MARSH

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

M. | MARSH MAGAZINE

Numero 23 — Giugno 2016

AMBIENTE, TECNOLOGIA E SANITÀ:

mai come ora è necessario che la resilienza diventi un imperativo.

MARSH | MERCER | GUY CARPENTER | OLIVER WYMAN | MARSH & McLENNAN COMPANIES

INDICE

4 *Più muri, più caldo, meno acqua: un mondo sempre più a rischio*

26 *Sanità pubblica italiana: in media 4 sinistri al giorno negli ultimi 10 anni*

2 *Insights on the market*
Marsh Insurance Market Report 2016

4 *Cover story*
Più muri, più caldo, meno acqua: un mondo sempre più a rischio

10 *International topic*
Mappa del Rischio Politico 2016: terrorismo e conflitti mettono alla prova gli equilibri internazionali

14 Responsabilità ambientale: dalla Direttiva UE a oggi, come è cambiata in pochi anni la percezione da parte delle aziende

15 Il virus Zika mette sotto pressione la sicurezza sanitaria internazionale

16 Navi commerciali sempre più grandi e dati batimetrici insufficienti mettono a rischio la navigazione commerciale e civile

18 Rischio Cyber: l'Unione Europea detta nuove regole sulla gestione dei dati

20 *Brink*
Non ignorare le minacce cyber causate dagli insider

22 *Mercer*
7 aziende su 10 scelgono candidati interni per i ruoli critici ma un dipendente su 3 pensa di lasciare la propria azienda nei prossimi 12 mesi

24 *Oliver Wyman*
Hacker e crisi energetica: una realtà possibile?

26 *Local focus*
Sanità Pubblica italiana: in media 4 sinistri al giorno negli ultimi 10 anni

29 *Local topic*
Le aziende italiane "promuovono" le novità sul Welfare aziendale

30 La copertura trade credit: mai così utilizzata

31 La protezione della proprietà intellettuale come leva strategica per una crescita sostenibile

32 Ecoreati puniti anche con 20 anni di reclusione

34 Un punto a favore dell'ambiente

35 *External Contributor*
Proprietà intellettuale: la priorità numero uno è conoscere gli asset di cui dispone l'azienda

INSIGHTS ON THE MARKET

MARSH INSURANCE MARKET REPORT 2016

Cybersecurity, rischio politico e terrorismo sono le principali preoccupazioni delle aziende.

L'ampia capacità assuntiva e una forte competizione fra gli assicuratori contribuiscono a mantenere una situazione favorevole per i buyer di assicurazioni, in particolare per quelle aziende con portafogli attraenti e una buona statistica sinistri.

Questa è la situazione fotografata dall'Insurance Market Report 2016 di Marsh per la regione Europa, Medio Oriente e Africa, anche se per il futuro vanno monitorati alcuni sviluppi del settore, insieme alle ultime trimestrali, cambiamenti nella leadership, ri-sottoscrizione di molte compagnie. Inoltre alcune dinamiche macro come le evoluzioni economiche, politiche, normative, tecnologiche e ambientali continueranno a influenzare il mercato nell'arco del 2016.

Fra i principali risultati del report:

- Il Cyber risk sembra essere uno dei temi più rilevanti per i CEO della regione EMEA, e questo si riflette su un significativo incremento di richieste di approfondimento

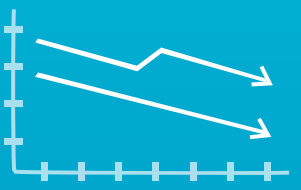
sul ruolo che le coperture assicurative possono avere nella gestione di questo rischio;

- alla luce dei recenti attacchi terroristici e dei crescenti flussi migratori, il terrorismo e i rischi connessi alla violenza politica sono spesso al centro delle riflessioni di molte organizzazioni;
- i tassi relativi alla copertura D&O sono rimasti stabili o sono diminuiti, registrando ribassi medi del 10%, ma anche con flessioni che hanno raggiunto il 20%;
- i premi relativi al Motor sono aumentati del 10% in 11 paesi e di oltre il 10% in Turchia e Romania. Questi aumenti sono dovuti alle perdite consistenti legate alla RCA e alle nuove normative che stanno aumentando i costi di sottoscrizione;
- i numeri delle Captive hanno registrato un aumento nel 2015, confermando la crescita significativa che ha caratterizzato gli ultimi 20 anni, nonostante il mercato assicurativo soft e gli ampi livelli di capacità.

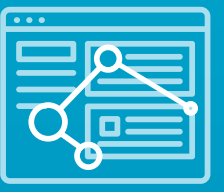
FOCUS SULL'ITALIA

Anche il mercato italiano rimane soft e non si prospettano modifiche a breve termine.

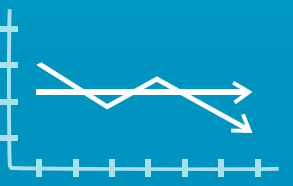
La capacità di sottoscrizione potrebbe diminuire a causa della fusione di ACE e Chubb. In generale i tassi delle principali coperture sono allineati alle tendenze dell'area EMEA, fatta eccezione per il Motor, dove si registra una flessione del 10%.



In calo i tassi delle coperture assicurative D&O, anche in Italia



Il Cyber Risk si conferma uno dei principali rischi da gestire



I tassi D&O sono stabili o in calo nella maggior parte dei Paesi dell'area EMEA

Il Motor registra in Italia una flessione del 10% dei tassi assicurativi, in controtendenza rispetto all'area EMEA

https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/EMEA Insurance Market Report 2016-02-2016.pdf

Tecnologia e quarta rivoluzione industriale, cittadini sempre più esautorati, sicurezza alimentare a rischio e pericolo pandemie: gli highlight del Global Risks 2016.

PIÙ MURI, PIÙ CALDO, MENO ACQUA: UN MONDO SEMPRE PIÙ A RISCHIO

Il fallimento delle politiche di mitigazione dei cambiamenti climatici e i flussi migratori sono i rischi globali che preoccupano di più per il loro potenziale impatto e per l'elevata probabilità di accadimento, secondo l'undicesima edizione del Global Risks, che mai come quest'anno sembra parlare di attualità.

Il Global Risks 2016, il report realizzato dal World Economic Forum, in collaborazione con alcuni partner strategici tra cui Marsh & McLennan Companies che ogni anno propone la classifica dei rischi globali a più alta probabilità e impatto, segna una forte differenza rispetto al passato, perché viene diffuso in un momento storico in cui è ormai inequivocabile il tributo pagato ai rischi, indipendentemente dalla loro matrice economica, politica, sociale, ambientale, o tecnologica.

Per la prima volta il riscaldamento climatico rischia di arrivare al record di 1°C al di sopra della temperatura media annuale del periodo preindustriale; inoltre, stando ai dati dell'UNHCR, il numero di persone costrette a fuggire dai loro paesi ha raggiunto nel 2014 i 59,5 milioni, quasi il 50% in più rispetto al 1940.

Non si tratta di due esempi casuali: secondo i 750 esperti che hanno valutato 29 diversi rischi globali, nel 2016 il fallimento delle politiche di mitigazione dei cambiamenti climatici è al primo posto fra i rischi a più alto impatto seguito da armi di distruzione massa (2° in classifica), crisi idriche (3° in classifica), migrazione involontaria su larga scala (4° in classifica) e forti variazioni del prezzo dell'energia – in aumento e in discesa – (5° in classifica). Mentre in vetta alla classifica dei rischi più probabili vi sono i flussi migratori su larga scala, seguiti dai rischi connessi a eventi meteorologici estremi (2° posto),dal fallimento delle politiche di mitigazione e adattamento dei cambiamenti climatici (3° posto), dai conflitti tra stati con conseguenze regionali – che scende dalla prima alla quarta posizione – , e infine le grandi catastrofi naturali (5° posto).

È la prima volta in 11 anni che il rapporto presenta un panorama di rischi così diversificati: nella top five dei rischi con il maggior potenziale di impatto sono rappresentate ben quattro diverse categorie: ambientale, geopolitica, sociale ed economica. L'unica eccezione è costituita dai rischi tecnologici, nell'ambito dei quali si segnala il rischio di attacchi informatici, all'11° posto sia per probabilità che per impatto.

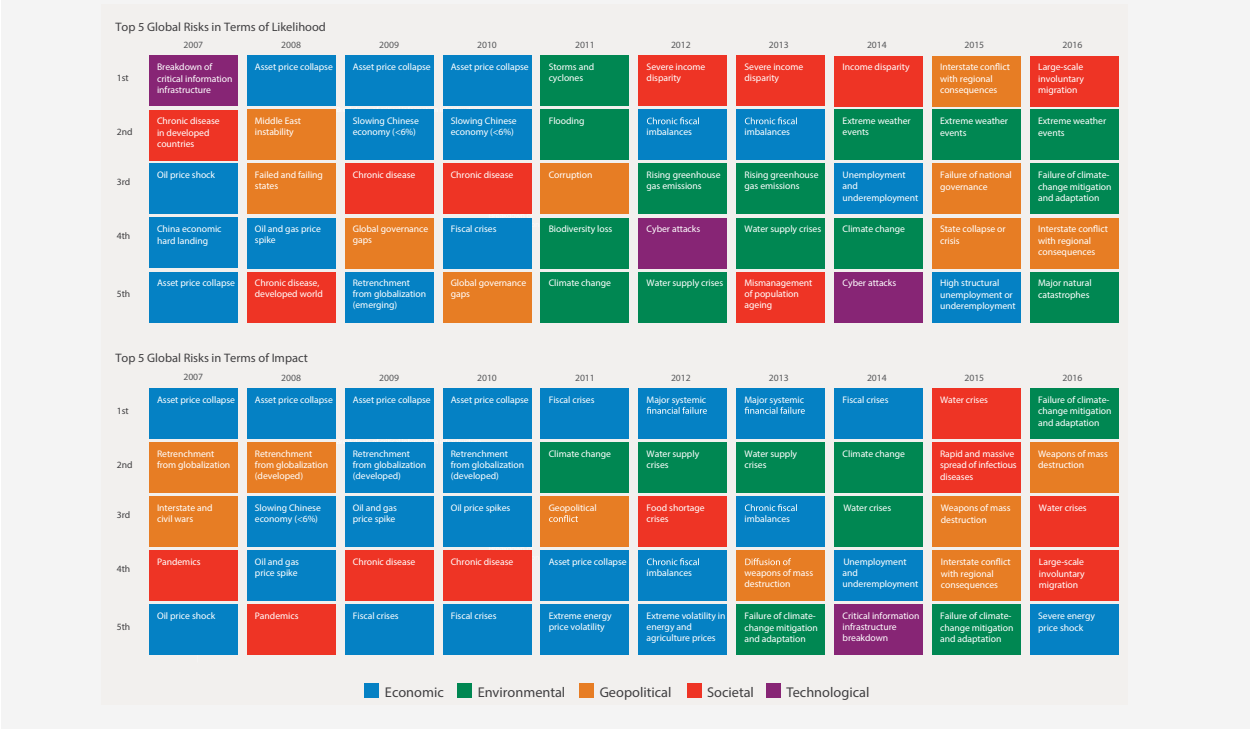
Oltre a misurare la probabilità e il potenziale impatto dei rischi globali, il Global Risks Report 2016 esamina anche le loro interconnessioni reciproche. A tal proposito i dati suggeriscono un maggiore consenso tra gli esperti nell'individuazione di un piccolo numero di rischi chiave che esercitano una grande influenza sugli altri, e in particolare due rischi strettamente interconnessi – profonda instabilità sociale e disoccupazione strutturale o sottoccupazione – rappresentano da soli il 5% di tutte le interconnessioni.

TECNOLOGIA E DIGITALIZZAZIONE STANNO PORTANDO ALLA COSIDDETTA QUARTA RIVOLUZIONE INDUSTRIALE

Un fattore inatteso e dal potenziale forte impatto – un *black swan*, come lo definiscono gli anglofoni – potrebbe essere costituito dai rischi tecnologici.
Se tecnologia e digitalizzazione sono alla base della cosiddetta quarta rivoluzione industriale in termini di sviluppo e opportunità, alcune innovazioni non hanno ancora mostrato completamente la loro potenzialità (cambiamenti in termini lavorativi, disuguaglianza e crescente cyber-dipendenza) e vi sono quindi rischi associati che non sono stati quantificati pienamente dagli esperti.

Un recente studio dimostra come le tecnologie legate ad internet, come ad esempio il mobile Internet, l'Internet delle cose e il cloud saranno la maggiore causa di rottura dei

The Evolving Risks Landscape, 2007–2016
Fonte: World Economic Forum 2007–2016, Global Risks Reports



modelli di business tradizionali e saranno capaci di generare un importante beneficio economico. Tuttavia, l'incapacità di comprendere e di rispondere adeguatamente ai rischi legati alla tecnologia, in primo luogo gli effetti a cascata dei rischi cyber o il danneggiamento di infrastrutture informative critiche, potrebbe avere conseguenze di vasta portata per nazioni, settori economici e aziende. Secondo una stima, i paesi europei che non sapranno reagire in modo adeguato ai cambiamenti tecnologici potrebbero perdere 600 miliardi di euro di valore aggiunto nel corso dei prossimi 10 anni.

Il Global Risks identifica i rischi cyber in quattro macro-categorie. La prima comprende gli **attacchi cyber e gli incidenti ad essi correlati** che, benché entrati nella classifica dei rischi più probabili e a più alto impatto solo negli ultimi due o tre anni, sono balzati in cima alla lista in ben otto paesi tra i quali Stati Uniti, Giappone, Germania, Svizzera e Singapore. I casi di attacchi sono aumentati sia in termini di frequenza sia di portata; inoltre fino ad ora si è trattato di casi isolati, che riguardano per lo più singole organizzazioni o paesi, ma la forte interconnessione e l'interdipendenza dovute alla rete potrebbe in futuro far aumentare le probabilità di un attacco informatico con un potenziale effetto a cascata in tutto "l'ecosistema informatico".

La seconda macro-categoria è rappresentata dallo **scambio di dati tra i paesi e tra organizzazioni**. I dati sono stati definiti "il combustibile del 21° secolo" ed è necessario prevedere la definizione di un quadro giuridico adeguato per realizzare appieno il potenziale della digitalizzazione. L'attuale regime di regolamentazione è fortemente arretrato rispetto alle esigenze e manca la necessaria certezza giuridica in settori come la privacy, l'uso della crittografia o la proprietà intellettuale.

La terza area di rischio legata al cyber riguarda **l'impatto dell'informatizzazione sul mondo del lavoro**. Anche se prevale ancora l'incertezza a riguardo, è innegabile che molte delle attuali tipologie di lavoro diverranno computerizzate. Il Dipartimento del lavoro degli Stati Uniti ha stimato che entro il 2022 il 47% dei lavoratori americani avrà un'alta probabilità di assistere all'automatizzazione del loro lavoro, per esempio in ambito manifatturiero, nella salute e nella diagnostica o nel settore del turismo e dell'accoglienza.

