CYBER SECURITY program 2025

Prepararsi ai nuovi rischi del Digitale

POSITION PAPER

TIG | THE INNOVATION GROUP

CYBER SECURITY program 2025

Prepararsi ai nuovi rischi del Digitale

POSITION PAPER

TIG THE INNOVATION GROUP

Realizzato da **TIG – The Innovation Group**

Edizione a cura di:
Elena Vaciago

Produzione e realizzazione grafica:
Alberto Villa

Chiuso in redazione a novembre 2025

INDICE

Position Paper Cybersecurity 2025: il valore strategico della sicurezza

Elena Vaciago
Research Manager, TIG - The Innovation Group

Il panorama della sicurezza informatica nel 2025 è definito da una crescente complessità, dall'adozione pervasiva di tecnologie dirompenti come l'Intelligenza Artificiale (AI) e dal rafforzamento del quadro normativo europeo. Il presente Position Paper Cybersecurity, parte del Programma annuale di TIG, fa il punto sullo stato dell'arte, analizzando le strategie di contrasto al cyber crime, l'evoluzione del ruolo del Chief Information Security Officer (CISO), le sfide cruciali della cyber resilienza, la sicurezza negli ambienti industriali (OT/IoT) e i rischi emergenti legati al futuro digitale, inclusi il cloud ibrido e il quantum computing. Analisi che provengono dall'attività convegnistica, interviste a esperti, ricerca e approfondimenti condotti nel corso del 2025, grazie al prezioso contributo di Keynote Speaker, dell'**Advisory Board del Programma**, della Community dei CISO che ci segue in queste iniziative.

L'insight principale che emerge dai lavori del 2025 è che la cybersecurity non è più un centro di costo o un mero adempimento tecnico, ma piuttosto un elemento sistemico e un abilitatore strategico di business, oggi fondamentale in tutte le organizzazioni, pubbliche e private, per conquistare e mantenere competitività e fiducia.

Il ruolo strategico del CISO e la gestione del rischio integrato

La figura del CISO o Responsabile cybersecurity è in rapida evoluzione in Italia, si sta trasformando da tecnico a leader strategico e manageriale. I risultati dell'indagine "Il Ruolo del CISO Survey 2025" realizzata da TIG e AssoCISO evidenziano una figura più matura, chiamata a **tradurre la sicurezza in valore per l'impresa e a guidare il cambiamento**. Tuttavia, il pieno riconoscimento e l'integrazione del ruolo rimangono sfide aperte: solo il 61% delle organizzazioni intervistate (che hanno già oggi una strategia formale di cybersecurity) ha un CISO dedicato e appena il 48% prevede un flusso di comunicazione strutturato verso il Consiglio di amministrazione (CDA).

Per allinearsi al business, il CISO deve adottare un approccio risk-based e integrato (Enterprise Risk Management - ERM), superando la gestione "a silos" dei rischi (cyber, finanziario, legale). Il rischio deve essere visto come una leva per guidare gli investimenti e garantire la continuità operativa. La mancanza di consapevolezza del rischio nel top mana-

gement è un ostacolo significativo, soprattutto nel settore pubblico. La carenza di competenze è la criticità più sentita dal 57% dei CISO intervistati. Questo non è solo un problema di quantità di personale, ma di allineamento delle competenze richieste. È fondamentale investire in formazione continua, mentoring e valorizzare le "power skills" (adattabilità, comunicazione).

AI: sfida di governance e potente alleato

L'Intelligenza Artificiale è un Game Changer per la cybersecurity. Se da un lato l'AI è un alleato cruciale per rafforzare le difese aziendali, grazie alla capacità di individuazione precoce delle minacce e all'automazione della risposta agli incidenti, dall'altro, la sua adozione disordinata e frammentata genera vulnerabilità. Il 71% delle aziende ha già adottato strumenti di AI in ambito sicurezza, ma il 64% sottolinea la necessità di una supervisione umana continua.
Le minacce esterne si evolvono con l'AI: il phishing si raffina, sfruttando la personalizzazione, e i deepfake (audio e video) emergono come strumenti per colpire la fiducia. All'interno delle aziende, i rischi più ricorrenti derivano dall'uso non governato di strumenti innovativi (ad esempio, assistenti virtuali che memorizzano contenuti sensibili senza policy adeguate). È imperativo definire ruoli chiari, processi trasparenti e integrare la sicurezza fin dalle prime fasi di progettazione di nuove soluzioni AI-based (security-by-design). Inoltre, l'AI richiede una governance rigorosa che ne consideri l'impatto etico e di sostenibilità (parametri ESG).

