

La Cyber Security nel 2027

Costruire resilienza attraverso governance strategica e autonomia operativa

forvis mazars

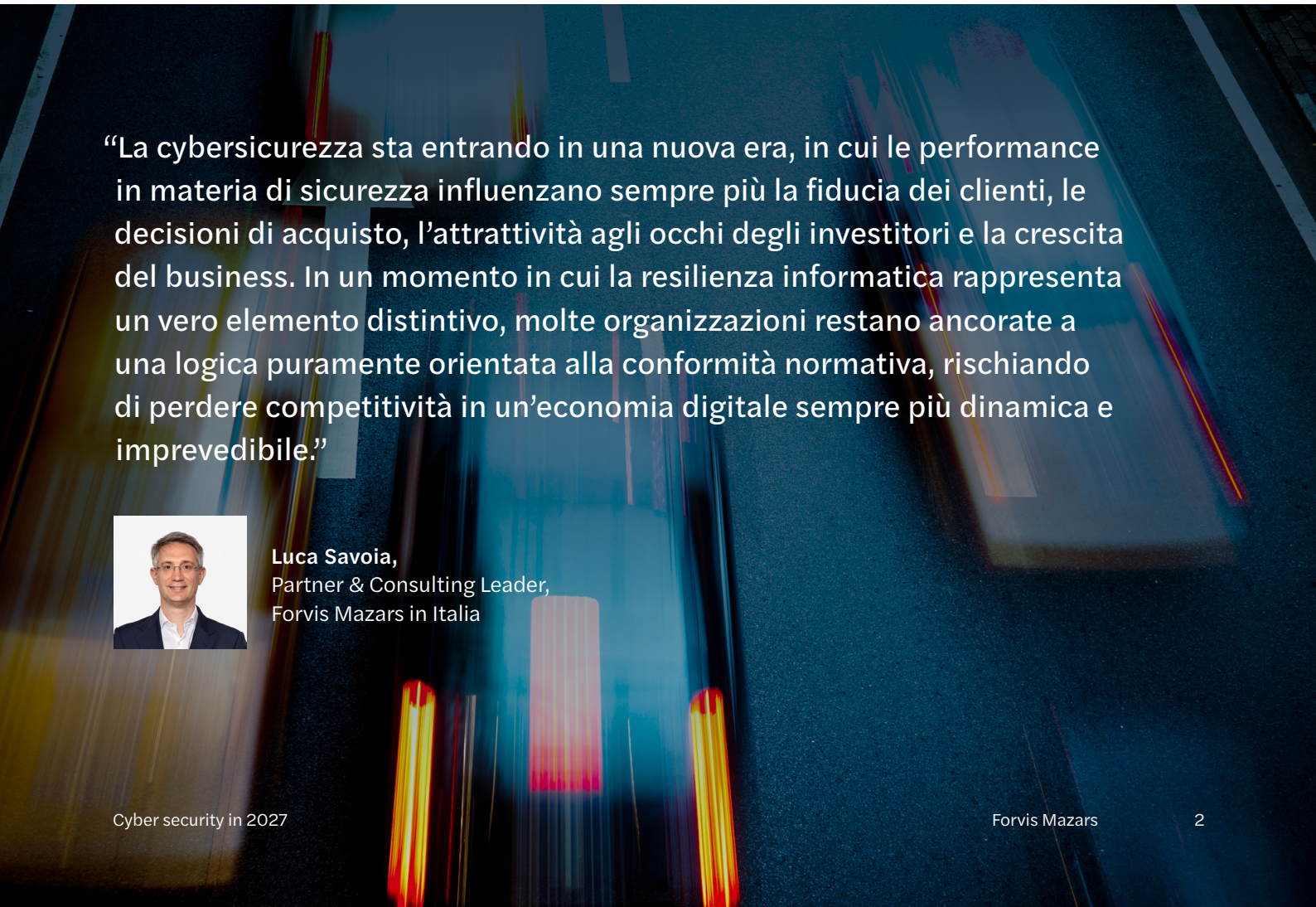
Prefazione

La cybersecurity si trova ad affrontare una convergenza di tecnologie in rapida evoluzione, normative in continuo cambiamento e minacce sempre più sofisticate. Per prepararsi alle sfide future, le organizzazioni dovranno adottare una governance strategica e promuovere un'innovazione intenzionale e consapevole.

Ogni anno, gli esperti di settore di Forvis Mazars si riuniscono per raccogliere approfondimenti sullo stato globale della cybersecurity e fornire indicazioni alle organizzazioni che devono orientarsi in un contesto sempre più complesso. Il report di quest'anno analizza come le organizzazioni possano sfruttare la tecnologia e orientarsi tra questioni globali complesse – come la regolamentazione, l'instabilità geopolitica e i temi legati alla sovranità digitale – per rafforzare resilienza e autonomia organizzativa.

Per andare avanti, le organizzazioni devono integrare la cyber security nelle proprie strategie di innovazione e implementazione, mantenendo al contempo l'agilità necessaria per adattarsi a minacce in continua evoluzione. Chi saprà farlo proteggerà i propri asset e otterrà un vantaggio competitivo nell'economia digitale.

L'intelligenza artificiale sta ridefinendo il panorama delle minacce, mentre i cambiamenti operativi, la regolamentazione e la sovranità digitale aggiungono ulteriore complessità. Insieme, queste pressioni stanno creando nuovi rischi e requisiti che richiedono un processo decisionale più strategico.



"La cybersicurezza sta entrando in una nuova era, in cui le performance in materia di sicurezza influenzano sempre più la fiducia dei clienti, le decisioni di acquisto, l'attrattività agli occhi degli investitori e la crescita del business. In un momento in cui la resilienza informatica rappresenta un vero elemento distintivo, molte organizzazioni restano ancorate a una logica puramente orientata alla conformità normativa, rischiando di perdere competitività in un'economia digitale sempre più dinamica e imprevedibile."

