La sicurezza informatica nell'era cognitiva

Attivare un sistema immunitario digitale

IBM Institute for Business Value

Come IBM può aiutarti.

I crimini informatici costituiscono minacce insidiose che hanno raggiunto livelli critici. Sebbene difficile da quantificare con precisione, le stime dei costi dei crimini informatici per l'economia globale vanno da 375 a 575 miliardi di USD all'anno. Nessun luogo e nessun settore sono immuni. IBM® ha un ampio portafoglio integrato di software e servizi di sicurezza per prevenire, rilevare, e rispondere agli attacchi al fine di aiutare le organizzazioni ad anticipare e agire tempestivamente per mitigare gli impatti dei rischi associati alla sicurezza informatica. IBM Security consente ai clienti di stabilire un 'sistema immunitario di sicurezza' supportato da analisi, difese in tempo reale ed esperti di comprovata affidabilità. Per ulteriori informazioni su come IBM collabora con le organizzazioni per proteggere le loro infrastrutture digitali, visitare il sito **ibm.com**/security.

Nuove capabilities per un 'era di sfide

I responsabili della sicurezza sono al lavoro per colmare tre gap nelle capabilities attuali: intelligence, velocità e precisione. Alcune organizzazioni stanno iniziando a esplorare il potenziale delle soluzioni di sicurezza cognitive per colmare queste lacune e prevenire rischi e minacce. Ci sono grandi aspettative per questa tecnologia. Il 57% dei responsabili della sicurezza che abbiamo intervistato ritiene che ciò possa rallentare in modo significativo le azioni dei criminali informatici. Il 22% degli intervistati, che noi chiamiamo "Pronti", hanno cominciato il loro percorso verso l'era cognitiva della sicurezza informatica e ritengono di possedere la familiarità, la maturità e le risorse di cui hanno bisogno. Per iniziare il percorso, è importante esplorare i propri punti deboli, stabilire come si desidera aumentare le proprie capacità con le soluzioni cognitive e pensare alla realizzazione di piani di formazione e di investimento per gli stakeholders aziendali.

Executive summary

Lo stato della sicurezza informatica sta raggiungendo un punto di non ritorno. Il numero di rischi e di eventi è in crescita esponenziale e i security operation team faticano a tenere il passo con il volume. Lo scenario delle minacce sta cambiando rapidamente e gli approcci tradizionali non sono adeguati per far fronte alla complessità delle minacce e al numero di varianti in continuo aumento. Le ripercussioni di incidenti e violazioni sono in aumento, con costi finanziari e rischi in rapida crescita. Infine, molte organizzazioni si trovano ad affrontare una carenza di esperti di sicurezza con le giuste competenze. Tutte queste diverse sollecitazioni rendono difficile per le organizzazioni mantenere in buono stato di salute i sistemi immunitari digitali di cui hanno bisogno per proteggersi.

Per questo rapporto, abbiamo intervistato 700 CISO (chief information security officers) e altri responsabili della sicurezza di 35 Paesi, in 18 settori diversi. I nostri obiettivi erano scoprire con quali sfide si devono confrontare queste persone, quali sono i loro punti deboli e che cosa stanno facendo al riguardo. Volevamo anche conoscere le loro opinioni sulle soluzioni di sicurezza cognitive: in che modo queste soluzioni possono risultare utili, quanto sono pronte a essere messe in pratica e che cosa ne impedisce l'implementazione.

Abbiamo scoperto che la sfida principale per i responsabili della sicurezza è rappresentata dalla complessità delle minacce e dalla velocità con cui sono in grado di rispondere a tali minacce. Si preoccupano di come gli incidenti di sicurezza incidono sulle operazioni oggi e come possono modellare la loro reputazione domani. I responsabili della sicurezza non si sentono efficaci tanto quanto potrebbero esserlo nel garantire la protezione della rete e dei dati e assicurare una risposta rapida, intelligente alle minacce. Tuttavia, mirano a risolvere tali carenze nei prossimi anni. È difficile acquisire le giuste risorse per affrontare questi problemi. A fronte di un aumento dei costi e della carenza di risorse qualificate in materia di sicurezza, i responsabili della sicurezza sono alla ricerca di modi in grado di giustificare meglio i loro investimenti nei confronti dei dirigenti dell'azienda.

La **sfida principale della sicurezza informatica** oggi e domani è **ridurre i tempi medi di risposta agli incidenti e per la loro risoluzione**.

Il 57% dei responsabili della sicurezza ritengono **che le soluzioni di sicurezza cognitive** possano rallentare **significativamente le azioni dei criminali informatici**.

Si prevede **una triplicazione** del numero di professionisti **in grado di implementare soluzioni di sicurezza cognitive** nel corso dei prossimi 2 - 3 anni.

Mentre le organizzazioni acquisiscono ulteriori dati sulla sicurezza e applicano più funzionalità di analisi, i carichi di lavoro stanno aumentando fino ai limiti di ciò che è possibile con mezzi manuali. Alcuni sono alla ricerca di soluzioni di sicurezza cognitive per gestire questa situazione e contribuire a colmare le lacune nel campo dell'intelligence, della velocità e dell'accuratezza. Sebbene le tecnologie cognitive per la sicurezza siano agli albori, ci sono grandi speranze e ottimismo circa il loro potenziale. I nostri intervistati hanno detto che i primi vantaggi che si aspettano dalle soluzioni di sicurezza cognitive sono migliori funzionalità di rilevazione e di risposta agli eventi, maggiore velocità di risposta agli incidenti e maggiore certezza nel distinguere tra semplici eventi e incidenti veri e propri. Nonostante le grandi aspettative, occorrono ancora molta formazione e preparazione prima che si possa realizzare l'adozione diffusa.

Abbiamo trovato un gruppo "pronto per l'era cognitiva" delle soluzioni di sicurezza. Quando abbiamo analizzato l'efficacia della sicurezza, la predisposizione cognitiva e le conoscenze, abbiamo identificato persone responsabili della sicurezza entusiaste che si sentono pronti ad entrare nell'era cognitiva delle odierne soluzioni di sicurezza. In generale, queste persone tendono ad avere una maggiore familiarità con le soluzioni cognitive, una maggiore fiducia generale nelle funzionalità di cui dispongono in materia di sicurezza e meno problemi relativi allo skill shortage.