Il quadro normativo europeo e la cyber resilienza

Il contesto normativo europeo, guidato da direttive come NIS2, DORA e il Cyber Solidarity Act, sta spingendo verso un livello comune elevato di sicurezza e una risposta coordinata. La NIS2, recepita in Italia con il D.Lgs. 138/2024, coinvolge circa 20.000 soggetti e impone principi cardine come l'accountability (che rende il Board direttamente responsabile) ma richiede anche molti sforzi per l'adeguamento e un approccio di multi-compliance. In ultima analisi, adeguarsi alla NIS2 non deve essere un mero adempimento burocratico, ma un'opportunità per migliorare la governance e la sicurezza.
La Cyber Resilienza è un pilastro essenziale, definita come la capacità di un'organizzazione di resistere, riprendersi e adattarsi agli attacchi, minimizzando l'impatto. Per ottenerla, la Risposta agli Incidenti (IR) deve essere robusta e strutturata in sei fasi chiave: Preparazione, Identificazione, Contenimento, Eradicazione, Ripristino e Apprendimento.
Un elemento cruciale per ottenere investimenti e aumentare la consapevolezza è l'uso di simulazioni ed esercitazioni (come Tabletop Exercises e Cyber Drills), che permettono al management di "toccare con mano" il rischio e misurare il divario tra procedure e risposta reale. Inoltre, l'efficacia della risposta post-incidente dipende dalla corretta gestione delle prove informatiche, che troppo spesso vengono compromesse o cancellate durante il ripristino dei sistemi. La legislazione italiana (L. 48/2008) in materia è considerata obsoleta, e gli esperti sottolineano la necessità di integrare la Digital forensics nelle procedure di IR.

L'espansione del perimetro di attacco: OT, supply chain e cloud

La trasformazione digitale ha amplificato la superficie d'attacco in settori cruciali:

- **OT/cybersecurity industriale:** la sicurezza negli ambienti OT/ICS è riconosciuta come una priorità alta o estremamente alta dalle imprese industriali. Tuttavia, il percorso è pieno di sfide: la principale è la mancanza di una visione integrata IT-OT e la carenza di competenze specializzate.
  Gli ambienti OT si caratterizzano per cicli di vita estremamente lunghi e provengono

da contesti storicamente meno sensibili alla cybersecurity. Le strategie di mitigazione richiedono segregazione spinta (di rete, Active Directory), processi di change management OT distinti e l'adozione di politiche Security-by-design per i nuovi approvvigionamenti.

- **Supply chain:** la catena di fornitura è un vettore di attacco principale, responsabile di circa un terzo degli incidenti informatici. Normative come NIS2 e DORA obbligano le aziende a estendere i requisiti di sicurezza ai fornitori, che spesso rappresentano l'anello debole della catena, specialmente se di piccole dimensioni. La NIS2 sottolinea che la responsabilità finale della sicurezza rimane in capo all'entità vigilata, anche in caso di esternalizzazione.
- **Cloud ibrido e multi-cloud:** la migrazione al cloud è un trend inarrestabile, ma la complessità del cloud ibrido e multi-cloud è nemica della sicurezza. Molte aziende sono preoccupate per la sicurezza nel cloud ibrido. Questa complessità deriva dalla gestione di interfacce/API mal configurate, dalla difficoltà nell'integrare soluzioni eterogenee e dalla necessità di competenze specifiche per ogni singola piattaforma. L'approccio Zero Trust, basato sul principio del minimo privilegio e sull'uso di strumenti come la micro-segmentazione e la Multi-factor authentication (MFA), è fondamentale per proteggere gli ambienti distribuiti e prevenire i movimenti laterali degli attaccanti.

Nuovi rischi e sovranità digitale

La cybersecurity è sempre più influenzata dalla situazione geopolitica, che impone un ripensamento delle scelte tecnologiche. Molte organizzazioni hanno già modificato le proprie scelte di vendor o servizi cloud a causa di dinamiche geopolitiche, e si prevede che tale influenza crescerà. L'Unione Europea sta rispondendo a questa crescente instabilità con un forte impulso verso l'autonomia tecnologica (che, come concetto, è leggermente meno forte dell'indipendenza tecnologica, perché si può essere autonomi, in grado di autoregolarsi e fare scelte libere, senza essere completamente indipendenti), supportando l'industria europea tramite il regolamento Digital Europe, l'EU Chips Act per i semiconduttori e i piani per le AI Factory.
Infine, il Quantum Computing non è più una minaccia futura, ma una realtà in accelerazione. L'algoritmo di Shor rende vulnerabile la crittografia attuale. Le contromisure si concentrano sulla Post-Quantum Cryptography (PQC) – algoritmi classici resistenti agli attacchi quantistici (con i primi standard definiti dal NIST nell'agosto 2024) – e sulla Quantum Key Distribution (QKD), basata su proprietà fisiche inviolabili. La corsa è iniziata, e le organizzazioni devono avviare la migrazione adesso per garantire la sicurezza futura.

1 Strategie di contrasto del cyber crime

Governare l'AI per la cybersicurezza del futuro

Gianluca Dotti
Giornalista, TIG - The Innovation Group

La vera sfida oggi non è tanto usare l'intelligenza artificiale, ma farlo in modo sostenibile, sicuro e tracciabile. Questa tecnologia è entrata nei processi aziendali come leva di produttività e innovazione, ma spesso senza un disegno preciso che ne governi l'impatto complessivo. Eppure, l'AI è un elemento sistemico, così potente da trasformare il modo in cui si prendono decisioni, si analizzano i dati e si costruiscono relazioni tra persone e macchine: proprio per questo, richiede un trattamento alla pari delle infrastrutture critiche.
Come emerso durante la discussione del tavolo di lavoro "Bilanciare AI e cybersecurity nei percorsi di trasformazione digitale" del CISO Panel di Roma, lo scorso 27 maggio, **molte realtà aziendali stanno integrando gli strumenti di AI** senza un piano strutturato. L'introduzione avviene spesso per iniziativa di singoli reparti, senza un coordinamento centralizzato con le funzioni di cybersicurezza e di compliance. Questo approccio frammentato porta a una proliferazione di soluzioni non presidiate, con responsabilità poco chiare e limitata visibilità sui processi. Il risultato è un rischio crescente di esposizione, non sempre percettibile nell'immediato, ma potenzialmente impattante nel medio periodo: la mancanza di policy condivise e strutture di governance solide rappresenta una delle principali debolezze nei percorsi di trasformazione digitale. Le aziende, insomma, si trovano spesso a reagire, piuttosto che a guidare l'innovazione.
Per garantire un utilizzo consapevole e sicuro dell'AI è fondamentale definire ruoli chiari, processi trasparenti e meccanismi di controllo, integrando la cybersicurezza fin dalle prime fasi di progettazione. Solo così l'adozione può diventare una leva di resilienza e non un elemento di fragilità.