Luca Savoia,
Partner & Consulting Leader,
Forvis Mazars in Italia

Punti chiave

- Le organizzazioni più all'avanguardia stanno individuando modalità strategiche per trasformare la cyber security in un vantaggio competitivo
- La sovranità digitale è un tema sempre più centrale, ma per le organizzazioni globali l'autonomia è un obiettivo più utile da perseguire
- La proliferazione di normative digitali in Europa, unita alla crescente tendenza alla deregolamentazione negli USA, rende un approccio basato sul rischio la risposta più efficace alla cosiddetta "compliance fatigue".
- Le tecnologie operative vengono integrate sempre più negli ecosistemi IT aziendali, generando nuove opportunità e nuovi rischi.
- AI ha innescato una corsa agli armamenti tra attaccanti e difensori, rendendo necessario contrastare l'IA con l'IA e adottare modelli di governance adeguati e proporzionati.
- La governance dei dati continua a essere il pilastro di una strategia efficace, ma deve essere proporzionata alle esigenze e ai rischi
- I team di cybersecurity devono beneficiare di investimenti continui per mantenere il giusto equilibrio tra stabilità operativa, agilità organizzativa ed evoluzione della sicurezza.



Lo stato globale della cyber security

Perché la cyber security sta diventando una priorità per le supply chain

Con infrastrutture tecnologiche e catene di fornitura sempre più complesse, le aziende che adottano solide misure di cybersecurity beneficiano sempre più di vantaggi reputazionali e di una posizione preferenziale all'interno delle supply chain. Questa tendenza è particolarmente evidente nei mercati B2B, dove RFP e gare includono ormai requisiti di cybersecurity sostanziali, escludendo automaticamente dalla selezione i fornitori le cui misure di sicurezza non soddisfano gli standard prescritti.

La complessità delle moderne supply chain fa sì che le organizzazioni spesso non abbiano una piena visibilità su dove risiedano i propri dati o su come questi vengano elaborati. Questa mancanza genera vulnerabilità significative, tanto più che tecnologie come l'intelligenza artificiale introducono nuove forme di condivisione ed elaborazione dei dati. Allo stesso tempo, la crescente integrazione tra sistemi aziendali core, piattaforme cloud e servizi di terze parti amplia la superficie di attacco e rende la resilienza dipendente dalla visibilità sull'intero ecosistema tecnologico.

In definitiva, oggi ci si aspetta che ogni organizzazione gestisca e monitori i rischi di cyber security sull'intero ecosistema in cui opera. Questo principio è alla base del ***Digital Operational Resilience Act*** (DORA) dell'UE e della Direttiva NIS2, che rafforzano entrambi i requisiti per la gestione dei rischi informatici legati a terze parti e supply chain.

Questo spostamento verso una responsabilità condivisa sta favorendo l'adozione di framework di ***third-party risk management*** (TPRM) sempre più sofisticati. Parallelamente, la diffusione di strumenti di monitoraggio di terze parti, che assegnano alle organizzazioni un punteggio basato su metriche di cyber security, ha generato una nuova forma di pressione di mercato. Le aziende stanno scoprendo che il proprio livello di maturità in ambito cyber può incidere direttamente sulla capacità di aggiudicarsi contratti, stringere partnership e mantenere la fiducia dei clienti.



Sovranità vs autonomia: la nuova geopolitica della cyber security

La cyber security è sempre più una questione di sovranità nazionale. I governi esaminano ormai con attenzione dove vengono conservati i dati critici, chi gestisce i servizi digitali strategici e da quali tecnologie dipendono le organizzazioni, perché gli attacchi informatici sono diventati veri e propri strumenti di politica. Gruppi come *Volt Typhoon* si sono infiltrati nelle infrastrutture civili per garantirsi una leva futura, mentre episodi come il blackout CrowdStrike del 2024 hanno messo a nudo la fragilità di una dipendenza eccessiva da fornitori esterni, in particolare quelli soggetti ad altre giurisdizioni.

La risposta normativa non si è fatta attendere, soprattutto in Europa: requisiti sempre più stringenti sulla localizzazione dei dati, iniziative di cloud sovrano e un quadro normativo in costante espansione, in cui NIS2 e DORA pongono particolare enfasi sulla resilienza operativa e sulla sicurezza della supply chain. La tendenza, tuttavia, va ben oltre i confini europei, e con essa con essa, si sta trasformando anche il concetto stesso di cybersecurity efficace.

Non basta più dimostrare la conformità alle normative: è necessario dimostrare la capacità di resistere agli incidenti e di ripristinare rapidamente le attività essenziali a seguito di un attacco informatico.

La sovranità digitale, però, non rappresenta di per sé una strategia di resilienza. Portata all'estremo, può infatti causare una frammentazione del panorama dei fornitori, la duplicazione delle infrastrutture e una limitazione nell'accesso alle tecnologie più efficaci. Ciò a cui le organizzazioni dovrebbero puntare è l'autonomia, ovvero la capacità di comprendere, controllare e, quando necessario, modificare le proprie dipendenze digitali

Cosa dovrebbero fare le organizzazioni



È importante sapere dove vengono archiviati e trattati i dati sensibili: compresi i backup e le funzioni di supporto, non solo quanto previsto dal contratto.



Comprendere l'esposizione geopolitica dei fornitori: dipendenze nascoste all'interno della catena di fornitura possono avere un impatto significativo tanto quanto i rapporti contrattuali più evidenti.



Nel processo di approvvigionamento occorre tenere conto dell'ubicazione e della giurisdizione del fornitore: l'esposizione legale e geopolitica di un fornitore critico rappresenta ormai un fattore di rischio legittimo.



Dimostrare resilienza, non solo conformità: integrare la sovranità in un programma di resilienza più ampio come uno dei tanti elementi che lo compongono.