La quarta area di rischio riguarda il fatto che **l'accesso alla tecnologia sta divenendo un elemento socialmente differenziante** e potrebbe esacerbare le differenze tra paesi. Quattro dei sette miliardi di persone che popolano il mondo

non hanno ancora accesso a internet e non avranno gli strumenti per approfittare della forza trainante dello sviluppo tecnologico.

DALLA SICUREZZA INTERNAZIONALE ALLE MINACCE PER LA SOCIETÀ: CITTADINI SEMPRE PIÙ ESAUTORATI, SICUREZZA ALIMENTARE A RISCHIO E DIFFUSIONE GLOBALE DI EPIDEMIE

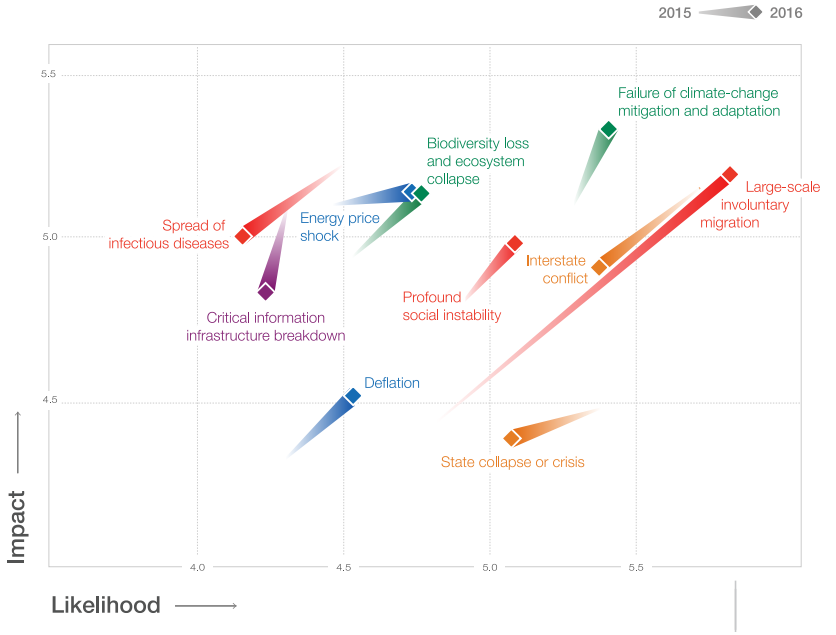
Le minacce alla sicurezza internazionale non provengono solo da terrorismo, armi di distruzione di massa o instabilità degli stati, ma sono anche quelle "interne", che derivano dallo "stato di salute" della società civile. Secondo il Report alcuni studi evidenziano come ci stiamo avvicinando ai livelli di protesta degli anni '80, quando i disordini sociali erano imputabili alla Guerra fredda, all'Apartheid o alle proteste di Piazza Tienanmen. La chiave per creare resilienza è, secondo il rapporto, la stabilità delle società: per questa ragione un ampio capitolo è dedicato all'approfondimento di alcuni scenari di stampo sociale.

Il primo fra questi affronta il fenomeno dell'aumento o diminuzione dei poteri del cittadino. Individui, società civile, gruppi e movimenti, se da un lato sono più connessi e informati, dall'altro si sentono sempre più esclusi dal processo decisionale ed esautorati dalla loro capacità di influenzare le istituzioni. Questo scenario mette in luce l'incombente instabilità sociale causata da interventi repressivi o comportamenti passivi dello stato e del mondo imprenditoriale, che, a loro volta, si sentono insicuri di fronte a una cittadinanza meglio informata, interconnessa ed esigente. Una situazione che potrebbe portare a un'accelerazione della spirale negativa costituita da perdita di fiducia e reazioni sempre più dure da entrambe le parti.

Il secondo scenario è costituito dai rischi legati alla sicurezza alimentare nel contesto del cambiamento climatico. Il Report esamina come i cambiamenti climatici e atmosferici possano compromettere la sicurezza alimentare e la produzione agricola a tutte le latitudini.

I paesi più vulnerabili ai cambiamenti climatici sono spesso quelli che dipendono prevalentemente dalla produttività agricola per sostenere la loro crescita e lo sviluppo economico. Nell'Africa sub-sahariana, per esempio, un aumento di 1,5 ° C delle temperature entro il 2030 potrebbe portare a una perdita del 40% delle aree adatte alla coltivazione del mais. Ma in anni recenti si sono rivelati vulnerabili anche paesi del G20 come l'India, la Russia e gli Stati Uniti (il granaio del mondo) e altri grandi produttori industriali di derrate agricole. I passi da compiere sono numerosi: la sperimentazione di raccolti

The Changing Global Risks Landscape 2015–2016: The 10 Most Changing Global Risks
Fonte: Global Risks Perception Survey 2014 and 2015, World Economic Forum



resistenti al cambiamento climatico, il miglioramento delle reti di distribuzione, nonché i meccanismi finanziari e assicurativi a sostegno delle popolazioni agricole potrebbero contribuire a mitigare gli aspetti socio-economici e pertanto è fondamentale che siano stanziati investimenti ingenti e vi sia un forte impulso alla ricerca. Dopo la crisi di Ebola, il rapporto dedica anche particolare spazio al diffondersi di epidemie a livello globale. L'incremento della popolazione, la rapida urbanizzazione e il crescente flusso transnazionale di merci, persone e animali accentuano il rischio di un'estesa propagazione di malattie infettive e nel contempo una diminuzione della capacità di reagire adeguatamente; tutto ciò in un'epoca di crescente resistenza dei microorganismi ai medicinali attualmente più efficaci, dimostrata dal riemergere di malattie che si pensavano ormai debellate come la febbre dengue, il tifo o la peste.

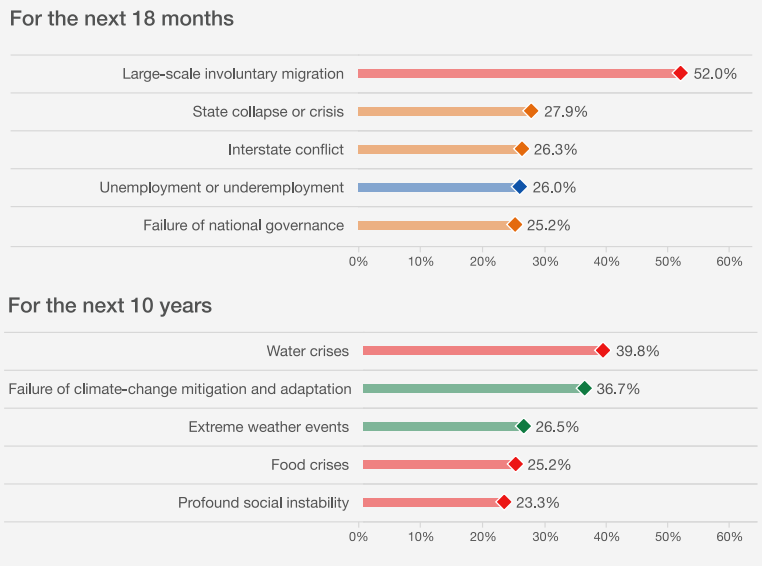
I possibili interventi preventivi e reattivi esistono e vanno da suggerimenti comportamentali, sostenuti ad esempio da campagne di comunicazione ed educazione, alla necessità di investire nella ricerca e sviluppo di strumenti diagnostici, medicinali e vaccini e nell'adeguamento legislativo. Su questo tema, più che mai, è necessario creare spazi di cooperazione interdisciplinare tra pubblico e privato per promuovere la disponibilità e l'analisi dei dati, un'agenda comune per la ricerca, finanziamenti a lungo termine e metodi per promuovere un utilizzo responsabile dei media come parte di un'efficace gestione della comunicazione durante le crisi.

LA CHIAMATA ALLA RESILIENZA

Se il "nuovo status quo" globale presenta un così elevato numero di rischi geopolitici e un'altrettanto forte interconnessione fra loro è evidente come – così conclude il Global Risks – sono sempre di più le parti interessate che necessitano di essere coinvolte in un processo di cambiamento e nella definizione di soluzioni globali. E' infatti dalla comprensione condivisa delle sfide che può partire un vero approccio multistakeholder, l'unico davvero efficace per affrontare i rischi globali e costruire la resilienza. Oltre alla collaborazione fra paesi e organizzazioni sovranazionali, un ruolo sempre più importante sarà quello del settore privato, chiamato a riconoscere le tendenze geopolitiche e a partecipare da protagonista a un vero e proprio "imperativo per la resilienza".

Infine il Report invoca una rinnovata attenzione alla prevenzione e alla preparazione, utilizzando i dati di cui ora possiamo disporre per monitorare lo stato di avanzamento dei fattori di rischio, alla condivisione di informazioni e a stabilire meccanismi di recupero in caso di emergenza. Non si tratta più solo di pensare a misure che possano mitigare i rischi globali, ma di andare oltre la semplice reazione alla minaccia, con un approccio più proattivo. Oltre a lavorare sulla governance dei paesi, sarà necessario quindi rafforzare la sicurezza tecnologica, pensare a nuove strade per la politica internazionale, presidiare i fattori economici, creare forme di partecipazione più attiva degli individui e a una crescita sostenibile.

The Top Five Global Risks of Highest Concern for the Next 18 Months and 10 Years
Fonte: Global Risks Perception Survey 2015, World Economic Forum



http://italy.marsh.com/Portals/56/Documents/The Global Risks Report 2016.pdf

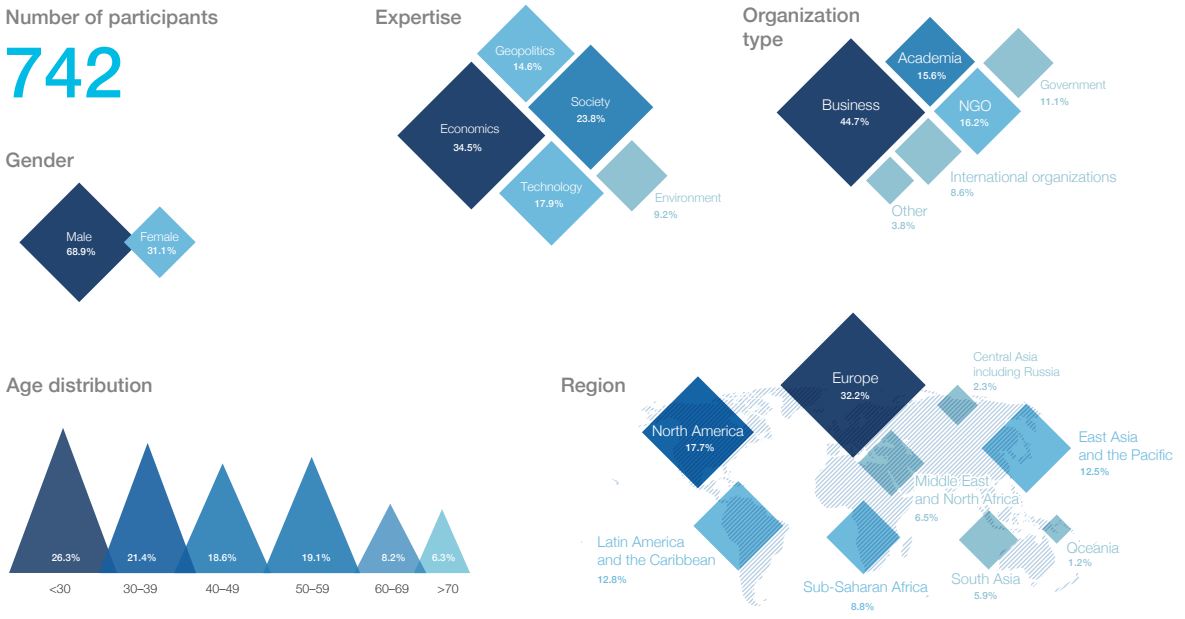
RISCHI PER LE IMPRESE: DISOCCUPAZIONE E SOTTOCCUPAZIONE PREOCCUPANO OLTRE UN PAESE SU 4

È il secondo anno che il Global Risks offre anche la prospettiva degli imprenditori sui principali rischi a livello nazionale. Un risultato sorprendente è la relativa assenza dei rischi ambientali tra le principali preoccupazioni delle aziende, in forte controtendenza rispetto alle priorità evidenziate da paesi e organizzazioni internazionali nella prima parte del Report.

È il rischio di disoccupazione e sottoccupazione a preoccupare maggiormente le imprese in oltre il 25% delle 140 economie nazionali considerate ed è ritenuto il maggior rischio soprattutto nell'Africa subsahariana, in Medio Oriente e nell'Africa settentrionale. Gli unici a non annoverare la disoccupazione tra i primi cinque rischi per le imprese sono gli Stati Uniti, che, insieme al Canada, vedono nei rischi informatici la loro preoccupazione principale.

Nelle risposte provenienti dai paesi europei dominano i rischi economici, che comprendono le crisi finanziarie, la disoccupazione e le bolle speculative, ma il secondo rischio più temuto è la forte variazione dei prezzi delle fonti energetiche: quest'ultimo è stato indicato fra i primi cinque rischi per le imprese in ben 93 economie nazionali.

Survey Sample Composition
Fonte: Global Risk Perception Survey 2015



MAPPA DEL RISCHIO POLITICO 2016: TERRORISMO E CONFLITTI METTONO ALLA PROVA GLI EQUILIBRI INTERNAZIONALI

La "Guerra del terrore", iniziata dopo gli attacchi dell'11 settembre 2001 negli Stati Uniti, è destinata a protrarsi con ogni probabilità per il prossimo decennio.

Questa è una delle principali evidenze elaborate da BMI Research, una delle fonti più autorevoli in tema di analisi del rischio politico, macroeconomico, finanziario, sulla base delle quali Marsh ha realizzato la Mappa del Rischio Politico 2016. Si tratta di una vera e propria mappa che fornisce una visione globale delle minacce che devono affrontare multinazionali e investitori, analizzando il livello di rischio di circa 200 paesi e territori con riferimento a tre variabili: rischio politico, macroeconomico e rischi operativi.

Negli ultimi dieci anni, le opportunità connesse al processo di globalizzazione, unitamente a un contesto internazionale caratterizzato da radicali cambiamenti e dal nascere di enormi tensioni geopolitiche, hanno imposto alle aziende la necessità di valutare attentamente i paesi e le aree geografiche in cui operare. In questo quadro, le aziende sono esposte a un numero crescente di rischi di matrice politica e commerciale e queste minacce – terrorismo e violenza politica, conflitti armati, movimenti politici anti-sistema sempre più potenti, minaccia di recessione globale oltre alla volatilità dei prezzi delle materie prime – non accennano a diminuire né in termini di frequenza né di severità.

