Capgemini contacts:
Raffaella Poggio
Marketing & Communication Director
Tel.: +39 347 4271901
E-mail: raffaella.poggio@capgemini.com

Michela Cotich
Marketing & Communication
Tel.: +39 347 3620244
E-mail: michela.cotich@capgemini.com

Community Group:
Michele Bon
Tel.: +39 338 6933868
E-mail: michele.bon@communitygroup.it

Carlo Carboni
Tel.: +39 348 9412226
E-mail: carlo.carboni@communitygroup.it

Cresce il gap digitale in ambito cybersecurity, le aziende faticano ad assumere le competenze ricercate

Una nuova ricerca rivela che la domanda da parte delle aziende di competenze legate alla sicurezza informatica cresce più rapidamente dell'offerta e c'è bisogno di idee innovative per colmare il gap, sia per acquisire sia per mantenere i talenti chiave

Milano, 21 febbraio 2018 – Un nuovo report del Digital Transformation Institute di Capgemini evidenzia un urgente e crescente divario legato ai talenti in ambito cybersecurity, che richiede nuove assunzioni e strategie per la retention dei dipendenti in grado di aiutare le aziende ad arginare i rischi informatici e creare un vantaggio competitivo. Dalla ricerca "*Cybersecurity Talent: The Big Gap in Cyber Protection*" emerge che, tra le varie competenze digitali necessarie a quelle società che vogliono ottenere una leadership digitale, quelle in ambito cybersecurity hanno il maggior divario tra domanda e fornitura interna.

Alla ricerca, a cui hanno partecipato 1.200 tra manager senior e addetti front line, ha anche analizzato il social media sentiment di oltre 8,000 dipendenti operanti in ambito cybersecurity. Il 68% delle società ha riportato un'alta domanda di competenze di sicurezza informatica rispetto al 61% che invece necessita di capacità nel campo dell'innovazione e il 64% in tema di analisi. La domanda di queste capacità è stata quindi confrontata con la disponibilità di competenze elevate già presenti all'interno dell'azienda. Per la sicurezza informatica è stato riportato un divario del 25% (con il 43% di competenze di alto livello già presenti in azienda), contro un gap del 13% per gli analytics (già presenti per il 51%) e un divario del 21% per l'innovazione (già presente al 40%).

"Il divario delle competenze in ambito cybersecurity ha un reale impatto sulle aziende di tutti i settori, rendendole pericolosamente esposte ai rischi legati ai crimini informatici", ha affermato **Alessandra Miata, HR Director di Capgemini Italia**. *"Le aziende devono urgentemente rivedere le propria attività di recruiting e le strategie di retention per i talenti già inseriti, soprattutto se hanno intenzione di massimizzare i benefici provenienti dagli investimenti nella digital trasformation. La velocità nell'attrarrre talenti con questo tipo di competenze è un elemento chiave di successo: una ricerca di personale che dura dei mesi, e non qualche settimana, per trovare i candidati ideali non solo è fattore di inefficienza, ma può costituire un reale impoedimento nell'attrarre i talenti necessari".*

Si stima che nei prossimi 2-3 anni crescerà la domanda di talenti competenti in ambito cybersecurity, con il 72% degli intervistati che si aspetta una maggiore richiesta di esperti di sicurezza informatica nel 2020, contro l'attuale 68%. Visto l'incremento degli attacchi informatici e il fatto che le società non solo hanno bisogno di proteggersi ma anche di massimizzare il vantaggio competitivo che proviene dalla digitalizzazione, il report delinea una serie di priorità che i leader aziendali devono tenere in considerazione:

Piorità 1- integrare la sicurezza
La prima priorità per le aziende è quella di valutare il grado di integrazione della sicurezza all'interno dell'azienda. Qual è la cultura della sicurezza informatica al di fuori del team che ha responsabilità diretta per la protezione dei dati? Quanto sono esperti in materia di sicurezza gli sviluppatori di app e i network manager?

"Non esiste una parte dell'azienda o un suo processo che non sia potenzialmente esposto a rischi di sicurezza informatica. Per questo è estremamente importante accrescere le competenze in ambito cybersecurity dell'intera organizzazione, allineando le aziende a principi e processi sicuri dall'inizio alla fine", ha spiegato Miata. *"Bisogna creare una base solida in termini di competenze di sviluppo delle applicazioni, essere in grado di creare codici sicuri, migliorare le competenze degli ingegneri di rete e degli architetti per mettere in sicurezza il cloud".*

Priorità 2 – massimizzare il set di competenze già esistente
"Per fare fronte allo skill gap, un'altra priorità è rappresentata dal riconoscere le competenze di cybersecurity già presenti all'interno dell'azienda. La metà dei dipendenti sta già investendo proprie risorse per sviluppare in autonomia competenze digitali[1]*. Le aziende che hanno difficoltà a trovare dei possibili candidati all'esterno potrebbero scoprire che al loro interno sono già presenti dei candidati con una buona base di partenza sulla quale lavorare. Le funzioni con competenze complementari e trasferibili comprendono network operation, database administration e application development".*

Inoltre, le aziende dovrebbero considerare i requisiti necessari per portare la sicurezza in qualsiasi servizio e applicazione e assumere persone con competenze di comunicazione per completare le caratteristiche tecniche dei loro team. Agli analisti e agli esperti di marketing dovrebbero essere assegnati dei ruoli in materia di cybersecurity per permettere l'implementazione delle best practice in tutta l'azienda.