In quest'ottica, è l'autonomia – e non la sovranità – a rappresentare l'obiettivo strategico e l'indicatore più attendibile della resilienza che le autorità di regolamentazione, i clienti e gli investitori realmente richiedono.

In che modo DORA e NIS2 stanno cambiando la regolamentazione della cyber security?

DORA e NIS2 stanno ridefinendo il panorama della compliance in materia di cyber security in tutta Europa, spostando l'attenzione dalla semplice conformità formale alla dimostrazione concreta di resilienza operativa. Per le organizzazioni multinazionali, gestire entrambe le normative in parallelo è diventata una delle sfide regolatorie più complesse del 2027.

Nell'UE, la sfida è in larga parte una questione di volume: sono ormai oltre un centinaio gli atti e le direttive in materia digitale attualmente in vigore, ciascuno dei quali si aggiunge a una rete fitta e interconnessa di obblighi. NLa Direttiva NIS2, è finalmente entrata nella fase di applicazione, mentre il prossimo Cyber Resilience Act (CRA) imporrà che i prodotti con componenti digitali rispettino specifici requisiti di cybersecurity. Poiché NIS2 è una direttiva, gli Stati membri ne recepiscono i principi nelle rispettive legislazioni nazionali con sfumature e interpretazioni differenti. Questo significa che le organizzazioni non possono semplicemente replicare il lavoro di conformità svolto in un Paese e riutilizzarlo automaticamente in un altro. La proposta di Digital Omnibus punta a rendere il quadro normativo più coerente e razionale, introducendo un approccio maggiormente calibrato sulle dimensioni e sul profilo di rischio delle organizzazioni, anche se non ha ancora dispiegato completamente i propri effetti.

Al di là dell'Atlantico, la situazione si ribalta. Gli Stati Uniti si stanno muovendo verso una significativa deregolamentazione, senza nulla che somigli a un quadro federale organico per la cyber security. Le norme esistenti riguardano prevalentemente settori specifici o ambiti governativi, tra cui spicca il *Cybersecurity Maturity Model Certification* (CMMC), destinato alle organizzazioni che collaborano con il Dipartimento della Difesa. Anche in questo caso, però, l'implementazione del framework ha subito ritardi, con un rallentamento della sua applicazione e conseguenze che si stanno riflettendo anche su settori adiacenti, come l'IT nei servizi finanziari.

Inoltre, negli USA non esiste una legge federale unica sulla privacy: la protezione dei dati è regolata a livello statale e l'attuale contesto politico sembra orientato più a mantenere questo approccio frammentato che a introdurre una normativa nazionale uniforme. Paradossalmente, anche questo modello più leggero genera una forma di "compliance fatigue". Alcuni framework sono estremamente prescrittivi, mentre altri lasciano alle organizzazioni ampi margini di interpretazione, costringendole a operare in un contesto di incertezza. Nel frattempo, le imprese globali devono affrontare la complessa sfida di conciliare simultaneamente approcci normativi profondamente diversi tra le varie aree geografiche.

Come un approccio basato sul rischio garantisce continuità senza costi eccessivi

Questa crescente complessità normativa rappresenta, secondo molti professionisti del settore, sia un onere sia un'opportunità. Se da un lato le nuove regolamentazioni sono concepite per rafforzare la resilienza e la continuità operativa delle organizzazioni, dall'altro il carico di attività necessario per garantire la conformità può gravare pesantemente su team già alle prese con risorse limitate.

Con l'aumentare della complessità e della sovrapposizione dei requisiti normativi, le organizzazioni che adottano un approccio puramente formale, basato sul semplice adempimento delle prescrizioni ("tick-box approach"), rischiano di trovarsi in difficoltà nel gestire richieste tra loro eterogenee e spesso ridondanti. Per mantenere sotto controllo costi e sforzi legati alla conformità, le aziende dovrebbero invece privilegiare valutazioni basate sul rischio. Un approccio di cybersecurity fondato sul rischio consente infatti ai team di sicurezza di concentrare attenzione, risorse e investimenti sulle minacce e sulle vulnerabilità realmente critiche per il business.

Lo stato globale della cyber security

Cos’è la sicurezza delle OT e perché è sempre più sotto attacco?

La tecnologia operativa (OT) è alla base delle infrastrutture critiche e delle operazioni industriali in tutto il mondo. Man mano che questi sistemi diventano sempre più interconnessi digitalmente, le minacce informatiche aumentano, mettendo a rischio ambienti che storicamente hanno ricevuto meno attenzione in termini di sicurezza rispetto ai sistemi IT convenzionali.

Per lungo tempo l’OT è stata considerata una questione ingegneristica più che di cyber security. La sua protezione si basava meno su sofisticati meccanismi di difesa e più sul fatto che questi sistemi fossero isolati dalle reti esterne. Questi sistemi, spesso caratterizzati da livelli di protezione limitati, rappresentano un obiettivo particolarmente attrattivo per attori ostili dotati di risorse significative e motivazioni geopolitiche. Solo nel dicembre 2025 si sono registrati tentativi di attacco contro infrastrutture in Venezuela e Polonia. Alla luce di episodi come quelli che hanno colpito *M&S* e *Jaguar Land Rover*, dove la continuità operativa è stata compromessa da attacchi informatici, emerge come le aspettative in termini di monitoraggio e controllo stiano aumentando.

Qui si nasconde un paradosso non da poco: la maggior parte dei responsabili tecnologici segnala una seria mancanza di visibilità sulla propria rete OT, e un’organizzazione non può governare ciò che non riesce a vedere. La risposta naturale è quella di intervenire e connettere sistemi, dati e altri strumenti affinché il rischio diventi leggibile e tracciabile. Ma è proprio questo intervento a generare la nuova esposizione. Gli ambienti OT sono sempre più collegati all’IT aziendale, alle piattaforme cloud e a strumenti di manutenzione remota, e ogni nuovo canale erode l’isolamento che, fino a quel momento, proteggeva questi asset. La ricerca di trasparenza può finire per generare proprio la vulnerabilità che si voleva individuare

Tuttavia, la protezione di questi asset sta diventando sempre più un obbligo imposto dalla regolamentazione digitale, in particolare quando sono coinvolte infrastrutture critiche.

