Ricerca Deloitte e The Innovation Group

"Cyber Risk Management Italia v1.0 - Modelli di governance dei rischi cyber e raccomandazioni di sviluppo per le aziende italiane"

- *Per il 31% delle Società italiane analizzate il rischio Cyber è considerato dalla funzione di Risk Management aziendale (solo) come un rischio tecnologico, rientrando nello specifico tra i rischi ICT. Nel 31% dei casi non viene incluso nell'Enterprise risk management reporting e molto spesso non viene monitorato costantemente. Solo il 35% dei rispondenti ha dichiarato di utilizzare estensivamente un framework strutturato per la gestione dei Cyber Risk*
- *Il modello di governo dei cyber risk prevede la presenza di un CISO (Chief Information Security Officer) solo nel 40% delle organizzazioni analizzate*
- *Il 50% delle Società analizzate non sembra aver formalizzato, all'attenzione del CdA e/o dei comitati di controllo specifici, momenti destinati strutturalmente alla discussione dei propri Cyber Risk*
- *Il 57% delle aziende intervistate dichiarano di avere uno skill shortage rispetto alle competenze necessarie a far fronte alle necessità attuali e future per la gestione dei Cyber Risk*
- *Gli investimenti in ambito cybersecurity mostrano una crescita, da valori pari al 1-2% del totale budget ICT verso valori del 3-5%*

Milano, 23 maggio 2016 – L'aumento incessante della digitalizzazione dei processi di business e la necessità di un sempre maggiore livello di collaboration-sharing-networking delle modalità produttive, associati alla globalizzazione e alla "commercializzazione" del cyber- crimine, hanno guidato una maggiore frequenza e gravità degli incidenti informatici e data breaches, attraverso modalità sempre più sofisticate di esecuzione di attacchi mirati al capitale informativo delle aziende.

Lo sviluppo di nuove tecnologie (Internet of Things, mobile Apps, etc.) sta producendo un numero crescente di oggetti fisici connessi a Internet e un maggiore rischio di "permeabilità" dei perimetri aziendali da parte di malicious attackers in grado di identificare le vulnerabilità generate dalla stratificazione di diverse tipologie di tecnologie, non sempre adeguatamente presidiate dalle organizzazioni. I rischi cyber non sono un problema relativo alla sola funzione ICT dell'azienda ma riguardano tutti gli aspetti della sostenibilità del business e la competitività delle aziende nel lungo periodo, in particolare se con strategie di sviluppo su mercati globali. Nonostante questo, il rischio Cyber sembra essere il rischio più sottovalutato da parte delle imprese, anche dalle stesse funzioni che hanno come proprio mandato il compito di supportare il management nel valutare e gestire adeguatamente i rischi nelle scelte strategiche e operative aziendali.

Consci di questo mutevole contesto, Deloitte e The Innovation Group hanno voluto effettuare una survey su un campione di 52 aziende italiane appartenenti ai diversi settori di mercato, per approfondire gli aspetti principali legati alla gestione del rischio Cyber: dal titolo "**Cyber Risk Management Survey 2015**".

I risultati della survey hanno evidenziato una forte preminenza della funzione ICT nella gestione delle tematiche legate ai cyber risk, che sono percepiti ancora principalmente come rischi IT, ma con una positiva tendenza da parte del top management ad interrogarsi sull'identificazione di più modalità di valutazione dei rischi Cyber che siano sempre più complete, quantitative e soprattutto che riescano a descrivere meglio i possibili impatti sul business.
Alla luce di quanto sopra, si nota come le priorità per le aziende si dovranno orientare sempre più verso l'adozione di robuste strutture di governance anche per la cybersecurity, capaci di garantire un completo presidio della materia anche attraverso la costituzione di specifici "momenti" nei quali i comitati di controllo e/o i CdA possano focalizzare la loro attenzione sul tema del Cyber Risk, magari introducendo nei Board dei Director con competenze in ambito cybersecurity e/o attraverso l'effettiva adozione di framework strutturati per la gestione dei Cyber Risk (Cyber Risk Management), che a oggi risultano ancora poco utilizzati in modo estensivo e completo (circa solo dal 35% dei rispondenti). (Figura 1)