UNA CORNICE NORMATIVA INSUFFICIENTE

Il tentativo di regolamentare l'uso dell'intelligenza artificiale in Europa si scontra con la realtà operativa delle aziende. Il quadro normativo attuale, rappresentato anzitutto dall'AI Act, non fornisce strumenti pratici per orientare le scelte quotidiane dei responsabili tecnologici e dei manager. I principi generali enunciati sono condivisibili, ma non bastano a coprire le specificità dei diversi settori o a rispondere alla velocità con cui l'innovazione avanza. In questo vuoto applicativo, molte aziende si affidano a soluzioni interne, spesso scollegate tra loro. Alcune hanno creato comitati dedicati, altre hanno formalizzato delle policy d'uso, ma manca una convergenza su modelli di governance replicabili e adattabili: la conseguenza è una **grande varietà di approcci** che rischia di aumentare la frammentazione e di rendere sempre più difficile il dialogo tra imprese, regolatori e stakeholder.

MALGOVERNO, PHISHING E DEEPFAKE

Nell'immaginario collettivo, l'AI è spesso associata a scenari catastrofici e minacce invisibili, ma nella pratica quotidiana i problemi reali si manifestano in modo più sottile. Le aziende non segnalano al momento episodi gravi di danni causati da intelligenze artificiali fuori controllo, mentre i rischi più ricorrenti derivano da utilizzi non governati, laddove degli strumenti innovativi vengono introdotti senza che ne siano stati valutati gli impatti in termini di sicurezza e protezione dei dati.

Un momento del CISO Panel di Roma, 27 maggio 2025

Tra gli esempi più comuni ci sono piattaforme di videoconferenza che registrano conversazioni senza un'adeguata gestione dei consensi, o assistenti virtuali che memorizzano contenuti sensibili senza adeguate policy di conservazione delle informazioni. Sono falle silenziose, spesso non eclatanti nell'immediato, ma potenzialmente critiche sul lungo periodo. Questi errori non derivano da malafede, bensì da un approccio troppo rapido, che antepone la funzionalità al controllo.
Anche sul fronte esterno si nota un'evoluzione nei metodi di attacco. Il phishing si sta raffinando, sfruttando la capacità dell'AI di personalizzare i messaggi, simulare il linguaggio aziendale, imitare toni e abitudini; i deepfake, in forma audio e video, stanno invece emergendo come strumenti per colpire la fiducia tra interlocutori. Queste tecniche, sebbene ancora limitate nei numeri, stanno cambiando il modo in cui il rischio si presenta. In questo scenario, la percezione delle imprese è ambivalente: da un lato l'interesse verso l'AI cresce, dall'altro lato resta forte la consapevolezza che un'adozione disordinata può generare vulnerabilità difficili da sanare.

L'AI CHE PIACE A CHI SI OCCUPA DI CYBERSICUREZZA

Le tecnologie basate su modelli AI non sono solo fonte di rischio: se utilizzate correttamente, rappresentano un potente alleato per rafforzare le difese aziendali. I principali ambiti di applicazione riguardano l'individuazione precoce delle minacce, l'analisi dei comportamenti anomali, la gestione delle vulnerabilità e l'automazione della risposta agli incidenti. Grazie alla velocità di elaborazione e alla capacità di apprendimento continuo, queste soluzioni permettono di migliorare i tempi di reazione e di alleggerire il carico sui team di sicurezza. I sistemi possono riconoscere pattern sospetti in grandi volumi di dati, correlare eventi distanti tra loro e suggerire azioni correttive in tempo reale.
Secondo l'indagine Cyber Risk Management 2025 di TIG – The Innovation Group e CSA – Cyber Security Angels, il 71% delle aziende ha già adottato strumenti di intelligenza artificiale almeno in un ambito della sicurezza informatica, mentre un ulteriore 19% è in fase di valutazione. Il 64% delle organizzazioni evidenzia anche l'importanza di mantenere una supervisione umana continua, indispensabile per gestire eventuali errori o falsi positivi. Per sfruttare appieno i vantaggi di queste tecnologie riducendo al minimo le criticità, è fondamentale inserirle in un

ecosistema strutturato composto da controlli regolari, audit indipendenti e aggiornamento costante delle competenze interne. Gli algoritmi non sostituiscono il giudizio umano, ma possono potenziarlo, a patto che siano utilizzati con consapevolezza e responsabilità.