“La spinta verso una maggiore visibilità sull’OT è necessaria, ma deve essere disciplinata. Quando sistemi rimasti a lungo isolati vengono connessi online senza una governance e controlli proporzionati, le organizzazioni rischiano di accrescere quel rischio operativo che intendevano evitare.”



Paolo Zuliani,
Partner, IT Risk & Advisory
Forvis Mazars in Italia

Come l'AI sta cambiando la cyber security?

L'intelligenza artificiale sta cambiando la natura della cyber security su entrambi i fronti del conflitto digitale. Gli aggressori la utilizzano per lanciare minacce sempre più sofisticate, personalizzate e scalabili, mentre i difensori la sfruttano per migliorare il rilevamento delle minacce, automatizzare le risposte agli incidenti e aumentare la resilienza organizzativa.

Finora l'AI è stata spesso descritta come un equilibrio tra opportunità e rischio. Oggi, però, questa interpretazione non è più sufficiente. L'AI rappresenta una disruption strutturale che sta ridefinendo l'intero ecosistema della cybersecurity. Il risultato è una vera e propria corsa agli armamenti tecnologica, nella quale il divario tra aggressori e difensori rischia di ampliarsi.

Una sfida asimmetrica

Si tratta di un divario tanto di possibilità quanto di capacità; aggressori e difensori possono disporre di tecnologie simili, ma gli aggressori agili, per loro natura, hanno spesso un vantaggio sui difensori vincolati dai processi. Gli aggressori non hanno nulla da mantenere: nessun onere legato alla continuità operativa, nessuna gestione del cambiamento, nessun obbligo normativo e nessun consiglio di amministrazione a cui rendere conto. I difensori sono vincolati da strati di politiche, processi ed etica – giustamente, poiché hanno un'organizzazione da proteggere – ma ogni strato aggiunge attrito, ed è proprio l'attrito ciò che gli aggressori mettono a frutto. Le prove di questa accelerazione sono ovunque:

- **Volume e realismo in crescita:** il numero degli attacchi informatici continua ad aumentare, in particolare le frodi supportate dall'AI. I deepfake sono diventati una minaccia concreta per il management e le funzioni aziendali più sensibili. Un caso emblematico ha coinvolto la società di ingegneria ***Arup***, che avrebbe subito una perdita di circa 25 milioni di dollari dopo che un dipendente è stato ingannato da una videochiamata deepfake che simulava dirigenti aziendali.
- **Self-rewriting malware:** il codice malevolo capace di riscriversi per eludere il rilevamento sta rendendo obsoleti i tradizionali sistemi di difesa basati sulle firme, costringendo i difensori a orientarsi verso indicatori comportamentali di compromissione piuttosto che su impronte note.
- **Catene d'attacco completamente automatizzate:** l'elemento più rivoluzionario è probabilmente l'emergere dell'AI agentica, capace di eseguire autonomamente una successione completa di attività offensive a cui nessun team umano può reggerne il ritmo, per quanto solide siano le sue difese. Le organizzazioni devono applicare patch in modo proattivo, monitorare costantemente e concentrarsi in primo luogo sui sistemi e sui dati la cui compromissione causerebbe i danni maggiori.

Se gli attaccanti utilizzano l'IA, anche i difensori devono farlo – e la buona notizia è che funziona.

"L'intelligenza artificiale amplifica la capacità di difendere, ma anche quella di attaccare: accelera l'analisi, automatizza la risposta e moltiplica la superficie del rischio. La sfida non è quindi scegliere tra AI e sicurezza, ma progettare un'AI che sia sicura per costruzione."



Francesco Pulcrano
Partner, IT Risk & Advisory
Forvis Mazars in Italia

Lo stato globale della cyber security

Secondo il report IBM "Cost of a Data Breach" 2026, le organizzazioni che utilizzano sistemi di rilevamento e risposta agli incidenti supportati dall'AI hanno registrato una riduzione media del costo di una violazione pari a quasi il 40%, con un risparmio di circa $1,93 milioni per incidente; le stesse tecniche utilizzati dagli attaccanti possono inoltre essere rivolte verso l'interno per sottoporre a stress test le difese dell'organizzazione.

L'obiettivo a cui si sta guardando sempre di più è l'AI agenticacapace non solo di rilevare una minaccia, ma di isolarla e affrontarla. L'IA agentica può aiutare a risolvere un paradosso centrale di questa corsa agli armamenti: implementare l'IA in sicurezza richiede regole chiare, ma la cyber security esiste proprio perché gli aggressori sfruttano l'ignoto; i difensori non possono definire in anticipo un guardrail per ogni possibile risposta che un agente difensivo potrebbe dover affrontare.

Gli aggressori, al contrario, non incontrano questo vincolo. L'IA agentica, se impiegata correttamente, può rispondere agli attacchi in modo semi-autonomo, senza bisogno di prevedere il futuro.

L'IA amplia anche il campo di battaglia: ogni strumento basato sull'IA crea una nuova superficie d'attacco, e la prompt injection è ormai un fenomeno mainstream, come ha scoperto DPD quando i clienti sono riusciti a manipolare il suo chatbot inducendolo a insultarli, o come è successo a McDonald's quando un chatbot per le candidature ha esposto i dati di milioni di candidati. È per questo che la governance dell'IA e la privacy dei dati, a lungo trattate come discipline separate seppur correlate, devono ora essere urgentemente consolidate in un'unica policy, un'unica libreria di controlli e un'unica strategia di supervisione dei fornitori

Le sfide dell'AI e strategie pratiche di implementazione

Le sfide chiave legate all'IA agentica riguardano la verifica di un'adeguata convalida degli input e il mantenimento di una supervisione umana significativa, senza però trasformarla in un freno per ogni singola azione. Anche la governance dell'IA deve essere proporzionata e basata sul rischio: non è mai stato possibile difendersi in modo assoluto, e gli attacchi automatizzati non fanno che renderlo più evidente. La security by design, standard di riferimento per la mitigazione del rischio, comporta compromessi con usabilità e ***time to market***, e pretendere la perfezione risulta controproducente.