Per operare al meglio in questo scenario, le aziende devono effettuare alcune scelte strutturali come valutare l'impatto potenziale di una crisi nei paesi in cui sono presenti o in cui hanno interessi, implementare procedure che consentano l'utilizzo di fornitori alternativi e adottare piani per la protezione dei propri asset e dei propri crediti, anche mediante coperture assicurative che garantiscano la tutela delle persone e la continuità dell'azienda. Secondo BMI e Marsh, i maggiori rischi politici che le organizzazioni e gli investitori dovranno affrontare nel prossimo anno sono il crescendo di attacchi terroristici e conflitti in Medio Oriente, l'andamento delle economie emergenti alle prese con tassi di crescita sempre più ridotti, e le elezioni negli Stati Uniti. A questi si aggiungono i partiti anti-sistema in Europa, in particolare i movimenti di estrema destra, la continua caduta dei prezzi delle materie prime, i rischi di successione in Paesi come Cuba, Angola, Arabia Saudita e Tailandia, lo scontro tra centralizzazione e federalismo (ne è un esempio il conflitto mai risolto nell'Ucraina dell'Est) e, infine, le rivalità tra le "grandi potenze", come le tensioni tra Cina e Giappone nel Mar Cinese dell'Est o tra Corea del Nord e del Sud.

TERRORISMO

Gli attacchi avvenuti nel 2015 e a inizio 2016 hanno riportato l'attenzione delle potenze mondiali verso la lotta al terrorismo. A preoccupare particolarmente è lo Stato Islamico, che rimane potente in Iraq e Siria e sta rafforzando sempre più la sua presenza in tutto il Medio Oriente e nel Nord Africa. Sebbene negli ultimi mesi sembra che l'avanzata dell'ISIS stia arretrando, la "guerra al terrore", che ha avuto inizio con l'attacco dell'11 settembre 2001, con molta probabilità continuerà per un altro decennio, secondo BMI. Stati Uniti e Russia hanno imparato la lezione del passato circa la difficoltà di combattere guerre via terra per lunghi periodi in Medio Oriente e Afghanistan, e nessuno dei due paesi sembra disposto a rischiare di rivivere quelle situazioni.

Si propenderà principalmente per attacchi via aria, che, però, potrebbero non essere sufficienti a sconfiggere lo Stato islamico. La prolungata instabilità nella zona del Medio Oriente aumenta il rischio di attacchi terroristici negli Stati Uniti, in Europa e nei paesi asiatici, e richiede misure di sicurezza più restrittive anche riguardo alle politiche di immigrazione.

LE ECONOMIE EMERGENTI

La Cina continua a lottare contro una crescita sempre più ridotta: il PIL cinese è sceso al 6,7% nel primo trimestre 2016 registrando la crescita più bassa dal primo trimestre del 2009. Le riforme economiche, un mercato immobiliare debole e l'aumento dei salari probabilmente continueranno a limitare la crescita nei prossimi anni, annullando un significativo vantaggio che fino ad oggi l'ha resa molto competitiva.

In Brasile, gli investimenti e i consumi rimangono invariati, accompagnati da significative perdite di posti di lavoro, un'elevata inflazione, tassi d'interesse alti e una corruzione dilagante. Si tratta di ostacoli che rendono probabile una contrazione del PIL del 4% per l'anno in corso. In Russia la crescita degli investimenti rimane a livelli minimi dal 2012 e la profonda recessione del 2015 ha ulteriormente esacerbato il problema. I consumi torneranno lentamente a risalire, ma l'inflazione rimarrà a livelli elevati e la crescita dei salari sarà minima. L'unico tra i paesi emergenti che sembra crescere in questa fase di stallo è l'India, per il quale Business Monitor International prevede una crescita del PIL del 7,2% nel 2016. Il modello per rilanciare gli investimenti economici promosso dal Primo Ministro dell'economia Narendra Modi rivolge l'attenzione anche a soggetti esteri, con particolare riferimento alla stabilizzazione della Rupia indiana. È inoltre previsto un aumento della produzione industriale dopo l'annuncio di molte aziende di voler costruire fabbriche in India nel corso del 2016.

ELEZIONI PRESIDENZIALI NEGLI STATI UNITI

Anche se negli Stati Uniti i sondaggi mostrano come la sicurezza nazionale stia molto a cuore all'opinione pubblica e agli elettori, la politica estera rimarrà un punto chiave nelle elezioni del 2016 e sarà di importanza elevata per la prossima amministrazione presidenziale. I candidati alla presidenza dei principali partiti politici hanno fortemente criticato l'approccio "distaccato" dell'amministrazione Obama alla politica estera, che, – ritengono – ha lasciato mano libera alla Cina nel Mare cinese dell'Est, all'intervento russo in Ucraina e alla continua espansione dello Stato islamico in Iraq e Siria.

Indipendentemente dal risultato elettorale delle elezioni 2016, gli esperti ritengono che il prossimo Presidente degli Stati Uniti d'America adotterà un approccio interventista per quanto riguarda la politica estera.

PARTITI ANTI - SISTEMA IN EUROPA

Il terrorismo, la crisi dei migranti, le misure di austerità, e numerosi fattori economici hanno contribuito alla crescita di partiti anti-sistema in paesi quali Danimarca, Francia, Germania, Grecia, Spagna e Regno Unito. Nella maggior parte dei casi, questi partiti non hanno particolari possibilità di conquistare il potere attraverso le elezioni, ma possono influenzare la retorica e l'ordine pubblico, come membri di coalizioni di governo con gli altri partiti. Molti partiti anti-sistema, in particolare quelli di estrema destra, hanno lanciato campagne molto severe in materia di immigrazione e difesa a seguito dei flussi migratori incessanti e dopo gli attentati a Parigi. La loro crescita continua a fare pressione sui principi che stanno alla base dell'UE mettendo a dura prova la libera circolazione dei lavoratori.

CROLLO DEI PREZZI DELLE MATERIE PRIME

Nel mese di giugno 2014 il prezzo si aggirava intorno ai 112 dollari al barile per poi scendere a 38 dollari al barile nel mese di dicembre 2015, il dato più basso registrato da luglio 2004 (secondo l'Energy Information Administration). Business Monitor International prevede un prezzo medio di 42,50 dollari al barile in tutto l'arco del 2016, che sarà in continuo calo con effetti negativi sulle economie dei paesi che esportano maggiormente il petrolio, aggiungendosi alle altre minacce politiche. I paesi a più altro rischio sono Angola, Congo-Brazzaville, Guinea equatoriale, Iran, Iraq, Nigeria e Venezuela. Inoltre, il basso costo del petrolio e le sanzioni economiche potrebbero far stagnare l'economia russa.

Oltre al petrolio, dall'inizio del 2014 i prezzi di una serie di altre materie prime hanno continuato a scendere: il prezzo del cotone che veniva venduto per 90 dollari alla libbra nel marzo 2014 è sceso al di sotto dei 65 dollari per libbra nel dicembre 2015; l'oro, che valeva 1.300 dollari all'oncia nel giugno 2014, è sceso al di sotto dei 1.100 dollari all'oncia nel dicembre 2015 e il prezzo del rame è sceso da 3,20 dollari per libbra nel giugno 2014 a poco più di 2 dollari per libbra nel dicembre 2015. Il declino globale di numerosi prezzi delle materie prime è stato attribuito in parte alla situazione economica in Cina, che non ha più lo stesso appetito per questi tipi di beni, ma anche all'aumento dei tassi di interesse e al crollo delle valute rispetto al dollaro

statunitense. Il calo dei prezzi delle materie prime, oltre a provocare l'aumento del rischio politico in molti mercati emergenti le cui economie si basano sull'esportazione di materie prime (ad esempio il Brasile), potrebbe anche ripercuotersi su economie già sviluppate come il Canada e Australia.

RISCHI DI SUCCESSIONE

Sono 20 i paesi al mondo guidati da un'unica persona da molto tempo. Quando alcuni leader del passato sono morti o sono stati destituiti – per esempio in Indonesia, in Iraq, in Libia, in Jugoslavia, e nello Zaire – il risultato è stato una guerra civile. Tra i paesi che purtroppo potrebbero trovarsi in una situazione analoga di agitazione nei prossimi anni ci sono l'Angola, il Camerun, Cuba, la Guinea Equatoriale, la Guinea, l'Iran, il Kazakhstan, l'Oman, l'Arabia Saudita, la Tailandia, l'Uzbekistan e lo Zimbabwe.

CENTRALIZZAZIONE VS. FEDERALIZZAZIONE

Il referendum del 2014 sull'indipendenza della Scozia e il successivo referendum del Regno Unito indetto dal partito conservatore per dare nuovi poteri al Parlamento scozzese sono solo esempi delle pressioni che i governi di tutto il mondo devono affrontare a fronte delle richieste di maggior indipendenza da parte di alcune regioni. Situazioni simili si sono verificate anche nel conflitto separatista in Ucraina orientale; in India, dove un movimento popolare ha portato alla divisione di Andhra Pradesh in due stati separati (Andhra Pradesh e Telangana) nel 2014; in Yemen con la ribellione Houthi e il separatismo meridionale e in Spagna, dove il governo ha bloccato il referendum sull'indipendenza della Catalogna. Secondo Business Monitor International, è probabile la formazione di molti nuovi Stati nei prossimi cinque anni.

RIVALITÀ FRA "POTERI FORTI"

Stiamo assistendo a una continua tensione tra le tre maggiori potenze mondiali – Stati Uniti, Russia e Cina – e tra queste potenze mondiali con altri stati. Nei prossimi mesi le tensioni potrebbero continuare a crescere tra Cina e Giappone nella zona orientale cinese; tra Cina e Stati Uniti nel Mar Cinese Meridionale, a causa della costruzione da parte della Cina di isole artificiali e piste di atterraggio; tra Corea del Nord e Corea del Sud, soprattutto dopo l'annuncio da parte del governo del Nord di un test nucleare; tra Russia e Turchia, dove la situazione si è aggravata a causa dell'abbattimento di un jet russo nel novembre 2015 vicino al confine tra Siria e Turchia.

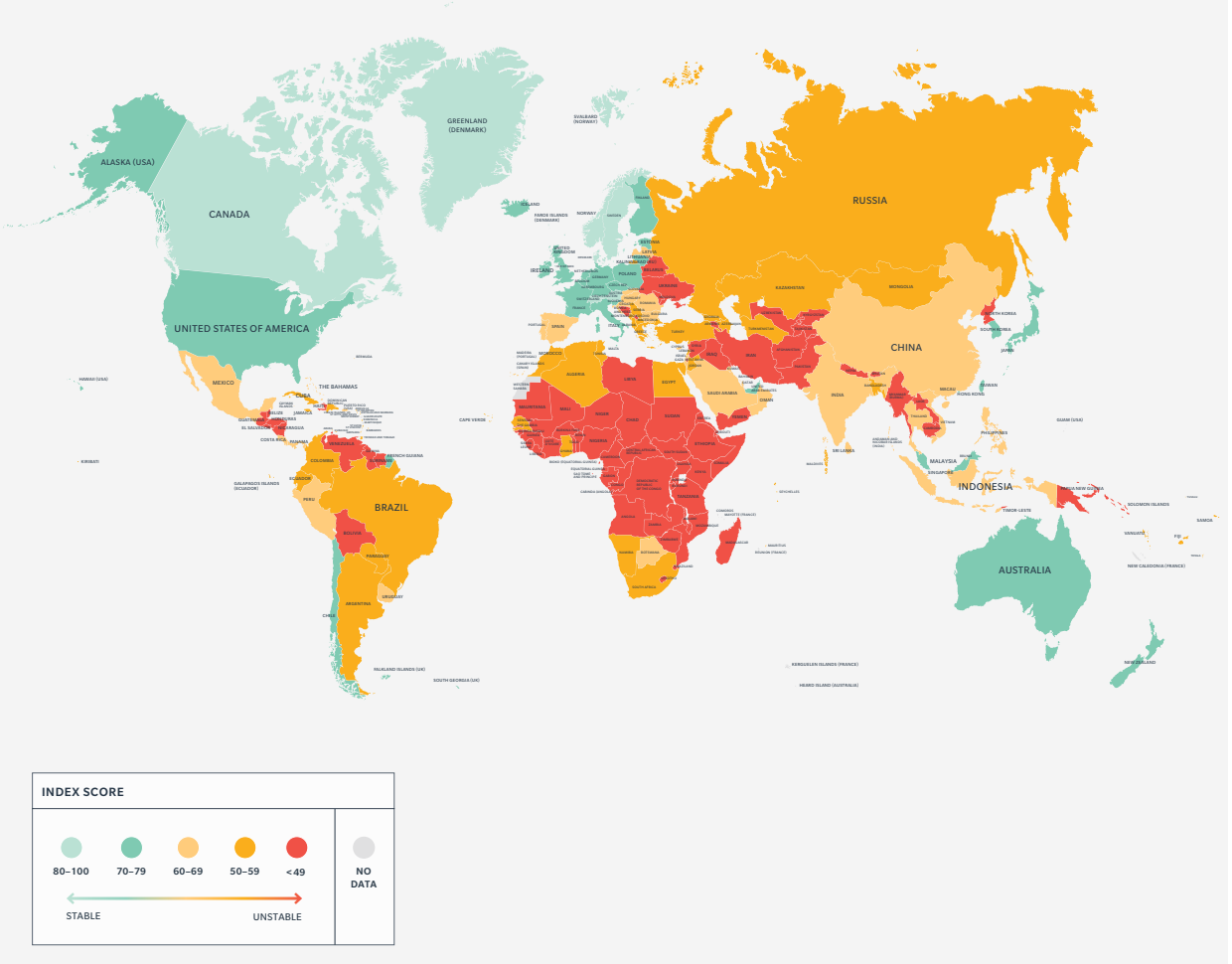
GESTIONE DEL RISCHIO POLITICO

Come ci hanno ricordato i recenti eventi accaduti a Parigi e Bruxelles, gli attacchi terroristici si verificano spesso senza preavviso. Inoltre, fattori come la caduta del prezzo del petrolio continuano a mettere sotto pressione le economie dei diversi paesi. È quindi fondamentale per le imprese essere preparate alla possibilità che violenza, disordini, o altri tipi di crisi si sviluppino rapidamente in qualsiasi parte del mondo – compresi quei paesi che storicamente sono sempre stati visti come sicuri e stabili –. Le aziende possono prepararsi a questi rischi in diversi modi:

- **gestione del rischio di credito.** Quando un governo crolla o entra in crisi, spesso perde la sua capacità di onorare i propri obblighi finanziari. Questo può creare una reazione a catena di default che si diffonde nel settore privato. Le imprese dovrebbero rivedere la loro gestione dei rischi di credito, le proprie politiche e procedure e valutare l'impatto potenziale di rischio politico sui paesi in cui i loro clienti e fornitori operano.
- **costruire catene di fornitura resilienti.** Ancor prima dello sviluppo di una crisi, un'organizzazione dovrebbe capire come un'eventuale emergenza all'interno di un paese possa compromettere la sua supply chain. Le aziende dovrebbero anche avere piani di intervento per consentire l'uso di fornitori alternativi e canali differenti per comunicare con i clienti e fornitori, in caso di necessità.
- **proteggere le persone.** Lo sviluppo e la pianificazione di un piano di gestione di crisi in anticipo può contribuire a mantenere aperto un canale di comunicazione attivabile non appena le problematiche si manifestano.
- **proteggere le risorse attraverso l'assicurazione.** Le assicurazioni sul rischio credito e sul rischio politico sono in grado di proteggere contro una varietà di rischi, compresi l'esproprio, la violenza politica, il mancato pagamento e la contract frustration.