SOSTENIBILITÀ: UN DIALOGO ANCORA INCOMPLETO

La discussione sull'AI raramente si intreccia con il tema della sostenibilità, se non per qualche riferimento all'impatto ambientale dei data center. Eppure, inserire **l'intelligenza artificiale all'interno dei parametri ESG** (Environmental, Social, Governance) è oggi una necessità strategica. Il consumo energetico associato alla potenza di calcolo necessaria per far funzionare i modelli è solo l'aspetto più visibile di un tema molto più ampio. L'impatto sociale dell'adozione di queste tecnologie è altrettanto rilevante, poiché può introdurre nuove forme di esclusione, discriminazione o marginalizzazione, specialmente quando i modelli vengono sviluppati su basi dati parziali o distorte. In questo contesto, l'equità nell'accesso, la trasparenza delle decisioni automatizzate e la tracciabilità dei processi non sono semplici requisiti tecnici, ma elementi chiave di una visione autenticamente sostenibile della trasformazione digitale. Sul piano della governance, così come per la cybersicurezza, servono strumenti adeguati a garantire l'accountability e il controllo effettivo dei sistemi automatizzati, assicurando che ogni decisione presa attraverso tecnologie intelligenti sia verificabile, giustificabile e conforme ai principi etici e normativi. La cybersecurity, in questo scenario, assume un ruolo cruciale, rappresentando proprio uno dei pochi ambiti già maturi nella gestione del rischio, nella definizione dei controlli e nella verifica della conformità.

La risposta coordinata europea sulla cybersecurity

Intervista a **Luca Tagliaretti**
Executive Director dell'European Cybersecurity Competence Center (ECCC)

La capacità di preparazione e risposta dei Paesi europei alle minacce cyber dipende dalla possibilità di collaborare più strettamente nella prevenzione e nella gestione degli incidenti. Abbiamo affrontato il tema con Luca Tagliaretti nel corso del Cybersecurity Summit 2025 di TIG, lo scorso 20 marzo a Milano.

Qual è il ruolo chiave dell'European Cybersecurity Competence Center (ECCC) nella strategia di difesa informatica dell'UE? Quali sono le principali iniziative dell'ECCC per rafforzare la cooperazione tra gli Stati membri in materia di cybersecurity?

Il ruolo del Centro europeo per la competenza sulla cybersecurity (ECCC) è quello di supportare l'innovazione tecnologica europea per la sicurezza tramite il sostegno a progetti di ricerca pura e applicata. Questo favorisce una maggiore competitività delle nostre società, che hanno così la possibilità di aprirsi a iniziative comuni di ricerca.

Luca Tagliaretti, Executive Director dell'European Cybersecurity Competence Center (ECCC)

Il Centro punta, inoltre, a rafforzare la resilienza del sistema digitale europeo agli attacchi cyber, sia tramite il sostegno a normative come NIS2, DORA, Cyber Solidarity Act, sia tramite la costruzione dei cross border hub previsti dai regolamenti, dei veri e propri SOC (Security operation center) europei. Questi sono realizzati insieme ai Paesi membri: due sono già in costruzione e altri due sono previsti per i prossimi anni. Rappresenteranno uno scudo di protezione e di allerta rivolto alle infrastrutture critiche. Il Centro eroga poi fondi per finanziare i progetti di cybersecurity, indirizzandosi in particolare alle PMI (con cofinanziamenti che arrivano al 75%) mentre le organizzazioni più grandi ricevono contributi del 50%. Tutto questo con strette collaborazioni con le imprese europee, le multinazionali, università e centri di ricerca, enti nazionali.

Negli ultimi anni abbiamo osservato incrementi sostanziali degli attacchi rivolti agli Stati europei da gruppi state-sponsored e cyber criminali avanzati. Le infrastrutture critiche europee sono sotto stress: come affrontare queste minacce su larga scala?
Questi attacchi, come ci dicono i rapporti dell'agenzia Enisa, continuano da anni e la pubblica amministrazione è particolarmente presa di mira. Lo sforzo legislativo è adeguamento e rivolge a tutti un perimetro di sicurezza ampio definito dalla NIS2. Quello che serve è un importante sforzo di preparazione, per una difesa comune basata sulla preparazione e sulla capacità di reazione, oltre che un impulso alle attività formative, quindi corsi, una Digital Skill academy europea. Abbiamo diverse iniziative realizzate a livello nazionale, come la CyberChallenge, un programma di addestramento per giovani talenti, o altre più ampie che puntano a formare le competenze richieste dal mercato del lavoro. Considerando che le nuove tecnologie rendono possibili attacchi sempre più sofisticati, queste iniziative devono proseguire, per far sì che la difesa cresca e sia adeguata.

