistati stessi.

Un dato peculiare riscontrato in Cina è il fatto che gli intervistati menzionano i concorrenti come gli autori più frequenti degli incidenti di sicurezza (21%), quasi il doppio della media globale del 12%.

SCHEDA AREA GEOGRAFICA: CINA

Risposte più frequenti date dai partecipanti al sondaggio.

Frodi

86 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 13% punti in più dal 2015

▲ 4% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Violazioni delle norme o della compliance	41%	21%
	Frodi nei processi di vendita, fornitura o approvvigionamento	37%	26%
	Furto di beni materiali o scorte	25%	29%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	25%	24%
	Corruzione e concussione	25%	15%
	Collusione nel mercato *(es. cartello dei prezzi)*	25%	17%
	Appropriazione indebita di fondi societari	25%	18%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Partner di joint venture *(ossia un partner che fornisce servizi produttivi di altra natura, oppure un affiliato)*	52%	23%
	Neoassunti in azienda	48%	39%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	43%	27%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	36%	26%
	Manager di primo o secondo livello in azienda	34%	30%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Partner, clienti e fornitori *(due diligence)*	90%	77%
	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	86%	79%
	Coinvolgimento del consiglio di amministrazione in politiche e procedure di cyber security	86%	75%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	55%	44%
	Indagine esterna	55%	36%

Cyber Security

86 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 1% punto sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI INFORMATICI PIÙ COMUNI	Attacco di phishing a mezzo e-mail	41%	26%
	Infezione da virus / worm	39%	33%
	Eliminazione o danneggiamento dei dati causato da malware o manipolazioni del sistema	39%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	25%	14%
OBIETTIVO PIÙ COMUNE	Dati dei clienti	82%	51%
	Segreti commerciali / R&S / PI	59%	40%
	Dati dei dipendenti	41%	40%
	Identità aziendale o dei dipendenti	41%	36%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN INCIDENTE INFORMATICO	Fornitore di servizi IT	34%	27%

Sicurezza

75 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 7% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI DI SICUREZZA PIÙ COMUNI	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	45%	27%
	Furto o perdita di PI	41%	38%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	25%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Concorrenti	21%	12%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI PER LA SICUREZZA	Violenza sul posto di lavoro	33%	27%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	31%	20%
	Eventi terroristici nazionali e internazionali	31%	18%

Cina: Sviluppo di una strategia per il contrasto alle frodi

DI VIOLET HO

Nell'edizione 2016 del Global Fraud and Risk Report di Kroll, la Cina si è distinta, ma non nel senso buono. Un quarto degli intervistati ha riportato di essere stato dissuaso dall'operare in Cina perché preoccupati da frodi e corruzione. Questo risultato è coerente con la situazione che riscontriamo nell'essere in prima linea nel contrasto alle frodi in Cina.

Negli ultimi dieci anni, le attività fraudolente in Cina sono diventate sempre più complesse e problematiche. Anche se i trend delle frodi in questo paese hanno alcune caratteristiche in comune con altri paesi in via di sviluppo, in Cina presentano anche alcuni aspetti peculiari.

Per esempio, le frodi sono spesso commesse dagli alti dirigenti, procurando potenzialmente perdite ancora più significative. Inoltre la ragnatela delle frodi si basa sulla collusione di vari settori e individui, tanto da vanificare le misure di controllo interno tradizionali. A complicare ulteriormente le cose c'è il fatto che il rapido avvicendamento del personale e l'espansione fulminea di molte organizzazioni si traduce in una mancanza di continuità nella governance aziendale e nell'accertamento delle frodi. In Cina, i truffatori stanno diventando sempre più organizzati e intraprendenti, capaci di rappresentare una minaccia significativa per le loro vittime.

Anche se alcuni soggetti intervistati hanno dichiarato di essere pronti ad allontanarsi dalla Cina per timore di cadere vittime di pratiche scorrette, non è detto che questo sia il modo più semplice (o necessariamente il più lungimirante) di affrontare la questione.

La Cina si è ormai affermata come la seconda economia più grande del mondo. Per questo motivo, per le aziende attive su scala mondiale diventa sempre più difficile rinunciare al business cinese. La Cina è anche il primo partner commerciale di molti paesi, oltre al fatto che i consumatori cinesi rappresentano flussi di reddito rilevanti che non si possono sicuramente ignorare.

La gestione del rischio di frode in Cina non è per nulla un compito facile, ma è un obiettivo realizzabile a patto che venga adottata una strategia chiara e coerente. Benché non esista una soluzione in grado di funzionare in totale autonomia, la nostra esperienza ci insegna che esistono una serie di misure di contenimento delle frodi che possono essere adottate da aziende di qualsiasi dimensione e operanti in qualsiasi settore. Le imprese devono essere vigili e dinamiche nel mettere in pratica l'approccio stabilito. Il contrasto alle frodi deve quindi essere concepito come una strategia a lungo termine, astenendosi dal cercare scorciatoie o aspettarsi miracoli.

VIOLET HO
Violet Ho è Senior Managing Director e Co-Direttrice della divisione Investigations & Disputes di Kroll in Cina. Con oltre 19 anni di esperienza professionale nel settore delle investigazioni ed una profonda conoscenza dell'economia cinese, Violet ha svolto con successo il ruolo di consulente in numerosi e delicati progetti investigativi, in Cina e in altri Paesi.

1 Ottenere il massimo dal vostro sistema di whistleblowing: Nella maggior parte dei casi le frodi sono perpetrate da soggetti interni alla società. Allo stesso tempo, sono proprio gli stessi dipendenti che il più delle volte le smascherano. Le denunce dei whistleblower, unite all'occhio vigile dei dirigenti, sono i canali più efficaci per il riconoscimento delle frodi in Cina. Molte imprese hanno creato un canale privilegiato di segnalazione per i whistleblower, ma non sempre ne fanno un uso ottimale.

Per esempio, Kroll ha lavorato insieme a una multinazionale per modificare e irreggimentare il suo sistema di whistleblowing. Per garantire che il whistleblower fornisca informazioni sufficienti e pertinenti , e che queste siano presentate in un formato che ne faciliti l'accesso e l'analisi, abbiamo progettato un questionario con domande e campi a risposta libera da sottoporre ai whistleblower durante il processo di segnalazione anonima. Abbiamo anche suggerito al cliente di implementare un protocollo per dettagliare la natura delle accuse specifiche di ogni segnalazione, tra cui il reparto e la posizione del personale implicato, il tipo e la durata della presunta frode.

In un periodo di 2-3 anni, l'azienda ha mantenuto un registro chiaro e verificabile di tutte le segnalazioni. Questo progetto è culminato nell'analisi d'insieme dei dati accumulati: questa procedura ha rivelato le vulnerabilità dei controlli interni e i rischi di frode presenti in particolari funzioni aziendali. Le indagini svolte dall'azienda successivamente, grazie a questo ulteriore apporto, si sono rivelate molto più efficaci.

2 La centralità del fattore umano: Indipendentemente dal tipo e dall'entità, tutte le frodi sono commesse da persone. Nella mia esperienza, molte aziende non fanno abbastanza per assicurarsi di assumere persone con una forte integrità ed un passato impeccabile. Spesso scopriamo, nel corso delle indagini, che i disonesti avevano già commesso frodi contro i loro datori di lavoro precedenti. Questa preziosa informazione avrebbe potuto essere scoperta effettuando controlli sui precedenti dei dipendenti. Procedure di due diligence strutturate, se intraprese nei confronti di dipendenti e fornitori, spesso rivelano indizi di potenziali conflitti di interesse o di accordi collusivi.

3 Garantire l'indipendenza delle indagini: Data la preponderanza delle frodi in Cina, fare luce su tutte le accuse può rivelarsi complicato o infattibile per una società. Di conseguenza è importante far sì che i dipendenti non abbiano la sensazione che le indagini siano state avviate nell'interesse (o nel disinteresse) di qualcuno. Affidandosi a consulenti professionali, si potrà rinforzare la credibilità dei dirigenti, tutelandola riservatezza e l'indipendenza dell'investigazione. Inoltre i consulenti esterni possono scoraggiare i disonesti nel loro tentativo di influenzare le indagini mediante giochi di potere.

4 Promuovere una forte cultura della compliance a partire dall'alto e in maniera credibile: Uno degli strumenti migliori per prevenire, individuare e rispondere alle frodi è la costituzione e la promozione di una cultura aziendale di tolleranza zero verso le frodi e la corruzione. Questo processo richiede tempo e non può fare a meno del sostegno da parte del management. Quando si impostano gli indicatori chiave di rendimento (KPI) per i dipendenti non si dovrebbe badare esclusivamente agli obiettivi finanziari. Ai dirigenti spetta anche la responsabilità di promuovere con decisione una cultura della compliance tra i membri dei loro team.

Quadro generale: India

FRODI

Gli intervistati che operano in India hanno comunicato una riduzione di 12 punti percentuali dell'incidenza delle frodi negli ultimi 12 mesi. La percentuale degli intervistati che si è dichiarata vittima di frode è stata del 68%, pari a quella del Brasile. Questi due paesi presentano l'incidenza più bassa dell'intera indagine. Il risultato ottenuto in India risulta essere 14 punti al di sotto della media globale dell'82%.

Tuttavia, quando a tutti gli intervistati è stato chiesto se fossero stati dissuasi dall'operare in una data giurisdizione per preoccupazioni dovute alle frodi, l'India (19%) è stata la seconda giurisdizione più menzionata dopo la Cina (25%).

Questo dato suggerisce l'esistenza di una discrepanza tra gli stakeholder interni ed esterni circa la percezione delle frodi in India.

I dirigenti indiani hanno menzionato i neoassunti in azienda (61%) come gli autori principali degli incidenti di frode. A seguire figurano gli agenti e gli intermediari che lavorano per l'impresa. Entrambi questi gruppi sono stati segnalati con uno scarto di 22 punti percentuali al di sopra delle medie globali (rispettivamente 39% e 27%).

Gli intervistati in India stanno implementando le dovute misure antifrode. Oltre l'85% degli intervistati contrasta le frodi attraverso il potenziamento dei controlli finanziari, effettuando due diligence su partner, clienti e fornitori, e sviluppando sistemi per la sicurezza delle informazioni e per i controlli sul personale.

Il 66% degli intervistati ha riportato che il mezzo più efficace di individuazione delle frodi è il whistleblowing.

CYBER SECURITY

Attestandosi a 12 punti percentuali al di sotto della media globale, il 73% degli intervistati in India ha riferito di aver subito un attacco informatico negli ultimi 12 mesi. Questo dato relativamente basso potrebbe derivare dal fatto che non tutti i settori di attività delle imprese indiane siano consci del rischio informatico. Questo accade poiché molti settori in India, escludendo i servizi finanziari, non sono digitalizzati come nei paesi più sviluppati, il che riduce la loro esposizione ai rischi legati alla cyber security. Un ulteriore motivo potrebbe risiedere nel fatto che i soggetti intervistati spesso non sono tenuti a rivelare le violazioni dei sistemi informatici a cui hanno assistito. Si capisce come la sensibilità a questo tipo di rischio sia ancora in evoluzione.

I tipi più comuni di attacchi informatici che minacciano le imprese indiane risultano essere la cancellazione dei dati dovuta a malware o manipolazioni del sistema (28%) e le azioni ostili del personale interno all'azienda (27%).