L'obiettivo della cybersecurity non è eliminare il rischio ma identificare e proteggere in modo adeguato gli asset più critici per l'organizzazione: dati sensibili, proprietà intellettuale, sistemi essenziali e processi di business strategici. In questo contesto, i team di cybersecurity devono evolvere da semplici funzioni di controllo a veri e propri partner del business:

Governance proporzionata: utilizzare per l'AI la stessa metodologia di valutazione delle altre tecnologie: trattarle allo stesso modo può ridurre l'efficacia dei controlli.

Tenere l'essere umano nel loop: definire chiaramente quali attività un agente AI possa svolgere autonomamente, e stabilire i casi in cui sia necessario il coinvolgimento di una persona, garantendo rigorosi meccanismi di validazione degli input.

Consolidare governance e privacy: gestire con un approccio unificato la governance dell'AI e la protezione dei dati, adottando policy condivise e strategie coordinate di supervisione dei fornitori, anziché trattarle come discipline separate.

Investire nelle competenze del team: l'aggiornamento continuo delle competenze è essenziale per tenere il passo con nuove tecniche di attacco e strumenti di difesa.

Quantum computing: prepararsi al cambio di paradigma

Sebbene il quantum computing non rappresenti ancora una minaccia immediata, il suo potenziale impatto è talmente significativo da rendere necessaria una preparazione fin da oggi. La minaccia quantistica segue una tempistica diversa dai tradizionali rischi cyber. Mentre i computer quantistici in grado di compromettere gli attuali standard crittografici potrebbero essere ancora lontani da una diffusione su larga scala, gli attori malevoli stanno già adottando strategie note come "steal now, decrypt later".

Questa realtà implica che le organizzazioni dovrebbero iniziare fin da subito a prepararsi alla transizione verso la crittografia resistente ai computer quantistici, iniziando con un inventario crittografico, definizione delle priorità di rischio e valutazione delle roadmap, prima che la minaccia diventi concreta e urgente.

Il *National Institute of Standards and Technology* (NIST), dopo aver finalizzato gli standard di crittografia post-quantistica nel 2024, ha iniziato a rendere disponibili strumenti e linee guida utili per supportare le organizzazioni in questo percorso di transizione.

Le organizzazioni dovrebbero intraprendere fin da ora attività di preparazione al cambiamento quantistico.



Inventario crittografico: mappare sistemi, app e dati che si basano su meccanismi crittografici per individuare le potenziali vulnerabilità future.



Prioritizzare gli asset: identificare quali dati e sistemi subirebbero il maggiore impatto in caso di compromissione delle tecnologie di crittografia.



Pianificare la transizione: sviluppare strategie di migrazione verso algoritmi quantum-safe.



Supply chain assessment: verificare che venditori e partner sono preparati alla transizione.

Strategia dei dati, trasformazione e governance

Il principio "garbage in, garbage out" richiede oggi un'attenzione più urgente che mai. Le decisioni supportate dall'AI dipendono dalla disponibilità di dati affidabili, accurati e ben gestiti, rendendo la data governance un elemento centrale delle strategie di cybersecurity. Una governance dei dati inefficace genera rischi che vanno ben oltre le tradizionali problematiche di protezione delle informazioni. Durante la gestione di incidenti informatici, molte organizzazioni scoprono l'esistenza di dati sconosciuti, archiviati in ambienti non monitorati e protetti da controlli poco chiari o insufficienti

Questa mancanza di visibilità non solo genera superfici di attacco sconosciute – i dati che non sono adeguatamente catalogati non possono essere protetti in modo adeguato – ma può anche comportare rischi di non conformità.

Third-party risk management e condivisione dei dati

Con l'aumento della complessità della condivisione dei dati, il TPRM è diventato essenziale per la gestione del rischio cyber. Le moderne supply chains rendono sempre più difficile comprendere con precisione come i dati vengano trattati, archiviati e protetti. Effective TPRM requires several key components: spesso articolate su più livelli di fornitori e subfornitori, rendono sempre più difficile comprendere con precisione come i dati vengano trattati, archiviati e protetti. Questa mancanza di trasparenza aumenta l'esposizione ai rischi e può compromettere sia la sicurezza sia la conformità normativa.

Per essere efficace, un programma di TPRM dovrebbe includere alcuni elementi chiave:

- **Service level agreements (SLAs) con controlli di sicurezza integrati:** i contratti con fornitori e partner dovrebbero definire requisiti di sicurezza, privacy e conformità normativa, prevedendo il diritto di audit, evitando di fare affidamento esclusivamente sulle autodichiarazioni dei fornitori.
- **Valutazione e monitoraggio continuo:** i programmi TPRM possono risultare più efficaci se prevedono un monitoraggio continuo e una rivalutazione periodica dei rischi legati ai fornitori, e il diritto di effettuare audit ha valore solo se viene effettivamente esercitato.
- **Gestione dei fornitori a più livelli:** non tutti i fornitori presentano lo stesso livello di rischio. Le organizzazioni dovrebbero adottare approcci a più livelli che concentrino la supervisione più intensiva sui fornitori più critici.

L'implementazione pratica della sicurezza e della governance dei dati

Le organizzazioni che desiderano rafforzare la propria data governance dovrebbero iniziare con attività pratiche e concrete, anziché concentrarsi esclusivamente sulla definizione di policy teoriche e documentazione formale. Un punto di partenza efficace è rappresentato dagli esercizi di business continuity, coinvolgendo attorno allo stesso tavolo figure sia tecniche sia non tecniche, iniziando da una semplice domanda: "Cosa succederebbe se domani il tuo telefono e il tuo computer smettessero di funzionare?". Da questo tipo di confronto emergono in modo naturale riflessioni più profonde su dipendenze dei dati e requisiti di protezione.