Come si sta sviluppando il coordinamento europeo in tema di cybersecurity, a partire dai CERT nazionali?
Il coordinamento tra i CERT nazionali è attivo ma vorrei rimarcare in particolare l'attività di coordinamento che sta nascendo tra i Paesi membri con i National Coordination Centres (NCC)[1]: sono oggi 27, presenti in ogni Paese (in Italia è presso l'ACN, Agenzia per la Cybersicurezza Nazionale) e agiscono sulla base di una strategia comune, sia per la reazione sia soprattutto per la preparazione futura. Lavorano per coordinarsi sulle iniziative di ricerca, sviluppo e implementazione di tecnologie. A partire da 2025 avremo anche una comunità cyber che raccoglie sia gli utilizzatori di tecnologia cyber sia i produttori, per creare un mercato europeo della sicurezza che sia più forte e più ricco di proposte. Il coordinamento va fatto anche sulla parte di preparazione, non solo su quella della risposta. Dal punto di vista legislativo, il Cyber Solidarity Act[2] europeo, oltre a prevedere meccanismi per testare il livello di preparazione cyber in settori critici, prevede disposizioni per una reazione "solidare" ad attacchi cyber, attraverso una "riserva" per la cibersicurezza che consisterà in servizi di risposta agli incidenti forniti da una serie fornitori di servizi privati ("fornitori fiduciari"), che potranno essere mobilitati su richiesta degli Stati membri o delle istituzioni, degli organi e delle agenzie dell'Unione, in caso di incidenti significativi o su vasta scala. La parte legislativa è definita, serve ora completarne l'implementazione.

1 https://cybersecurity-centre.europa.eu/nccs_en
2 https://digital-strategy.ec.europa.eu/it/policies/cyber-solidarity

Parliamo di innovazione e sovranità digitale: quanto è strategica l'indipendenza tecnologica dell'UE nella cybersecurity? L'Europa può competere con USA e Cina in questo settore? Come l'ECCC sta incentivando la ricerca e lo sviluppo di soluzioni europee per la sicurezza informatica?

L'indipendenza tecnologica è essenziale per quanto riguarda i temi della cybersecurity. Il regolamento "Digital Europe" (Regolamento (UE) 2021/694), che regola tutti gli investimenti europei a sostegno dell'innovazione, limita i fondi alle società europee, con una verifica di ownership delle stesse per far sì che i fondi europei vadano a sostegno dell'industria europea. Il nostro Centro è parte di questo sforzo per aumentare la sovranità in ambito cyber, ad esempio tramite il supporto alle attività per l'indipendenza tecnologica su AI e quantum computing. L'EU Chips Act (Regolamento (UE) 2023/1781), approvato nel 2023, ha invece l'obiettivo di rafforzare la sovranità tecnologica dell'Unione Europea nel settore dei semiconduttori, riducendo la dipendenza dalle forniture asiatiche e statunitensi e incrementando la produzione di semiconduttori in Europa, mentre il piano per le AI Factory è stato pensato per sfruttare la capacità di supercalcolo di EuroHPC per sviluppare modelli di AI generativa affidabili e all'avanguardia.

Sicurezza cercasi. La cybersecurity nell'era dell'AI

A cura della **Redazione**

L'integrazione dell'intelligenza artificiale con la cybersicurezza è una delle evoluzioni più interessanti che riguardano il vasto ambito dell'AI. Già utilizzata per rilevare gli attacchi informatici, l'AI è fondamentale per rispondere efficacemente in caso di attacco. L'intelligenza artificiale, tuttavia, può sfociare anche in utilizzi malevoli, cui il responsabile della cybersecurity deve prestare molta attenzione: tra le minacce più insidiose vi è sicuramente il deepfake, una tecnica che impiega l'AI generativa per creare identità sintetiche che riproducono, nella voce e nelle sembianze, persone reali.

Il futuro della cybersecurity sarà sempre più legato alle evoluzioni dell'AI: man mano che le minacce informatiche evolveranno, diventando più sofisticate, le soluzioni basate sull'AI potranno apprendere dall'esperienza e continuare a progredire. Obiettivo del libro **Sicurezza cercasi. La cybersecurity nell'era dell'AI** edito da Egea[3], che, curato da Elena Vaciago, Research Manager di TIG – The Innovation Group, si avvale dei contributi di numerosi esperti e responsabili aziendali della cybersecurity, è quello di approfondire come bilanciare intelligenza artificiale e cybersicurezza, perché questi due approcci metodologici e tecnologici possano convergere e rendere più sicuro il mondo digitale che ci aspetta.

3 https://www.egeaeditore.it/eng/products/ict-e-sistemi-informativi/sicurezza-cercasi.aspx

2 Rispondere all'evoluzione delle minacce, tenere il passo con il digitale

IL CYBER FUSION CENTER DI MAIRE: TECNOLOGIA, BUSINESS E COLLABORAZIONE AL CENTRO DELLA CYBERSECURITY

Intervento di **Andrea Licciardi**
Cybersecurity Manager MBA, Maire Group

IL PROGRAMMA DI CYBERSECURITY DI RINA: FORMAZIONE CONTINUA E ATTENZIONE ALLA SUPPLY CHAIN

Intervento di **Fabio Musso**
Global IT Cyber Security Director, Rina

QUELLO DEL CISO È UN RUOLO SEMPRE PIÙ STRATEGICO E COMPLESSO

Elena Vaciago
Research Manager, TIG - The Innovation Group

FAR PERCEPIRE AL BUSINESS L'IMPORTANZA DELLA CYBERSECURITY

Intervista a **Andrea Succi**
CISO, Ferrari Group

I VANTAGGI E LE SFIDE DI UN APPROCCIO RISK BASED

Camilla Bellini
Research & Content Manager,
TIG - The Innovation Group

SVILUPPARE UN MODELLO NIS2 IN OTTICA DI MULTI-COMPLIANCE

Intervento di **Valentina Frediani**
Founder e CEO di Colin & Partners

NIS2, QUALE L'APPROCCIO CORRETTO?