IL RISCHIO POLITICO NEL 2016

Sulla base degli scenari disegnati da BMI Research, una delle fonti più autorevoli in tema di analisi del rischio politico, macroeconomico e finanziario, Marsh ha elaborato la Mappa del Rischio Politico 2016, che evidenzia (tramite i colori) il livello di rischio di circa 200 paesi e territori considerando tre variabili: rischio politico, macroeconomico e rischi operativi. Da quest'anno è disponibile una versione interattiva della Mappa del Rischio Politico 2016: cliccando su un paese, si accede a un breve testo descrittivo sulla situazione locale e a un punteggio relativo al rischio paese e al rischio operativo. La mappa è disponibile su marsh.com.



Fonte: Geopolitical Threats for the Year

http://articles.marsh.com/politicalRiskMap2016.aspx

http://italy.marsh.com/Portals/56/Documents/Geopolitical Threats for the Year Ahead - Marsh's Political Risk Map 2016.pdf

RESPONSABILITÀ AMBIENTALE: DALLA DIRETTIVA UE A OGGI, COME È CAMBIATA IN POCHI ANNI LA PERCEZIONE DA PARTE DELLE AZIENDE

In Italia, il caso recente di sversamento di petrolio nel genovese ha riportato l'ambiente nell'agenda di governo e amministrazioni locali.

Il ricordo delle quasi 500 tonnellate di greggio uscite dall'esplosione di una tubatura di un oleodotto in provincia di Genova, solo per citare l'ultimo episodio, è troppo vivido per dimenticare quali potenziali effetti dannosi derivino da un disastro ambientale, per l'ecosistema e anche per l'economia della regione geografica interessata. Ma nell'ultimo decennio molto è stato fatto in tema ambientale, in particolare dal punto di vista della responsabilità e anche la percezione delle aziende su questo argomento è fortemente mutata.

Precursore di questo cambio di pensiero è stata la Direttiva dell'Unione Europea "Environmental Liability Directive" (ELD), che ha introdotto il principio "chi inquina paga" e una variazione del perimetro delle misure correttive necessarie. Per citare solo un esempio, nel caso non sia possibile riportare un'area danneggiata alle condizioni originarie, il responsabile del fatto dovrà intraprendere progetti di ripristino di altre aree, fornendo così una sorta di risarcimento all'ambiente per i danni causati. Inoltre potrebbero essere richiesti provvedimenti provvisori, in attesa che la bonifica e il ripristino degli ambienti danneggiati siano effettuati.

La direttiva introduce anche un principio di "precauzione", oltre al principio "chi inquina paga", per cui gli operatori di un'attività potenzialmente pericolosa sono tenuti ad adottare tutte le misure opportune per prevenire e, se necessario, per rimediare ai danni ambientali provocati.

Secondo uno studio del governo francese, con l'attuale regime di responsabilità ambientale, le richieste di risarcimento hanno subito aumenti tra 10 e 40 volte.

Per dimostrarlo lo studio ha analizzato due casi di disastro ambientale realmente avvenuti comparando i costi sostenuti dalle aziende che li avevano provocati prima della Direttiva con il calcolo della cifra potenziale che le stesse dovrebbero versare oggi per il medesimo danno. Per un incendio in un impianto di clorato di sodio, avvenuto negli anni '90, che ha portato a un diffuso inquinamento di un fiume e alla distruzione dell'habitat naturale circostante, i costi di ripristino erano stati stimati in 10.000 euro, oggi invece lo stesso danno costerebbe 4 milioni di euro. In un altro caso, il rilascio di sostanze chimiche nocive dal mulino di una cartiera che hanno provocato la distruzione totale di tutta la fauna e la flora delle falde acquifere è costato all'azienda responsabile 42.000 euro mentre sotto la Direttiva l'incidente avvenuto è stato stimato in 425.000 euro.

Marsh, nell'Environmental Benchmarking Report, ha analizzato 700 polizze assicurative relative al rischio ambientale, evidenziando come la normativa dei singoli Stati abbia portato a una maggiore attenzione alla salvaguardia dell'ambiente e alla prevenzione di danni all'ecosistema, a seguito del recepimento della direttiva. Una presa di coscienza importante del rischio ambientale: l'acquisto di polizze assicurative è infatti aumentato del 13,6% in tutti i settori tra il 2007 e il 2014. Le aziende che operano nei settori dell'energia, dei rifiuti e nell'industria pesante hanno aumentato i massimali delle loro polizze tra l'8% e il 15%, mentre i premi, in diminuzione tra il 2006 e il 2009, sono ora in aumento in tutti i tre settori.

https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/EMEA Environmental Benchmarking Report 2015-11-2015.pdf

IL VIRUS ZIKA METTE SOTTO PRESSIONE LA SICUREZZA SANITARIA INTERNAZIONALE

Con l'avvicinarsi dei Giochi Olimpici in Brasile, il dibattito sulla pericolosità del virus Zika e sui rischi di una pandemia si rianima e se gli esperti sono divisi, l'OMS (Organizzazione Mondiale della Sanità) sconsiglia alle donne incinte di recarsi in Brasile dove, tuttavia, grazie a un'efficace campagna informativa si assiste a una diminuzione dei contagi.

Nel frattempo però il virus Zika continua a diffondersi in altri stati dell'America del Sud e per la prima volta è stato identificato in America centrale, in Messico, provocando anche un stato di allerta negli Stati Uniti.

Per l'OMS la diffusione del virus Zika è un'emergenza sanitaria di rilevanza internazionale che accresce il rischio di una possibile epidemia a livello globale. Secondo Margaret Chan, segretario generale dell'organizzazione, il virus si sta diffondendo velocemente in oltre 20 paesi nel centro e sud America, ma non si esclude che possa colpire anche paesi in Asia e Africa.

Ad oggi gli esperti hanno rilevato che il virus è trasmesso dalle zanzare. Sebbene i primi casi di infezione si siano manifestati in Brasile nel maggio del 2015, quando è stato registrato un aumento di bambini nati con microcefalia nello stato federale di Pernambuco, lo stato di emergenza nel paese è stato dichiarato solo a dicembre. La microcefalia infatti, oltre a complicanze di tipo neurologico, è uno degli effetti del virus più evidenti che sono stati riscontrati fino ad oggi, mentre rimangono ancora sconosciute le cause del contagio (infettive, chimiche o ambientali).

Data la crescita della popolazione, la rapida urbanizzazione e il costante flusso di merci, persone e animali, aumenta la possibilità di trasmissione di malattie infettive in diverse aree geografiche, mettendo alla prova la capacità dei paesi di individuare una risposta efficace alla crisi.

Fenomeni di questa portata, non sono di fatto prevedibili in anticipo: per questo, in una simile fase di incertezza, il coinvolgimento e l'impegno della comunità internazionale in termini di ricerca di nuovi farmaci e sviluppo di test diagnostici e vaccini, è fondamentale per contrastare un'eventuale epidemia a livello globale.

Non solo i governi, ma anche le organizzazioni con risorse che operano nelle aree colpite dal virus, o che si devono spostare in questi paesi, dovrebbero adottare precauzioni per tutelare il proprio personale e salvaguardare il proprio business.
Le attività di prevenzione sono fondamentali ed è proprio su questo punto che le aziende possono impegnarsi nel creare programmi per affrontare un'epidemia attraverso semplici passi:

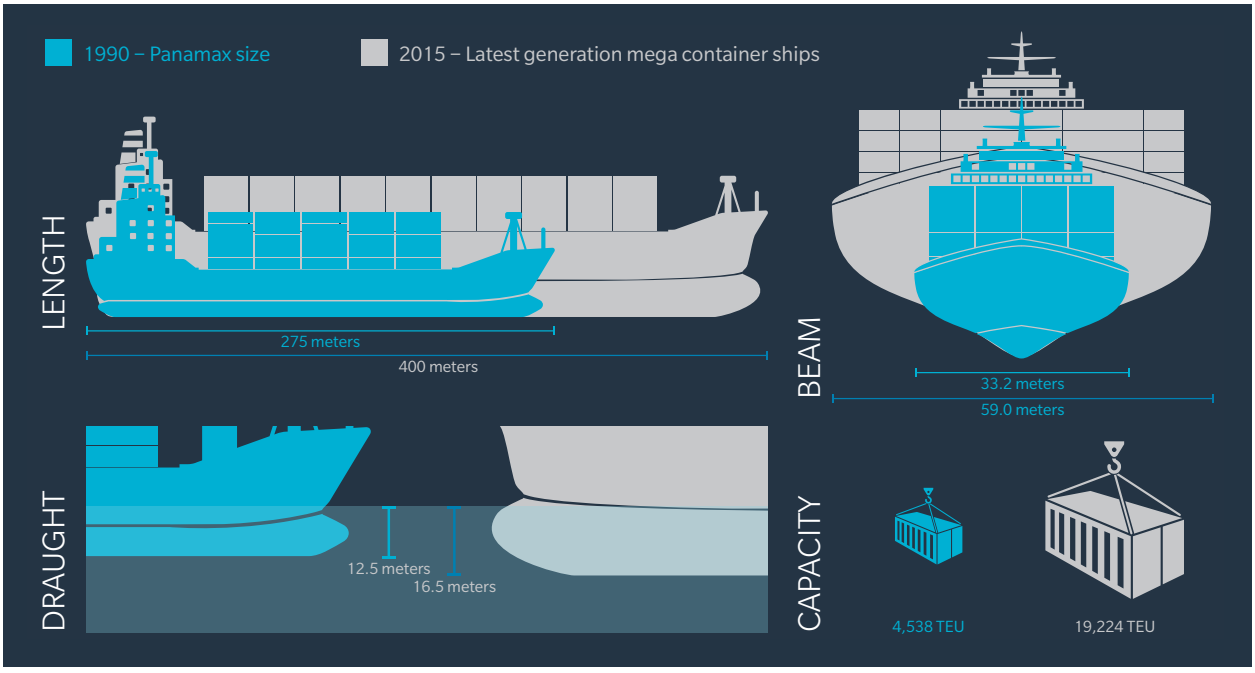
- rivedere le policy aziendali su viaggi e trasferte, norme igieniche e controlli medici, così come le policy in materia di farmaci antivirali e di supporto sanitario;
- rivedere i flussi informativi verso i dipendenti circa l'evoluzione della pandemia, le modalità di prevenzione delle infezioni, lo stato delle attività aziendali nelle aree colpite;
- implementare un piano di business continuity per mantenere la normale operatività dell'azienda o di una sua funzione cruciale "vulnerabile" come un sito produttivo;
- rivedere la struttura aziendale in modo che sia pronta a gestire l'impatto e le conseguenze di un evento pandemico;
- assicurarsi che il crisis management e i piani di business continuity includano protocolli dettagliati per le pandemie e che il reperimento delle tecnologie e la mappatura delle infrastrutture necessarie ad affrontare l'infezione siano effettuati con adeguato anticipo.

NAVI COMMERCIALI SEMPRE PIÙ GRANDI E DATI BATIMETRICI INSUFFICIENTI METTONO A RISCHIO LA NAVIGAZIONE COMMERCIALE E CIVILE

Il report Plumbing the Depths: Hydrographic Concerns for Modern-Day Large Vessels, pubblicato da Marsh, rielabora i dati dell'International hydrographic organization (Iho) dimostrando che le innumerevoli lacune nelle conoscenze batimetriche sono purtroppo diffuse su tutto il globo e possono creare seri problemi nella navigazione soprattutto in un'epoca, come la nostra, di gigantismo navale.

Navi commerciali di enormi dimensioni, in termini di lunghezza, larghezza e profondità, stanno infatti già solcando, e sempre più solcheranno, i mari di tutto il mondo, seguendo rotte che nella maggior parte dei casi non sono mai state esplorate con mezzi di tali dimensioni. Tutto questo risponde alla necessità di incrementare il commercio internazionale abbattendo il più possibile i costi di trasporto, in accordo con i governi di tutto il mondo, inclini a favorire la presenza di questi tipi di navi nei propri porti. Tuttavia, questi giganti dei mari sono esposti a numerosi rischi, partendo dalle carte di navigazione in loro possesso che contengono dati obsoleti, non in linea con gli standard moderni o, peggio

Comparative Size of Large Container Ships 1990 – 2015
Fonte: MSC Available at: https://www.msc.com/getattachment/9b03c189-75b8-45b0-9970-0875ffbc3965
Hofstra Available at: https://people.hofstra.edu/geotrans/eng/ch3en/conc3en/containership_draft_size.html



ancora, in cui il rilievo idrografico del fondale marino non è mai stato effettuato.

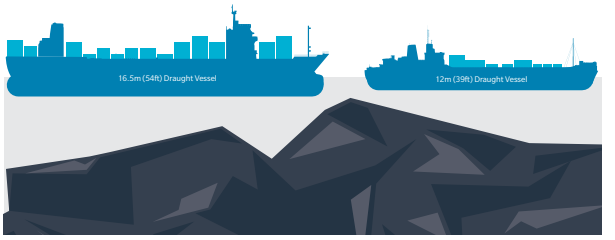
Se abbiamo a disposizione mappe di Marte e della Luna migliori di quelle dei fondali oceanici, sappiamo invece pochissimo della maggior parte dell'oceano. Dal report si comprende come i dati batimetrici sono incompleti o inesistenti per gran parte degli oceani e dei mari del mondo, con ampie aree la cui profondità non è stata mai misurata o, in caso contrario, sono il frutto di rilevazioni risalenti al secolo scorso. A preoccupare è anche la navigazione in acque per cui le carte nautiche e i sistemi elettronici vengono reputati più affidabili: meno della metà delle aree prese a campione risultano misurate in maniera sufficiente. La percentuale cala precipitosamente se prendiamo in considerazione la penisola antartica dove si avventurano sempre più navi, soprattutto da crociera. La situazione qui è ancora più preoccupante, con lo 0% delle acque adeguatamente sorvegliate, il 40% non adeguato e il 60% privo di precedenti misurazioni.

L'importanza di conoscere i fondali fino ai minimi dettagli è emersa in maniera evidente nel 2012, dopo l'incidente della "Costa Concordia" al largo dell'Isola del Giglio, avvenuto a pochi mesi di distanza dalla complicata situazione della portacontainer "Msc Rena", incagliata sulla barriera corallina a 22 chilometri dal porto di Tauranga, il principale della Nuova Zelanda. Ma per gli armatori mercantili un forte campanello d'allarme è arrivato con la "Indian Ocean", una portacontainer rimasta per alcuni giorni incagliata all'ingresso di uno dei più grandi porti europei, quello di Amburgo, dove ogni anno transitano migliaia di navi. Le dinamiche dell'incidente non sono chiare: un errore di manovra, un guasto, oppure la semplice scoperta di un limite delle nuove portacontainer. Probabilmente la risposta sta nell'ipotesi che, con portacontainer di tali dimensioni, basta un piccolo inconveniente per causare un serio incidente.