È interessante osservare come i manager non abbiano indicato una categoria di autori ben definita, ma abbiano invece dichiarato che la causa degli incidenti è in massima parte il posizionamento accidentale dei dati sensibili su un motore di ricerca (statuito dal 25% dei partecipanti, 15 punti percentuali in più rispetto alla media globale del 10%).

SICUREZZA

Le problematiche legate agli incidenti in materia di sicurezza risultano prevalenti in India, superando di 4 punti percentuali la media globale del 68%, coerentemente con l'esperienza di Kroll nel paese. Il danno da calamità naturali è più alto di 13 punti percentuali rispetto alla media globale del 27%. Rispetto ai mercati più sviluppati, il furto di proprietà intellettuale risulta leggermente inferiore alla media globale (rispettivamente 35% e 38%).

Gli autori di incidenti in materia di sicurezza più diffusi sono stati identificati principalmente nei dipendenti a tempo indeterminato delle società. Anche se i partecipanti hanno dichiarato di sentirsi più vulnerabili a fattori come la violenza sul posto di lavoro (52%), seguita da altre forme di violenza come il terrorismo nazionale o internazionale (45%), i rischi ambientali figurano al terzo posto (37%) pur essendo citati come la causa più frequente di un incidente legato alla sicurezza.

SCHEDA AREA GEOGRAFICA: INDIA

Risposte più frequenti date dagli intervistati

Frodi

68 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▼ 12% punti in meno dal 2015

▼ 14% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	28%	29%
	Conflitto di interessi del management	27%	21%
	Corruzione e concussione	27%	15%
	Frodi nei processi di vendita, fornitura o approvvigionamento	27%	26%
	Collusione nel mercato *(es. cartello dei prezzi)*	27%	17%
	Frode finanziaria interna *(manipolazione dei risultati aziendali)*	25%	20%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti in azienda	61%	39%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	49%	27%
	Freelance / dipendenti a termine	41%	27%
	Manager di primo o secondo livello in azienda	37%	30%
	Partner di joint venture *(ossia un partner che fornisce servizi produttivi di altra natura, oppure un affiliato)*	37%	23%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Finanziaria *(controlli finanziari, accertamento delle frodi, indagini interne o esterne, politiche antiriciclaggio)*	87%	77%
	Partner, clienti e fornitori *(due diligence)*	87%	77%
	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	85%	82%
	Personale *(controlli sui precedenti)*	85%	74%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	66%	44%

Cyber Security

73 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▼ 12% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Cancellazione o danneggiamento dei dati causato da malware o manipolazioni del sistema	28%	22%
	Cancellazione dei dati premeditata da parte di risorse interne	27%	19%
	Infezione da virus / worm	23%	33%
	Attacco Denial of Service (DoS)	23%	14%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Divulgazione accidentale di dati sensibili indicizzati da un motore di ricerca *(es. Google)*	25%	10%
OBIETTIVO PIÙ COMUNE	Dati dei dipendenti	59%	40%
	Informazioni commerciali confidenziali / R&S / PI	48%	40%
	Dati dei clienti	45%	51%
	Beni materiali/denaro	45%	38%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN INCIDENTE INFORMATICO	Fornitore di servizi IT	34%	27%

Sicurezza

72 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 4% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	40%	27%
	Violenza sul posto di lavoro	37%	23%
	Furto o perdita di PI	35%	38%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	35%	22%
AUTORI PIÙ COMUNI	Dipendenti a tempo indeterminato dell'impresa	26%	17%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI PER LA SICUREZZA	Violenza sul posto di lavoro	52%	27%
	Eventi terroristici nazionali e internazionali	45%	18%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	37%	20%

India: Cogliere le contraddizioni

DI RESHMI KHURANA

Nell'indagine Global Fraud and Risk condotta da Kroll nel 2016 l'India figurava in seconda posizione - dopo la Cina - nell'elenco delle giurisdizioni in cui i dirigenti sono stati dissuasi dall'operare. Secondo quasi un quinto (19%) degli intervistati, il rischio di frode in India era abbastanza elevato da rappresentare un fattore di dissuasione decisivo. Una percentuale equivalente di intervistati ha indicato i rischi in materia di sicurezza come fattore principale di deterrenza.

Dalle statistiche emergono così le contraddizioni dell'economia indiana. Da un lato, l'India resta una meta attraente per gli investitori stranieri. Si tratta infatti di uno dei mercati emergenti con la crescita più rapida; è politicamente più stabile rispetto al passato e il governo del Partito del Popolo Indiano (BJP) sta intraprendendo le tanto attese riforme economiche per attirare gli investimenti esteri diretti. D'altra parte, la nostra indagine mostra come gli investitori siano scoraggiati dalla presenza di frodi, corruzione e problemi di sicurezza.

Molti investitori ritengono che il mercato indiano sia troppo grande per essere ignorato, così gli investitori strategici spesso scelgono di entrare in joint venture con partner locali che si occupano di controllare le attività delle imprese nazionali. Gli investitori stranieri ritengono che i partner in questione siano più capaci di districarsi nell'ambiente economico indiano, in virtù delle strette relazioni tra imprese, governo e burocrati, destando però sospetti di affari sconvenienti.

Mentre le imprese locali sono in grado di vedere dietro le quinte, per gli investitori stranieri non è semplice; questo crea un terreno favorevole per le attività fraudolente. Per esempio, il management locale può stringere accordi fraudolenti con terze parti al fine di gonfiare le fatture delle forniture o praticare assunzioni fasulle, assicurandosi una fetta di profitti illegali. Pratiche del genere possono impedire agli investitori di capire se i profitti sono investiti per scopi commerciali legittimi (come per esempio l'acquisto di terreni o il pagamento dei braccianti) o per il pagamento di tangenti ai funzionari governativi.

RESHMI KHURANA
Reshmi Khurana è Managing Director nonché Responsabile delle operazioni Kroll in Asia Meridionale presso la sezione Investigations and Disputes di Mumbai. Reshmi lavora da oltre 16 anni negli Stati Uniti, nel Subcontinente Indiano e nel Sud-Est Asiatico, conducendo indagini complesse sulla corruzione, progetti di assistenza nei contenziosi e due diligence sulla gestione, le attività e i modelli di business delle organizzazioni. La sua esperienza le permette di aiutare i clienti a individuare e colmare le lacune nei controlli interni e nella governance aziendale per mezzo di specialisti, processi e tecnologie.

Come per la Cina, la collusione fraudolenta tra dipendenti, fornitori, clienti e altri soggetti può raggiungere livelli elevati anche in India. Le frodi possono annidarsi negli accordi con terze parti, ma anche essere commesse da gruppi di dipendenti. Dopo l'accertamento di una frode, spesso non è facile licenziare i dipendenti o interrompere le relazioni con i fornitori principali, in quanto questo potrebbe compromettere il morale e la continuità operativa. Le imprese devono quindi procedere con la massima cautela quando affontano accuse di frode.

Per esempio, Kroll ha condotto di recente un'indagine per conto di un importante conglomerato di livello mondiale in seguito alla ricezione di una denuncia anonima da parte di un whistleblower. Questi sosteneva che il suo amministratore delegato locale prendesse tangenti da determinati fornitori. Il cliente si mostrava comprensibilmente preoccupato dell'impatto delle indagini sul morale dell'impresa locale e sulla sua capacità di garantire la continuità operativa nel corso delle indagini. Kroll ha dunque aiutato il cliente a far luce sulle accuse esaminando le prove digitali, conducendo indagini sul campo con la massima discrezione e analizzando i dati delle transazioni con i fornitori in questione, al fine di minimizzare l'interruzione delle attività.

L'indagine ha rivelato che la cultura del management, i processi contabili e la governance aziendale locale avevano probabilmente portato allo sviluppo di un terreno favorevole e maturo per le frodi. Abbiamo scoperto che i top manager erano a conoscenza delle lacune nella governance aziendale, nonché delle frodi che ne erano scaturite. Kroll ha aiutato il cliente ad avere un quadro completo del problema, che ha comportato l'allontanamento dell'amministratore delegato e di altri dipendenti.

Anche i problemi legati alla sicurezza stanno diventando sempre più prioritari: quasi un quinto degli intervistati ha dichiarato che questo tipo di rischi li ha dissuasi dall'investire in India.

Tuttavia questi rischi possono essere gestiti. Per evitare le frodi, consigliamo agli investitori, esperti o meno che siano, di:

1 **Valutare:** Una valutazione qualitativa del contesto operativo e dei potenziali partner - su fattori come la loro reputazione, le connessioni con la politica, gli standard etici e le pratiche commerciali - riveste un'importanza paragonabile alla revisione dei conti, dei registri finanziari e dei documenti legali.

2 **Comprendere:** Gli investitori stranieri devono comprendere appieno le dinamiche del business e della politica in India per sbloccare saggiamente gli investimenti.

3 **Preparasi a dovere:** Gli investitori non dovrebbero essere influenzati dalle pressioni competitive dell'ambiente di investimento in India, dove troppo spesso molti investitori perseguono le stesse opportunità. Dovrebbero prendersi il tempo necessario in modo da essere pronti a fare un investimento ben informato.

4 **Rifiutare il compromesso:** Per avere la certezza che i fornitori di due diligence siano davvero indipendenti e garantiscano l'integrità del processo, gli investitori devono sceglierli seguendo una politica che rifiuti qualunque forma di compromesso.

Quadro generale: Brasile

FRODI

Il Brasile è stato uno dei tre paesi esaminati nei quali l'incidenza delle frodi è risultata inferiore rispetto alla media globale dell'82%. Gli altri due sono stati India e Italia. Poco più dei due terzi (68%) degli intervistati che operano in Brasile è stato vittima di frode negli ultimi 12 mesi, un dato inferiore di 14 punti rispetto alla media globale.

I furti sono un grave problema per le imprese brasiliane, con quasi un quarto (24%) degli intervistati ad aver subito furti di beni materiali. Inoltre più di un quinto (21%) degli intervistati ha indicato furti di informazioni e frodi nella vendita, nella fornitura o nell'approvvigionamento. Tuttavia, in linea con i dati complessivi registrati in Brasile, l'incidenza di queste frodi è inferiore alla media globale.

Una grande maggioranza (85%) degli intervistati ha investito nei metodi antifrode focalizzati sul management; si sono dunque registrati tassi elevati di adozione dei registri di beni materiali (88%) e di misure di sicurezza per le informazioni (88%).

Il metodo di accertamento delle frodi più usato dalle imprese brasiliane è stato l'audit esterno, menzionato dal 43% degli intervistati.

Una percentuale significativa (43%) degli intervistati ha puntato il dito contro gli ex dipendenti come i principali responsabili delle frodi. I freelance / dipendenti a termine e i neoassunti sono stati indicati come coinvolti in incidenti fraudolenti, rispettivamente, da circa un quarto (26%) e un quinto (22%) degli intervistati.

CYBER SECURITY

Gli intervistati in Brasile si sono dichiarati vittime di incidenti di cyber security in misura minore rispetto alle altre regioni, attestandosi a 9 punti percentuali in meno rispetto alla media globale (85%). Tuttavia, come testimoniato dai tre quarti degli intervistati (76%) che segnalano di aver subito un caso di attacco informatico negli ultimi 12 mesi, la maggior parte delle imprese brasiliane coinvolte nell'indagine risulta ancora vulnerabile.