Orazio Mardente
Business Development – Soluzioni Risk & Compliance, Cybersel

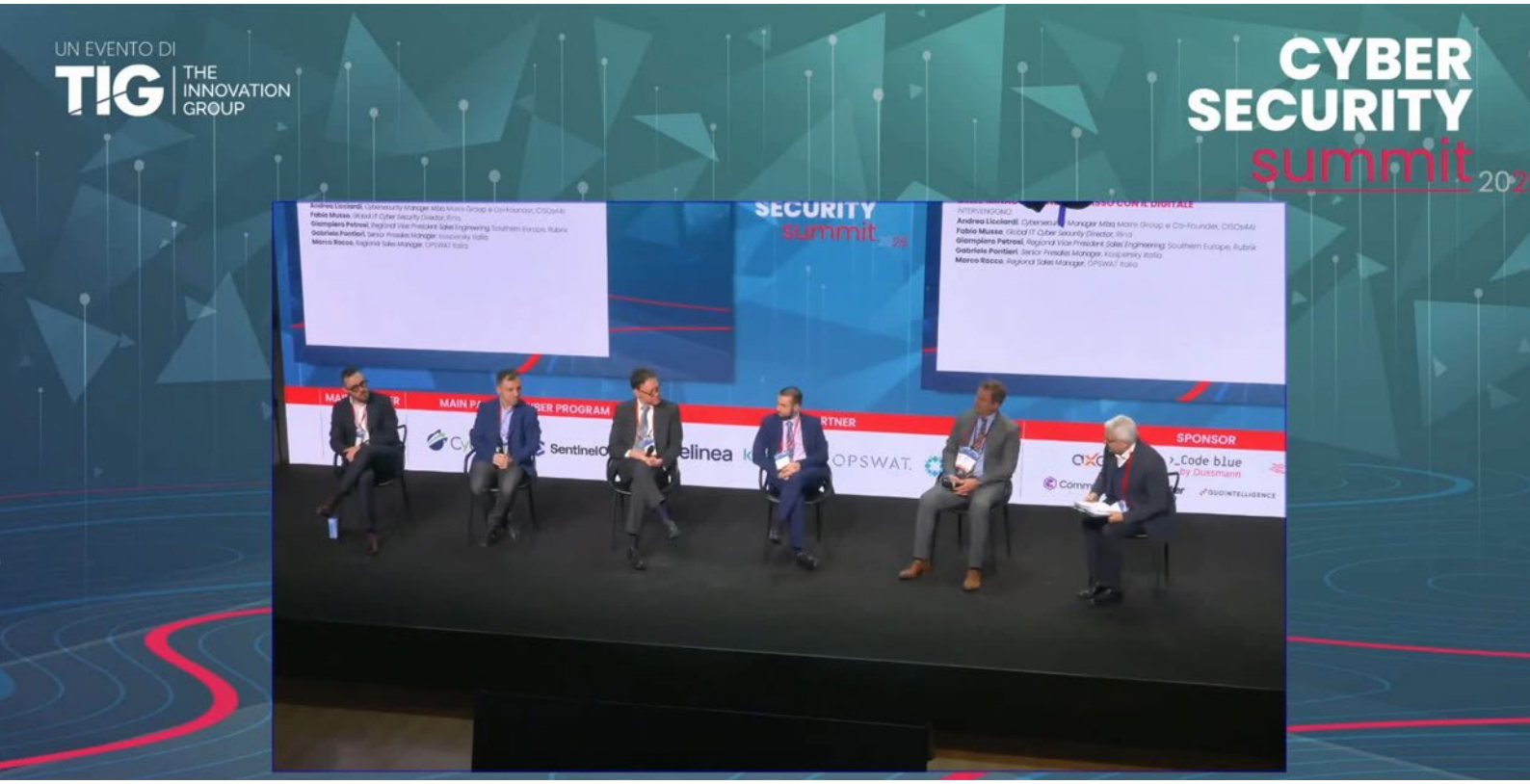
CYBERSECURITY: PIÙ CHE UNA QUESTIONE DI NUMERI, UNA SFIDA DI COMPETENZE

A cura della **Redazione**

L'AGENDA 2025 DEL CISO, COME TENERE IL PASSO CON IL DIGITALE

Come stanno evolvendo i programmi di cybersecurity nelle aziende italiane, quali devono essere i punti di attenzione e le priorità da considerare a livello strategico?
Come è emerso nel corso della Roundtable "L'Agenda 2025 del CISO" del Cybersecurity Summit 2025 di Milano, le priorità vanno nella direzione di assicurare:

- Una corretta identificazione e gestione del rischio informatico, in linea con le specificità del business e in collaborazione stretta con il resto dell'organizzazione
- Il migliore sfruttamento di tecnologie allo stato dell'arte, in primis l'intelligenza artificiale che promette grandi benefici
- Un'elevata attenzione alla formazione e sensibilizzazione degli utenti
- Non dimenticarsi dei rischi legati alle terze parti, come ci ricorda oggi anche la compliance alla NIS2
- Essere pronti alla recovery e al ripristino della situazione in caso di incidente
- Ricorrere a una combinazione di tecnologie avanzate e competenze umane ove possibile, anche ricercandole all'esterno, nei servizi MDR
- Approccio integrato, utilizzo dell'approccio Zero Trust e capacità di neutralizzare minacce anche in contesti complessi come l'OT/ICS e l'IoT.