Nell'interesse comune è importante che i governi intraprendano le azioni necessarie per adempiere agli obblighi previsti dalla Convenzione sulla salvaguardia della vita in mare (SOLAS), per contribuire a mappare i fondali di tutto il mondo e aumentare la sicurezza degli oceani. È auspicabile inoltre una maggiore collaborazione tra i paesi per garantire la mappatura delle acque internazionali (oltre il limite delle acque territoriali) dove le informazioni sulle profondità degli oceani a disposizione sono davvero esigue.

The Arctic Sea Routes
Fonte: www.swmaps.com

Existing "large" vessels sail over rock protrusions that the latest mega-ships may strike, due to their deeper draughts
Fonte: MSC Available at: https://www.msc.com/getattachment/9b03c189-75b8-45b0-9970-0875ffbc3965
Hofstra Available at: https://people.hofstra.edu/geotrans/eng/ch3en/conc3en/containership_draft_size.html



http://italy.marsh.com/Portals/56/Documents/Plumbing the Depths - Hydrographic Concerns for Modern Day Large Vessels.pdf

RISCHIO CYBER: L'UNIONE EUROPEA DETTA NUOVE REGOLE SULLA GESTIONE DEI DATI

È entrato in vigore ieri il nuovo Regolamento UE sulla General Data Protection (GDPR), che ha mandato di fatto in pensione la Direttiva sulla Data Protection del 1995.

Il Regolamento è parte di un pacchetto normativo per la tutela dei dati personali approvato ad aprile dal Parlamento Europeo, che include anche la Direttiva che regola il trattamento di dati personali nei settori di prevenzione, contrasto e repressione dei crimini.

Il pacchetto definisce un quadro normativo comune per tutti gli stati membri, condizione ritenuta fondamentale per agevolare la libera circolazione dei dati nel mercato unico digitale, e al tempo stesso sottolinea come un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento dei diritti degli interessati e degli obblighi di coloro che trattano i dati personali.

La Direttiva del '95 fu adottata quando Internet non era ancora diffuso: i social network come Facebook non esistevano ancora, e neanche Google, mentre Amazon nasceva proprio quell'anno. Oggi l'evoluzione tecnologica ha modificato il modo in cui i dati vengono raccolti e utilizzati e necessitava di un aggiornamento che ha richiesto più di quattro anni di lavoro dalla pubblicazione della prima bozza del Regolamento.

Tra le principali novità introdotte dal GDPR, vi sono:

- la creazione di una normativa organica a livello europeo per la protezione dei dati che comprende il diritto di sapere quando i nostri dati personali sono stati violati, e potrebbero essere, quindi, oggetto di trattamenti non autorizzati;

- l'implementazione di misure di sicurezza adeguate da parte delle aziende che processano dati personali. Queste misure prevedono fra le altre cose la nomina, all'interno del proprio organigramma, delle figure del Data Processor e del Data Controller e lo svolgimento di un "Data protection impact assessment (DPIA)";

- nuove restrizioni relative ai dati di profilazione;

- le aziende/organizzazioni sono tenute, nel caso avvenisse una violazione dei dati, a notificarla all'autorità di controllo competente entro e non oltre le 72 ore (a meno che la violazione non comporti una situazione di rischio per i diritti e la libertà delle persone), e a comunicarla "senza indebito ritardo" ai soggetti interessati;

- nuovi e ampliati diritti di cancellazione e accesso ai propri dati (comunemente indicato come "diritto all'oblio");

- l'applicazione di sanzioni severissime, fino a 20 milioni di euro o il 4% del fatturato globale annuo dell'azienda, in caso di violazioni accertate.

Per quanto riguarda le organizzazioni è importante sottolineare che il Regolamento sarà applicato non solo a società o enti con sede sul territorio europeo, ma a tutte le realtà che processano dati personali di soggetti che sono all'interno dell'Unione e rivolgono i propri servizi verso paesi dell'Unione, indipendentemente dal fatto che tale servizio comporti un'obbligatorietà di pagamento o meno.

Questo significa che tutti i possessori o gestori di siti o applicazioni che offrono beni o servizi all'interno dell'UE, o software in grado di monitorare i comportamenti di navigazione dei cittadini che si trovano in paesi membri dell'Unione Europea, saranno soggetti al Regolamento.

Entrambi i provvedimenti sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea lo scorso 4 maggio: il Regolamento è entrato in vigore dopo 20 giorni dalla pubblicazione, mentre la Direttiva è vigente già dal 5 maggio. Gli Stati membri dovranno recepirne le disposizioni nel diritto nazionale entro 2 anni, così questa fase transitoria permetterà alle autorità preposte di sorvegliare e al tempo stesso agevolerà le organizzazioni pubbliche e private ad affrontare questo indispensabile cambiamento.

http://italy.marsh.com/Portals/56/Documents/GDPR Adviser final-CE.PDF

NON IGNORARE LE MINACCE CYBER CAUSATE DAGLI INSIDER

Basie von Solms, Director of the Centre for Cyber Security at University of Johannesburg

Alcune delle violazioni informatiche più significative sono avvenute negli ultimi due anni e questo non è un caso, visto che il rischio cyber è in continuo aumento con dati a dir poco allarmanti.

Gli attacchi informatici avvengono sotto varie forme e possono avere portate diverse; inoltre i cyber criminali hanno a loro disposizione una vasta gamma di mezzi per compromettere il corretto funzionamento delle tecnologie aziendali. Fra i rischi cyber ipotizzabili, vengono spesso trascurate le minacce interne, ad opera di dipendenti dell'azienda. Un recente sondaggio sui rischi cyber, condotto da Marsh a livello europeo, ha messo in luce come molte aziende vedono proprio nelle minacce interne la causa principale dei danni cyber (il 40% delle risposte per la Francia, il 36% per Russia e il 56% per la Spagna).

È importante distinguere tra attacchi informatici esterni e problematiche create da insider. Quando si parla di attacchi informatici esterni, si fa riferimento ad attacchi provenienti da soggetti che sono al di fuori della vita aziendale, ma possono coinvolgere anche i dipendenti, come nel caso dello spear phishing. Si tratta di una tipologia di attacco informatico molto utilizzato, nel quale il dipendente risponde a un'email apparentemente innocua, contribuendo così a diffondere l'attacco. Questo avviene soprattutto a causa della mancanza di consapevolezza e di conoscenza delle procedure di sicurezza. Spesso questi attacchi sono classificati come attacchi insider anche se non è propriamente corretto definirli tali: i dipendenti non producono l'attacco ma ne sono l'obiettivo.

Se invece gli attacchi insider provengono veramente dall'interno dell'azienda, sono commessi solitamente da persone che sono autorizzate ad accedere alle risorse elettroniche della stessa azienda. Il dipendente, in questo caso, è "la minaccia che proviene dall'interno". Le minacce interne sono più difficili da contrastare e non possono essere affrontate solo con la tecnologia. È necessario un approccio di difesa meno tecnico, ma più umano: mettersi al riparo da attacchi cyber di insider è un processo complesso e molto spesso le aziende non prendono nemmeno in considerazione le minacce interne, perché sono focalizzate nel cercare di fermare le intrusioni che avvengono dall'esterno.

I report e le statistiche indicano chiaramente che le minacce cyber create da insider sono in continua crescita e stanno diventando sempre più rischiose. Se si identifica l'insider come un dipendente che possiede tutti gli accessi ai sistemi informatici di una società, si sta già sottovalutando il rischio. Chiunque abbia accesso ai beni tecnologici aziendali deve essere considerato un possibile insider, per cui l'attenzione dovrebbe essere rivolta a quasi tutti i dipendenti e collaboratori, inclusi consulenti, visitatori e dipendenti temporanei.

Il più grande rischio cyber è probabilmente il dipendente insoddisfatto, che, per qualsiasi motivo, decide di rubare o compromettere le risorse tecnologiche dell'azienda, aiutato spesso dall'evoluzione tecnologica che rende tutto ancora più semplice. Basti pensare alle semplici chiavette USB, veri e propri contenitori di informazioni, dalle dimensioni così ridotte che è improbabile impedire che fuoriescano dalla società con dati riservati. Inoltre nel caso in cui il dipendente venga scoperto potrebbe facilmente affermare che aveva salvato dei dati che gli sono necessari per lavorare da casa.

Un ulteriore pericolo per l'azienda viene rappresentato dalle piattaforme di cloud storage che rendono ancora più facile l'invio di informazioni verso l'esterno, senza nemmeno entrarne in possesso fisicamente. Inoltre, l'approccio molto diffuso "bring-your-own-device" è un altro fattore che contribuisce ad aumentare la minaccia insider.

CONTRASTARE LA MINACCIA INSIDER

Implementare misure di sicurezza per impedire totalmente le minacce interne è impossibile. Cosa si può fare allora per affrontare il rischio di insider? Quali contromisure di base devono adottare le aziende?

E' ovvio che più le aziende credono nei dipendenti, meno possibilità ci sono che i lavoratori diventino delle "canaglie",

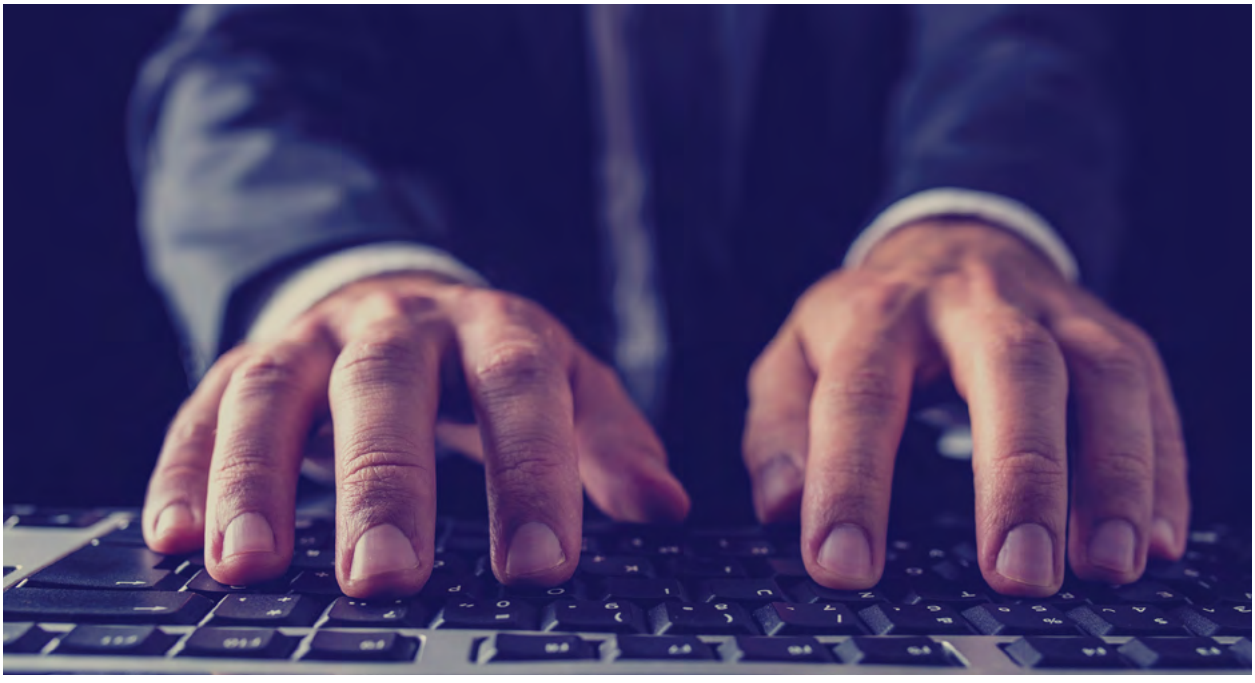
trasformandosi in vere e proprie minacce interne. Un buon modo per evitare queste situazioni sarebbe gestire al meglio il ciclo completo del rapporto che il lavoratore ha con l'azienda; partendo dalla pre-assunzione fino ad arrivare al momento della cessazione del rapporto di lavoro.

Lo standard internazionale ISO/ IEC 27002, pubblicato congiuntamente dalla International Organization for Standardization e dalla Commissione Elettrotecnica Internazionale nel 2013, specifica i vari tipi di controlli che possono essere implementati per creare un ambiente informato e sicuro. Lo standard si compone di 114 operazioni di controllo raccolte in 14 sezioni. Fra queste, la settima, "Human Resources Security", riguarda specificamente le minacce interne e prevede una serie di raccomandazioni:

- **prima dell'assunzione:** effettuare la fase di screening pre-assunzione, di cui viene sottolineata l'importanza, e per la quale vengono fornite linee guida concrete su ciò che andrebbe verificato;
- **durante il periodo di attività:** lavorare per una maggiore conoscenza della sicurezza, con attività di educazione e formazione, nonché mettendo a punto azioni disciplinari di non conformità rispetto a procedure di sicurezza e specifiche procedure aziendali;
- **al termine del rapporto di lavoro:** gestire la chiusura dei diritti di accesso e le questioni connesse.

Le aziende dovrebbero studiare lo standard ISO – nello specifico la clausola numero 7 – in maniera dettagliata così da poter attuare i necessari controlli di sicurezza. Si tratta di un lungo cammino per poter affrontare i vari aspetti delle minacce interne, che può essere sintetizzato nelle seguenti tre fasi:

- avere piena consapevolezza delle minacce insider dando loro il giusto peso a livello di rischio informatico per l'azienda;
- utilizzare anche un approccio non tecnico alle minacce cyber da parte degli insider, insieme ai provvedimenti tecnici che svolgono un ruolo importante;
- utilizzare le raccomandazioni del punto 7 dello standard ISO / IEC 27002 come approccio di base alle minacce interne.



http://www.brinknews.com/dont-ignore-the-insider-cyber-threat/

7 AZIENDE SU 10 SCELGONO CANDIDATI INTERNI PER I RUOLI CRITICI MA UN DIPENDENTE SU 3 PENSA DI LASCIARE LA PROPRIA AZIENDA NEI PROSSIMI 12 MESI

Il "Global talents trends study" di Mercer rivela differenze significative, rispetto allo sviluppo del talento, tra le prospettive delle imprese e la percezione dei dipendenti. In Italia i manager sono percepiti come poco attenti allo sviluppo dei collaboratori.

In Italia il 76% degli intervistati valuta come "insufficiente o appena sufficiente" la capacità di "coaching" dei leader rispetto ad una media globale pari al 58%, e a una media europea pari al 66%. Sempre in Italia, oltre l'80% dei dipendenti giudica che la propria azienda non stia facendo abbastanza rispetto all'aggiornamento delle loro competenze – un dato peggiore rispetto alla media mondiale pari a 70%.

In un mercato del lavoro sempre più complesso, attraverso lo studio "Global Talent Trends" Mercer ha voluto per la prima volta confrontare i punti di vista di datori di lavoro e lavoratori. La ricerca ha coinvolto 1.730 HR leader e oltre 4.500 dipendenti in rappresentanza di tutti i settori industriali, in 17 Paesi.