Quando le soluzioni di sicurezza cognitive si affermeranno maggiormente e diventeranno più popolari, ogni organizzazione potrà sfruttarne i vantaggi. Se ci si sente pronti e si decide di iniziarne l'adozione, il primo passo è individuare i punti deboli da rinforzare con le soluzioni di sicurezza cognitive. Successivamente, occorre conoscere i potenziali casi d'uso e utilizzarli per indirizzare i propri punti deboli. In un ambiente in cui è necessario giustificare gli investimenti, parte del tempo viene dedicato alla comunicazione dei vantaggi delle soluzioni di sicurezza cognitive ai propri interlocutori aziendali. Sottolineare, in un linguaggio che possa essere compreso dai dirigenti aziendali, che queste soluzioni possono migliorare la security posture complessiva. Con questi primi passi, si prepara l'organizzazione per l'era cognitiva della sicurezza informatica.

Il contesto attuale

A prima vista, si potrebbe avere l'impressione trasmessa dai responsabili della sicurezza da noi intervistati che la situazione è gestibile. Questi professionisti hanno piena fiducia nelle loro crescenti capacità tecnologiche e organizzative. Una maggioranza — il 77% — di coloro ai quali abbiamo chiesto riguardo al livello di preparazione nei confronti della sicurezza informatica ritiene di essere alla pari con i colleghi del settore. Gli intervistati sono anche molto ottimisti circa la loro security posture nel corso dei prossimi due o tre anni, e l'86% di loro dichiara di essere in una posizione *Migliore* rispetto ai loro colleghi del settore.

Queste risposte potrebbero non sorprendere, ma è importante esaminarle: i responsabili della sicurezza ritengono che il loro operato non sia peggiore di quello di altri e sono sicuri che stanno facendo progressi e che continueranno a farne. Quasi i tre quarti pensano di essere efficaci nell'affrontare le basi della sicurezza organizzativa, con il 72% che dichiara di essere efficace in termini di IT hygiene e il 71% che rivendica la massima efficacia in termini di consapevolezza del rischio in tutta l'azienda. Ma cerchiamo di approfondire per vedere che cosa sta realmente accadendo con le sfide, gli impatti, le funzionalità, il finanziamento e il ritorno sugli investimenti in tema di sicurezza.

L'esigenza di velocità

La sfida numero uno per i responsabili della sicurezza oggi è ridurre i tempi medi di risposta agli incidenti e i tempi di risoluzione. Il 45% degli intervistati ha identificato questi tempi come la massima sfida posta attualmente dalla sicurezza informatica. Le organizzazioni non ritengono che questa sfida sarà risolta nei prossimi due - tre anni. Guardando al futuro, il 53% degli intervistati ritiene che la riduzione dei tempi di risposta rimarrà la principale sfida posta dalla sicurezza informatica (vedere la Figura 1).

"È proprio come essere un mercante su un vascello nell'epoca d'oro della pirateria, senza la protezione di una marina o di forze di polizia. Si è da soli. E non basta. Molti non sanno come condurre le loro imbarcazioni e non possono rispondere a chi attacca (è illegale). Si cerca letteralmente di sopravvivere in un mondo ostile con entrambe le braccia legate dietro la schiena. Tuttavia, ci sono alcuni strumenti davvero interessanti e sofisticati da usare e che svelano tutti i retroscena delle minacce."

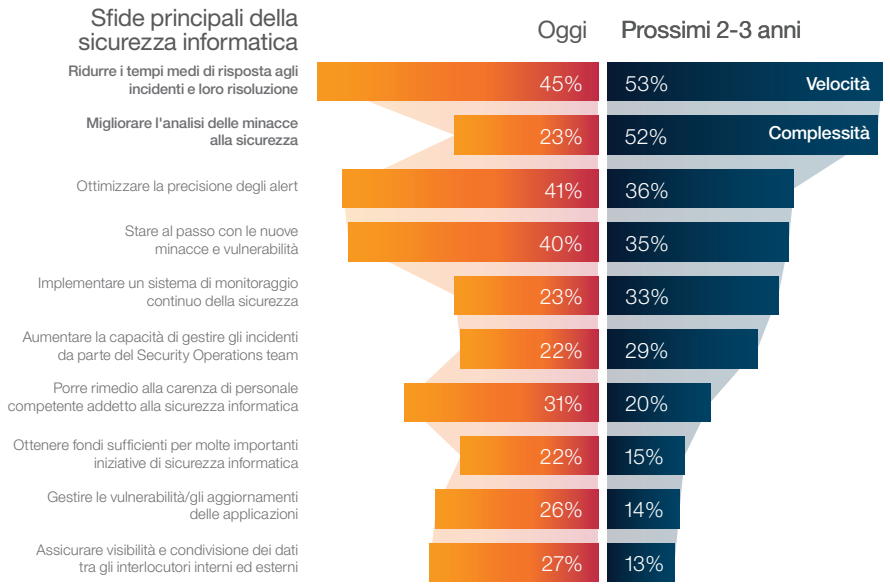
David Shipley, Director of Strategic Initiatives, Information Technology Services, University of New Brunswick

Il tempo è sinonimo di maggiore rischio

In uno studio del 2016, il Ponemon Institute ha scoperto che il tempo medio necessario per identificare una violazione è di 201 giorni e il tempo medio necessario per contenere una violazione è di 70 giorni. Inoltre, l'utilizzo di un team di risposta agli incidenti è stato il fattore che ha contribuito maggiormente alla riduzione dei costi associati a una violazione dei dati.[1]

Figura 1

Sfide principali oggi in termini di sicurezza informatica identificate dai responsabili della sicurezza e sfide che si porranno secondo loro nel prossimo futuro



Queste preoccupazioni persistono nonostante il fatto che l'80% delle organizzazioni dichiari che la loro velocità di risposta agli incidenti è molto superiore rispetto a due anni fa (maggiore in media del 16%). L'86% desidera che i miglioramenti della velocità siano ancora più veloci nei prossimi due - tre anni (con un obiettivo di miglioramento medio del 24%).

Questa è una questione molto importante per le organizzazioni. Più tempo impiega un'organizzazione per rispondere a un incidente, maggiore è il danno che potrebbe subire e il costo che potrebbe sostenere per gestire la crisi. Il tempo accresce sicuramente il rischio di perdita.

Un'altra sfida importante per i responsabili della sicurezza riguarda il miglioramento dell'analisi delle minacce alla sicurezza. Il 23% degli intervistati identifica questa sfida come la più urgente oggi, mentre il 52% ritiene cheil miglioramento dell'analisi delle minacce alla sicurezza sia la principale sfida per la sicurezza informatica nel corso dei prossimi due-tre anni. Gli analisti di sicurezza hanno bisogno di aiuto nell'acquisizione di informazioni, nel determinare quali minacce sono più urgenti e nello stabilire rapidamente modelli e deviazioni nell'attività. I responsabili della sicurezza sono alla ricerca di tutto ciò che può contribuire a migliorare la velocità e a gestire la complessità delle minacce che devono affrontare.