Un momento del Cybersecurity Summit di Milano, 20 marzo 2025.

Il Cyber Fusion Center di Maire: tecnologia, business e collaborazione al centro della cybersecurity

Intervento di **Andrea Licciardi**
Cybersecurity Manager MBA, Maire Group

Cos'è il Cyber Fusion Center di Maire e come sta evolvendo il programma di cybersecurity? Quali le iniziative in corso?

«Il termine fusion può sembrare ambiguo, ma ci piace utilizzare concetti che esprimano al meglio la nostra visione. Il nostro approccio alla cybersecurity va oltre la tecnologia: è integrato con il business», ha detto Andrea Licciardi, Cybersecurity Manager MBA di Maire group, società di ingegneria e tecnologia per la transizione energetica. «L'obiettivo è sviluppare un programma di cybersecurity che tenga conto delle esigenze aziendali, non solo degli aspetti tecnici. Questo ci consente di dialogare efficacemente con i nostri stakeholder e di far percepire la sicurezza come un vero fattore di valore per l'impresa.»

Un elemento chiave, secondo Licciardi, è la gestione del rischio. «Dobbiamo essere in grado di **comunicare in modo corretto con il business** e di costruire percorsi che generino valore. Inoltre, è fondamentale governare adeguatamente le informazioni aziendali. Utilizzando i dati in modo strategico, riusciamo a identificare i rischi, stabilire le priorità e ottimizzare gli interventi: è impossibile affrontare tutto contemporaneamente. Per questo consideriamo i rischi non solo dal punto di vista tecnologico, ma anche da quello di business.»

OTTIMIZZAZIONE DELLE RISORSE E INTELLIGENZA ARTIFICIALE

In un contesto dove le risorse non sono infinite — a differenza di quelle di cui spesso dispongono gli attaccanti — il Cyber Fusion Center di Maire punta su efficienza e innovazione. «Grazie all'intelligenza artificiale possiamo elaborare rapidamente grandi volumi di dati, migliorando le nostre capacità di rilevamento, risposta e recupero», sottolinea Licciardi. «Questo approccio ci ha permesso di **ridurre drasticamente i tempi di gestione degli incidenti**: oggi riusciamo a intervenire in soli 60-70 minuti, un risultato impensabile solo tre anni fa.»

KPI ORIENTATI AL BUSINESS E SINERGIA CON I DECISORI AZIENDALI

Un altro pilastro della strategia è la capacità di tradurre i dati tecnici in KPI comprensibili per il business. «Non ci limitiamo a estrarre dati dalle piattaforme, ma li contestualizziamo per renderli chiari a CFO, azionisti e decisori aziendali», prosegue Licciardi.

La collaborazione con il top management è continua: «Interagiamo quotidianamente con i CFO e gli altri dirigenti. Per noi, la **cybersecurity è un elemento centrale per il business**: lavoriamo con clienti di livello mondiale, essere riconosciuti come partner affidabili è decisivo per consolidare e far crescere il nostro business.»

Il programma di cybersecurity di Rina: formazione continua e attenzione alla supply chain

Intervento di **Fabio Musso**
Global IT Cyber Security Director, Rina

Quali sono oggi le priorità del programma di cybersecurity di Rina e quali criticità restano da affrontare?

«Negli ultimi 3-4 anni, Rina ha seguito una roadmap tecnologica per rafforzare il proprio sistema di cybersecurity», ha spiegato Fabio Musso, Global IT Cyber Security Director di Rina. «Ma la verità è che in questo campo non esiste un traguardo finale: **la sicurezza è un percorso di miglioramento continuo**. A un certo punto, però, è fondamentale fermarsi per valutare i progressi e affrontare le lacune principali.»

Secondo Musso, oggi il problema non è tanto tecnologico quanto culturale: «I principali gap riguardano la consapevolezza degli utenti. Finora abbiamo utilizzato corsi tradizionali, ma la partecipazione è limitata e spesso questi programmi sono percepiti come noiosi e poco utili. Chi lavora nell'IT tende a dare per scontati concetti che invece, per chi non ha una formazione tecnologica, non sono affatto banali.»

FORMAZIONE E SENSIBILIZZAZIONE DEGLI UTENTI: VERSO UN NUOVO MODELLO

Le difficoltà sono emerse chiaramente anche durante le simulazioni di phishing, i cui risultati sono peggiorati nel tempo. «Questo ci ha fatto capire che nel 2025 dovremo **ripensare radicalmente il processo di sensibilizzazione**. Non sarà più sufficiente una formazione periodica: serve un supporto costante, capace di ricordare ogni giorno agli utenti i rischi che corrono — ad esempio già all'accensione del PC.»

Un cambiamento che richiederà uno sforzo collettivo. «Sarà fondamentale il coinvolgimento di tutta l'organizzazione, dal board alle risorse umane, fino alla comunicazione interna. Stiamo lavorando a un nuovo modello, con il supporto di partner specializzati, e contiamo di vedere i primi risultati concreti entro la fine del 2025.»

L'INTELLIGENZA ARTIFICIALE E LA GESTIONE DELLA SUPPLY CHAIN

Parallelamente, Rina ha avviato un'esplorazione delle potenzialità dell'intelligenza artificiale in ambito cybersecurity. «Prima di entrare nel dettaglio di queste tecnologie, però, vorrei sottolineare un altro aspetto critico: la gestione della supply chain», precisa Musso.