I dati raccolti in Brasile mostrano che gli intervistati sono stati vittime di attacchi di virus e worm, nonché di violazioni che hanno comportato la perdita di dati dei clienti e dei dipendenti.

Gli attacchi mediante virus e worm fanno registrare 8 punti in più rispetto alla media mondiale (33%), con il 41% degli intervistati che si è dichiarata vittima di questo metodo di attacco. I dati dei clienti sono stati i principali obiettivi degli aggressori, seguiti dai dati dei dipendenti, e dalle identità delle aziende e dei propri dipendenti.

La percentuale degli ex dipendenti che istigano attacchi informatici è pari al 38%, quasi il doppio della media globale (20%).

SICUREZZA

Poco più della metà (53%) degli intervistati in Brasile ha dichiarato di esser stata vittima di un incidente in materia di sicurezza. Questo dato è significativamente inferiore (15 punti percentuali) rispetto alla media globale del 68%. Il tipo di incidente più comune è stato il furto e la perdita di proprietà intellettuale, seguito dagli eventi di natura ambientale e geopolitica.

SCHEDA AREA GEOGRAFICA: BRASILE

Risposte più frequenti date dai partecipanti al sondaggio.

Frodi

68 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▼ 9% punti in meno dal 2015

▼ 14% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	24%	29%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	21%	24%
	Frodi nei processi di vendita, fornitura o approvvigionamento	21%	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	43%	27%
	Freelance / dipendenti a termine	26%	27%
	Neoassunti in azienda	22%	39%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	17%	26%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	17%	27%
	Partner di joint venture *(ossia un partner che fornisce servizi produttivi di altra natura, oppure un affiliato)*	17%	23%
	Clienti	17%	19%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	88%	79%
	Informazioni *(sicurezza informatica, contromisure tecniche)*	88%	82%
	Gestione *(controlli dall'alto, incentivi, supervisione esterna come le commissioni d'indagine)*	85%	74%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine esterna	43%	36%

Cyber Security

76 Percentuale degli intervistati vittime di incidenti informatici negli ultimi 12 mesi.

▼ 9% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	41%	33%
	Violazione dei sistemi risultante in perdite di dati dei clienti o dei dipendenti	29%	23%
	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	21%	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	38%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	46%	51%
	Dati dei dipendenti	42%	40%
	Identità aziendale o dei dipendenti	42%	36%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN INCIDENTE INFORMATICO	Provider di spazi/siti web	23%	9%

Sicurezza

53 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 15% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	32%	38%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	18%	27%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	12%	22%
AUTORI PIÙ COMUNI	Ex dipendenti	39%	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI PER LA SICUREZZA	Furto o perdita di PI	21%	19%
	Violenza sul posto di lavoro	18%	27%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	15%	12%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	15%	20%

Quadro generale: Colombia

FRODI

Le frodi sono state riportate da quasi tutti (95%) gli intervistati che operano in Colombia: si tratta del dato percentuale più alto dell'intera indagine, con un aumento di 12 punti percentuali rispetto al 2015.

Gli intervistati hanno riferito che il tipo più comune di frode deriva dai conflitti di interesse da parte del management, seguito dalle frodi nelle forniture e nell'approvvigionamento, infine dal furto di beni materiali. Le categorie di autori più diffuse sono risultate essere ex dipendenti, freelance / dipendenti a termine e venditori/fornitori: ognuno di questi gruppi è stato menzionato da poco più di un terzo degli intervistati operanti in Colombia (35%).

Le opinioni raccolte dagli intervistati in Colombia hanno indicato che sono stati fatti dei passi considerevoli per attuare le misure antifrode: i dirigenti elencano i loro sforzi per stabilire controlli finanziari, strategie di gestione dei beni materiali e controlli sui precedenti del personale.

Due terzi degli intervistati in Colombia hanno riferito che le frodi sono state scoperte perlopiù attraverso indagini interne.

CYBER SECURITY

Gli intervistati colombiani hanno segnalato attacchi informatici (95%) in misura maggiore a tutte le altre aree geografiche, un dato superiore di 10 punti percentuali rispetto alla media globale dell'85%. Oltre la metà degli intervistati operanti in Colombia ha dichiarato di aver subito attacchi come infezioni di virus e worm (52%), seguiti dagli attacchi di phishing tramite e-mail (38%). La cancellazione o le perdite di dati sono state riportate dal 29% dei dirigenti in Colombia, 5 punti in più della media globale.

I principali obiettivi degli attacchi informatici in Colombia riguardano i dati dei clienti, i beni materiali e i dati dei dipendenti: questi dati sono sostanzialmente in linea con le medie globali. Anche l'identificazione degli autori delle frodi coincide coi valori registrati in altre aree geografiche: gli ex dipendenti sono stati identificati come i principali colpevoli degli incidenti informatici da un quarto degli intervistati colombiani.

SICUREZZA

Gli intervistati in Colombia hanno dichiarato una prevalenza degli incidenti in materia di sicurezza leggermente inferiore alla media globale (62%). La violenza sul posto di lavoro è stato il caso più comune legato a incidenti in materia di sicurezza. Ancora una volta, i freelance e i dipendenti a termine sono risultati le categorie di autori più compromesse, secondo il 38% degli intervistati colombiani.

SCHEDA AREA GEOGRAFICA: COLOMBIA

Risposte più frequenti date dagli intervistati

Frodi

95 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 12% Punti in più dal 2015

▲ 13% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Conflitto di interessi del management	**43%**	21%
	Frodi nei processi di vendita, fornitura o approvvigionamento	**43%**	26%
	Furto di beni materiali o scorte	**38%**	29%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**35%**	27%
	Freelance / dipendenti a termine	**35%**	27%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	**35%**	26%
	Manager di primo o secondo livello in azienda	**20%**	30%
	Neoassunti in azienda	**20%**	39%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Finanziaria *(controlli finanziari, accertamento delle frodi, indagini interne o esterne, politiche antiriciclaggio)*	**95%**	77%
	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	**95%**	79%
	Personale *(controlli sui precedenti)*	**95%**	74%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine interna	**50%**	39%

Cyber Security

95 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 10% punti sopra la media globale (85%)

			Media glob.
TIPOOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	**52%**	33%
	Attacco di phishing a mezzo e-mail	**38%**	26%
	Cancellazione dei dati o perdita di dati dovute a manipolazioni dei sistemi	**29%**	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**25%**	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	**50%**	51%
	Beni materiali/denaro	**45%**	38%
	Dati dei dipendenti	**40%**	40%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN ATTACCO INFORMATICO	Azienda specializzata nella risposta agli incidenti	**15%**	14%
	Portale compagnia assicurativa	**15%**	15%
	Provider di spazi/siti web	**15%**	9%

Sicurezza

62 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 6% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Violenza sul posto di lavoro	**24%**	23%
	Furto o perdita di PI	**24%**	38%
	Eventi terroristici nazionali e internazionali	**19%**	15%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	**38%**	16%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Eventi terroristici nazionali e internazionali	**19%**	18%
	Violenza sul posto di lavoro	**19%**	27%
	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	**14%**	20%

Quadro generale: Messico

FRODI

La maggioranza (82%) degli intervistati in Messico è stata vittima di frodi negli ultimi 12 mesi, un incremento di 2 punti percentuali rispetto al 2015.

Il dato più sorprendente che emerge dall'indagine sui dirigenti messicani è la frequenza delle frodi compiute da fornitori e venditori: il 52%, ossia la più alta tra tutti i paesi presi in esame e doppia rispetto alla media globale (26%).

Allo stato attuale, i due meccanismi adottati più comunemente dai partecipanti messicani per combattere le frodi sono la due diligence sui partner, venditori o fornitori e i controlli finanziari, entrambi menzionati dall'82% degli intervistati.

Il modo più diffuso per il rilevamento delle frodi è l'indagine interna, menzionata dal 44% degli intervistati in Messico.

CYBER SECURITY

Il numero di attacchi informatici riportati si attesta leggermente sotto la media globale (82%). I metodi di attacco più comuni sono stati le infezioni di virus e worm, gli attacchi di phishing tramite e-mail e la cancellazione dei dati dovuta a malware o manipolazioni dei sistemi.

La responsabilità per la maggior parte degli attacchi è risultata ascrivibile ai concorrenti. In Messico gli intervistati sono stati identificati come autori principali degli informatici con un tasso tre volte superiore alla media mondiale.

Gli intervistati messicani che hanno subito l'attacco hanno preferito rivolgersi in prima battuta alle forze dell'ordine federali.

SICUREZZA

Gli intervistati operanti in Messico hanno riportato il tasso di incidenti in materia di sicurezza più basso dell'intera indagine. Meno della metà degli intervistati (48%) ha dichiarato di aver subito questo tipo di incidente, un dato che si colloca ben al di sotto - quasi del 20% - rispetto alla media globale (68%). Gli incidenti riportati più di frequente sono stati gli eventi di natura ambientale (27%), seguiti dalla perdita di proprietà intellettuale e dagli eventi geopolitici.

Gli intervistati messicani hanno dichiarato di sentirsi vulnerabili alla violenza sul posto di lavoro e al terrorismo, anche se non hanno segnalato eventi del genere nella classifica dei tre incidenti più comuni.

SCHEDA AREA GEOGRAFICA: MESSICO

Risposte più frequenti date dagli intervistati

Frodi

82 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 2% punti in più dal 2015

= pari alla media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Frodi nei processi di vendita, fornitura o approvvigionamento	52%	26%
	Furto di beni materiali o scorte	30%	29%
	Corruzione e concussione	18%	15%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	33%	27%
	Neoassunti in azienda	30%	39%
	Freelance / dipendenti a termine	30%	27%
	Venditori/Fornitori *(es. un fornitore di tecnologie o servizi per l'impresa)*	30%	26%
	Agenti e/o intermediari *(ossia terze parti che lavorano per conto dell'impresa)*	26%	27%
MISURE ANTIFRODE PIÙ DIFFUSE	Partner, clienti e fornitori *(due diligence)*	82%	77%
	Finanziaria *(controlli finanziari, accertamento delle frodi, indagini interne o esterne, politiche antiriciclaggio)*	82%	77%
	Rischio *(sistema di gestione del rischio e risk officer)*	81%	78%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine interna	44%	39%

Cyber Security

82 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▼ 3% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	39%	33%
	Attacco di phishing a mezzo e-mail	33%	26%
	Cancellazione o danneggiamento dei dati causato da malware o manipolazioni del sistema	33%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Concorrenti	22%	6%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Identità aziendale o dei dipendenti	52%	36%
	Dati dei clienti	48%	51%
	Beni materiali/denaro	37%	38%
RICHIESTA DI ASSISTENZA PIÙ FREQUENTE IN SEGUITO A UN ATTACCO INFORMATICO	Forze dell'ordine federali	30%	8%

Sicurezza

48 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 20% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Rischio ambientale *(compresi i danni dovuti a calamità naturali quali uragani, tornado, inondazioni, terremoti, ecc.)*	27%	27%
	Furto o perdita di PI	24%	38%
	Rischio geografico e politico *(operazioni in zone di conflitto)*	21%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	31%	16%
	Ex dipendenti	31%	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	24%	27%
	Eventi terroristici nazionali e internazionali	21%	18%
	Furto o perdita di PI	18%	19%

Quadro generale: costruzioni, ingegneria e infrastrutture

FRODI

L'indagine di quest'anno mostra che il settore costruzioni, ingegneria e infrastrutture può essere considerato una storia di successo. Anche se il 70% degli intervistati operanti nel settore continua ad essere vittima di frodi, il dato si posiziona significativamente al di sotto della media globale, facendo di questo settore il meno colpito tra tutti quelli presi in considerazione. Il secondo dato più basso è stato registrato nel settore tecnologia, media e telecomunicazioni (TMT), dove il 79% degli intervistati si è detto vittima di frode.