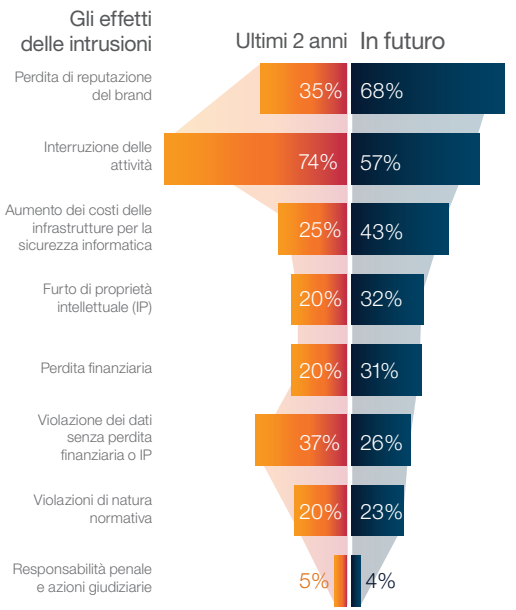
Grandi timori all'orizzonte

Quasi i tre quarti degli intervistati hanno dichiarato che le intrusioni hanno determinato notevoli interruzioni operative nel corso degli ultimi due anni. Tuttavia, ciò che gli intervistati si aspettano nei prossimi anni è qualcosa di nettamente diverso.

Le aziende sono sempre più preoccupate che le intrusioni si tradurranno in futuro in una perdita di reputazione del brand — . La preoccupazione per la perdita di reputazione aumenta quasi del doppio quando gli intervistati guardano al futuro: in questo caso il 35% la identifica come un risultato nel corso degli ultimi due anni, mentre per il 68% è fonte di apprensione negli anni a venire (vedere la Figura 2). Questo cambiamento dimostra che molti responsabili della sicurezza temono gli effetti crescenti delle intrusioni. Sempre più spesso, le conseguenze non compromettono solo le operazioni, ma la reputazione; un offuscamento della reputazione può incidere sugli utili se la fiducia diminuisce e i clienti si allontanano.

Figura 2

Le organizzazioni hanno segnalato una serie di ramificazioni derivanti dalle intrusioni negli ultimi due anni, ma prevedono conseguenze di natura diversa in futuro



Se già a partire da oggi l'aumento dei costi delle infrastrutture della sicurezza informatica costituisce un problema di rilievo, lo sarà ancora di più in futuro. Dal momento che persiste il rischio di intrusioni che vanno a segno, le organizzazioni omettono di spendere più soldi per risolvere il problema. I responsabili della sicurezza spesso ritengono che se subiscono un'intrusione c'è qualcosa che non va, quindi per stare al sicuro cercano di aggiornare le persone, indicano soluzioni e infrastrutture.

Varchi nella sicurezza

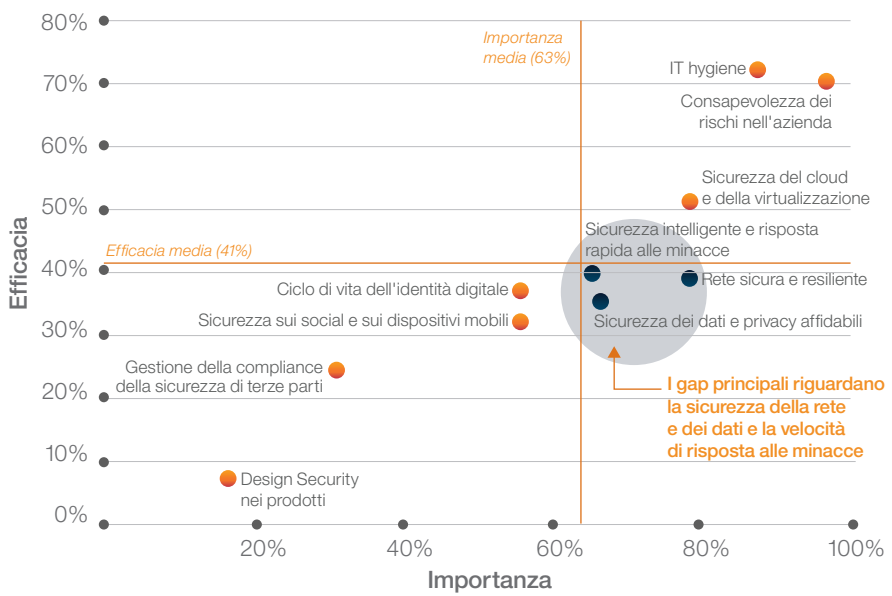
Abbiamo chiesto a persone impegnate in vari aspetti della sicurezza che cosa pensano sia importante per garantire una posizione di sicurezza e in che cosa ritengono di essere efficaci. I responsabili della sicurezza in genere sentono di dover trattare quasi tutto come importante, perché non vogliono che sfugga loro alcunché. Tuttavia, con risorse limitate, è difficile essere all'avanguardia in tutte le aree e in ogni momento, soprattutto con l'emergere continuo di nuove tecnologie, nuovi approcci e nuove sfide.

Molti intervistati hanno dichiarato di essere soddisfatti riguardo ai sistemi di protezione informatica e di gestione dei rischi adottati nell'azienda, il minimo indispensabile dal punto di vista sia tecnologico che organizzativo. Le aree ritenute importanti dagli intervistati, ma nelle quali si reputano inefficaci, sono quelle che vogliamo esaminare (vedere la Figura 3). Rientra in questa categoria la protezione della rete e dei dati associata alla risposta alle minacce.

Gli intervistati hanno dichiarato di non essere efficaci quanto dovrebbero esserlo in termini di velocità di risposta alle minacce, rilevamento dell'attività di rete, filtering, classificazione dei dati e prevenzione delle perdite. Naturalmente, è fondamentale che le organizzazioni stiano al passo con il crescente volume e complessità dei rischi per la sicurezza; concentrandosi sulla loro velocità di risposta e sulla gestione della complessità attraverso una migliore analisi delle minacce, le organizzazioni possono rafforzare le loro difese in modo significativo.

Figura 3

Importanza rispetto a efficacia di varie funzionalità di sicurezza



"Abbiamo scoperto una serie di risparmi tangibili sui costi in tutta l'azienda che ha avuto origine dal monitoraggio e dall'analisi della sicurezza. Abbiamo ridotto i costi della larghezza di banda, dismesso risorse di scarso utilizzo e aumentato la produttività dei dipendenti, riducendo in modo significativo lo spam, solo per citarne alcuni."