Tra i dipendenti è diffusa l'insoddisfazione legata alla mancanza di prospettive di sviluppo, a processi HR che non colgono le nuove motivazioni dei dipendenti, e a carenze nella leadership. Nove aziende su dieci prevedono un'aumentata concorrenza per acquisire i migliori talenti, e più di un terzo si aspetta che questo aumento sia significativo (35%). Tuttavia, nonostante il 70% delle società abbia dichiarato l'intenzione di coprire ruoli critici rimasti vacanti promuovendo candidati già all'interno dell'azienda,

un dipendente su 3 (28%) ipotizza di uscire nei prossimi 12 mesi, indipendentemente dal ruolo ricoperto. Può sembrare paradossale ma questo è vero (26%) anche in mercati a più elevata disoccupazione quale quello europeo.

Nell'85% dei casi anche le società avvertono la necessità di rivedere i propri programmi e le politiche di gestione dei talenti. Una verifica che richiede necessariamente il contributo attivo del management, affiancato da una funzione HR come partner strategico del vertice nel cambiamento.

In Italia il possesso di una "Global Mindset" è la richiesta prioritaria fatta dalle aziende ai candidati, mentre si tratta di una caratteristica vista come meno critica per il successo del business in paesi come Sud Africa, Messico, Australia e US. In dettaglio oltre la metà (51%) dei dirigenti delle risorse umane in Italia ritiene che nei prossimi 12 mesi sarà di fondamentale importanza potersi avvalere di una forza lavoro sempre più eterogenea.

TREND E PRIORITÀ

IN EUROPA

Diversity

Il 67% delle società partecipanti all'indagine ha affermato di essere focalizzato sulla creazione di team di vertice diversi e inclusivi. Uno sforzo riconosciuto solo dal 45% dei dipendenti.

Orientamento della leadership allo sviluppo dei collaboratori

Solo la metà dei lavoratori in Europa (51%) rileva un impegno diretto della leadership sui temi dello sviluppo.

Reward

Mentre 7 società su 10 (69%) giudicano chiare e trasparenti le proprie politiche di remunerazione, solo il 43% degli intervistati le reputa tali.

Retention

Il 69% degli interpellati HR ha dichiarato l'intenzione di coprire eventuali ruoli rimasti vacanti promuovendo candidati validi dall'interno dell'azienda. Tuttavia un dipendente su 4 (26%) prende in considerazione di dimettersi nei prossimi 12 mesi, proprio a causa della percepita mancanza di opportunità di carriera.

Processi HR

Più di 3 realtà su 4 in Europa ammettono di non avere costruito nel tempo processi HR semplici ed efficienti. Una considerazione disincantata che, questa volta, accomuna il punto di vista di aziende e dipendenti (66%).

NEL MONDO

Nel mondo del business globalizzato di oggi, le strategie HR di successo dipendono dalla capacità di un'azienda di attrarre, coinvolgere, trattenere e fare crescere il talento di dipendenti di diverse generazioni, età, provenienze, formazione. L'indagine Mercer mette in evidenza come la Diversity, ovvero la gestione di un pool di risorse tanto eterogeneo, sia uno dei tre trend percepiti come più di impatto nel mondo HR, dopo l'ingresso delle economie emergenti sullo scenario competitivo e la scarsità di talento disponibile.

L'importanza attribuita dalle società allo sviluppo di una forza lavoro diversificata non si è tuttavia tradotta in azioni visibili ai dipendenti. Mentre il 73% delle aziende dichiara di lavorare alla costruzione di un team di vertice rappresentativo delle differenze, solo il 54% dei dipendenti riconosce questo impegno alla propria società.

La ricerca documenta come le aziende dovranno compiere sforzi mirati ad attrarre, trattenere e garantire la produttività del proprio capitale umano nel prossimo futuro e per il 2016 stabilisce cinque priorità operative:

- costruire team caratterizzati da talenti eterogenei;
- abbracciare la nuova "equazione del lavoro", ossia tenere presente le forti istanze in termini di personalizzazione del Reward, di trasparenza nei criteri retributivi, di flessibilità nei tempi del lavoro e di opportunità di crescita oggi diffuse tra le popolazioni aziendali;
- progettare percorsi di carriera motivanti e sfidanti per la propria popolazione aziendale;
- semplificare i processi HR tenendo presente l'esperienza offerta agli utenti, sempre più evoluti dal punto di vista digitale;
- ridefinire la centralità della funzione HR.

HACKER E CRISI ENERGETICA: UNA REALTÀ POSSIBILE?

Negli ultimi mesi, il numero di attacchi informatici nel settore Oil & Gas è cresciuto rapidamente. Nell'estate del 2014, oltre 1.000 organizzazioni, con attività in più di 84 paesi sono state vittime di spionaggio industriale attraverso un malware che ne ha compromesso gli asset, bloccando turbine eoliche, gasdotti, centrali elettriche e impianti industriali più in generale. Questo è solo uno dei recenti esempi di cyber attack, a cui assistiamo sempre più di frequente.

La produzione e raffinazione petrolifera, gli oleodotti, la generazione e trasmissione di energia elettrica e molte altre attività alla base della value chain del settore energetico, sono fortemente legate all'Information Technology (IT), che permette di incrementare produttività ed efficienza operativa, fonte di vantaggio competitivo. Tuttavia, se da un lato si trae beneficio dalla crescente interazione fra operations e IT, dall'altro le organizzazioni sono sempre più esposte al rischio di attacchi informatici.

L'ultimo rapporto del World Economic Forum realizzato in collaborazione con alcuni partner, tra cui Oliver Wyman, e intitolato "Global Risks", classifica gli attacchi informatici tra le dieci più probabili cause di una potenziale crisi globale. Anche il World Energy Council si è espresso in tal senso, segnalando i cyber risk tra i cinque maggiori rischi per l'infrastruttura energetica mondiale. In risposta a tale scenario, più di 30 paesi, tra cui l'Italia, hanno definito e comunicato le proprie strategie per la sicurezza informatica. Lo scorso 29 giugno la presidenza lettone del Consiglio UE ha raggiunto un'intesa con il Parlamento Europeo sui principi fondamentali di quella che potrebbe presto diventare una direttiva unificata per difendere le infrastrutture critiche.

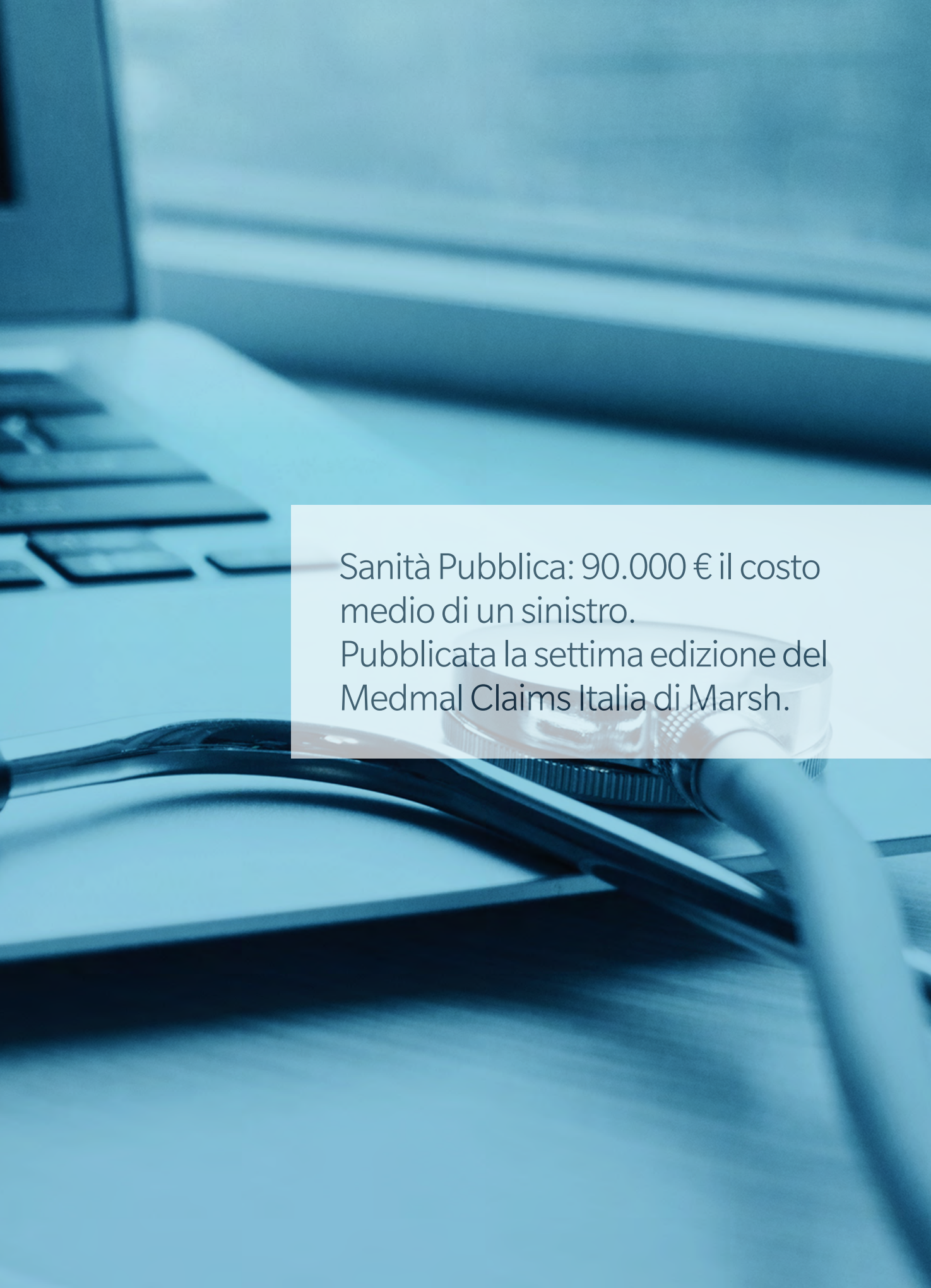
L'ex direttore della National Security Agency degli Stati Uniti, il generale Keith Alexander, ha dichiarato che i diversi paesi

dovrebbero adottare dei sistemi di difesa integrati, affinché il settore energetico possa proteggersi adeguatamente dai rischi informatici. Ad ogni modo, predisporre le risorse necessarie a proteggere in modo più ampio e adeguato le società del settore richiederà tempo, come dimostrano i recenti disaccordi tra la Casa Bianca e i repubblicani in merito all'istituzione di un nuovo Cyber Threat Intelligence Integration Centre.

Intanto, i rischi informatici continuano a crescere e potrebbero presto avere ripercussioni più estese di quanto si possa immaginare. I sistemi di controllo industriale (ICS) non sono più ben protetti da minacce esterne come lo erano un tempo. Oggi, ad esempio, le utility per l'energia elettrica dipendono da controlli automatizzati per la gestione delle proprie reti, che sono a loro volta governate da sistemi interconnessi tra loro. Le società petrolifere si affidano a reti di dati per il controllo degli impianti e per l'interpretazione della geologia e della sismica, e le raffinerie si appoggiano a reti di dati per il governo della produzione e l'analisi della domanda.

Molte società hanno cercato di far fronte alla minaccia di attacchi informatici realizzando nuove e più costose soluzioni IT al fine di mitigare i rischi e stipulando polizze assicurative per il trasferimento del rischio. C'è però ancora molta strada da fare per affrontare il problema in maniera strutturata. E' necessario trattare i rischi informatici come problematiche organizzative (e non funzionali).
A differenza dei rischi strategici, operativi e finanziari, quelli informatici vengono spesso affrontati con priorità secondaria e di stretta pertinenza dell'IT. Inoltre, è importante notare che i sistemi di controllo industriale (ICS) non sempre rientrano nelle responsabilità dei Chief Information Security Officers (CISO). Spesso i manager preposti a garantire la conformità alle policy aziendali non hanno le competenze tecniche per l'analisi del rischio dei sistemi di controllo industriale. Il management sempre più di frequente sottovaluta la reale esposizione ai rischi informatici, che raramente vengono quantificati o correlati al reale potenziale impatto sul business, rendendo pressoché impossibile una solida analisi di costi-benefici sulle iniziative da intraprendere.

E' di vitale importanza che il top management sia promotore di un'adeguata cultura di gestione del rischio informatico, affinché venga assimilata dai dipendenti. Il rischio informatico deve essere parte fondamentale degli obiettivi di performance e degli incentivi aziendali. Gli incidenti informatici devono essere posti in primo piano nelle valutazioni manageriali, soprattutto in merito a violazioni con diretto impatto sulla reputazione della società o che potrebbero alterare gli standard in materia di salute, sicurezza e ambiente.
Ignorare la minaccia potrebbe dar vita a una vera e propria crisi energetica.



Sanità Pubblica: 90.000 € il costo medio di un sinistro.
Pubblicata la settima edizione del Medmal Claims Italia di Marsh.

SANITÀ PUBBLICA ITALIANA: IN MEDIA 4 SINISTRI AL GIORNO NEGLI ULTIMI 10 ANNI

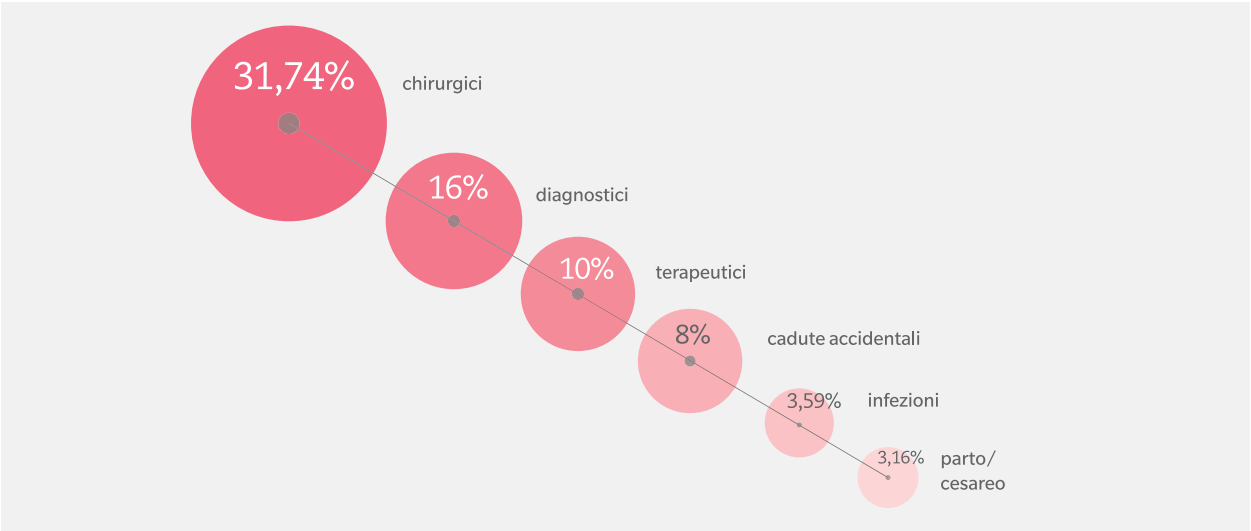
Nel 2014, ultimo anno analizzato dal Report, si registra una lieve riduzione nel numero di sinistri per struttura, mentre si confermano in cima alla classifica quelli causati da errori chirurgici.