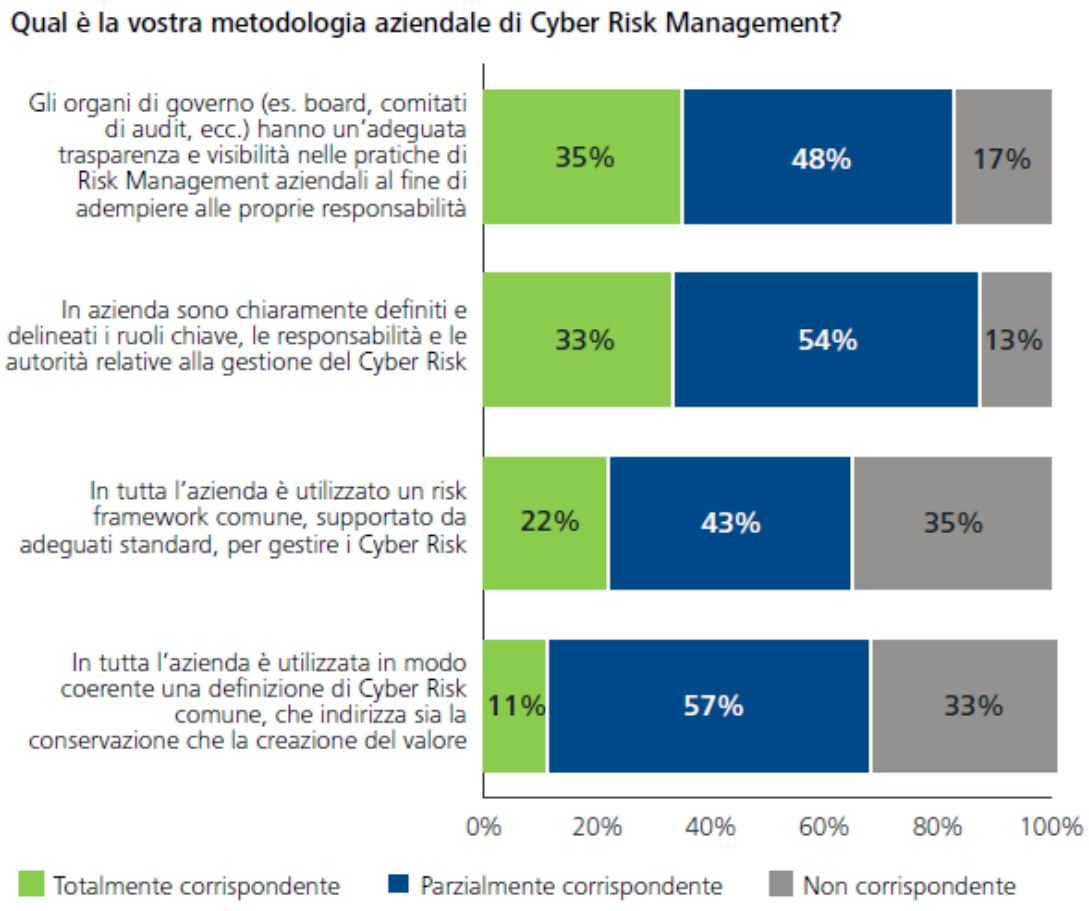

Figura 1: Modello adottato per il Cyber Risk Management

Anche se a oggi questi aspetti non sempre risultano adeguatamente presidiati, la survey rileva delle chiare dichiarazioni di intenti:

- Il 12% delle organizzazioni dichiara di aver istituito un comitato specifico per discutere i rischi cyber; il 39% delle aziende li gestisce nell'ambito di altri comitati (Comitati Risk & Compliance/CdA) e i momenti di "confronto" con il Board sono limitati.