Un dirigente canadese responsabile di protezione finanziaria e gestione delle risorse

Gestione del bilancio

I responsabili della sicurezza devono gestire importi di notevole entità. Prevedono anche forti aumenti dei costi per garantire una sicurezza informatica efficace e non vedono nel prossimo futuro alcuna riduzione delle spese. Il 78% ha assistito a un aumento dei costi associati alla sicurezza informatica nel corso degli ultimi due anni e l'84% prevede che continueranno ad aumentare nel corso dei prossimi due - tre anni. Infatti, oltre il 70% degli intervistati spende più del 10% del loro intero budget IT in sicurezza informatica (e la maggior parte spende tra il 10 e il 15%). Queste spese vanno soprattutto alla prevenzione e alla rilevazione. In casi estremi, abbiamo riscontrato una spesa da parte di istituzioni finanziarie superiore a 500 milioni di dollari all'anno per la sicurezza informatica.[2] Poiché più denaro non garantisce necessariamente maggiore protezione, importi di tale entità non sono sostenibili nel lungo periodo; Pertanto i responsabili della sicurezza si troveranno inevitabilmente di fronte a una sempre maggiore pressione di giustificare i loro investimenti.

Il 92% degli intervistati dichiara che per essere approvate le loro richieste di finanziamento delle iniziative di sicurezza informatica devono essere giustificate da un ritorno sull'investimento (ROI) o da un'altra analisi finanziaria. Nell'ambito di questo contesto, i due elementi principali che servono per giustificare gli investimenti includono una chiara comunicazione dell'attuale esposizione al rischio per l'organizzazione (secondo il 61% degli intervistati) e il sostegno da parte di dirigenti addetti a finanza, gestione del rischio, operazioni e altri con responsabilità strategiche (secondo il 51% degli intervistati). I responsabili della sicurezza devono quindi comunicare le loro esigenze nel linguaggio del business.[3] Inoltre, devono cercare nuovi modi per giustificare il costo degli investimenti per la sicurezza informatica e dimostrarne il valore. Va sfatata la visione che la sicurezza è semplicemente una polizza assicurativa o un costo associato all'impresa in sé.

Gestione delle carenze

L'aspetto positivo è che i responsabili della sicurezza intervistati sembrano essere consapevoli delle carenze e prevedono di porvi rimedio quanto prima. Le organizzazioni stanno perseguendo una serie di diverse iniziative per migliorare il loro livello di preparazione al rischio (vedere la Figura 4). Gli sforzi attuali sono centrati principalmente (da parte del 67% delle organizzazioni) sul miglioramento dei comportamenti dei dipendenti attraverso la formazione. Il 40% degli intervistati sta anche implementando software di monitoraggio dell'identità. Queste opzioni tendono a essere generalmente considerate fondamentali.

Figura 4
Le iniziative che i responsabili della sicurezza stanno intraprendendo per migliorare il livello di preparazione ai rischi per la sicurezza informatica

Ranking oggi		Ranking tra 2-3 anni	Iniziative
1	▼-30%	5	Migliorare il comportamento dei dipendenti attraverso corsi e formazione
2	▼-25%	7	Implementare software di monitoraggio delle identità (attività degli utenti)
3	▲+8%	4	Creare report su misure di sicurezza operative/strategiche con nuovi strumenti di analisi
4	▲+28%	1	**Migliorare il monitoraggio della rete, delle applicazioni e della sicurezza a livello dei dati**
5	▲+17%	3	**Migliorare la metodologia, i processi e la velocità di risposta agli incidenti**
6	▼-9%	8	Assumere e formare più analisti di sicurezza
7	▼-16%	10	Test di sicurezza delle applicazioni (comprese quelle mobili, API)
8	▲+36%	2	**Creare o aggiornare le capabilities dei SOC**
9	▲+14%	6	Implementare soluzioni di sicurezza abilitate da tecnologie cognitive
10	▲+1%	9	Integrare tecniche forensi nelle operazioni di sicurezza

"I dirigenti sono sempre meno inclini a sprecare denaro nella sicurezza, senza una rassicurazione riguardo al fatto che tutta la spesa precedente è servita a garantire maggiore sicurezza. I responsabili della sicurezza devono andare oltre per giustificare gli investimenti. Non possono limitarsi a fare una valutazione, identificare le lacune e chiedere soldi per colmare quelle lacune."

Chad Holmes, Principal and Cyber-Strategy, Technology and Growth Leader (CTO) presso Ernst & Young LLP

Nel corso dei prossimi due-tre anni si prevede un grande cambiamento in queste iniziative di miglioramento. Infatti, gli intervistati hanno indicato che le prime tre iniziative saranno completamente diverse da quelle di oggi. Per il 57%, la numero uno sarà il miglioramento della sicurezza a livello di rete, di applicazioni e e di dati. La numero due riguarderà l'aggiornamento delle capabilities del SOC. Infine, migliorare la velocità dei tempi di risposta agli incidenti si collocherà al terzo posto. Tutte queste aree corrispondono alle carenze di efficacia individuate in precedenza.

Sebbene sia positivo vedere che i responsabili della sicurezza cercano rimedi alle loro carenze, un significativo cambiamento delle priorità può creare nuovi gap, o allargare quelli esistenti. Comunque sia, chi è preposto alla sicurezza deve occuparsi di ciò che è rilevante per l'azienda. La vera questione è se queste iniziative future saranno sufficienti.

Esposizione dei gap

Tutte queste sfide, aree di debolezza, iniziative e pressioni mettono in evidenza tre lacune critiche in intelligence, velocità e precisione. I responsabili della sicurezza devono colmare questi gap e gestire nel contempo costi e pressione esercitate dal ROI.

Gap di intelligence

- L'aspetto più problematico a causa dell'insufficienza delle risorse è la ricerca delle minacce, secondo il 65% degli intervistati
- Il 40% degli intervistati dichiara che stare al passo con le nuove minacce e vulnerabilità è una sfida significativa per la sicurezza informatica.

Gap di velocità

- La massima sfida per la sicurezza informatica oggi e domani è la riduzione dei tempi medi di risposta agli incidenti e i tempi di risoluzione, sebbene l'80% dichiari che la loro velocità di risposta agli incidenti è molto maggiore rispetto a due anni fa
- Gli intervistati prevedono di aumentare la loro attenzione in quest'area nei prossimi anni. Solo il 27% dichiara di avere iniziative in corso per migliorare la risposta agli incidenti, ma che questa aumenterà al 43% nei prossimi due-tre anni.