1 miliardo e quattrocento milioni di euro in risarcimenti: questo è il valore (tra somme effettivamente liquidate e somme stanziate dalle assicurazioni) dei sinistri nella sanità pubblica in Italia sul campione analizzato da Marsh nel periodo 2004 - 2014. Se questa cifra è da capogiro, non è meno impegnativo il costo medio di 90.000 euro all'anno per sinistro, in aumento del 13% dall'inizio del periodo considerato. Questo è quanto emerge dalla settima edizione del Medmal Claims Italia, il report di Marsh che quest'anno ha analizzato le richieste di risarcimento danni dal 2004 al 2014, su un campione di 59 strutture della sanità pubblica, per un totale di circa 15.600 sinistri.

Andando a considerare solo gli importi liquidati, si registra un incremento continuo del costo medio per anno di chiusura dall'inizio del periodo considerato, ma fra questi i risarcimenti per errori da parto si confermano come i più elevati in assoluto in termini di importo liquidato medio, con un caso che ha toccato oltre 4 milioni di euro. Gli errori da parto costituiscono, infatti, quasi il 20% dei top claim, ovvero i sinistri in cui il costo di denuncia è uguale o superiore ai 500.000 euro. Il medesimo trend in aumento si riscontra nell'andamento degli importi riservati medi per anno di denuncia, che rilevano un aumento di circa il 20% dal 2013 al 2014.

La frequenza annua dei sinistri è di 30 per ogni singola struttura nel 2014, in leggera diminuzione rispetto all'anno precedente (35), una cifra che fa registrare un tasso di rischio di 7 sinistri ogni 100 medici, di 3 ogni 100 infermieri e di 1 ogni 1000 ricoveri, per valori assicurativi che superano i 6.000 euro per medico e si attestano sui 2.400 euro per infermiere.

Classifica degli errori più frequenti in Sanità Pubblica
Fonte: Medmal Claims Italia di Marsh



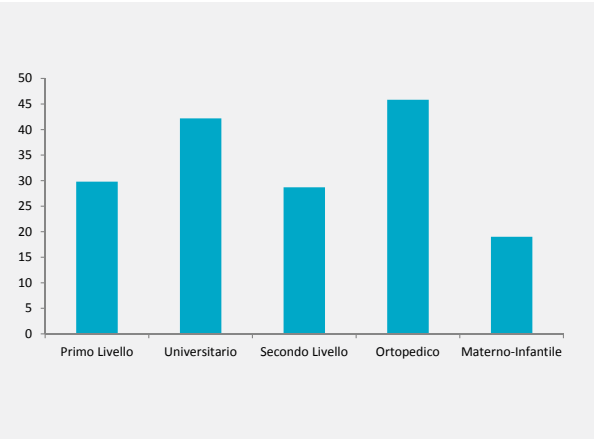
La classifica degli errori vede anche quest'anno gli errori chirurgici al primo posto (31,64%), seguiti da errori diagnostici (16%) e terapeutici (10%). Dopo le cadute accidentali all'8%, troviamo una prevalenza di infezioni (3,59%) ed errori da parto/cesareo (3,16%). Andando ad analizzare l'incidenza dei sei errori che impattano maggiormente nel periodo di tempo analizzato, la percentuale degli errori chirurgici negli ultimi anni sta diminuendo, anche come conseguenza del miglioramento delle tecniche chirurgiche, mentre la percentuale degli errori da parto sta aumentando.

Si confermano, come nelle precedenti edizioni, tempi molto lunghi per le denunce dei sinistri, basti pensare che meno dell'80% delle richieste di risarcimento danni per le infezioni e per gli errori da parto è denunciato entro i primi 4 anni. Solo gli errori diagnostici vengono denunciati molto rapidamente ed entro il primo anno raggiungono il 50%, per superare la quota di 80% entro i tre anni. E' però interessante rilevare che sono ancora numerosi i casi in cui il sinistro viene denunciato in prossimità dei termini di prescrizione: ciò significa che non è possibile ritenere completato il manifestarsi di un'intera generazione di sinistri neppure a distanza di 10 anni dall'erogazione delle prestazioni.

Le specialità cliniche che subiscono la maggiore frequenza di richieste di risarcimento danni sono Ortopedia e Traumatologia (13 %), seguita da Chirurgia Generale (12%), DEA/Pronto Soccorso (12%), Ostetricia e Ginecologia (8%) e le parti comuni/la struttura con quasi il 7%. Da un esame complessivo di tutte le tipologie di eventi all'interno delle Unità Operative si può riscontrare che in Ortopedia l'errore più diffuso è quello chirurgico (ad esempio lesione dopo un intervento di protesi all'anca), seguito da quello diagnostico; in Chirurgia Generale si riscontra una prevalenza di errori chirurgici e di infezioni; in DEA/Pronto Soccorso gli errori più frequenti sono quelli diagnostici (ad es. fratture non diagnosticate) e quelli terapeutici (ad esempio errato trattamento prescritto per l'ipertensione), seguiti dalle cadute accidentali; in Ostetricia e Ginecologia invece si rileva una maggioranza di errori chirurgici (come un errato intervento di chirurgia all'ovaio), mentre al secondo posto si trovano gli errori da parto/cesareo (ad esempio la morte di un neonato a seguito di parto); nelle parti comuni della struttura si possono riscontrare soprattutto cadute accidentali, ma anche infortuni ad operatori.

Se poi si analizzano gli errori per tipologia di ospedale, i risultati mostrano che gli ospedali ortopedici presentano il più alto livello di rischio con oltre 45 sinistri per anno, seguono gli ospedali universitari, le strutture di primo livello, quelle di secondo livello e infine quelle materno-infantili.

N. sinistri medi all'anno per tipo di ospedale
Fonte: Medmal Claims Italia di Marsh



Unità operative maggiormente soggette a sinistro
Fonte: Medmal Claims Italia di Marsh

UNITÀ OPERATIVE	%
Ortopedia e Traumatologia	13,14%
Chirurgia Generale	12,16%
DEA/ Pronto Soccorso	11,58%
Ostetricia e Ginecologia	8,39%
Struttura/ Parti Comuni	6,98%

La tipologia di procedimento più frequente è quella stragiudiziale (72.3%), a conferma di un trend di crescita del ricorso al procedimento stragiudiziale che non si è mai arrestato nel corso degli anni presi in esame dal report. Se il maggiore ricorso al procedimento stragiudiziale può aiutare ad abbreviare i tempi di chiusura dei sinistri – il 68,3% di questi viene chiuso entro il secondo anno –, occorre comunque aspettare in media otto anni per chiudere la totalità dei sinistri aperti in un dato anno.

LE AZIENDE ITALIANE "PROMUOVONO" LE NOVITÀ SUL WELFARE AZIENDALE

A distanza di qualche mese dall'approvazione della legge di Stabilità, un'indagine di Marsh e Edenred coglie la prima impressione delle aziende sui cambiamenti proposti dal Governo sul Welfare.

Se la maggioranza degli intervistati ritiene che la legge di Stabilità apra nuove opportunità per ripensare il piano benefit, in realtà solo 3 su 10 pensano che le aziende sul territorio siano pronte a gestire questo cambiamento.

Per 6 aziende su 10 le novità introdotte dalla Legge di Stabilità 2016 in materia di Welfare aziendale sono un'opportunità per ripensare e modificare il pacchetto di benefit per i dipendenti. Si tratta di una sostanziale promozione delle modifiche normative recentemente previste dal Parlamento*, secondo l'indagine condotta da Marsh e Edenred, azienda leader nel settore del welfare aziendale e dei benefit per i dipendenti, su un campione di 186 aziende in Italia, rappresentative di tutti i settori merceologici e di tutte le classi dimensionali.

Le più positive sembrano soprattutto le aziende di grandi dimensioni (oltre i 1.000 dipendenti) che in 6 casi su 10 vedono questa riforma utile anche nelle negoziazioni sindacali. Ma in generale il feedback raccolto non cambia molto in base alla dimensione o al settore di appartenenza.

Oltre la metà del campione ritiene che non tutte le aziende italiane siano già pronte e che manchino soprattutto le competenze/risorse necessarie a cogliere quest'opportunità. E questo è particolarmente vero per le imprese sotto i 50 dipendenti dove la preoccupazione sale al 70%.

La possibilità di detassare completamente il premio di produttività finalizzandolo all'acquisto di beni e servizi viene visto come un'opportunità di aumentare il potere d'acquisto

dei dipendenti. Lo conferma il 67% del campione. Chiamato a esprimersi su una delle principali innovazioni dalla Legge di Stabilità, ovvero la cura dei familiari (in particolare bambini e anziani), il 50% degli intervistati ritiene che favorirà un miglior equilibrio tra impegni personali e lavorativi dei propri dipendenti; per il 15% migliorerà l'engagement; per un 14% incrementerà la produttività favorendo una riduzione delle assenze, e un altro 15%, pur prevedendo effetti positivi su benessere e produttività, non è in grado di stimarli.

In conclusione, le novità introdotte dalla Legge di Stabilità favoriscono quella flessibilità in materia di benefit che oggi ancora manca in molte aziende e che riflette i mutati bisogni ed esigenze dei dipendenti. Le risposte al sondaggio fotografano, infatti, un panorama aziendale che è sempre più convinto del legame tra benessere dei dipendenti, produttività e engagement e in cui le aziende sono maggiormente propense a ripensare il welfare.

*La legge di Stabilità 2016 ha introdotto importanti novità in materia di welfare aziendale, attraverso un chiaro contesto normativo caratterizzato da vantaggi fiscali e contributivi sia per le aziende sia per i dipendenti. La nuova normativa allarga inoltre il paniere di prestazioni e servizi che possono essere offerti ai dipendenti e ai loro familiari con la finalità di colmare i gap sempre più ampi del nostro welfare pubblico.

LA COPERTURA TRADE CREDIT: MAI COSÌ UTILIZZATA

Il mancato pagamento dei debiti commerciali è l'ennesima conseguenza della persistente crisi economica.

In questi anni si è registrato, secondo la BCE, un forte incremento nell'utilizzo delle coperture trade credit, un trend che è destinato a crescere anche nel 2016, anche se le previsioni assicurano che i sinistri legati a questa polizza, ovvero i mancati pagamenti, sono destinati quantomeno a stabilizzarsi.

Il maggior ricorso alla polizza credito rappresenta un chiaro segno di instabilità della nostra economia, ma, se visto in una logica più ampia, si tratta di una leva che contribuisce alla crescita delle aziende, perché ne agevola l'attività di espansione commerciale, consentendo di coltivare relazioni di business anche con nuovi acquirenti.

L'obiettivo primario rimane proteggere l'attivo del bilancio, rendendo l'azienda più solida e meno esposta alle incertezze del mercato. Per raggiungere questo obiettivo è importante che le aziende prestino sempre più attenzione alla gestione del rischio credito, vedendo l'assicurazione come uno strumento di prevenzione, quale essa è effettivamente, piuttosto che un mero strumento di indennizzo delle perdite.

In uno scenario di mercato che vede per le aziende un tendenziale aumento dei rischi legati ai mancati incassi e alle insolvenze dei propri clienti, diventa essenziale adottare una politica di credit management idonea a prevenire, controllare e gestire tale problematica.

Questo è vero in particolare per alcuni settori come le costruzioni e l'agroalimentare i cui mancati pagamenti sembrano essere più elevati rispetto al 2014.
Alcuni segnali di miglioramento, seppur deboli, sono stati invece registrati dal tessile, servizi, meccanica e chimica.

Con la polizza trade credit, l'attività viene protetta sia dal punto di vista finanziario che del risultato economico, grazie al miglioramento dei tempi di incasso e a una maggiore puntualità dei pagamenti, a una pianificazione commerciale facilitata dalla riduzione dei rischi inattesi, alla diminuzione dei crediti inesigibili e alla riduzione delle controversie e dei reclami. Si liberano così risorse da dedicare ad attività più remunerative, come l'apertura di nuove linee d'affari.

A più lungo termine, la copertura per i crediti commerciali favorisce anche l'incremento del fatturato grazie alle vendite con pagamento dilazionato, senza intaccare il proprio bilancio per finanziare i rischi che ne potrebbero derivare. Infine, contribuisce all'equilibrio finanziario dell'azienda, che in forza della copertura assicurativa ottiene più agevolmente il finanziamento dei crediti commerciali concessi ai propri clienti e condizioni di prestito agevolate.

PRINCIPALI COPERTURE ASSICURATIVE – TRADE CREDIT

Whole Turnover o Globale
Struttura di servizi correlata a una copertura assicurativa che ha lo scopo di supportare l'impresa in tutte le fasi del processo di gestione del credito commerciale. E' la più nota e funziona attraverso il principio di affidamento dei singoli clienti/debitori dell'assicurato.

Excess of loss
Copertura studiata per le realtà medio-grandi, operanti nel mercato OCSE, che dispongono di una struttura di Credit Management. La Compagnia mette a disposizione dell'assicurato un massimale annuo per coprire le perdite eccedenti un livello predefinito, rappresentato dalla franchigia globale annua.

Rischi singoli
Questo tipo di soluzione, contrariamente al principio di globalità ed antiselezione del rischio tipico delle coperture tradizionali, consente la copertura di singole forniture o di tutte le vendite a singoli clienti scelti dall'assicurato.

Key buyer
Questo tipo di contratto prevede la limitazione della copertura assicurativa ai soli principali clienti dall'assicurato.

Top Up
Soluzione a integrazione di una copertura "base" già attivata. Deve prevedere il coordinamento con la polizza base per quanto riguarda l'attribuzione dei recuperi.

LA PROTEZIONE DELLA PROPRIETÀ INTELLETTUALE COME LEVA STRATEGICA PER UNA CRESCITA SOSTENIBILE

L'Italia è un "innovatore moderato", così ci descrive la European Innovation Union Scoreboard 2015 che evidenzia, anche con alcuni indicatori virtuosi quali la crescita della diffusione di pubblicazioni scientifiche internazionali (+9,5% rispetto al 2014), di dottorati extraeuropei (+19%) e dei ricavi generati da licenze e brevetti internazionali (+18%), una sempre maggiore attenzione verso tematiche di innovazione, ricerca e sviluppo a livello sia micro che macro-economico.

Il cosiddetto "know-how" aziendale risiede in un set di informazioni critiche, identificabili come Intellectual Property Asset (IP Asset), che sono la base su cui viene costruita una crescita sostenibile. Per mantenere lo sviluppo e il vantaggio competitivo, le aziende devono poter massimizzare lo sfruttamento degli IP Asset e nello stesso tempo proteggerli, impedendo che attuali o «futuri» competitor se ne approprino.