Il settore costruzioni, ingegneria e infrastrutture è stato l'unico a conoscere un calo delle frodi dal 2015 al 2016, con una riduzione di 5 punti percentuali sul totale degli intervistati.

In linea con quanto avviene negli altri settori, la categoria di autori delle frodi più diffusa è quella dei neoassunti, indicati come responsabili nel 45% dei casi. Gli ex dipendenti sono stati identificati come responsabili in un terzo della totalità dei casi.

Considerata l'incidenza del dato relativo ai dipendenti, le misure antifrode adottate più di frequente sono quelle relative al personale. Queste includono corsi di formazione, linee telefoniche dedicate per i whistle-blower e attività di background screening sui neoassunti. Gli internal audit si sono rivelati il metodo più diffuso per identificare le frodi in questo settore .

CYBER SECURITY

Per quanto riguarda gli attacchi informatici, oltre tre quarti degli intervistati ha dichiarato di esserne stato vittima negli ultimi 12 mesi. Se pur sotto la media globale, i casi di attacco informatico sono tuttora diffusi: obiettivo principale di tali attacchi, condotti tramite infezioni da virus o worm, email phishing e cancellazione o perdita dei dati dovute a manipolazioni dei sistemi, è costituito dai dati dei clienti

SICUREZZA

Più della metà (63%) degli intervistati operanti nel settore costruzioni, ingegneria e infrastrutture ha subito un evento legato ai rischi in materia di sicurezza negli ultimi 12 mesi. I rischi ambientale e geopolitico sono risultati superiori alla media globale; d'altra parte, il furto e la perdita di proprietà intellettuale sono considerati dagli intervistati un rischio secondario, se pur identificati come un'area di vulnerabilità.

COSTRUZIONI, INGEGNERIA E INFRASTRUTTURE

Risposte più frequenti date dagli intervistati.

Frodi

70 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▼ 5% punti in meno rispetto al 2015

▼ 12% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Frodi nei processi di vendita, fornitura o approvvigionamento	28%	26%
	Frode finanziaria interna *(manipolazione dei risultati aziendali)*	21%	20%
	Corruzione e concussione	19%	15%
	Appropriazione indebita di fondi societari	19%	18%
	Furto di beni materiali o scorte	19%	29%
CATEGORIA DI AUTORI PIÙ DIFFUSE	Neoassunti	45%	39%
	Ex dipendenti	33%	27%
	Management di primo o secondo livello	30%	30%
	Freelance / dipendenti a termine	30%	27%
	Venditori/fornitori	30%	26%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Personale *(formazione, linee telefoniche dedicate ai whistleblower).*	81%	76%
	Personale *(attività di background screening)*	79%	74%
	Partner, clienti e fornitori *(due diligence)*	79%	77%
	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	79%	82%
	Rischio *(sistema di gestione del rischio e risk officer)*	79%	78%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine interna	38%	39%

Cyber Security

77 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▼ 8% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	35%	33%
	Attacco di phishing a mezzo e-mail	30%	26%
	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	30%	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	20%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	59%	51%
	Dati dei dipendenti	45%	40%
	Beni materiali/denaro	43%	38%

Sicurezza

63 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 5% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI DI SICUREZZA PIÙ COMUNI	Rischio ambientale	33%	27%
	Furto o perdita di PI	32%	38%
	Rischio politico e geografico	23%	22%
	Violenza sul posto di lavoro	23%	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	25%	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Furto o perdita di PI	18%	19%
	Rischio ambientale	18%	20%
	Violenza sul posto di lavoro	12%	27%

Quadro generale: beni di consumo

FRODI

La maggioranza (82%) degli intervistati operanti nel settore dei beni di consumo ha dichiarato di essere stata vittima di frode negli ultimi 12 mesi, un dato in linea con la media globale. Rispetto all'anno precedente, si è registrato un aumento di 10 punti percentuali. I casi più comuni sono stati il furto, la perdita o l'attacco alle informazioni, pari a quasi un terzo (32%) delle frodi subite.

Nel 43% dei casi, agenti e intermediari sono stati identificati come gli autori delle frodi. Si tratta dell'unico settore nel quale agenti ed intermediari figurano in cima alla classifica degli autori della frode.

L'adozione di misure antifrode è risultata relativamente bassa nel settore dei beni di consumo. Le misure volte a tutelare la sicurezza delle informazioni e dei beni materiali sono state quelle adottate più di frequente, ma entrambe in misura inferiore alla media mondiale. Inoltre il dato relativo all'adozione di misure per la sicurezza delle informazioni risulta essere più basso che in qualsiasi altro settore, eccezion fatta per i servizi professionali.

CYBER SECURITY

Il phishing a mezzo e-mail è stato il tipo di attacco informatico subito con maggior frequenza nel corso dell'anno passato (28%), seguito dalla violazione dei sistemi risultante in perdite di dati dei clienti o dei dipendenti (27%) e dalle infezioni da virus / worm (27%). L'obiettivo di quasi due terzi (62%) degli attacchi sono stati i dati dei clienti, la più alta percentuale di tutti i settori di attività, ad eccezione dell'industria manifatturiera.

SICUREZZA

In merito ai rischi per la sicurezza, i casi più comuni nel settore dei beni di consumo sono il furto e la perdita di proprietà intellettuale e i rischi ambientali. Il terrorismo occupa la terza posizione in classifica, ma il dato in questione - un quinto degli intervistati in questo settore se ne dichiara vittima - risulta superiore alla media globale.

BENI DI CONSUMO

Risposte più frequenti date dagli intervistati.

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 10% punti in più dal 2015

= pari alla media globale (82%)

			Media glob.
TIPOLOGIA DI FRODI PIÙ COMUNI	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	**32%**	24%
	Furto di beni materiali o scorte	**28%**	29%
	Frodi nei processi di vendita, fornitura o approvvigionamento	**28%**	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Agenti e/o intermediari	**43%**	27%
	Neoassunti	**37%**	39%
	Venditori/fornitori	**35%**	26%
	Partner di joint venture	**31%**	23%
	Management di primo o secondo livello	**24%**	30%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	**77%**	82%
	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	**77%**	79%
	Coinvolgimento del consiglio di amministrazione in politiche e procedure di cyber security	**73%**	75%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	**53%**	44%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▼ 2% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Attacco di phishing a mezzo e-mail	**28%**	26%
	Violazione dei sistemi risultante in perdite di dati dei clienti o dei dipendenti	**27%**	23%
	Infezione da virus / worm	**27%**	33%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**28%**	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	**62%**	51%
	Informazioni commerciali confidenziali / R&S / PI	**54%**	40%
	Identità aziendale o dei dipendenti	**30%**	36%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 7% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**27%**	38%
	Rischio ambientale	**27%**	27%
	Terrorismo	**20%**	15%
	Rischio politico e geografico	**20%**	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**31%**	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Furto o perdita di PI	**22%**	19%
	Violenza sul posto di lavoro	**20%**	27%
	Rischio ambientale	**18%**	20%

Quadro Generale: Servizi Finanziari

FRODI

Dall'analisi dei dati raccolti nel settore dei servizi finanziari, emerge un incremento consistente (19%) delle frodi, con l'89% del totale degli intervistati che ne riportano almeno un tipo durante l'anno appena trascorso. I casi più comuni sono stati il furto di beni materiali e scorte (subito dal 39% degli intervistati) e le frodi nella vendita, nella fornitura o nell'approvvigionamento (32% degli intervistati). La percentuale di dirigenti intervistati nel settore dei servizi finanziari che ha sostenuto di aver subito il furto di proprietà intellettuale (PI), la pirateria e la contraffazione, ammonta al 27%, quasi il doppio della media globale.

Gli intervistati hanno adottato misure antifrode in misura leggermente più ampia rispetto alla media globale: la misura adottata più di frequente, e non è una sorpresa vista la tipologia del settore, è la nomina di un risk officer e l'implementazione di un sistema di gestione del rischio. Dal sondaggio emerge inoltre una maggiore propensione all'adozione di misure di gestione del rischio per tutelare la PI, la più elevata di tutti i settori, eccezion fatta per la sanità.

Anche se il whistleblowing è il fattore principale per scoprire le frodi negli altri settori, in quello finanziario sono le indagini esterne a ricoprire il ruolo di punta.

CYBER SECURITY

Gli intervistati operanti nel settore dei servizi finanziari hanno fatto registrare un'incidenza più elevata della media anche per gli attacchi informatici: i casi più frequenti sono stati le cancellazioni o le perdite di dati dovute a manipolazioni dei sistemi. Gli attacchi hanno riguardato in massima parte i dati dei clienti, seguiti da informazioni commerciali confidenziali, R&S e PI.

SICUREZZA

Anche se nel settore dei servizi finanziari i dirigenti riportano i tassi più elevati di tutti i settori in termini di frodi e attacchi informatici, quest'ambito risulta essere quello meno colpito dagli incidenti in materia di sicurezza. Poco meno di tre quinti (57%) dei dirigenti ha riferito di aver subito un incidente in materia di sicurezza, un valore inferiore di 11 punti percentuali rispetto alla media globale. Il furto o la perdita di PI sono stati indicati dagli intervistati come l'incidente in materia di sicurezza più frequente sebbene nel settore finanziario la maggior parte dei dirigenti ritenga di essere altamente vulnerabile al terrorismo.

SERVIZI FINANZIARI

Risposte più frequenti date dagli intervistati .

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 19% punti in più dal 2015

▲ 7% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	**39%**	29%
	Frodi nei processi di vendita, fornitura o approvvigionamento	**32%**	26%
	Furto di PI *(es. Informazioni commerciali confidenziali, pirateria o contraffazione)*	**27%**	16%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti	**38%**	39%
	Ex dipendenti	**34%**	27%
	Management di primo o secondo livello	**32%**	30%
	Venditori/fornitori	**24%**	26%
	Freelance / dipendenti a termine	**22%**	27%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Risk *(sistema di gestione del rischio e risk officer)*	**88%**	78%
	Informazioni *(sicurezza informatica, contromisure tecniche)*	**84%**	82%
	PI *(valutazione del rischio per la proprietà intellettuale e programma di monitoraggio dei marchi)*	**84%**	75%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine esterna	**40%**	36%

Sicurezza informatica

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 4% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	**30%**	24%
	Attacco di phishing a mezzo e-mail	**27%**	26%
	Infezione da virus / worm	**27%**	33%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**28%**	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	**42%**	51%
	Informazioni commerciali confidenziali / R&S / PI	**38%**	40%
	Identità aziendale o dei dipendenti	**38%**	36%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 11% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**34%**	38%
	Rischio politico e geografico	**20%**	22%
	Violenza sul posto di lavoro	**16%**	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	**31%**	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Terrorismo	**21%**	18%
	Violenza sul posto di lavoro	**20%**	27%
	Furto o perdita di PI	**18%**	19%

Quadro generale: sanità, farmaceutica e biotecnologie

FRODI

Gli intervistati operanti nel settore sanità, farmaceutica e biotecnologie hanno fatto registrare un'incidenza delle frodi inferiore rispetto alla media globale. Tuttavia, con quattro intervistati su cinque dichiaratasi vittima di frode negli ultimi 12 mesi, è chiaro che si tratta di un problema rilevante per il settore.