Gap di precisione

- Secondo gli intervistati, la seconda area più problematica oggi è l'ottimizzazione degli alert di precisione (attualmente ci sono troppi falsi positivi)
- Il 61% degli intervistati dichiara che un'altra area notevolmente problematica a causa dell'insufficienza delle risorse è rappresentata dall'identificazione delle minacce, dalla valutazione delle minacce e dalla difficoltà di sapere quali potenziali incidenti sottoporre a un livello di attenzione superiore.

I vantaggi attesi da una soluzione di sicurezza cognitiva più citati

1. Intelligence

Migliorare le funzionalità di rilevazione e accelerare il processo decisionale di risposta agli incidenti

2. Velocità

Accelerare sensibilmente i tempi di risposta agli incidenti

3. Precisione

Garantire maggiore fiducia nel distinguere tra semplici eventi e incidenti veri e propri

Incremento di 3 volte

nell'adozione programmata di soluzioni di sicurezza cognitive nei prossimi 2-3 anni

Come sarà utilizzata la sicurezza cognitiva?
I sistemi cognitivi saranno utilizzati per analizzare i trend di sicurezza e trasformare enormi volumi di dati strutturati e non strutturati in informazioni utili. Responsabili e analisti della sicurezza non possono realisticamente assorbire tutte le conoscenze sulla sicurezza generate dagli esseri umani, tra cui documenti di ricerche, pubblicazioni di settore, rapporti e blog degli analisti. I sistemi cognitivi cercano di unire queste informazioni con dati sulla sicurezza più tradizionali. Le soluzioni di sicurezza cognitive saranno utilizzate in combinazione con tecnologie, tecniche e procedure di sicurezza automatiche basate sui dati, contribuendo a garantire i massimi livelli di contesto e precisione.

Le soluzioni di sicurezza cognitive possono contribuire a migliorare le capacità degli analisti SOC, aiutandoli ad aumentare la velocità di risposta, a identificare meglio le minacce, a rafforzare la sicurezza delle applicazioni e a ridurre il livello complessivo del rischio di impresa. L'obiettivo è di allontanare gli analisti da attività di sicurezza banali e ripetitive per destinarli a un lavoro più stimolante sul piano intellettuale.

Accesso a soluzioni di sicurezza cognitive

Per colmare le lacune, sono necessarie tecnologie e approcci diversi. Le organizzazioni non possono continuare a spendere o a trovare da sole il modo migliore per raggiungere gli obiettivi. Non può funzionare così nel lungo termine. Grazie all'evoluzione tecnologica, le soluzioni di sicurezza nel corso degli anni, sono passate da semplici controlli perimetrali (ad esempio concentrandosi su difese statiche) a funzionalità di security intelligence più avanzate (ad esempio concentrandosi su informazioni in tempo reale e deviazioni dai modelli).

Oggi, stiamo cominciando a entrare nell'era cognitiva della sicurezza, definita da soluzioni in grado di capire contesto, comportamento e significato, analizzando i dati sulla sicurezza sia strutturati che non strutturati. La sicurezza cognitiva mira a sbloccare una nuova collaborazione tra gli analisti della sicurezza e la loro tecnologia. Queste soluzioni possono interpretare e organizzare le informazioni, fornire spiegazioni sul loro significato e offrire una base razionale per le conclusioni. All'aumentare dei dati, esse sono, inoltre, in grado di apprendere continuamente e di ricavare conoscenze dall'interazione.

Vantaggi delle soluzioni di sicurezza cognitive
Le soluzioni dotate di tecnologie cognitive consentono di:

- Migliorare le capacità dei SOC analyst junior permettendo loro di accedere a processi ottimali e conoscenze che in passato richiedevano anni di esperienza
- Migliorare la velocità di risposta mediante l'applicazione di funzionalità di intelligence esterne fornite da blog e da altre fonti, in modo da poter intervenire prima che siano disponibili le firme
- Identificare rapidamente le minacce, accelerare l'individuazione di comportamenti sospetti ed evitare l'esfiltrazione e l'infezione dei dati da parte dei malware, utilizzando metodi di analisi avanzati
- Ottenere un contesto meglio definito relativo a incidenti di sicurezza attraverso l'automazione della raccolta e dell'elaborazione dei dati locali ed esterni

La promessa e le sfide

Molti degli intervistati ritengono che i vantaggi delle soluzioni di sicurezza cognitive colmeranno le lacune esistenti al momento. Sebbene la sicurezza cognitiva sia una tecnologia emergente, il 57% ritiene che le soluzioni di sicurezza cognitive possano rallentare in modo significativo le azioni dei criminali informatici.

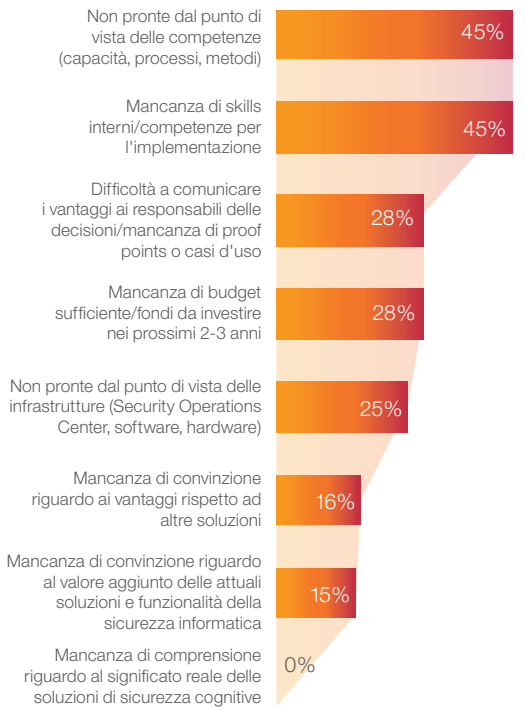
Quando abbiamo chiesto ai responsabili della sicurezza di selezionare i vantaggi di una soluzione di sicurezza potenziata dal cognitivo, il 40% ha indicato la migliore capacità di prendere decisioni in merito alla rilevazione e alla risposta agli incidenti, il 37% ha indicato la significativa accelerazione dei tempi di risposta agli incidenti e il 36% ha indicato la maggiore affidabilità nel distinguere tra eventi e incidenti veri e propri. Gli intervistati vogliono soluzioni di sicurezza cognitive per essere in grado di colmare i gap principali. Hanno bisogno di queste soluzioni per gestire intelligence, velocità e precisione.