Un approccio conversazionale di questo tipo aiuta a rendere la sicurezza comprensibile anche per chi non possiede competenze tecniche. I team di cybersecurity dovrebbero chiedersi: Le policy sono facilmente comprensibili? Un utente non tecnico è in grado di applicarle correttamente? Formazione e sensibilizzazione possono aiutare i dipendenti a rispettare le regole, aumentare la consapevolezza dei rischi e consentire ai team di comprendere meglio le esigenze operative dell'organizzazione.

Solo attraverso questa collaborazione è possibile progettare misure di sicurezza realmente efficaci e sostenibili.

Questo equilibrio tra sicurezza dei dati e abilitazione del business rappresenta una sfida centrale per la governance. Policy eccessivamente rigide portano spesso a soluzioni alternative rischiose, alimentando la diffusione dello *shadow IT*. Un approccio efficace all'abilitazione del personale combina controlli tecnici e iniziative culturali. Una collaborazione con le business unit può favorire una comprensione reciproca e controlli compensativi come il monitoraggio possono mantenere i team informati sul comportamento degli utenti.

Team cyber e competenze

La forza lavoro della cyber security si trova ad affrontare sfide senza precedenti, mentre il settore evolve rapidamente e il divario di competenze continua ad allargarsi. Le organizzazioni hanno bisogno di professionisti che comprendano sia i principi tradizionali della sicurezza sia le tecnologie emergenti.

Il ruolo del *Chief Information Security Officer* (CISO), in particolare, si è evoluto in modo significativo negli ultimi anni. Ci si aspetta che agiscano come leader di business piuttosto che come semplici specialisti tecnici, con responsabilità che si estendono alla compliance normativa, al reporting verso il CdA e alla pianificazione strategica. Questa evoluzione riflette la trasformazione della cyber security da funzione tecnica a leva abilitante per il business.

Di conseguenza, la retribuzione per i ruoli di CISO è aumentata, a riflesso sia dell'ampliamento delle responsabilità sia dell'importanza crescente del ruolo. Questa tendenza, tuttavia, mette anche in luce la difficoltà di sviluppare una pipeline di candidati qualificati: molte organizzazioni si stanno rivolgendo a CISO virtuali come soluzione per colmare le lacune all'interno del proprio bacino di talenti e per disporre di un contesto di esperienza più ampio.

La sfida dell'innovazione

Una delle sfide più significative per la forza lavoro consiste nel trovare professionisti capaci sia di innovare sia di gestire, soprattutto nelle organizzazioni di medie dimensioni. Il rapido ritmo del cambiamento tecnologico implica che i professionisti cyber debbano apprendere continuamente nuove tecnologie, mantenendo al contempo una solida competenza sui principi fondamentali della sicurezza.

Questa sfida è particolarmente acuta in ambiti come AI e *quantum computing*, dove l'intersezione tra tecnologia all'avanguardia e sicurezza genera complessità che pochi professionisti comprendono appieno. Le organizzazioni si rivolgono sempre più spesso ad advisor e consulenti di fiducia per colmare questo divario di competenze.

Costruire team cyber sostenibili

Il tradizionale approccio basato sull'assunzione di singoli esperti di cyber sta diventando sempre meno sostenibile per molte organizzazioni. La competizione per i migliori talenti sta spingendo le retribuzioni verso livelli che molte aziende non possono sostenere, mentre il rapido ritmo del cambiamento rende difficile per i team interni restare al passo con tecnologie emergenti.

Automazione e AI consentono naturalmente ai team di scalare le proprie operazioni, ma i modelli di servizio condiviso stanno diventando sempre più comuni, in particolare negli scenari di M&A, dove società madri o fondi di investimento forniscono capacità e supporto in ambito cyber alle società del proprio portafoglio o controllate. Anche le partnership esterne acquisiscono un valore crescente, portando approcci di implementazione collaudati e aiutando le organizzazioni a colmare le lacune di competenze in modo economicamente sostenibile.

"Oggi i CISO devono essere in grado di quantificare il valore di business della cyber security, comunicare con dirigenti non tecnici e allineare la strategia di sicurezza agli obiettivi aziendali. Tutto questo richiede competenze tecniche e trasversali che molte organizzazioni non riescono a permettersi finché non ne hanno un bisogno ormai impellente."



Luca Savoia,
Partner & Consulting Leader,
Forvis Mazars in Italia

Quantificare il valore della cyber

Le organizzazioni stanno superando le mere metriche tecniche per valutare l'efficacia della cyber security attraverso il suo impatto sul business, considerando risultati come le interruzioni evitate e i ricavi resi possibili da una sicurezza solida. Questo cambio di prospettiva è fondamentale per ottenere finanziamenti e dimostrare il ROI.

La questione dei costi: la cyber security come investmento, non come spesa

La proliferazione delle minacce e la complessità degli ambienti tecnologici moderni possono far percepire la cyber security come un centro di costo in continua espansione. Le organizzazioni più all'avanguardia, tuttavia, stanno ridefinendo la spesa in cyber security come un investimento strategico.

Molte organizzazioni stanno riconoscendo il vantaggio competitivo derivante da solide pratiche di cyber security. Un robusto sistema di sicurezza informatica rappresenta un elemento di differenziazione sempre più prezioso sul mercato, in particolare nei settori B2B, dove i clienti lo valutano come parte della propria gestione del rischio.