In linea con la maggior parte degli altri settori, i neoassunti sono citati come gli autori più comuni delle frodi, mentre gli agenti e gli intermediari presentano un rischio di coinvolgimento simile a quello registrato in settori come beni di consumo (43%) e trasporti, tempo libero e turismo (35%).

Gli intervistati nel settore della sanità sono risultati i più propensi all'attuazione delle misure antifrode, con oltre il 90% dei partecipanti ad aver adottato misure di natura gestionale, finanziaria, di protezione delle informazioni e di gestione del rischio (nomina di un risk officer e implementazione di un RMS). Per il rilevamento delle frodi in questo settore, i whistleblower svolgono un ruolo fondamentale, essendo stati responsabili dell'accertamento del 63% del totale degli incidenti scoperti nell'anno appena trascorso.

SICUREZZA INFORMATICA

Quasi nove partecipanti su dieci (86%) hanno indicato che la loro impresa aveva subito un attacco informatico negli ultimi 12 mesi. In linea con i dati registrati in altri settori, gli attacchi più comuni sono stati le infezioni con virus/worm, il phishing tramite e-mail e le violazioni dei sistemi con conseguente perdita di dati dei clienti o dipendenti, oppure la cancellazione o il danneggiamento dei dati riconducibile a malware o manipolazioni dei sistemi. I cyber-criminali hanno attaccato principalmente i dati di clienti e dipendenti o le loro identità.

SICUREZZA

Quasi i due terzi (65%) degli intervistati operanti nel mondo della sanità sono stati esposti a rischi per la sicurezza negli ultimi 12 mesi: il caso più frequente è il rischio ambientale, con un dato di 8 punti più alto rispetto alla media globale. Anche i rischi di natura geografica e politica sono stati riportati in modo più frequente rispetto alla media, ma la minaccia rappresentata dalla violenza sul posto di lavoro è ancora percepita come il fattore di massima vulnerabilità dai partecipanti.

È interessante notare che in questo settore gli autori più comuni di incidenti legati alla sicurezza sono i dipendenti a termine e i freelance, al contrario di quanto avviene nella maggioranza degli altri settori dove i colpevoli sono individuati perlopiù fra gli ex dipendenti.

SANITÀ, FARMACEUTICA E BIOTECNOLOGIE

Risposte più frequenti date dagli intervistati.

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 11% punti in più dal 2015

▼ 2% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Frodi nei processi di vendita, fornitura o approvvigionamento	37%	26%
	Furto di beni materiali o scorte	31%	29%
	Appropriazione indebita di fondi societari	27%	18%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti	44%	39%
	Agenti e/o intermediari	37%	27%
	Management di primo o secondo livello	34%	30%
	Ex dipendenti	29%	27%
	Partner di joint venture	27%	23%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Finanziaria *(controlli finanziari, accertamento delle frodi, indagini interne o esterne, politiche antiriciclaggio)*	94%	77%
	Informazioni *(sicurezza informatica, contromisure tecniche)*	92%	82%
	Gestione *(controlli dall'alto, incentivi, supervisione esterna come le commissioni d'indagine)*	92%	74%
	Rischio *(sistema di gestione del rischio e risk officer)*	92%	78%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	63%	44%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 1% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	45%	33%
	Attacco di phishing a mezzo e-mail	35%	26%
	Violazione dei sistemi risultante in perdite di dati dei clienti o dei dipendenti	29%	23%
	Cancellazione o danneggiamento dei dati causato da malware o manipolazioni del sistema	29%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	20%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	48%	51%
	Dati dei dipendenti	48%	40%
	Identità aziendale o dei dipendenti	45%	36%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 3% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Rischio ambientale	35%	27%
	Furto o perdita di PI	31%	38%
	Rischio politico e geografico	27%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	15%	16%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	35%	27%
	Terrorismo	25%	18%
	Furto o perdita di PI	20%	19%
	Rischio ambientale	20%	20%

Quadro generale: industria manufatturiera

FRODI

La frode è un problema che colpisce pressoché la totalità delle aziende manifatturiere. Il settore ha fatto registrare le incidenze più elevate di frodi nel 2015 e la tendenza si conferma anche per il 2016, con un aumento di 7 punti percentuali rispetto all'ultima indagine. Ciò significa che quasi 9 su 10 intervistati nel settore manifatturiero hanno subito almeno un tipo di frode nel corso dell'anno passato.

I partecipanti di questo settore sono stati colpiti in particolare da furti, perdite o attacchi alle informazioni; a pari merito con gli intervistati attivi nel settore tecnologia, media e telecomunicazioni, in questo ambito sono risultati secondi solo a chi opera nel settore dei beni di consumo. Gli intervistati operanti nel settore manifatturiero hanno subito in maniera maggiore le violazioni delle norme o in materia di compliance rispetto a quelli di qualsiasi altro settore.

In materia di prevenzione e accertamento delle frodi, il dato relativo agli intervistati del settore manifatturiero che hanno dichiarato di aver già adottato misure antifrode risulta essere il più elevato rispetto agli altri settori. Mentre negli altri settori i whistleblower hanno un ruolo fondamentale, gli intervistati operanti nel manifatturiero hanno scoperto poco più della metà delle frodi attraverso un'indagine interna.

CYBER SECURITY

Le aziende manifatturiere sono state duramente colpite dagli attacchi informatici e dalla perdita, dal furto o dagli attacchi alle informazioni. La quasi totalità degli intervistati nel settore manifatturiero (91%) ha subito almeno un incidente nel corso dell'anno appena trascorso. Anche se l'attacco più comune resta quello delle infezioni da virus o worm, come nella maggior parte dei settori, gli intervistati operanti nel manifatturiero hanno fatto registrare un tasso particolarmente elevato per le violazioni dei sistemi con conseguente perdita di proprietà intellettuale, ricerca e sviluppo o informazioni commerciali confidenziali.

Segreti commerciali, R&S e PI sono stati menzionati come bersaglio degli attacchi da poco più della metà (52%) degli intervistati, mentre il primato spetta ai dati dei clienti (riportato dal 63% sul totale dei partecipanti).

Un dato insolito è rappresentato dalla responsabilità degli incidenti informatici attribuita in massima parte a un agente o un intermediario, autori in quasi un quarto (23%) di tutti i casi. In genere, per la maggior parte dei settori sono gli ex dipendenti a macchiarsi di reati di natura informatica, fatta eccezione per il settore tecnologia, media e telecomunicazioni.

SICUREZZA

Gli incidenti di sicurezza sono molto diffusi anche in questo settore, con oltre i quattro quinti (81%) degli intervistati che citano almeno un tipo di incidente di sicurezza subito nel corso dell'anno passato. Si tratta del dato più elevato riscontrato in tutti i settori. Il tipo più comune di incidente in materia di sicurezza è stato il furto fisico di proprietà intellettuale (PI).

Si tratta dell'unico settore in cui i concorrenti sono indicati come responsabili della maggioranza degli incidenti in materia di sicurezza, da quasi un quarto (24%) degli intervistati.

Anche se la principale minaccia per le aziende manifatturiere è relativa alle informazioni e alla PI, gli intervistati hanno risposto di sentirsi estremamente vulnerabili ai rischi ambientali e alla violenza sul lavoro, in misura maggiore rispetto a furti o perdite di PI.

INDUSTRIA MANIFATTURIERA

Risposte più frequenti date dagli intervistati

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 7% punti in più rispetto al 2015

▲ 7% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	30%	24%
	Violazioni regolamentari o di compliance	30%	21%
	Furto di PI *(es. Informazioni commerciali confidenziali, pirateria o contraffazione)*	26%	16%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti	39%	39%
	Freelance / dipendenti a termine	37%	27%
	Management di primo o secondo livello	33%	30%
	Ex dipendenti	33%	27%
	Venditori/fornitori	33%	26%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Gestione *(controlli dall'alto, incentivi, supervisione esterna come le commissioni d'indagine)*	88%	74%
	Informazioni *(sicurezza informatica, contromisure tecniche)*	86%	82%
	Personale *(formazione, canali per whistleblower)*	79%	74%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine interna	51%	39%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 6% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	39%	33%
	Violazione dei sistemi risultante in perdita di informazioni commerciali confidenziali/ PI / R&S	35%	19%
	Attacco di phishing a mezzo e-mail	35%	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Agenti e/o intermediari	23%	13%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	63%	51%
	Informazioni commerciali confidenziali/ R&S / PI	52%	40%
	Dati dei dipendenti	44%	40%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 13% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	56%	38%
	Rischio ambientale	28%	27%
	Violenza sul posto di lavoro	26%	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Concorrenti	24%	12%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Rischio ambientale	28%	20%
	Violenza sul posto di lavoro	21%	27%
	Furto o perdita di PI	21%	19%

Il contenimento del rischio nella produzione globalizzata

DI BRIAN WEIHS, NICOLE LAMB-HALE E BRIAN SPERLING

Il rischio di subire una frode aumenta esponenzialmente quando le aziende si affidano a soluzioni come l'off-shore e l'outsourcing, o trasferiscono in altro modo la loro produzione nei mercati emergenti. Per mitigare le frodi, è necessario adottare un insieme di strumenti e strategie consolidate, tra cui due diligence, auditing e monitoraggio estensivi di partner e società controllate, nonché lo sviluppo di misure antifrode a tutti i livelli dell'impresa.

A causa della notevole crescita della classe media in molti mercati emergenti, le imprese attive nel settore manifatturiero devono essere presenti anche sul mercato locale per restare competitive. Tra i fattori che rendono l'espansione un imperativo per le imprese del settore, si annoverano il fascino esercitato da costi di produzione inferiori, i vantaggi offerti dai centri manifatturieri specializzati presenti in certe aree geografiche e la vicinanza alle filiere di distribuzione globali dei clienti. Sfortunatamente, tale espansione ha reso il settore manifatturiero in assoluto il più vulnerabile, come evidenziato dall'indagine Global Fraud and Risk di Kroll, dalla quale emerge che il 91% degli intervistati del settore aveva subito frodi negli ultimi 12 mesi, l'incidenza più elevata registrata tra tutti i settori presi in esame.

Uno dei rischi principali del settore consiste nella perdita di proprietà intellettuale (PI). Per fare un esempio legato a uno dei casi di alto profilo gestiti da Kroll, un'industria tessile venne a conoscenza del fatto che i propri prodotti originali, invece delle merci contraffatte, erano venduti attraverso filiere di distribuzione non autorizzate a un prezzo di gran lunga inferiore a quello di mercato. I metodi tradizionali di accertamento e verifica delle frodi, come per esempio le procedure di controllo e le valutazioni di altro tipo condotte in azienda, si sono rivelate inadeguate nell'identificare l'origine delle merci in questione.

L'indagine condotta da Kroll ha rivelato che il fornitore asiatico della società tessile stava agendo scorrettamente sulla sovrapproduzione della fabbrica e sulle merci di qualità inferiore (le "seconde scelte"). Invece di essere smaltite secondo le norme, le merci prodotte in eccesso e le seconde scelte venivano dirottate dai dirigenti e vendute sul "mercato grigio".