Oggi, solo il 7% degli intervistati sta implementando soluzioni di sicurezza dotate di tecnologie cognitive per migliorare la preparazione ai rischi per la sicurezza informatica. Esiste questa aspettativa data la novità della soluzione. Tuttavia, in un prossimo futuro il numero di coloro che vorranno implementare queste soluzioni si triplicherà arrivando al 21%. Nei prossimi anni si assisterà all'adozione accelerata in quanto i responsabili della sicurezza, in numero sempre maggiore, si rivolgeranno a questa funzionalità per migliorare i loro sistemi immunitari digitali.

Gli intervistati hanno, però, visto le sfide potenziali all'adozione di soluzioni di sicurezza cognitive. Non è che i responsabili della sicurezza non comprendono la tecnologia a livello concettuale o non sono convinti del valore o dei vantaggi rispetto ad altre soluzioni; le sfide riguardano per lo più le competenze, i processi e i metodi. Il 45% degli intervistati ha dichiarato che le difficoltà principali per l'adozione consistono nel fatto che non si è pronti da un punto di vista della competenza e la mancanza di capacità interne di implementazione (vedere la Figura 5). Per dissipare queste preoccupazioni, occorrono più formazione e più preparazione.

Figura 5

Difficoltà principali per l'implementazione delle soluzioni di sicurezza cognitive identificate dai responsabili della sicurezza



"Siamo pronti a fare il passo successivo con soluzioni cognitive e intelligenti in grado di elaborare, organizzare e contestualizzare una quantità enorme di informazioni e conoscenze in materia di sicurezza che assorbono oggi moltissimo tempo e tantissime risorse."

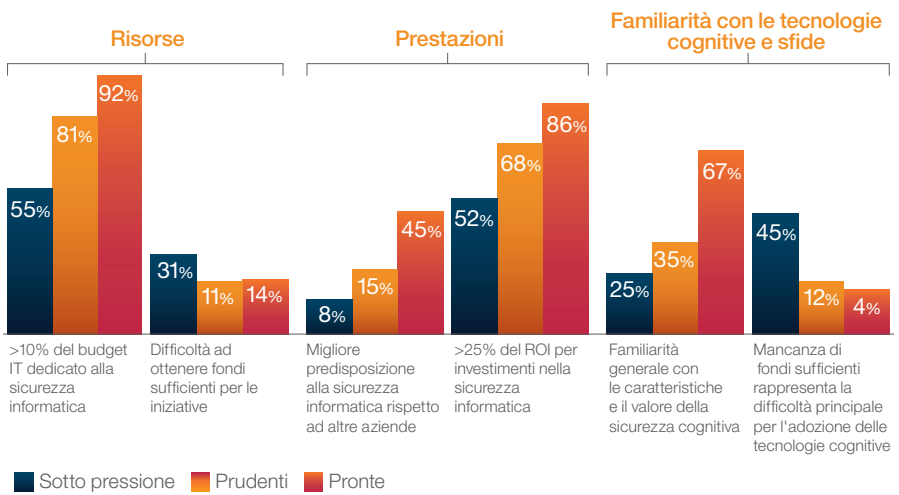
Un dirigente canadese responsabile di protezione finanziaria, gestione delle risorse

Pronti per l'era cognitiva

Per capire chi è pronto a entrare nell'era cognitiva della sicurezza oggi, abbiamo tracciato un profilo dei nostri intervistati in base al loro livello di efficacia, comprensione del cognitive e preparazione riguardo alla sicurezza così come lo hanno descritto essi stessi. L'analisi delle risposte ha rivelato tre gruppi distinti (vedere la Figura 6).

Figura 6

Le organizzazioni sotto pressione, prudenti e pronte descrivono il loro livello di preparazione



Quelle *sotto pressione*, che costituiscono il 52% del nostro campione, sono caratterizzate da problemi di budget e personale e una scarsa familiarità generale con le caratteristiche e il valore della sicurezza cognitiva. In genere, hanno una bassa percentuale di budget IT assegnato alla sicurezza informatica e molto spesso segnalano difficoltà nell'ottenere fondi sufficienti e risolvere le carenze di personale. Hanno anche indicato la mancanza di fondi sufficienti come

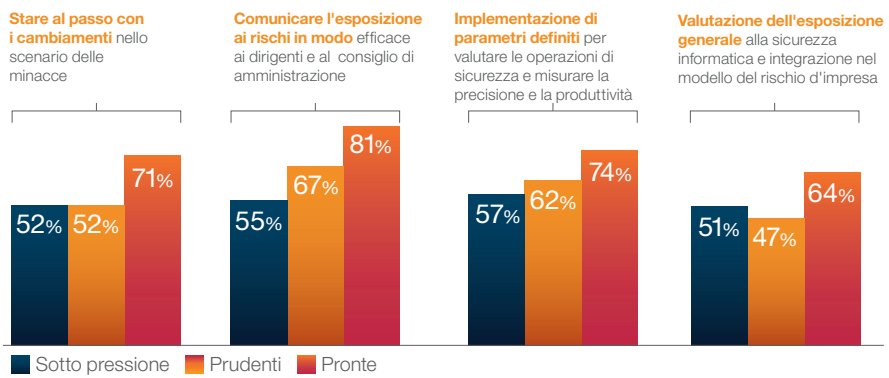
un problema per l'adozione delle tecnologie cognitive. (Per dettagli su come sono stati stabiliti e definiti questi gruppi, vedere la sezione "Demografia e metodologia" a pagina 20.)

Quelle *Prudenti*, che costituiscono il 27% del campione, non hanno le stesse difficoltà in termini di risorse indicate da quelle sotto pressione, ma non sono ancora del tutto pronte ad attuare oggi le tecnologie cognitive di sicurezza di nuova generazione.

Quelle *Pronte*, il 22% del campione, sono le più informate e le più entusiaste delle soluzioni di sicurezza cognitive. Le prudenti hanno una maggiore familiarità con la sicurezza cognitiva e fiducia, bilancio e ROI superiori rispetto alle altre. Ritengono di avvalersi di un approccio più maturo alla sicurezza; un'elevata percentuale dichiara che il loro security operation team è in grado di tenere il passo con i cambiamenti che avvengono nell'ambito delle minacce. Esse comunicano in modo efficace l'esposizione al rischio ai rispettivi dirigenti e consigli di amministrazione e integrano l'esposizione al rischio informativo nel loro modello di rischio di impresa (vedere la Figura 7).

Figura 7

I vari approcci alla sicurezza riportati dalle organizzazioni sotto pressione, prudenti e pronte



"C'è un rumore enorme là fuori; il cervello umano non può elaborarlo tutto giorno per giorno. Abbiamo bisogno di qualcosa che ci aiuti, qualcosa come intelligenza artificiale o tecnologie cognitive."