Apparentemente però la difesa della proprietà intellettuale non è fra le priorità nel nostro paese: l'edizione 2015 di IPRI (International Property Rights Index), l'indice che dal 2007 misura la diffusione dei sistemi di tutela in materia di diritti di proprietà (fisica ed intellettuale), ci colloca in cinquantunesima posizione nel mondo, 10 posizioni in meno rispetto all'edizione 2014, e diciottesima tra i paesi EU. A pesare è l'incertezza del sistema giudiziario che nell'ultimo anno è crollato da 1.2 a 4.2, mentre altri parametri sono rimasti identici al 2014, come la stabilità politica e il livello della corruzione. Inoltre, è aumentato il livello della pirateria mentre la protezione dei brevetti è rimasta invariata.

Quale indagine ci rappresenta meglio? Probabilmente entrambe le fonti raccontano una verità sull'Italia, è però certo che i sistemi di protezione e controllo degli IP Asset aziendali presentano delle mancanze:

- disallineamento tra obiettivi strategici aziendali in termini di Innovation Strategy e soluzioni di protezione degli IP Asset implementate (ad esempio, lo sfruttamento di un contributo di un partner esterno nello sviluppo di innovazioni senza aver adottato misure contrattuali e IT preventive);
- presidio della sola attività di brevettazione come strumento di protezione dell'IP Asset;
- scarsa consapevolezza nella gestione dei flussi delle informazioni critiche sia all'interno dell'organizzazione (tra diversi dipartimenti), sia verso l'esterno (clienti, fornitori, partner, etc.)

Un'efficace strategia di protezione e sfruttamento degli IP Asset deve tenere in considerazione le diverse possibili aree di presidio dell'informazione e fare in modo che queste operino in maniera sinergica e coerente con gli obiettivi strategici aziendali. Le aree su cui sarebbe opportuno intervenire sono quattro:

- **Information Technology:** identificare le informazioni critiche e implementare soluzioni di protezione con riferimento sia ai flussi interni, sia ai flussi esterni;
- **Legal & Contractual:** delineare opportuni presidi contrattuali nei confronti di collaboratori interni e terze parti, finalizzati a definire la proprietà intellettuale e impedire che la stessa venga divulgata e condivisa ulteriormente;
- **Patent:** definire, coerentemente con l'indirizzo strategico, un processo di brevettabilità degli IP Asset che consideri la valutazione di diversi aspetti (requisiti di brevettabilità, previsioni economico-finanziarie, etc.);

- **Procedures and Organization:** armonizzare le policy interne al fine di porre un focus sulla gestione delle informazioni critiche e istituire, laddove necessario, una funzione dedicata alla gestione delle tematiche connesse alla protezione degli IP Asset.

Si tratta di un passaggio obbligato per le aziende che vogliono crescere, ma anche per l'intero sistema paese: i risultati dell'International Property Rights Index 2015 dimostrano chiaramente come i paesi che più tutelano la proprietà sono anche quelli che crescono più stabilmente, sono più competitivi e producono maggiore innovazione. Solo per citare i casi più eclatanti, le nazioni in cima alla classifica come Finlandia, Norvegia e Nuova Zelanda, godono di un PIL medio pro capite nazionale di 44.500 dollari, mentre le medie registrate nei paesi che occupano le posizioni più arretrate della classifica scendono fino a 1.880 dollari.

ECOREATI PUNITI ANCHE CON 20 ANNI DI RECLUSIONE

Pene alla persona, ma anche aggravio della posizione di enti e organizzazioni: tutti i provvedimenti e le conseguenze per le aziende, a distanza di dodici mesi dall'entrata in vigore della legge "Disposizioni in materia di delitti contro l'ambiente".

Anche se non sono mancate critiche sulla scarsa chiarezza di alcuni passaggi, la portata innovativa della norma è stata imponente, perché il reato ambientale è entrato nella categoria dei delitti sanzionati dal Codice Penale con cinque nuove fattispecie: l'inquinamento ambientale e la sua forma aggravata da morte o lesioni, il disastro ambientale, il traffico e l'abbandono di materiale ad alta radioattività, l'impedimento del controllo e l'omessa bonifica.

Riguardo all'inquinamento ambientale, chiunque abusivamente cagioni una compromissione o un deterioramento "significativi e misurabili" dello stato preesistente "delle acque o dell'aria, o di porzioni estese o significative del suolo e del sottosuolo o di un ecosistema, della biodiversità, anche agraria, della flora o della fauna" sarà punibile con la reclusione da 2 a 6 anni, la multa da 10.000 a 100.000 euro e la confisca dei beni. Rientrano in questi casi la contaminazione significativa del suolo attraverso perdite dalla rete fognaria, l'inquinamento dell'aria con contaminanti rilasciati attraverso le emissioni in atmosfera (per esempio polveri sottili) o l'affidamento di materiale ad alta radioattività a società non autorizzate. Sono inoltre previste delle aggravanti a seconda che dall'inquinamento ambientale comporti a una persona una lesione personale grave, gravissima o la morte; inoltre, se gli eventi lesivi derivati dal reato sono molteplici e a carico di più persone, si applica la pena che dovrebbe infliggersi per il reato più grave aumentata anche del triplo, fino a 20 anni di reclusione.

Il reato di disastro ambientale riguarda un'alterazione irreversibile dell'equilibrio di un ecosistema, la cui

eliminazione risulti particolarmente onerosa e conseguibile solo con provvedimenti eccezionali. La sua gravità è determinata con riferimento all'estensione della compromissione ambientale o dei suoi effetti lesivi e al numero delle persone offese o esposte al pericolo. Le pene applicabili sono la reclusione da 5 a 15 anni, con un aggravio nel caso in cui il reato sia commesso in un'area protetta o sottoposta a vincolo o in danno di specie animali o vegetali protette.

L'art. 452-sexies prevede per il reato di pericolo di traffico e abbandono di materiali ad alta radioattività la reclusione da 2 a 6 anni e la multa da 10.000 a 50.000 euro, mentre l'impedimento del controllo ambientale, che avviene negando o ostacolando l'accesso ai luoghi, ovvero mutando artificiosamente il loro stato, è punito con la reclusione da 6 mesi a 3 anni.

Infine, il reato di omessa bonifica, che punisce chi, pur obbligato, non provvede alla bonifica, al ripristino e al recupero dello stato dei luoghi, prevede pene tra un minimo di un anno e un massimo di 4, con una multa da 20.000 a 80.000 euro.

Oltre a riformare il sistema dei delitti ambientali, la legge 68/2015 è intervenuta anche sulla responsabilità degli enti, aggiungendo le nuove fattispecie tra i reati contemplati dal modello 231/2001 e prevedendo sanzioni fino a 1 milione e mezzo di euro, con possibilità di applicazione di tutte le sanzioni interdittive fino ad un massimo di 1 anno.

Si tratta di sanzioni severe, che possono pregiudicare l'esistenza di un'azienda di piccole e medie dimensioni. Il nuovo contesto legislativo, quindi, obbliga le aziende – e le più avvedute si stanno già attrezzando – a munirsi di misure utili al monitoraggio delle proprie attività, per prevenire la commissione dei reati ambientali.

Diventa dunque essenziale sapere in che modo l'azienda può compromettere le matrici ambientali (acqua, aria, suolo); quali misure tecniche e organizzative sono state messe in atto per prevenire e controllare fenomeni di inquinamento e se queste sono efficaci; in che modo l'azienda assicura la piena collaborazione e trasparenza con gli Enti e, infine, quali verifiche vengono eseguite sugli appaltatori e subappaltatori per assicurare la corretta gestione, anche dal profilo ambientale, delle attività.

UN PUNTO A FAVORE DELL'AMBIENTE

La ratifica dell'Accordo sul Clima di Parigi pone le basi per un vero impegno globale a tutela del Pianeta.

Il 22 aprile 2016 è stato ratificato l'Accordo sul clima raggiunto durante Cop21, la Conferenza di Parigi sui cambiamenti climatici. "Una giornata storica" così l'ha definita il segretario delle Nazioni Unite Ban-Ki moon perché mai prima d'ora così tanti Paesi – 175 quelli che hanno ratificato l'accordo contro i 194 che lo hanno siglato – si sono uniti in un fronte comune per la salvaguardia dell'ambiente.

Ma l'accordo di Parigi sarà efficace? Lo sperano tutti e la sua semplicità ne è una buona premessa. Il documento si articola, infatti, sostanzialmente, su tre punti chiave; il primo, che è stato il vero successo della Conferenza, è la riduzione delle emissioni che alterano il clima in modo da contenere il riscaldamento climatico in un range compreso tra i +2°C e +1,5°C entro il 2050. Agli inizi della Conferenza, i singoli Paesi proponevano riduzioni insufficienti delle emissioni (che avrebbero comportato un aumento di 4°C della temperatura), ma la volontà di raggiungere una soluzione epocale ha mosso tutti verso un'unica direzione.

Il secondo punto prevede un incentivo finanziario di 100 miliardi di dollari fino al 2020 a disposizione dei paesi in via di sviluppo per adottare modelli di progresso meno inquinanti: in questo caso si tratta di un buon compromesso tra Paesi in via di sviluppo, che reclamavano sia il diritto a inquinare sia gli investimenti finanziari delle economie avanzate per iniziare a farlo meno, e dall'altra i Paesi più maturi che invece cercavano di imporre una crescita green anche ai Paesi in via di sviluppo.

Infine, il terzo punto, quello più tecnico. La questione centrale era se il rispetto dell'accordo dovesse essere vincolante o meno. Alcuni Paesi, infatti, tra cui gli Stati Uniti, tradizionalmente non sottoscrivono accordi vincolanti. Tuttavia, altre nazioni (o gruppi di nazioni, come l'Unione Europea) ritenevano fondamentale, data la materia

dell'accordo, che fosse vincolante, ovvero che prevedesse un meccanismo di controllo e di sanzione in caso un firmatario non rispettasse l'impegno. La soluzione trovata è stata quella di prevedere un meccanismo di controllo del rispetto dell'Accordo, ma (al momento) non di sanzione.

L'accordo entrerà in vigore 30 giorni dopo che almeno 55 paesi, che rappresentano il 55% delle emissioni globali di gas a effetto serra, depositeranno gli strumenti di ratifica o di accettazione presso il segretario generale e, ad oggi, sono solo 15 i Paesi ad averlo già fatto.

PROPRIETÀ INTELLETTUALE: LA PRIORITÀ NUMERO UNO È CONOSCERE GLI ASSET DI CUI DISPONE L'AZIENDA

Massimiliano Pappalardo (D&P Legal)

Il punto di partenza per una strategia di protezione della proprietà intellettuale di un'azienda può certamente essere individuata in una corretta identificazione degli IP asset.

Non sempre, pur a fronte di significativi investimenti di risorse finanziarie e umane in sede di sviluppo, le aziende prestano un'eguale attenzione riguardo alla tutela del risultato del processo creativo e all'individuazione delle modalità più efficienti per la sua protezione.

Trattandosi di beni immateriali, di "intangibles", quanto detto è particolarmente vero laddove il processo di sviluppo di un procedimento o di un nuovo prodotto, come spesso accade, non sfoci in una soluzione brevettuale e, quindi, in un titolo di proprietà industriale ben individuato.

Senza una corretta identificazione dei set di informazioni relativi al processo o al prodotto, capaci di attribuire all'azienda un vantaggio competitivo, diviene impossibile approntare un'adeguata protezione degli stessi, all'interno dell'azienda e nei rapporti con partner esterni.

A tal riguardo, è opportuno sottolineare che la normativa italiana (articolo 98 D.Lgs. N.30/2005) attribuisce diritti di privativa – in termini di possesso ed esercizio esclusivo – non solo all'invenzione brevettata, ma, altresì, alle informazioni aziendali e alle esperienze tecnico-industriali soggette al legittimo controllo dell'azienda. Se si tratta di informazioni segrete, nel senso che non sono nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti e agli operatori del settore, hanno valore economico e devono essere sottoposte a misure tali da ritenersi ragionevolmente adeguate a mantenerle segrete.

La normativa italiana riconosce tutela, in quanto asset di proprietà aziendale, ai cosiddetti "trade secret", la cui protezione è anche oggetto di una proposta di direttiva in ambito UE. Naturalmente per poter verificare la sussistenza dei requisiti sopra specificati e, in particolare, l'implementazione di adeguate misure di protezione interne ed esterne, è imprescindibile la consapevolezza da parte dell'azienda circa quali siano le informazioni meritevoli di una simile protezione.

AUSTRIA
Vienna

AZERBAIJAN
Baku

BELGIO
Antwerp
Bruxelles
Liegi
Roeselare

BULGARIA
Pleven
Sofia
Varna

CROAZIA
Osijek
Spalato
Zagabria

REPUBBLICA CECA
Brno
Liberec
Praga

CIPRO
Limassol

DANIMARCA
Virum

ESTONIA
Tallinn

FINLANDIA
Espoo
Oulu

FRANCIA
Aix-en-Provence
Bordeaux
Lille
Lione
Orange
Parigi
Tolosa

GERMANIA
Berlino
Detmold
Düsseldorf
Francoforte
Amburgo
Lipsia
Monaco
Stoccarda

GRECIA
Atene

UNGHERIA
Budapest

ISRAELE
Ramat Gan

ITALIA
Ancona
Bologna
Brescia
Cagliari
Catania
Firenze
Genova
Mantova
Milano
Padova
Palermo
Roma
Torino

KAZAKISTAN
Almaty

LETTONIA
Riga

LITUANIA
Vilnius

LUSSEMBURGO
Lussemburgo

PAESI BASSI
Amsterdam
Rotterdam
Hertogenbosch

NORVEGIA
Kristiansand
Oslo
Trondheim

PORTOGALLO
Lisbona
Oporto

POLONIA
Gdańsk
Krakow
Poznan
Varsavia
Wroclaw

ROMANIA
Bucarest
Cluj-Napoca
Timisoara

RUSSIA
Mosca
San Pietroburgo

SERBIA
Belgrado

SLOVACCHIA
Bratislava
Kosice

SLOVENIA
Lubiana

SPAGNA
La Coruña
Barcellona
Bilbao
Canarias
Gijón
Madrid
Murcia
Pamplona
Siviglia
Valencia

SVEZIA
Goteborg
Malmö
Stoccolma

TURCHIA
Adana
Ankara
Bursa
Gaziantep
Istanbul
Izmir

UCRAINA
Kiev

Marsh S.p.A .
Viale Bodio 33, 20158 Milano
Tel. 02.48538.1
www.marsh.it
communication-italy@marsh.com

Direttore responsabile Barbara Ghirimoldi
Coordinamento redazionale Chiara Valenti
Design grafico Gloria Derba

Hanno collaborato:
Marco Bagattin
Marco Lazzari (MRC)
Miriam Marchetti (MRC)
Sandro Melis (Oliver Wyman)
Elisa Notarangelo (MRC)
Angelo Rosiello (Oliver Wyman)
Silvio Sperzani (Oliver Wyman)
Silvia Vanini (Mercer)

External Contributor
Massimiliano Pappalardo (D&P Legal)

M. BOLLETTINO D'INFORMAZIONE DI MARSH SPA - Registrato al Tribunale di Milano n. 253, 25 maggio 2009
Stampatore: Grafiche Milani S.p.a. Via Marconi 17, 20090 Segrate (Mi) Italia