- La struttura organizzativa per la gestione del cyber risk vede per il 40% delle aziende intervistate la presenza di un CISO e in questi casi il 67% dei CISO riportano al CIO, all'interno dell'unita di ICT operations o in staff allo stesso CIO.
- Nella maggioranza dei casi i rischi cyber non sono inclusi, della funzione preposta al monitoraggio dei rischi aziendali, tra i rischi strategici, ma valutati all'interno delle categorie dei rischi operativi o dei rischi ICT (che sommate contano circa il 50% dei casi). Spesso sono vengono identificati strutturalmente, ma lasciati in gestione (e visibilità) solo della funzione ICT che li rende resi noti agli executive solo in caso di incidenti rilevanti (che sommati contano circa il 33% dei casi). (Figura 2)
- Solo in pochissimi casi sono stati identificati KRI (key risk indicator) per la misurazione del rischio cyber (18%), o metriche allineate con il business (19%) e documentate periodicamente, ma circa il 50% dei rispondenti dichiara di avere un programma di sicurezza come parte integrante dell'ERM aziendale, molto focalizzato sulla protezione del business, in cui l'Information security Management & Reporting è una top priority.
- Al momento una percentuale del 2% del nostro campione fa ricorso a coperture assicurative per il trasferimento del rischio cyber, ma è evidente un interesse in queste forme di trasferimento del rischio.

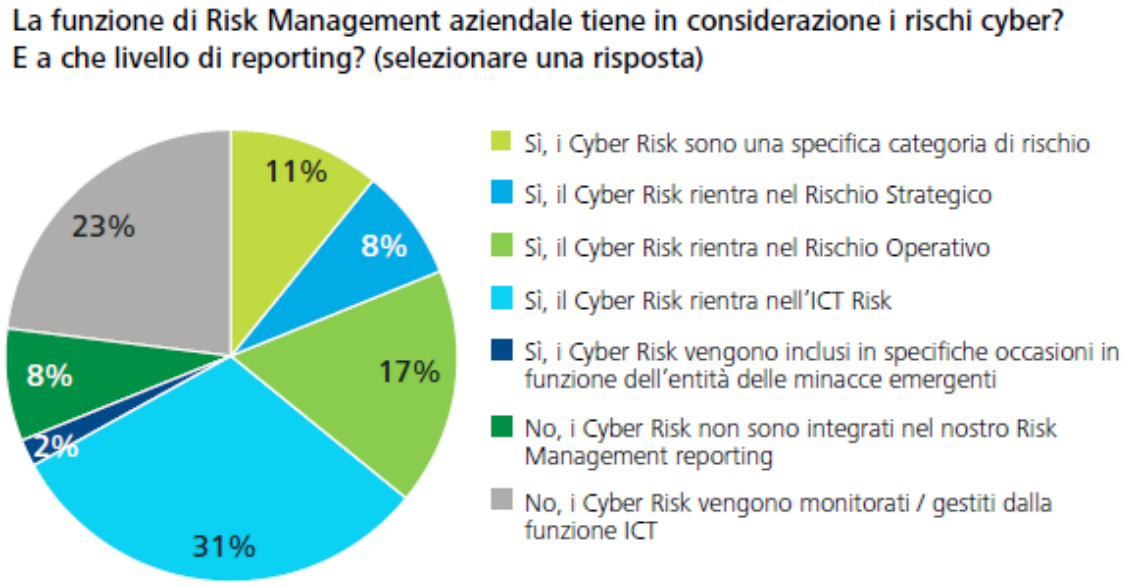

Figura 2: Solo per l'8% delle aziende il rischio cyber è considerato strategico

Dalla survey emerge l'intenzione chiara di investire nei prossimi anni nell'applicazione di un framework di Cyber Risk Management mutuati dalle leading practice internazionali, nell'Incident Response e nell'aumento di consapevolezza degli utenti finali, in linea con quanto indicato anche in Italia da parte del recente Framework Nazionale per la Cyber Security. (Figura 3)