Chad Holmes, Principal and Cyber-Strategy, Technology and Growth Leader (CTO) presso Ernst & Young LLP

"La natura ininterrotta delle operazioni di sicurezza rappresenta una sfida costosa per molte organizzazioni in termini di personale, e consiste proprio in questo l'attrattiva della sicurezza cognitiva che non dorme mai e non si stanca mai."

Michael Pinch, Chief Information Security Officer, University of Rochester

Cosa si aspettano i responsabili della sicurezza dalle soluzioni di sicurezza cognitive quando si apprestano ad adottarle? Nel corso delle conversazioni con quelle pronte, abbiamo riscontrato che vogliono soluzioni di sicurezza cognitive in grado di:

- Essere sempre attive, per fornire un'assistenza continua
- Aiutare a ridurre i falsi positivi e rilevare anomalie nel comportamento
- Comprendere meglio lo scenario delle minacce e fornire un contesto agli incidenti
- Supportare la governance, la gestione del rischio e la conformità, in base al settore specifico, alla posizione geografica e ad altri requisiti normativi
- Cambiare la natura del lavoro relativo alla sicurezza, aiutando gli analisti a operare meglio e fornire un più alto livello di valore

C'è da aspettarsi che i responsabili della sicurezza che si sentono più maturi e hanno un minor numero di limiti in termini di risorse saranno i primi a esplorare una tecnologia emergente come la sicurezza cognitiva. Tuttavia, è importante rendersi conto che tutti, con più conoscenza ed esperienza, possono applicare le tecnologie cognitive per ovviare alle carenze ed estendere i limiti dei loro analisti al fine di migliorare le operazioni di sicurezza.

Raccomandazioni

Abbiamo esplorato l'attuale scenario della sicurezza per comprendere le pressioni, le sfide e le priorità dei soggetti intervistati. Sulla base di ciò che abbiamo osservato, abbiamo raccolto le raccomandazioni per aiutare la tua organizzazione a diventare pronti per l'era della sicurezza informatica cognitiva.

Riconoscere i propri punti deboli
I responsabili della sicurezza vogliono aumentare la loro capacità di risposta e ridurre la complessità e sono sempre più preoccupati per la perdita di reputazione in conseguenza degli incidenti. Cercare i principali punti deboli e la vulnerabilità all'interno della propria organizzazione. In che modo sono collegati? Quale è una priorità?

- Mancano funzionalità necessarie quali intelligence e capacità di ricerca delle minacce?
- I tempi di risposta agli incidenti e i tempi di risoluzione sono abbastanza veloci per le operazioni?
- Ci sono difficoltà a distinguere tra semplici eventi e incidenti veri e propri, o inserire le le cose nel contesto giusto?

Acquisizione di informazioni corrette sulle funzionalità di sicurezza cognitive
È opportuno adottare un approccio olistico e formale per conoscere le soluzioni di sicurezza cognitive. Ci potrebbero essere molte idee sbagliate nella vostra organizzazione dal punto di vista delle capacità, dei costi e dell'implementazione.

- Comprendere i potenziali casi di utilizzo per le soluzioni di sicurezza cognitive e applicarli alle aree carenti all'interno dell'organizzazione. Sono necessari un contesto più ampio per gli incidenti di sicurezza, dati solidi per migliorare il processo decisionale o nuovi modi per valutare in modo dinamico il rischio?
- Pensare a come comunicare i vantaggi delle soluzioni di sicurezza cognitive agli stakeholder di business e tecnici, quindi creare un piano per formare il proprio team e i dirigenti.

"La sicurezza cognitiva ha un notevole potenziale: può colmare le lacune rappresentate dalla carenza di personale, ridurre il profilo di rischio e aumentare l'efficienza della risposta. Può aiutare a capire la storia narrativa. Le persone consumano storie: è successo questo, poi è successo questo, con questo impatto, da parte di questa persona. Inoltre, le tecnologie cognitive possono ridurre le competenze necessarie per occuparsi di sicurezza informatica. Consentono di introdurre nuove prospettive provenienti da ambienti non-IT nella risoluzione del problema."

David Shipley, Director of Strategic Initiatives, Information Technology Services, University of New Brunswick

- Identificare e colmare le lacune in termini di competenze che possono impedire l'adozione della tecnologia all'interno della propria organizzazione.

Definire un piano di investimenti

È difficile costruire un caso di investimento quando una tecnologia è nuova e non collaudata nel mercato, Non si hanno molti esempi a cui fare riferimento . Dal momento che la stragrande maggioranza degli intervistati ha dichiarato che le loro richieste di finanziamento richiedono un ROI o un'altra analisi finanziaria, è imperativo che i responsabili della sicurezza adottino un approccio diverso per le soluzioni di sicurezza cognitive.

- Trattare le soluzioni di sicurezza cognitive come qualcosa di distinto. Evitare di concentrarsi sulla giustificazione tradizionale degli investimenti in sicurezza, come ad esempio i costi dei fix. Concentrarsi, invece, sul fatto che la sicurezza cognitiva è una funzionalità che può migliorare l'efficacia complessiva delle operazioni di sicurezza.
- Prendere il piano di formazione sviluppato e usarlo per ottenere il sostegno di altri dirigenti del settore e sfruttare il loro contributo per concretizzare gli investimenti.
- Pensare in modo creativo e cercare modi nuovi, oltre al ROI, per ottenere gli investimenti nella sicurezza cognitiva necessari per l'azienda.

Mirare ad aumentare le capacità, indipendentemente dal livello di maturità

Le organizzazioni identificate come pronte in linea di massima avevano più risorse a loro disposizione, più fiducia nelle loro capacità e la predisposizione a implementare subito le soluzioni di sicurezza cognitive; ciò non significa, però, che la sicurezza cognitiva è riservata a un gruppo scelto. Le soluzioni di sicurezza cognitive rappresentano una tecnologia emergente e le loro caratteristiche uniche possono essere utili per le organizzazioni di tutte le dimensioni.

- *Per coloro che si riconoscono nelle organizzazioni sotto pressione:* Identificare misure aziendali e carenze di competenze specifiche che le soluzioni di sicurezza cognitive potrebbero contribuire a migliorare, quindi costruire il caso di investimento
- *Per coloro che si riconoscono nelle organizzazioni prudenti:* Concentrarsi su come ottenere informazioni maggiori e corrette per diminuire la mancanza di competenze
- *Per coloro che si riconoscono nelle organizzazioni pronte:* Incanalare l'entusiasmo, scegliere un caso d'uso molto specifico per un'implementazione cognitiva pilota e assicurarsi che non sia isolata dalle operazioni di sicurezza a più ampio spettro.