Per citare un altro caso, le magliette utilizzate all'interno di una grande competizione sportiva erano state contraffatte in Cina. La qualità delle magliette contraffatte le rendeva indistinguibili dal prodotto originale; sulle

BRIAN WEIHS
Brian Weihs è Managing Director della sezione Investigations and Disputes di Kroll e dirige la filiale messicana della società. Con oltre 20 anni di esperienza nella consulenza alla clientela su questioni complesse in diversi settori, Brian è un punto di riferimento per le indagini interne alle aziende, la governance e la compliance aziendale, la gestione delle crisi e il ripristino della reputazione. Ha anche diretto progetti di gestione del rischio e indagini in tutta l'America Latina.

NICOLE LAMB-HALE
Nicole Y. Lamb-Hale ricopre il ruolo di Managing Director nella sezione Investigations and Disputes presso la sede di Washington D.C. Di Kroll. Nicole svolge compiti di livello dirigenziale da oltre venti anni e offre un punto di vista unico sulle questioni commerciali e di compliance di livello mondiale, derivante dalla sua vasta esperienza nel settore pubblico e nel privato. Oltre a ricoprire il ruolo di Assistant Secretary e Deputy General Counsel presso il Dipartimento del Commercio degli Stati Uniti, Nicole vanta una carriera brillante come consulente strategico e avvocato presso i più rinomati studi legali e di consulenza statunitensi.

BRIAN SPERLING
Brian Sperling è membro associato della sezione Investigations and Disputes presso la sede Kroll di Philadelphia. Grazie alle vaste conoscenze accumulate in settori come l'informatica e l'economia politica internazionale, Brian è un esperto di due diligence, indagini aziendali, indagini patrimoniali e assistenza nei contenziosi.

magliette veniva perfino impresso il codice a barre corrispondente a un rivenditore statunitense. Pertanto l'autorità sportiva non è stata in grado di determinare se fossero magliette contraffatte o eccessi di produzione. L'indagine di Kroll ha aiutato a individuare i responsabili delle frodi e a favorirne la chiusura, mentre il produttore ha adottato tecnologie antifrode brevettate al fine di prevenire ulteriori episodi di contraffazione.

Diventa dunque complesso, per quei produttori che investono in mercati lontani e molto vasti, garantire un'integrazione adeguata e sicura della propria strategia globale. Le indagini di Kroll hanno fatto luce su numerosi esempi di partner o di dirigenti locali che, approfittando della distanza, hanno dirottato sistematicamente la produzione, i clienti e gli utili verso operazioni parallele a proprio vantaggio.

In due casi recenti, verificatisi in un paese dell'America Latina, le indagini condotte da Kroll hanno rivelato che le attività locali di un fornitore per l'industria automobilistica e di una società di imballaggio per beni di consumo erano praticamente invisibili alle rispettive sedi centrali. Queste attività erano così ben nascoste al management che le sedi locali potevano operare a esclusivo beneficio dei propri interessi, generando notevoli responsabilità giuridiche e reputazionali alle proprie multinazionali di riferimento. Solo attraverso una comprensione completa di queste reti parallele, le multinazionali sono state in grado di riprendere il controllo dell proprie attività in loco ed evitare ulteriori perdite sui profitti e problemi di responsabilità giuridica.

In che modo le imprese possono cogliere le opportunità offerte da nuovi mercati e contenere la propria esposizione alle frodi?

1 Prima di stabilire relazioni con partner e terze parti in un dato paese, è opportuno condurre analisi di due diligence relative - a titolo indicativo e non limitativo - alla reputazione di persone e imprese, agli eventuali precedenti e alle pratiche commerciali. Questi risultati (oltre alle parti interessate) dovrebbero essere monitorati sulla base di un piano prestabilito.

2 Quando si intende entrare in una joint venture o acquisire un'impresa nel settore manifatturiero, non basta informarsi sul partner o sull'impresa: devono essere analizzati anche i punti di forza (e i rischi) delle loro filiere produttive e delle loro reti relazionali. Diventa dunque determinante per il successo dell'operazione, la mappatura delle esigenze fondamentali di business e di ciò che sarà necessario cambiare al momento dell'insediamento.

3 Quando si conduce la valutazione o la gestione dei rischi nella "catena di valore" di un'industria, non bisogna limitarsi alle frodi e alla corruzione, ma indagare anche sugli altri aspetti legati alla compliance. Per fare un esempio, il lavoro (lavoro minorile, schiavitù moderna, condizioni di lavoro inaccettabili) e le questioni i cui effetti ricadono sulla comunità e sull'ambiente. Inoltre è opportuno esaminare le attività dell'impresa e quelle dei suoi fornitori.

4 Una volta firmato il contratto, bisogna assicurarsi che le migliori pratiche e le strutture di controllo stabilite dagli standard mondiali del settore siano integrate nelle attività locali di recente acquisizione, facendo sì che il partner o il personale locale ne comprendano il ruolo fondamentale all'interno della strategia globale dell'azienda.

5 Bisogna condurre verifiche frequenti e dettagliate sulle operazioni all'estero per garantire la compliance alle leggi in vigore. Le aree di indagine dovrebbero includere, a titolo indicativo e non limitativo, la compliance con le norme anticorruzione e antiriciclaggio, considerando anche le eventuali sanzioni.

6 È necessario identificare i punti vulnerabili nella protezione della proprietà intellettuale e introdurre misure appropriate per mettere in sicurezza il patrimonio prima di subire un'eventuale perdita.

Queste strategie aiuteranno a massimizzare le opportunità per le industrie manifatturiere nei mercati esteri e ridurre significativamente l'impatto delle frodi sul rischio d'impresa.

Quadro generale: Risorse naturali

FRODI

In misura simile a quanto avviene nella maggior parte degli altri settori, gli intervistati operanti nel settore delle risorse naturali hanno riscontrato un aumento dei casi di frode nell'anno appena trascorso. Quattro intervistati su cinque dichiarano di essere stati vittime di frodi.

Si tratta dell'unico settore in cui il riciclaggio di denaro occupa la classifica dei tre rischi più comuni. Difatti il riciclaggio è stata la frode subita più di frequente dagli intervistati operanti nel settore delle risorse naturali nel 2016, insieme alle frodi legate alla vendita, alla fornitura e all'approvvigionamento.

Mentre nella quasi totalità degli altri settori i neoassunti sono stati identificati come responsabili della maggioranza delle frodi, per gli intervistati che operano nel settore delle risorse naturali, il rischio maggiore è rappresentato da freelance e dipendenti a termine. Anche i casi di frode imputabili agli organi di controllo si attestano su un valore doppio rispetto alla media globale.

Secondo i dirigenti operanti nel settore delle risorse naturali, la metà dei casi di frode è stata scoperta grazie al contributo di un whistleblower.

CYBER SECURITY

Gli intervistati attivi nel settore delle risorse naturali hanno fatto registrare un'incidenza superiore alla media degli attacchi informatici, con quasi nove dirigenti su 10 (86%) che ha riportato di aver subito un incidente negli ultimi 12 mesi. In linea con i dati raccolti negli altri settori, gli attacchi informatici più comuni sono le infezioni da virus o worm. Tre intervistati su dieci operanti nel settore delle risorse naturali hanno subito la perdita di apparecchiature contenenti dati sensibili, un valore quasi doppio rispetto a quello registrato in altri settori. Gli obiettivi più frequenti degli attacchi sono i dati dei clienti e dei dipendenti, a pari merito con i beni materiali o il denaro.

SICUREZZA

L'incidente in materia di sicurezza segnalato più di frequente dagli intervistati del settore delle risorse naturali negli ultimi 12 mesi è stato il furto o la perdita di proprietà intellettuale. Nella maggior parte dei casi, gli autori sono stati identificati in dipendenti a tempo indeterminato.

RISORSE NATURALI

Risposte più frequenti date daigli intervistati

Frodi

80 Percentuale di intervistati vittime di frodi negli ultimi 12 mesi.

▲ 3% punti in più dal 2015

▼ 2% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Frodi nei processi di vendita, fornitura o approvvigionamento	30%	26%
	Riciclaggio di denaro	30%	15%
	Conflitto di interessi del management	28%	21%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	35%	27%
	Neoassunti	30%	39%
	Ex dipendenti	30%	27%
	Partner di joint venture	30%	23%
	Management di primo o secondo livello	28%	30%
	Organi di controllo	28%	14%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	80%	82%
	PI *(valutazione del rischio per la proprietà intellettuale e programma di monitoraggio dei marchi)*	80%	75%
	Finanziaria *(controlli finanziari, accertamento delle frodi, indagini interne o esterne, politiche antiriciclaggio)*	78%	77%
	Partner, clienti e fornitori *(due diligence)*	78%	77%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	50%	44%

Cyber Security

86 Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 1% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	36%	33%
	Perdita di supporti contenenti dati sensibili	30%	17%
	Violazione dei sistemi risultante in perdite di dati dei clienti o dei dipendenti	24%	23%
	Violazione dei sistemi risultante in perdita di informazioni commerciali confidenziali/ PI / R&S	24%	17%
	Cancellazione dei dati premeditata da parte di risorse interne	24%	19%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	19%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei dipendenti	58%	40%
	Dati dei clienti	53%	51%
	Beni materiali/denaro	47%	38%

Sicurezza

70 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 2% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	40%	38%
	Rischio ambientale	38%	27%
	Violenza sul posto di lavoro	36%	23%
AUTORI PIÙ COMUNI	Dipendenti a tempo indeterminato dell'impresa	26%	17%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	36%	27%
	Rischio ambientale	26%	20%
	Furto o perdita di PI	24%	19%

Quadro generale: servizi professionali

FRODI

Una maggioranza significativa (84%) degli intervistati operanti nelle aziende che offrono servizi professionali ha dichiarato di aver subito casi di frode negli ultimi 12 mesi. Insieme agli intervistati attivi nel settore manifatturiero, questo settore ha conosciuto l'incremento più consistente nel corso dell'ultimo anno, con un aumento di 12 punti percentuali rispetto al 2015. I neoassunti sono stati identificati come i maggiori responsabili delle frodi, mentre i manager di primo e secondo livello sono risultati coinvolti in un minor numero di casi rispetto ad altri settori.

Per quanto riguarda l'accertamento e la prevenzione delle frodi, la maggioranza delle aziende che offrono servizi professionali (82%) ha implementato processi di due diligence per partner, clienti e fornitori. Dati quasi equivalenti (80%) sono stati riportati per la nomina di un risk officer e l'implementazione di un sistema di gestione del rischio.

Come avviene nella maggioranza degli altri settori di attività, i whistleblower hanno fatto luce sulla maggior parte dei casi di frode nel corso dell'anno passato, ma anche il management ha fatto la sua parte. Più di un terzo (37%) dei casi di frode è stato scoperto dagli alti dirigenti, mentre in altri settori questo dato si attesta al 32%.

CYBER SECURITY

Nel settore dei servizi professionali, la cyber security resta sicuramente una delle preoccupazioni più consistenti, con oltre quattro intervistati su cinque (84%) che riportano almeno un caso di attacco informatico subito dall'azienda, un dato in linea con la media globale. Il tipo, la frequenza, gli obiettivi e i responsabili degli attacchi informatici nel settore dei servizi professionali sono decisamente in linea con le tendenze degli altri settori. Tuttavia, gli attacchi di tipo denial-of-service (DoS) sono avvenuti con maggior frequenza, mentre le informazioni commerciali confidenziali, di ricerca e sviluppo o proprietà intellettuale sono state oggetto di attacchi in misura minore rispetto ad altri settori.