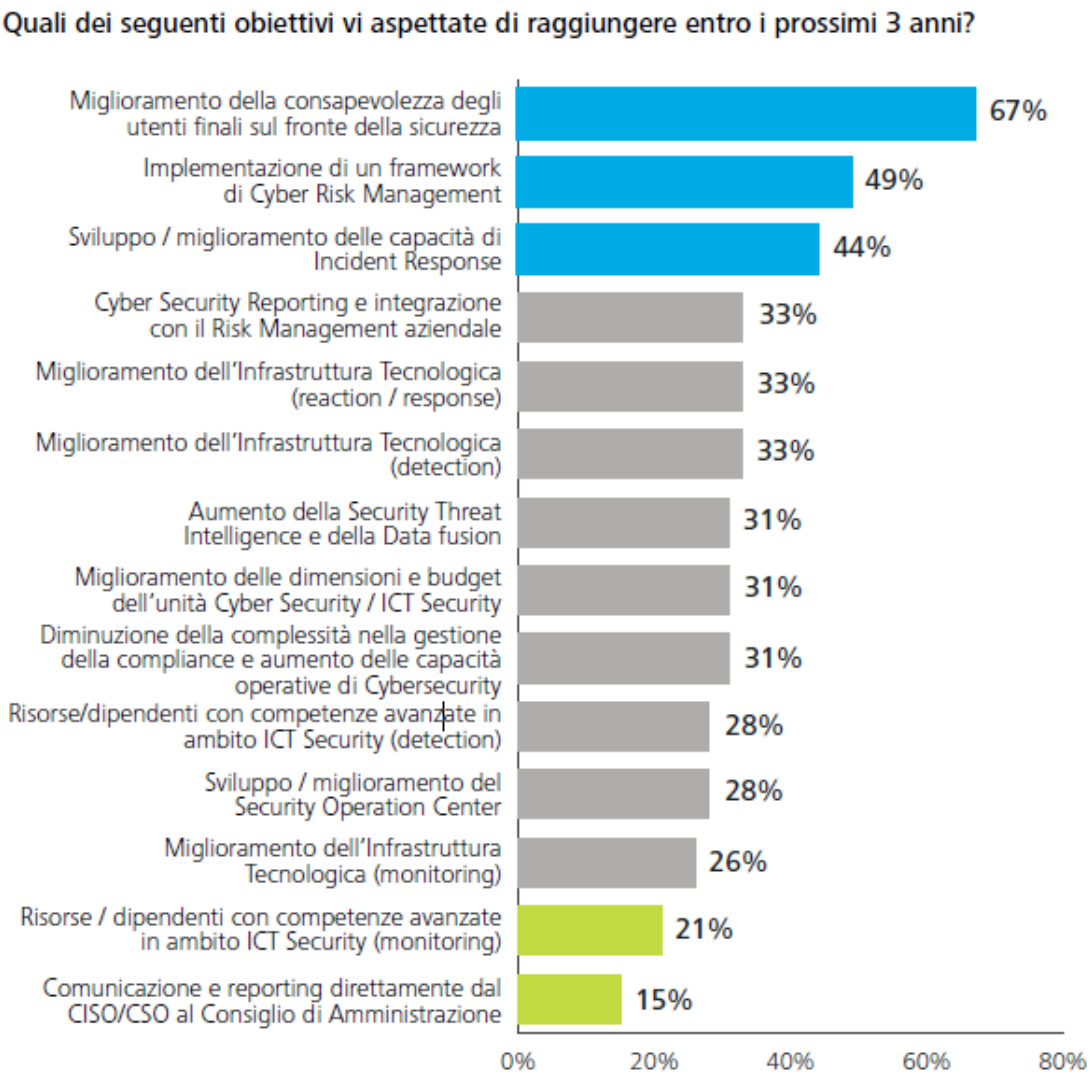

Figura 3: Obiettivi a 3 anni del programma per la Cybersecurity

Nel corso del 2015, all'interno dei piani strategici di cybersecurity delle aziende intervistate, sembrano emergere nuovi ambiti quali ad esempio Measurement e reporting, Advanced Threat Management, Threat intelligence e security analytics, che rispetto al 2014 mostrano un aumento della maturità complessiva e mostrano come le aziende italiane abbiano intenzione di intraprendere le giuste azioni di sviluppo, in relazione anche alle necessità di una gestione più manageriale della cybersecurity.