Priorità 3 – Pensare fuori dagli schemi
La terza priorità è rappresentata dal fatto che il pensiero delle aziende deve andare oltre le tradizionali strategie di selezione e comprendere le competenze alla base della cybersecurity. Lo sguardo va rivolto anche ai candidati che solitamente non verrebbero presi in considerazione, studiando le competenze e caratteristiche richieste per altri tipi di posizioni. Per esempio, chi lavora nel campo della matematica molto spesso è anche portato per il riconoscimento dei pattern. *"Pensare fuori dagli schemi vuol dire individuare le competenze trasferibili e considerare candidature "impensabili" in altri contesti",* ha affermato Alessandra Miata*. "Per esempio, ci sono persone provenienti da contesti distanti da quello aziendale ma che hanno abilità straordinarie nel riconoscimento dei pattern e dotate di grandi capacità numeriche e di problem solving, attenzione ai dettagli, correlate con un approccio metodico al lavoro - tutte caratteristiche utili in ambito di sicurezza informatica che potrebbero restare invisibili alle aziende".*

Priorità 4 – rafforzare la retention
L'ultima priorità riguarda la *retention* dei talenti. In un mercato del lavoro altamente competitivo, le aziende devono prestare attenzione all'engagement dei dipendenti per assicurarsi che il divario non aumenti.

Il report evidenzia che i dipendenti in ambito di sicurezza informatica danno più valore alle aziende che offrono orari di lavoro flessibili, incoraggiano il training e danno priorità all'avanzamento di carriera. Sui social media, lo scarso equilibrio tra vita lavorativa e privata è stato considerato dai professionisti del mondo

[1] Report pubblicato da Capgemini in partnership con LinkedIn: "The Digital Talent Gap—Are Companies Doing Enough?"

della cybersecurity come il principale motivo che li spinge ad abbandonare l'azienda o a sentirsi insoddisfatti della stessa. La stragrande maggioranza dei talenti in area cybersecurity (81%) è d'accordo con questa frase: *"Preferisco lavorare per società all'interno delle quali c'è un chiaro avanzamento di carriera",* contro il 62% di tutti i partecipanti al sondaggio.

La percentuale sale ulteriormente (84%) per i dipendenti della Generazione Y e la Generazione Z[2], i quali hanno evidenziato che la mancanza di avanzamento professionale rappresenta la loro preoccupazione più grande. La gestione di queste problematiche minori ma ugualmente importanti è un requisito fondamentale per creare un'offerta in ambito cybersecurity che sia realizzabile e sostenibile.

Metodologia della ricerca
Il Digital Transformation Institute di Capgemini ha intervistato 753 dipendenti e 501 manager dal livello senior in su di società i cui ricavi dell'esercizio fiscale 2016 superano i 500 milioni di dollari, il cui organico supera le 1.000 unità. Il sondaggio è iniziato a luglio 2017 e ha coperto 9 paesi – Francia, Germania, India, Italia, Olanda, Spagna, Svezia, Regno Unito e Stati Uniti – e sette settori industriali – Automotive, Bancario, Beni di Consumo, Assicurativo, Vendite al dettaglio, Telecomunicazioni e Utility.

Capgemini ha inoltre intervistato diversi recruiter di multinazionali, associazioni per la sicurezza informatica e il mondo accademico per comprendere quali siano le best practice per mitigare il divario in ambito cybersecurity. Infine, Capgemini ha analizzato il sentiment di 8.400 tra dipendenti ed ex dipendenti di 53 società operanti nella sicurezza informatica con almeno 100 dipendenti sui social media. Le società selezionate si occupano principalmente (ma non solo) di cybersecurity in ambito di data security, mobile security, enterprise security, email security e application security.

Per scaricare una copia del report cliccare qui.

Capgemini

Leader mondiale nei servizi di consulenza e tecnologia, Capgemini è all'avanguardia nell'innovazione per consentire ai suoi clienti di orientarsi al meglio in un mondo costantemente in evoluzione del cloud, del digitale e delle piattaforme. Forte di 50 anni di esperienza e di una profonda conoscenza degli specifici settori di mercato, Capgemini sostiene le organizzazioni nel realizzare le proprie ambizioni di business, offrendo una gamma di servizi che vanno dalla strategia alle operations. Capgemini è mossa dalla convinzione che il valore di business della tecnologia sia creato dalle e attraverso le persone. Con un'organizzazione multiculturale di 200.000 dipendenti presenti in più di 40 paesi nel mondo, nel 2017 il Gruppo Capgemini ha registrato ricavi per 12,8 miliardi di euro.
Visita il nostro sito www.it.capgemini.com. *People matter, results count.*

Digital Transformation Institute
Il Digital Transformation Institute è il think-tank interno di Capgemini dedicato a tutto ciò che è digitale. L'istituto pubblica lavori di ricerca sull'impatto delle tecnologie digitali sulle grandi aziende tradizionali. Il team fa leva sul network mondiale di esperti Capgemini e lavora a stretto contatto con partner accademici e tecnologici. L'istituto possiede centri di ricerca dedicati nel Regno Unito, in India e negli Stati Uniti.

[2] Alla Generazione Y e alla Generazione Z appartengono i giovani tra i 18 e i 36 anni