SICUREZZA

I rischi in materia di sicurezza risultano essere meno diffusi tra le aziende che offrono servizi professionali, con un'incidenza inferiore di 5 percentuali rispetto alla media negli ultimi 12 mesi. In merito agli incidenti riportati, gli ex dipendenti sono stati identificati come la categoria di autori più diffusa, mentre la violazione più frequente è il furto di proprietà intellettuale (PI).

Un intervistato su cinque (20%) inoltre ha dichiarato il verificarsi di un episodio di violenza sul posto di lavoro: questo dato si riflette nella percezione del rischio al quale i dirigenti si ritengono più vulnerabili, visto che più di un quarto (27%) dei dirigenti menzionava proprio questo tipo di minaccia fisica.

D'altro canto, più di un terzo (35%) di loro ha riportato di aver subito un furto o una perdita di PI, mentre solo uno su dieci ha dichiarato di sentirsi molto vulnerabile a una minaccia di questo tipo.

SERVIZI PROFESSIONALI

Risposte più frequenti date dagli intervistati

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 12% punti in più dal 2015

▲ 2% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Conflitto di interessi del management	29%	21%
	Furto di beni materiali o scorte	29%	29%
	Furto, perdita o attacchi alle informazioni *(controlli sui precedenti del personale)*	20%	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti	35%	39%
	Freelance / dipendenti a termine	28%	27%
	Ex dipendenti	26%	27%
	Management di primo o secondo livello	23%	30%
	Clienti	21%	19%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Partner, clienti e fornitori *(due diligence)*	82%	77%
	Rischio *(sistema di gestione del rischio e risk officer)*	80%	78%
	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	78%	79%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	42%	44%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▼ 1% punti sotto la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	35%	33%
	Attacco Denial of Service (DoS)	20%	14%
	Cancellazione o danneggiamento dei dati causato da malware o manipolazioni del sistema	20%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	23%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	53%	51%
	Informazioni commerciali confidenziali / R&S / PI	30%	40%
	Identità aziendale o dei dipendenti	28%	36%
	Beni materiali/denaro	28%	38%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▼ 5% punti sotto la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	35%	38%
	Rischio ambientale	22%	27%
	Violenza sul posto di lavoro	20%	23%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	38%	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	27%	27%
	Terrorismo	14%	18%
	Furto o perdita di PI	10%	19%
	Rischio ambientale	10%	20%

Quadro generale: vendita al dettaglio, all'ingrosso e distribuzione

FRODI

Gli intervistati nel settore vendita al dettaglio, all'ingrosso e distribuzione hanno registrato un leggero aumento (4%) dei casi di frode nel corso degli ultimi 12 mesi, innalzando il numero dei soggetti di vittime di frode all'83%. Il furto di beni materiali o scorte risulta essere il tipo più comune, mentre l'appropriazione indebita dei fondi societari è riportata in maniera significativamente più frequente rispetto agli altri settori. Si tratta dell'unico settore nel quale l'appropriazione indebita dei fondi societari si colloca tra i due tipi più comuni di frode.

In linea con i dati raccolti negli altri settori di attività, i neoassunti sono indicati come i principali responsabili. Anche i clienti sono inclusi nell'elenco dei cinque autori di frodi più comuni, risultando coinvolti in più di un quarto (26%) del totale dei casi.

Gli intervistati operanti nella vendita al dettaglio, all'ingrosso e nella distribuzione hanno riferito di aver adottato misure come controlli sulle finanze, sui beni materiali e sulle informazioni a livelli superiori alla media. Questo settore è in cima alla classifica per l'adozione di misure volte alla sicurezza del proprio patrimonio materiale.

CYBER SECURITY

I dati sugli attacchi informatici raccolti in questo settore risultano leggermente superiori alla media mondiale: gli intervistati dichiarano di averne subito numerosi tipi. Gli attacchi di phishing a mezzo e-mail e i furti di informazioni riservate come dati dei clienti o dei dipendenti da parte del personale interno sono stati i tipi di attacchi informatici riportati più di frequente, con i dati dei clienti noti per essere la categoria di obiettivo più diffusa.

La natura degli autori coinvolti negli attacchi informatici risulta molto eterogenea, rendendo particolarmente complessa la gestione dei rischi informatici in questo settore. Ex dipendenti, freelance e dipendenti a termine e partner di joint venture risultano tutti coinvolti nella stessa misura (13%). Il settore della vendita al dettaglio è l'unico in cui il posizionamento accidentale dei dati sensibili all'interno di un motore di ricerca, con la conseguente indicizzazione, è stata una delle cause più comuni dei casi di attacco informatico.

SICUREZZA

Gli intervistati operanti nella vendita al dettaglio riportano il secondo più alto livello di incidenti in materia di sicurezza dopo il settore manufatturiero. Quasi i quattro quinti (79%) degli intervistati hanno dichiarato di aver subito almeno un tipo di incidente in materia di sicurezza nel corso degli ultimi 12 mesi. La minaccia terroristica risulta più consistente in questo settore rispetto ad altri. È stata riportata come il secondo tipo più comune di rischio in materia di sicurezza, con quasi un terzo (31%) degli intervistati che si ritiene molto vulnerabile.

VENDITA AL DETTAGLIO, ALL'INGROSSO E DISTRIBUZIONE

Risposte più frequenti date dagli intervistati

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 4% punti in più dal 2015

▲ 1% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	**33%**	29%
	Appropriazione indebita di fondi societari	**25%**	18%
	Furto, perdita o attacco alle informazioni *(es. sottrazione di dati)*	**17%**	24%
	Frodi nei processi di vendita, fornitura o approvvigionamento	**17%**	26%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti	**37%**	39%
	Management di primo o secondo livello	**33%**	30%
	Venditori/fornitori	**33%**	26%
	Agenti e/o intermediari	**26%**	27%
	Partner di joint venture	**26%**	23%
	Clienti	**26%**	19%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Beni materiali*(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	**85%**	79%
	Finanziaria *(controlli finanziari, accertamento delle frodi, indagini interne o esterne, politiche antiriciclaggio)*	**83%**	77%
	Informazioni *(sicurezza informatica, contromisure tecniche)*	**83%**	82%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	**42%**	44%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 2% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Attacco di phishing a mezzo e-mail	**25%**	26%
	Furto interno di dati dei clienti o dei dipendenti	**21%**	19%
	Violazione dei sistemi risultante in perdite di dati dei clienti o dei dipendenti	**19%**	23%
	Violazione dei sistemi risultante in perdita di informazioni commerciali confidenziali/ PI / R&S	**19%**	17%
	Attacco Denial of Service (DoS)	**19%**	14%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	**13%**	14%
	Ex dipendenti	**13%**	20%
	Partner di joint venture	**13%**	6%
	Divulgazione accidentale di dati sensibili indicizzati da un motore di ricerca *(es. Google)*	**13%**	10%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	**44%**	51%
	Dati dei dipendenti	**40%**	40%
	Beni materiali/denaro	**36%**	38%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 11% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	**38%**	38%
	Terrorismo	**19%**	15%
	Rischio politico e geografico	**19%**	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	**22%**	16%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Terrorismo	**31%**	18%
	Violenza sul posto di lavoro	**29%**	27%
	Rischio politico e geografico	**19%**	12%

Quadro generale: tecnologia, media e telecomunicazioni

FRODI

Gli intervistati nel settore tecnologia, media e telecomunicazioni (TMT) hanno registrato uno dei valori più bassi in termini di incidenza delle frodi negli ultimi 12 mesi. Si tratta di uno dei due settori - l'altro è ingegneria, costruzioni e infrastrutture - a non aver riportato un aumento di questo fenomeno rispetto all'anno precedente.

Tuttavia, quasi i quattro quinti (79%) degli intervistati si sono dichiarati vittima di almeno un tipo di frode nel periodo in questione.

Il furto di beni materiali o scorte risulta essere il tipo più comune (riportato dal 35% degli intervistati). In seconda posizione troviamo il furto, la perdita o gli attacchi alle informazioni, subiti dal 30% delle aziende operanti nel settore TMT. Si tratta di 6 punti percentuali in più rispetto ai tassi rilevati in tutti gli altri settori. Un altro dato superiore alla media è il conflitto di interessi del management, riportato da un quarto degli intervistati.

Rispetto ad altre aree di attività, gli intervistati operanti nel settore TMT riportano, in media, un numero sensibilmente minore di casi di frode nella vendita, nella fornitura e nell'approvvigionamento (-8%).

Le aziende del settore TMT sono risultate più attive nell'adozione di misure antifrode per proteggere i beni materiali in confronto ali altri settori.

CYBER SECURITY

In controtendenza rispetto al trend globale, gli intervistati hanno dichiarato di essere stati vittime di attacchi informatici in misura minore rispetto alle frodi. È interessante notare, vista la natura delle loro attività, che le percentuali riportate di attacchi informatici, furti e perdite di informazioni sono risultate significativamente più basse rispetto alla media globale (8 punti percentuali in meno).

Il settore TMT è stato l'unico nel quale i freelance e i collaboratori temporanei figurano in cima alla lista degli autori di attacchi informatici, probabilmente a causa dell'impiego più diffuso di dipendenti freelance, in particolare nelle imprese ad alta tecnologia.

SICUREZZA

Il settore TMT si colloca al terzo posto nella classifica degli incidenti in materia di sicurezza nel corso dell'ultimo anno, preceduto soltanto dagli intervistati che operano nel manifatturiero e nella vendita al dettaglio. Quasi tre quarti (72%) dei dirigenti ha dichiarato di aver subito un incidente in materia di sicurezza, mentre quasi la metà di loro è stata vittima di furto o danni alla proprietà intellettuale.

Anche per gli incidenti legati alla sicurezza i responsabili principali sono stati individuati nei freelance e nei dipendenti a termine, con oltre un quarto (27%) del totale degli incidenti subiti dagli intervistati del settore TMT negli ultimi 12 mesi.

TECNOLOGIA, MEDIA E TELECOMUNICAZIONI

Risposte più frequenti date dagli intervistati.

Frodi

79 Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

= pari al 2015

▼ 3% punti sotto la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	35%	29%
	Furto, perdita o attacco alle informazioni	30%	24%
	Conflitto di interessi del management	25%	21%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti	42%	39%
	Management di primo o secondo livello	36%	30%
	Ex dipendenti	27%	27%
	Freelance / dipendenti a termine	22%	27%
	Venditori/fornitori	22%	26%
	Organi di controllo	22%	14%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	82%	79%
	Finanziaria *(controlli finanziari, indagini interne o esterne, politiche antiriciclaggio)*	79%	77%
	Partner, clienti e fornitori *(due diligence)*	79%	77%
	Rischio *(sistema di gestione del rischio e risk officer)*	79%	78%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Indagine interna	40%	39%

Cyber Security

77 Percentuale degli intervistati vittime di attacch informatici negli ultimi 12 mesi.

▼ 8% punti sotto la media globale (85%)

			Media glob.
TIPOOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	37%	33%
	Attacco di phishing a mezzo e-mail	32%	26%
	Cancellazione dei dati o perdita di dati dovute a manipolazioni dei sistemi	23%	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	23%	14%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Beni materiali/denaro	48%	38%
	Informazioni commerciali confidenziali / R&S / PI	43%	40%
	Identità aziendale o dei dipendenti	43%	36%

Sicurezza

72 Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 4% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI IN MATERIA DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	46%	38%
	Rischio ambientale	33%	27%
	Rischio politico e geografico	26%	22%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Freelance / dipendenti a termine	27%	16%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	28%	27%
	Terrorismo	21%	18%
	Rischio ambientale	18%	20%

Quadro generale: turismo, tempo libero e trasporti

FRODI

Con l'85% degli intervistati che riportano attività fraudolente, il settore turismo, tempo libero e trasporti fa registrare un aumento di 10 punti percentuali nel corso degli ultimi 12 mesi, 3 punti in più rispetto alla media globale.