Gli aspetti di cybersecurity si stanno progressivamente inserendo all'interno della vita aziendale, e si nota come gli investimenti relativi stiano crescendo da valori pari al 1 e 2% del totale budget ICT verso valori del 3-5%, ma anche con pochi (circa 10%) dei rispondenti che dedica già il 6 e il 10% (Figura 4). Valutando anche la necessità di crescita di competenze nell'area IOT, i valori sembrerebbero essere sottostimati, considerando il fatto che in tutte le grandi implementazioni infrastrutturali la componente "implicita" risulta essere poco tracciata e visibile.

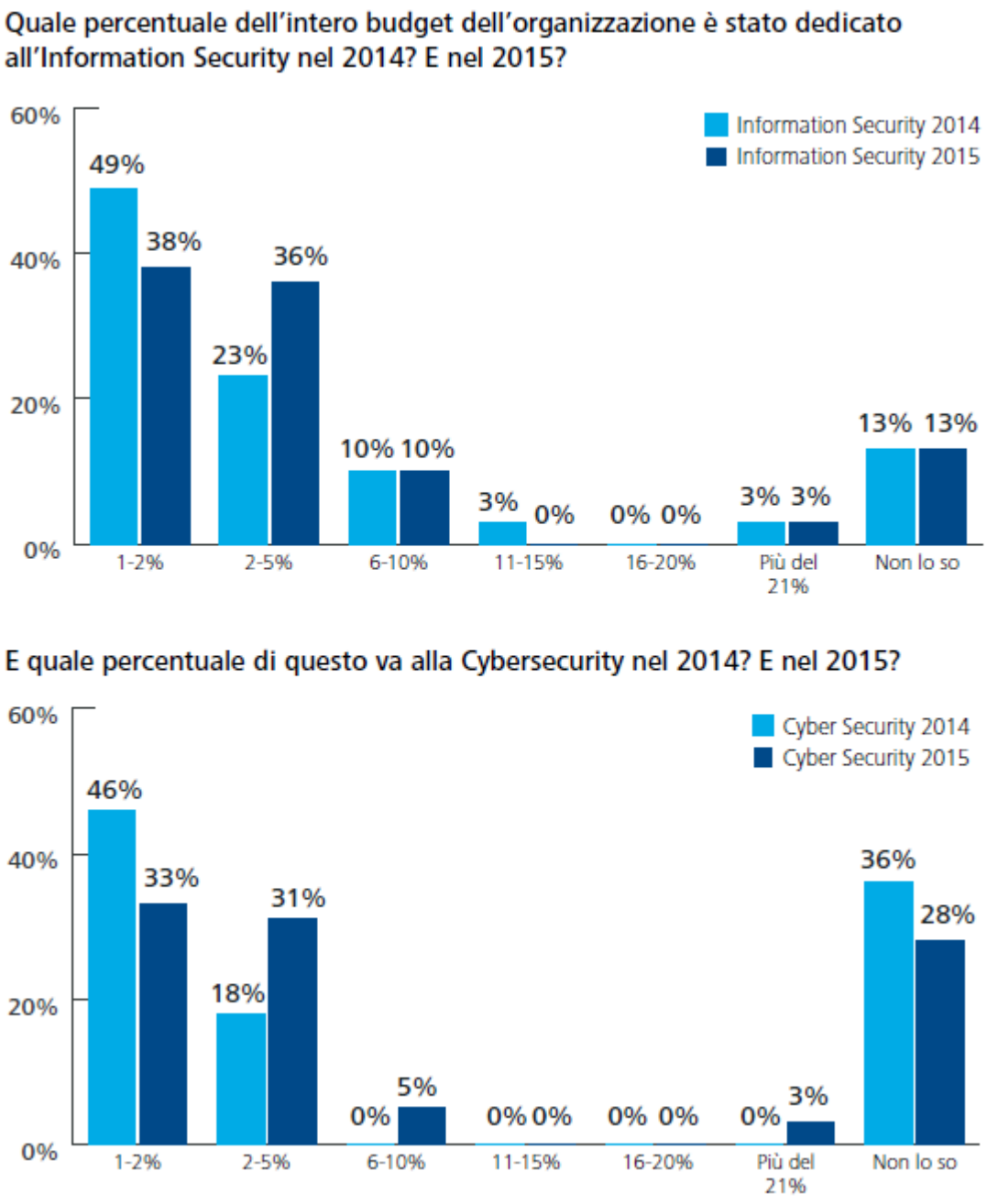

Figura 4: Information Security e Cybersecurity Budget: 2014 vs 2015

Lo studio mostra una tendenza progressiva nello spostarsi da investimenti in prevenzione verso lo sviluppo di capacità di