In questa crescente attenzione è presente anche una componente di compliance – i clienti devono considerare le proprie supply chain ai fini della loro stessa conformità – ma spesso citano anche incidenti di grande risonanza quando sollevano requisiti di cyber security, a dimostrazione di una crescente consapevolezza di mercato riguardo al potenziale impatto di un'interruzione. I team di capaci di quantificare e comunicare il valore di questo vantaggio possono ottenere livelli di adesione senza precedenti.

Naturalmente, la cyber security non è rilevante solo per i clienti. Le compagnie di assicurazione informatica sono comprensibilmente più attente che mai alle misure adottate, e le istituzioni finanziarie stanno sempre più integrando la preparazione in ambito cyber security nelle proprie valutazioni del rischio. Sia il settore assicurativo sia quello finanziario offrono quindi un incentivo quantificabile a favore di programmi di sicurezza solidi.



Quantificare il valore della cyber security





Misurare ciò che conta davvero

LLe organizzazioni più all'avanguardia stanno superando le tradizionali metriche di sicurezza per concentrarsi su modalità di misurazione del successo direttamente collegate ai risultati di business e al valore per gli stakeholder. Tra queste rientrano:

- **Obiettivi di tempo di ripristino:** con quale rapidità è possibile ripristinare le normali operazioni dopo un incidente?
- **Metriche di impatto sul business:** qual è il costo effettivo degli incidenti di sicurezza in termini di ricavi, relazioni con i clienti e posizionamento competitivo?
- **Indicatori di fiducia degli stakeholder:** in che modo le capacità di sicurezza influiscono sulla fiducia di clienti, investitori e partner?
- **Abilitazione dell'innovazione:** con quale efficacia il programma di sicurezza sostiene l'innovazione del business?

Ottimizzare il ROI della spesa in cyber

Le organizzazioni che investono in misure di cyber security proattive dimostrano sistematicamente risultati migliori rispetto a quelle che adottano approcci reattivi. Tuttavia, poiché le risorse sono limitate anche nelle organizzazioni più grandi, le seguenti aree di investimento possono contribuire a ottimizzare il ROI e ridurre il rischio:

- **Prioritizzazione basata sul rischio:** concentrare risorse umane e capitale sulla protezione degli asset più critici, anziché tentare di proteggere ogni cosa allo stesso livello.
- **Security by Design:** integrare i requisiti di sicurezza in sistemi e processi fin dall'inizio, anziché cercare di aggiungerli successivamente.
- **Approcci integrati:** ricercare soluzioni di sicurezza in grado di rispondere contemporaneamente a più requisiti, riducendo la necessità di soluzioni puntuali.
- **Automazione ed efficienza:** investire in strumenti e processi che amplificano le capacità umane anziché limitarsi ad aggiungere personale.
- **Formazione dei dipendenti:** attuare programmi regolari di formazione e sensibilizzazione che riducano la probabilità di incidenti.
- **Preparazione alla risposta agli incidenti:** sviluppare e testare regolarmente, in modo completo, le capacità di risposta agli incidenti.
- **Servizi condivisi:** valutare, ove opportuno, servizi di cyber security condivisi o virtuali, in particolare per competenze specialistiche che non richiedono risorse interne a tempo pieno.

Lo stato globale della cyber security

Come possono le aziende migliorare la propria resilienza nel 2027?

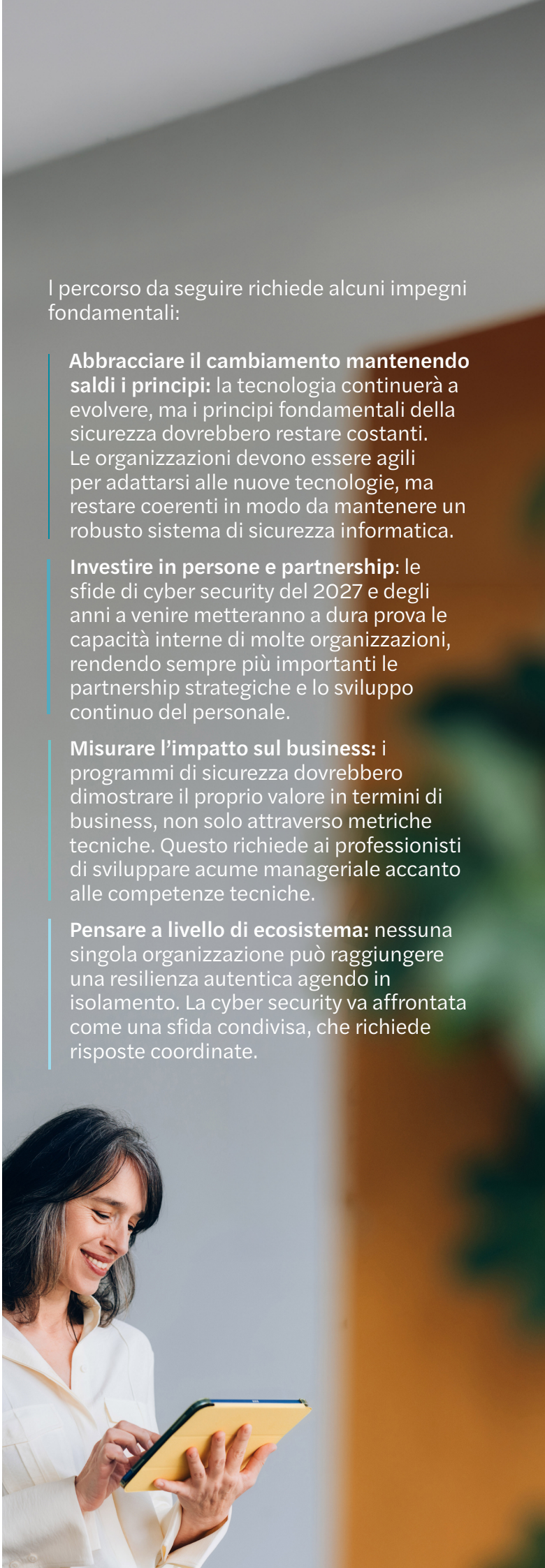
Guardando al 2027, le organizzazioni dovranno dimostrare di saper anticipare gli attacchi, mantenere operative le funzioni critiche e adattarsi al mutare delle minacce. Sempre più sistematicamente, ci si aspetterà che le organizzazioni dimostrino a clienti, autorità di regolamentazione e assicuratori che le considerazioni di sicurezza sono parte integrante della progettazione dei processi aziendali.