Come avviene per altri settori, i neoassunti sono stati identificati come le categorie di autori più diffuse (responsabili del 39% di tutti i casi di frode), seguiti da agenti e intermediari (35%).

In questo settore si riscontra l'adozione più elevata di tutte le misure antifrode elencate dagli intervistati, un dato secondo solo a quello dei professionisti del settore sanità. Oltre l'80% dei dirigenti ha implementato ognuna delle prime quattro misure elencate nella scheda di riferimento.

CYBER SECURITY

Questa settore conquista, a pari merito con altri, il terzo posto (87%) nella diffusione degli attacchi informatici, perlopiù infezioni da virus e worm. Gli intervistati operanti nel settore dei trasporti hanno subito l'alterazione o la modifica dei dati dei clienti a un tasso quasi doppio rispetto alla media mondiale.

SICUREZZA

Oltre i due terzi (70%) degli intervistati del settore dichiarano di aver subito un incidente in materia di sicurezza negli ultimi 12 mesi, con particolare rilevanza per il furto di proprietà intellettuale (PI). Con un'incidenza del 30%, la violenza sul posto di lavoro si colloca a 7 punti percentuali al di sopra dei livelli medi globali, la cui responsabilità ricade a pari merito tra ex dipendenti o dipendenti a tempo indeterminato.

TURISMO, TEMPO LIBERO E TRASPORTI

Risposte più frequenti date dagli intervistati

Frodi

Percentuale degli intervistati vittime di frodi negli ultimi 12 mesi.

▲ 10% punti in più dal 2015

▲ 3% punti sopra la media globale (82%)

			Media glob.
TIPOLOGIA DELLE FRODI PIÙ COMUNI	Furto di beni materiali o scorte	33%	29%
	Frodi nei processi di vendita, fornitura o approvvigionamento	30%	26%
	Violazioni regolamentari o di compliance	26%	21%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Neoassunti	39%	39%
	Agenti e/o intermediari	35%	27%
	Freelance / dipendenti a termine	30%	27%
	Management di primo o secondo livello	26%	30%
	Partner di joint venture	22%	23%
MISURE ANTIFRODE PIÙ DIFFUSE *Percentuale di intervistati che hanno implementato la misura antifrode.*	Informazioni *(sicurezza dei sistemi informativi, contromisure tecniche)*	89%	82%
	Beni materiali *(sistemi di sicurezza fisica, inventari delle scorte, etichettatura, registro dei beni)*	87%	79%
	Coinvolgimento del consiglio di amministrazione in politiche e procedure di cyber security	85%	75%
	Personale *(controlli sui precedenti)*	85%	74%
	Rischio *(sistema di gestione del rischio e risk officer)*	78%	78%
MEZZI DI ACCERTAMENTO PIÙ COMUNI	Whistleblower interno all'impresa	46%	44%

Cyber Security

Percentuale degli intervistati vittime di attacchi informatici negli ultimi 12 mesi.

▲ 2% punti sopra la media globale (85%)

			Media glob.
TIPOLOGIA DEGLI ATTACCHI INFORMATICI PIÙ COMUNI	Infezione da virus / worm	37%	33%
	Alterazione o modifica dei dati dei clienti	31%	16%
	Cancellazione o perdita di dati dovuti a manipolazioni dei sistemi	30%	24%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Ex dipendenti	19%	20%
CATEGORIE DI OBIETTIVI PIÙ DIFFUSE	Dati dei clienti	51%	51%
	Beni materiali/denaro	51%	38%
	Dati dei dipendenti	45%	40%
	Informazioni commerciali confidenziali / R&S / PI	45%	40%

Sicurezza

Percentuale degli intervistati vittime di incidenti in materia di sicurezza negli ultimi 12 mesi.

▲ 2% punti sopra la media globale (68%)

			Media glob.
TIPOLOGIA DEGLI INCIDENTI DI SICUREZZA PIÙ COMUNI	Furto o perdita di PI	43%	38%
	Violenza sul posto di lavoro	30%	23%
	Rischio ambientale	26%	27%
CATEGORIE DI AUTORI PIÙ DIFFUSE	Dipendenti a tempo indeterminato dell'impresa	24%	17%
	Ex dipendenti	24%	23%
GLI INTERVISTATI SONO PIÙ PROPENSI A SENTIRSI MOLTO VULNERABILI AI SEGUENTI RISCHI IN MATERIA DI SICUREZZA	Violenza sul posto di lavoro	41%	27%
	Rischio ambientale	35%	20%
	Furto o perdita di PI	31%	19%

Nota di chiusura

Ci auguriamo che il nostro report sia stato una lettura utile e ricca di informazioni. Questa panoramica sul mondo degli affari, vista attraverso gli occhi dei vostri colleghi, potrà essere di stimolo per le vostre attività; a prescindere dal fatto che abbia avuto il potere di rassicurarvi o di spingervi a valutare azioni per migliorare, speriamo in ogni caso che sia stata illuminante.

Quando io e il mio co-presidente Tommy Helsby (l'autore dell'introduzione di questo rapporto) abbiamo iniziato a lavorare in Kroll più di 30 anni fa, abbiamo condotto indagini su dipendenti corrotti e su altri malfattori che avevano rubato denaro, informazioni commerciali confidenziali, prodotti e beni aziendali. Alcuni di questi avevano corrotto i funzionari governativi per ottenere appalti, altri avevano accettato tangenti dai fornitori per gli approvvigionamenti interni, per non parlare di chi trafficava prodotti contraffatti. Quelli a cui piaceva rubare in grande - noi li chiamavamo i "carnivori" - cercavano di occultare i loro guadagni illeciti dietro un reticolo inestricabile di società anonime.

Ebbene, i crimini non sono cambiati, ma gli strumenti per compierli non sono più quelli di una volta. L'equivalente odierno dei vecchi assegni contraffatti o delle cartelle sottratte da un cassetto sono le ruberie compiute con mezzi elettronici. Le imprese sono perennemente sotto attacco da parte di hacker e phisher.

Inoltre, le aziende devono affrontare sfide sempre più complesse in uno scenario caratterizzato da globalizzazione e connettività. Gran parte degli illeciti di natura economica nascono dall'opportunità. E i nostri risultati mostrano che alcuni tra gli autori più opportunisti sono dipendenti e altri soggetti interni all'azienda, passati e presenti.

Partendo da questa constatazione, in che modo la vostra azienda può scoraggiare questo tipo di criminalità? Sulla base della nostra esperienza e delle opinioni raccolte tra i dirigenti intervistati, possiamo concludere che i programmi di gestione del rischio che adottano un approccio articolato, agendo su prevenzione, accertamento e riposta, sono una buona soluzione per scoraggiare i truffatori e limitare i potenziali danni.

I miei colleghi che hanno dato il loro contributo a questo report, attraverso i loro articoli di approfondimento, hanno messo a vostra disposizione le migliori pratiche ed esempi reali tratti dalla loro esperienza, mostrando come le imprese possano trarre vantaggi significativi quando integrano e investono risorse in questi ambiti strategici. Sappiamo bene, però, che ognuno di noi vive una situazione a sé. Da 45 anni a questa parte, Kroll è pronta ad aiutare la vostra azienda a indagare su qualsiasi tipo di frode e tenere sotto controllo i rischi.

DANIEL KARSON
Co-Presidente, Investigations and Disputes di Kroll

Rivolgersi a Kroll

Per informazioni sui servizi di Kroll, si prega di contattare i responsabili di uno dei nostri uffici di seguito indicati o visitare il sito www.kroll.com

SEDE CENTRALE

600 Third Avenue, New York, NY 10016

Rappresentanti nel mondo

AMERICA DEL NORD

Bill Nugent
Philadelphia
T +1 215.568.8090
bnugent@kroll.com

EUROPA, MEDIO ORIENTE E AFRICA

Tom Everett-Heath
London
T +44 20 7029.5067
teverettheath@kroll.com

ASIA

Tadashi Kageyama
Singapore
T +65 6645.4959
tkageyama@kroll.com

AMERICA LATINA

Recaredo Romero
Bogotá
T +57 1 742.5556
rromero@kroll.com

Uffici locali

AMERICA DEL NORD

Dan Karson
New York
T +1 212.833.3266
dkarson@kroll.com

Daniel Linskey
Boston
T +1 617. 210.7471
daniel.linskey@kroll.com

Peter Turecek
Chicago
T +1 312.765.8753
pturecek@kroll.com

Erik Rasmussen
Los Angeles
T +1 213.443.1128
erik.rasmussen@kroll.com

Mark Ehlers
Philadelphia
T +1 215.568.8305
mehlers@kroll.com

Betsy Blumenthal
San Francisco
T +1 415.743.4825
bblument@kroll.com

Peter McFarlane
Toronto
T +1 416.813.4401
pmcfarlane@kroll.com

EUROPA, MEDIO ORIENTE E AFRICA

Zoë Newman
London
T +44 20 7029.5154
znewman@kroll.com

Yaser Dajani
Dubai
T +971 4 4496714
ydajani@kroll.com

Marcelo Correia
Madrid
T +34 91 274.79.74
marcelo.correia@kroll.com

Marianna Vintiadis
Milan
T +39 02 86998088
mvintiadis@kroll.com

Alex Volcic
Moscow
T +7 495 9692898
avolcic@kroll.com

Béchir Mana
Paris
T +33 1 42678146
bmana@kroll.com

ASIA

Colum Bancroft
Hong Kong
T +852 2884.7788
cbancroft@kroll.com

Violet Ho
Beijing/Shanghai
T +86 10 5964.7600
vho@kroll.com

Reshmi Khurana
Mumbai
T +91 22 6724.0504
rkhurana@kroll.com

Richard Dailly
Singapore
T +65 6645.4521
rdailly@kroll.com

Omer Erginsoy
Singapore
T +65 6645.4530
oerginsoy@kroll.com

Naoko Murasaki
Tokyo
T +81 3 3509.7103
nmurasaki@kroll.com

AMERICA LATINA

James Faulkner
Miami
T +1 305.789.7130
jfaulkner@kroll.com

Recaredo Romero
Bogotá
T +57 1 742.5556
rromero@kroll.com

Brian Weihs
Mexico City
T +52 55 5279.7250
bweihs@kroll.com

Juan Cruz Amirante
Buenos Aires
T +54 11 4706.6000
jcamirante@kroll.com

Glen Harloff
São Paulo
T +55 11 3897.0892
gharloff@kroll.com

kroll.com