monitoraggio e di risposta agli eventi cyber, per sviluppare maggiormente la propria Cyber-Resilience. A oggi solo il 48% delle aziende intervistate afferma di avere un processo di Incident Detection ritenuto valido e, di queste, solo il 16% lo gestisce in modalità end-to-end, mediante strumenti di monitoraggio (Figura 5).

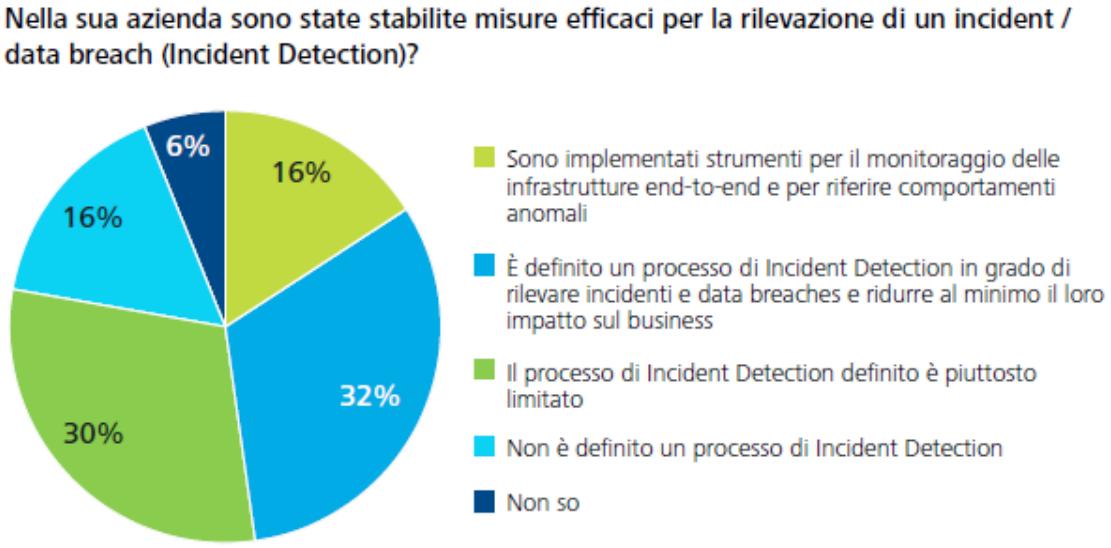

Figura 5: Processi di Incident Detection solo nella metà delle aziende

Sul processo di Incident Response si rileva invece un maggiore livello di maturità in quanto il 65% delle aziende lo ha opportunamente definito e documentato integrandolo nel Crisis Management, nel piano di Business Continuity o di Disaster Recovery.
Più in dettaglio, i risultati dell'indagine sugli aspetti di monitoraggio, Incident Detection, Management & Response sono:

- Le principali attività svolte per il monitoraggio della security sono gli audit di sicurezza (79%) e i vulnerability assessment/penetration test (79%).
- Aspetti critici sono invece la review dei log applicativi (svolta dal42% degli intervistati, una percentuale inferiore rispetto a quanti svolgono review su log relativi alle infrastrutture, 61%), oltre che una review delle informazioni ottenibili in caso di incidente (37%).
- Solo il 13% delle aziende afferma di avere soluzioni complete di cybersecurity intelligence per monitorare lo stato della sicurezza informatica.
- Incident Detection, il processo per rilevare incidenti, comportamenti anomali e data breaches è adottato solo dal 48% delle aziende del campione. Di queste, solo un 16% lo gestisce in maniera ottimale mediante utilizzo di adeguati strumenti di monitoraggio.
- Incident Response: si rileva in questo caso un maggiore livello di maturità in quanto il 65% delle aziende lo ha opportunamente definito e documentato integrandolo nel Crisis Management, nel piano di Business Continuity o di Disaster Recovery dell'organizzazione. Tuttavia, anche per questo ambito rimangono gap da colmare, con un 21% delle aziende che non dispone di un piano di Incident Response. (Figura 6)

• Un ulteriore aspetto fortemente sottovalutato nella gestione della risposta agli incidenti è rappresentato dal test periodico delle procedure di Incident e Crisis Management, che viene effettuato solo da un 15% delle aziende, nonostante sia fondamentale per assicurare che il processo sia sempre aggiornato, conosciuto e efficace in caso di necessità di attivazione, anche rispetto ai mutamenti di contesto aziendale (e.g. cambiamenti organizzativi, modifiche di processi, provider, partner, …).

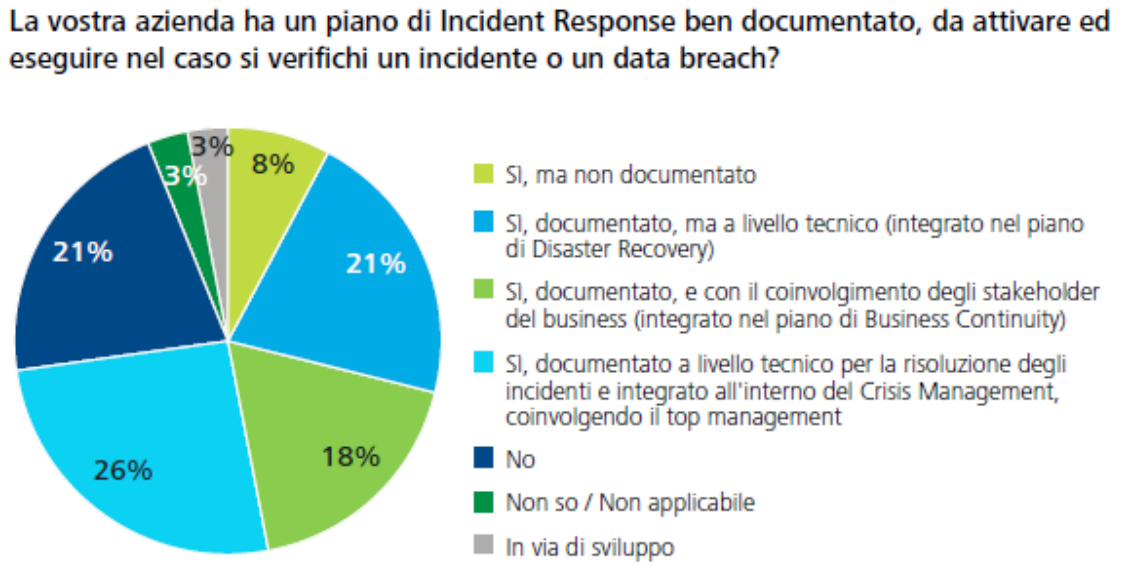

Figura 6: Livello di maturità raggiunto per l'Incident Response

Questi importanti cambiamenti necessitano di adeguato presidio e quindi di modelli di Governance che includano anche, necessariamente, le tematiche cybersecurity e l'attuazione di strategie mirate alla gestione dei cyber risk. Risulta essere indispensabile lo sviluppo delle professionalità e delle competenze del personale operativo ma anche un incremento di competenze da parte degli executive e dei componenti dei CdA aziendali e degli ulteriori organi di controllo preposti (e.g. Comitato Controllo e Rischi).
In questo senso, viene evidenziata dal 57% delle aziende rispondenti una percezione di carenza di competenze, anche per i dipendenti che si occupano più direttamente di sicurezza informatica, mostrando una consapevolezza incoraggiante. (Figura 7)

Figura 7: Lo skill shortage è il principale problema attuativo per un'efficace Cyber Risk Management

Per colmare queste carenze le aziende italiane stanno investendo sulla formazione e sulla sensibilizzazione di tutti dipendenti (47% dei rispondenti), anche adottando modalità innovative di erogazione (storytelling, video, comics), e su sviluppi mirati per aree specialistiche (es. Incident management).