Per ulteriori informazioni

Per saperne di più su questo studio dell'IBM Institute for Business Value, inviare un'e-mail all'indirizzo iibv@us.ibm.com. Segui @IBMIBV su Twitter e visita il seguente sito Web per consultare il catalogo completo delle nostre ricerche o iscriverti alla nostra newsletter mensile: **ibm.com**/iibv.

Per accedere agli approfondimenti dell'IBM Institute for Business Value da dispositivo mobile scaricare le app gratuite "IBM IBV" per telefono o tablet dall'App Store.

Il partner ideale per un mondo in continua evoluzione

In IBM, collaboriamo con i nostri clienti, mettendo a fattor comune informazioni di business, ricerche e tecnologie avanzate, così da riuscire a offrire loro un vantaggio esclusivo all'interno dello scenario attuale caratterizzato da una così rapida evoluzione.

IBM Institute for Business Value

IBM Institute for Business Value, divisione di IBM Global Business Services, sviluppa studi strategici per dirigenti aziendali senior relativi a problematiche centrali relative al settore pubblico e privato.

Partecipanti
Lisa van Deth, Program Marketing Manager, Campaign & Thought Leadership Strategy, IBM Security; Christophe Veltsos, Associate Professor, Department of Computer Information Science presso Minnesota State University, Mankato.

Ringraziamenti
Caleb Barlow, Vice President, WW Portfolio Marketing, IBM Security; Maria Battaglia, CMO, Resilient, IBM Security; Wangui McKelvey, Director, Portfolio Marketing - Security Services & Web Fraud, IBM Security; Kevin Skapinetz, Director of Strategy, IBM Security; Oxford Economics, per l'assistenza con l'amministrazione della raccolta dei dati del sondaggio.

Note e fonti

1 "2016 Cost of Data Breach Study: Global Analysis." Ponemon Institute. Giugno 2016. http://www-03.ibm.com/security/data-breach/

2 Friedman, Gabe. "JPMorgan Chase Atty: Bank Will Spend $500M on Cyber Security." 29 gennaio 2016 https://bol.bna.com/jpmorgan-chase-atty-bank-will-spend-500m-on-cyber-security/. Accesso effettuato il 21 settembre 2016.

3 Kelley, Diana and Carl Nordman. "Securing the C-suite: Cybersecurity perspectives from the boardroom and C-suite." IBM Institute for Business Value. 2016. ibm.biz/csuitesecurity

Demografia e metodologia
Per comprendere meglio quali sfide di sicurezza le organizzazioni si trovano ad affrontare, come le stanno affrontando e come vedono le soluzioni di sicurezza cognitive e il loro potenziale, l'Institute for Business Value e Oxford Economics hanno intervistato, tra maggio e luglio del 2016, una distribuzione equilibrata di 700 CISO e altri professionisti della sicurezza in 35 Paesi, con una rappresentanza di 18 settori.

Per determinare i nostri gruppi (le organizzazione pronte, quelle prudenti e quelle sotto pressione) abbiamo applicato un algoritmo di clustering k-means che ha rivelato tre distinti modelli di comportamento. Questi erano basati su domande relative all'efficacia in termini di sicurezza, alla comprensione delle tecnologie cognitive e al livello di preparazione a implementarle.

Informazioni sugli autori
Diana Kelley è Executive Security Advisor (ESA) presso IBM Security e responsabile di IBM Security Newsroom. Come ESA, si avvale degli oltre 25 anni di esperienza nella sicurezza IT per fornire consulenza e orientamento ai CISO e ai professionisti della sicurezza. Ha contribuito al rapporto di IBM X-Force e pubblica spesso importanti articoli sul blog Security Intelligence. Attualmente è membro di facoltà presso IANS Research e fa parte dell'Advisory Board di InfoSec World e del Content Committee dell'Executive Women's Forum. Diana è spesso invitata come relatrice in convegni di sicurezza ed è stata citata come esperta di sicurezza in *The New York Times, TIME*, MSNBC.com, *Information Security* E *The Wall Street Journal*. È co-autrice del libro *Cryptographic Libraries for Developers*. È possibile contattare Diana all'indirizzo drkelley@us.ibm.com.

Vijay Dheap è Program Director della IBM Security Division specializzata nella conversione di tecnologie emergenti in offerte commerciali. Al momento gestisce una serie completa di offerte in Security Intelligence che comprendono Advanced Analytics, Cognitive e SaaS. In passato si è occupato di cyber-forensic e mobile security. Vijay è fondamentalmente un tecnico al quale è stato assegnato il titolo di IBM Master Inventor. Il suo portafoglio di brevetti comprende mobile, collaborazione aziendale e innovazioni di sicurezza. Ha conseguito un MBA internazionale presso la Duke Fuqua School of Business e un master in ingegneria informatica presso la University of Waterloo, Canada. È possibile contattare Vijay all'indirizzo vdheap@us.ibm.com.

David Jarvis è Security e CIO Lead per l'IBM Institute for Business Value. È responsabile dello sviluppo e dell'esecuzione di un programma che esplora argomenti nuovi di carattere commerciale e tecnologico per le aree di sua competenza. Inoltre, è un esperto appassionato nello sviluppo e nella gestione di conoscenze di mercato, thought leadership e progetti di previsione strategica e ha ricoperto più posizioni in IBM in queste aree. È autore di numerosi rapporti di thought leadership in materia di sicurezza, comprese le Valutazioni dei CISO di IBM negli anni 2012 – 2014. Oltre alle sue responsabilità nel campo della ricerca, David insegna previsioni commerciali e risoluzione dei problemi in modo creativo. È possibile contattare David all'indirizzo djarvis@us.ibm.com.

Carl Nordman è Global Director del C-suite Study Program e CFO Research Lead per l'IBM Institute for Business Value. È responsabile della realizzazione di ricerche primarie in entrambi i domini. Svolge studi per scoprire i trend e le prospettive relative a questioni strategiche attuali. Carl possiede un'esperienza di oltre 25 anni nel settore dei rischi e delle frodi finanziarie. In passato ha ricoperto posizioni in IBM's Consulting Services, offrendo incarichi di CFO in aziende Fortune 1000 e gestendo i servizi di Finance e Accounting BPO in qualità di Account Executive per diversi clienti. È possibile contattare Carl all'indirizzo carl.nordman@us.ibm.com.

IBM Italia S.p.A
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

SEL03111-ITIT-00