Inoltre, le aziende dovranno guardare oltre i propri confini, per prendere in considerazione la sicurezza dell'intero ecosistema di business. Questo include non solo i tradizionali partner della supply chain, ma anche fornitori tecnologici, service provider.

Tra le componenti chiave figurano:

- **Threat intelligence condivisa:** collaborare con i partner per identificare e rispondere a minacce che coinvolgono più organizzazioni o entità.
- **Risposta coordinata agli incidenti:** sviluppare capacità di risposta in grado di operare oltre i confini organizzativi.
- **Valutazione standardizzata del rischio:** utilizzare framework e metriche comuni per valutare e comunicare il rischio lungo tutto l'ecosistema.
- **Capacità di difesa collettiva:** partecipare a iniziative settoriali finalizzate a sviluppare capacità difensive condivise.

Le organizzazioni che affronteranno le sfide cyber in modo strategico – abbracciando tecnologie avanzate ma con una governance solida, investendo in persone e competenze pur sfruttando l'automazione, e considerando la sicurezza come una leva abilitante e non come un vincolo – si troveranno a godere di un vantaggio competitivo significativo.



Il percorso da seguire richiede alcuni impegni fondamentali:

Abbracciare il cambiamento mantenendo saldi i principi: la tecnologia continuerà a evolvere, ma i principi fondamentali della sicurezza dovrebbero restare costanti. Le organizzazioni devono essere agili per adattarsi alle nuove tecnologie, ma restare coerenti in modo da mantenere un robusto sistema di sicurezza informatica.

Investire in persone e partnership: le sfide di cyber security del 2027 e degli anni a venire metteranno a dura prova le capacità interne di molte organizzazioni, rendendo sempre più importanti le partnership strategiche e lo sviluppo continuo del personale.

Misurare l'impatto sul business: i programmi di sicurezza dovrebbero dimostrare il proprio valore in termini di business, non solo attraverso metriche tecniche. Questo richiede ai professionisti di sviluppare acume manageriale accanto alle competenze tecniche.

Pensare a livello di ecosistema: nessuna singola organizzazione può raggiungere una resilienza autentica agendo in isolamento. La cyber security va affrontata come una sfida condivisa, che richiede risposte coordinate.

Dalla conformità alla resilienza: l'AI cambia il ritmo della sicurezza in Italia

Regolatori e mercato convergono su un messaggio: la conformità formale non basta più

Le minacce legate all'AI sono ormai un tema di primo piano, tanto per i regolatori quanto per le organizzazioni di ogni settore. I modelli più avanzati sono in grado di individuare vulnerabilità e generarne lo sfruttamento a una velocità che mette sotto pressione gli approcci alla sicurezza costruiti su ritmi più lenti.

In Italia, il segnale più chiaro arriva dal settore finanziario, il più normato e attenzionato, che da sempre funziona da *trend setter*: è successo con la NIS 2, che il mondo finanziario ha affrontato prima di quello industriale. Con la Comunicazione al mercato del 17 luglio 2026, Banca d'Italia ha chiesto a banche, istituti di pagamento, SIM, SGR e agli altri intermediari direttamente vigilati di rileggere i requisiti DORA già in vigore alla luce dell'AI.

Non si tratta di un nuovo framework, ma di un'interpretazione più esigente di uno già esistente, e arriva a dieci giorni da una lettera con cui la BCE ha chiesto lo stesso alle banche significative dell'area euro. Il messaggio, che è anche il filo conduttore di questo report, è che la conformità formale non basta più.

La Comunicazione chiede ai Consigli di Amministrazione di esaminare il tema in seduta congiunta con il Collegio Sindacale e di avviare una relazione, corredata da un piano di lavoro, che fotografi l'esposizione al rischio su governance, igiene informatica, gestione degli asset, gestione delle vulnerabilità, monitoraggio e test di resilienza. Sono le aree su cui qualunque organizzazione, a prescindere dal settore, è chiamata a interrogarsi. La scadenza è solo il punto di arrivo di un esercizio che andrà comunque affrontato, con o senza obbligo formale: capire quanto i propri programmi di resilienza reggano davvero di fronte a un avversario che oggi si muove alla velocità dell'AI.

"Le minacce informatiche si evolvono più rapidamente che mai, spinte dall'intelligenza artificiale, da ecosistemi sempre più interconnessi, dalle tensioni geopolitiche e da un quadro normativo sempre più articolato. Eppure la risposta resta la stessa: un approccio basato sul rischio, in grado di proteggere ciò che conta davvero e di considerare la resilienza come il vero parametro di misura della cybersecurity."



Paolo Zuliani,
Partner, IT Risk & Advisory
Forvis Mazars in Italia

Contatti

Luca Savoia
Partner e Consulting Leader,
Forvis Mazars in Italia
luca.savoia@forvismazars.com

Francesco Pulcrano
Partner, IT Risk & Advisory,
Forvis Mazars in Italia
francesco.pulcrano@forvismazars.com

Paolo Zuliani
Partner, IT Risk & Advisory
Forvis Mazars in Italia
paolo.zuliani@forvismazars.com

Forvis Mazars Group SC is an independent member of Forvis Mazars Global Limited, a leading professional services network. Operating as an internationally integrated partnership in over 100 countries and territories, Forvis Mazars Group specialises in audit, tax and advisory services. The partnership draws on the expertise and cultural understanding of over 40,000 professionals across the globe to assist clients of all sizes at every stage in their development.

© October 2026

forvismazars.com