"L'aumento della digitalizzazione dei processi di business e della networked economy, associato alla "commercializzazione" di capability cyber-offensive sempre più sofisticate, comporta una sempre maggiore esposizione delle aziende italiane ad attacchi informatici rispetto ai quali, a quanto dichiarano anche dalle aziende intervistate, non si ritengono completamente preparate. Il Governo e le aziende italiane stanno avviando piani di sviluppo atti a dotarsi delle di migliori competenze tecniche e manageriali per rispondere adeguatamente a questa minaccia – dichiara **Stefano Buschi, Partner e responsabile per i Cyber Risk Services di Deloitte in Italia** – *Nonostante questo, il rischio Cyber sembra non essere pienamente "visibile" al management aziendale, che spesso lo identifica come un rischio la cui gestione e interamente delegabile alla funzione ICT, mentre andrebbe valutato e gestito considerando i molteplici aspetti legati agli impatti sulla sostenibilità del proprio business e sulla la competitività della propria azienda nel medio- lungo periodo".*

"Dai risultati dell'indagine emergono alcuni gap importanti che le aziende italiane devono puntare a colmare in tempi rapidi - afferma **Ezio Viola, Amministratore Delegato di The Innovation Group** - *oggi non è più sufficiente dotarsi di misure preventive, bisogna essere in grado di rilevare attacchi che avvengono per lo più in modo silente e persistente, e soprattutto sapere come reagire prontamente quando si ha evidenza di essere stati presi di mira o di aver subito un data breach".*

Deloitte è una tra le più grandi realtà nei servizi professionali alle imprese in Italia, dove è presente dal 1923. Vanta radici antiche, coniugando tradizione di qualità con metodologie e tecnologie innovative. I servizi di audit, tax, consulting e financial advisory sono offerti da diverse società e studi specializzati in singole aree professionali e tra loro separati e indipendenti, ma tutti facenti parte del network Deloitte. Questo oggi conta oltre 2.900 professionisti, i quali assistono i clienti nel raggiungimento di livelli d'eccellenza grazie alla fiducia nell'alta qualità del servizio, all'offerta multidisciplinare e alla presenza capillare sul territorio nazionale.

Grazie ad un network di società presenti in 150 Paesi, Deloitte porta i propri clienti al successo grazie al suo know how di alta qualità e a una profonda conoscenza dei singoli mercati in cui è presente. Obiettivo dei circa 200.000 professionisti di Deloitte è quello di mirare all'eccellenza dei servizi professionali forniti. Il nome Deloitte si riferisce a una o più delle seguenti entità: Deloitte Touche Tohmatsu Limited, una società inglese a responsabilità limitata, e le member firm aderenti al suo network, ciascuna delle quali è un'entità giuridicamente separata e indipendente dalle altre. Si invita a leggere l'informativa completa relativa alla descrizione della struttura legale di Deloitte Touche Tohmatsu Limited e delle sue member firm all'indirizzo www.deloitte.com/about.

Deloitte Touche Tohmatsu Limited

The Innovation Group è una società di advisory e di ricerca indipendente specializzata, in attività di supporto alle aziende per lo sviluppo dei processi di innovazione attraverso l'utilizzo delle tecnologie ICT e digitali. Si rivolge ad Aziende ed organizzazioni che vogliono concretamente sviluppare strategie di crescita attraverso iniziative e progetti di innovazione del business, del "go to market", della produzione e gestione integrata della conoscenza dell'azienda attraverso le tecnologie.

The Innovation Group Srl