Il punto di attenzione? Non sempre i fornitori più grandi rappresentano il rischio maggiore. «Spesso si pensa che i principali pericoli vengano da grandi fornitori e outsourcer. In realtà, un **hacker oggi sceglierebbe bersagli più facili**: piccoli fornitori non considerati critici — ad esempio una ditta di pulizie o magari un consulente indipendente. Ed è proprio attraverso anelli deboli di questo tipo che abbiamo visto attacchi contro aziende più grandi.»

RIVEDI QUI
LA SESSIONE

Quello del CISO è un ruolo sempre più strategico e complesso

Elena Vaciago
Research Manager, TIG - The Innovation Group

TIG - The Innovation Group e AssoCISO hanno presentato il **19 novembre**, in occasione del Cybersecurity Summit 2025 di Roma, i risultati della prima edizione dell'Indagine **"Il Ruolo del CISO Survey 2025"**, che ha avuto l'obiettivo di analizzare come si sta configurando oggi la figura del Responsabile Cybersecurity (Chief Information Security Officer, CISO) nelle organizzazioni italiane, alla luce dei cambiamenti tecnologici, normativi e geopolitici.
La ricerca, condotta tra luglio e settembre 2025, ha raccolto 172 risposte da professionisti del settore in Italia, in prevalenza CISO e manager della cybersecurity. La maggior parte dei rispondenti appartiene a organizzazioni di grande dimensione (60% con oltre 1.000 addetti) e, in misura minore, a realtà medie (24%) e piccole (16%). I settori più rappresentati sono Industria e Finanza, confermando la rilevanza del tema per i comparti più esposti ai rischi cyber.
I risultati dell'indagine **"Il Ruolo del CISO Survey 2025"** delineano una figura professionale in forte evoluzione: più matura, più integrata nei processi decisionali, ma ancora alle prese con sfide legate a risorse, competenze e riconoscimento interno. Con la cybersecurity ormai divenuta parte integrante del business, il ruolo del CISO è sempre più strategico e trasversale. Alle competenze tecniche si affiancano oggi abilità manageriali e comunicative, fondamentali per dialogare con il top management, guidare il cambiamento e tradurre la sicurezza in valore per l'impresa.
La maggior parte dei rispondenti è consapevole del ruolo critico del CISO nella propria organizzazione: il periodo in cui il CISO fornisce maggiore valore all'organizzazione è tra i 5 e i 14 anni, un dato che sottolinea sia l'elevata pressione a cui è sottoposto il CISO, sia anche le numerose opportunità di crescita, fino a posizioni di Chief Security Officer, CIO, membro del CDA o consulente strategico.

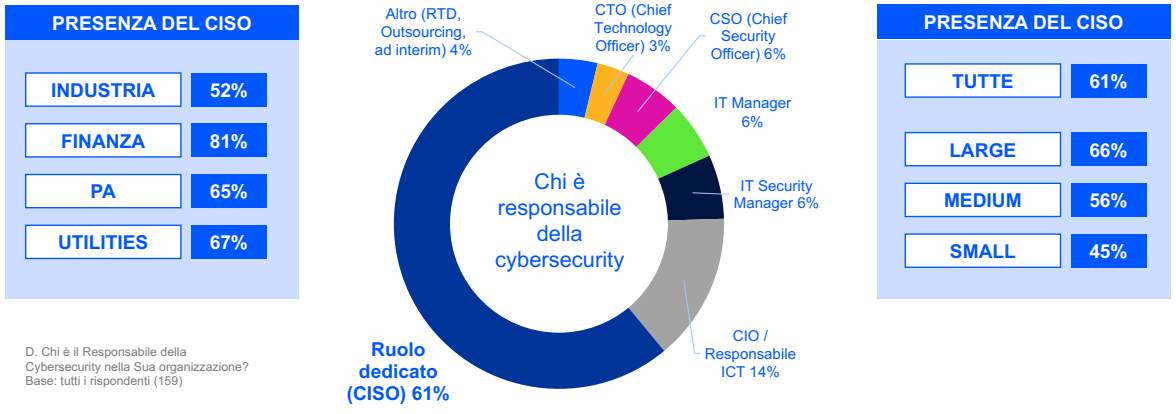
I **messaggi chiave** che emergono dall'indagine:

- **Il CISO evolve verso un ruolo di leadership strategica.**
  Dalla survey emerge una figura sempre più matura, chiamata non solo a proteggere, ma anche a guidare il cambiamento e a tradurre la sicurezza in valore per l'impresa. Il percorso professionale del CISO si allunga e si diversifica, aprendo la strada a ruoli di vertice.
- **Il ruolo del CISO si consolida ma con differenze di maturità e riconoscimento.**
  Il CISO è presente nel 61% delle organizzazioni intervistate (nonostante si tratti di un campione composto in prevalenza di grandi aziende, che dispone nel 94% dei casi di una strategia formale di cybersecurity), con una diffusione crescente in funzione della dimensione e del settore. Tuttavia, la sua collocazione e la relazione con il vertice aziendale non sono ancora omogenee: solo la metà delle aziende prevede un flusso strutturato di comunicazione verso il CDA, mentre altrove il dialogo resta sporadico o intermediato. Questo limita la capacità del CISO di influenzare le decisioni strategiche.

- **La governance della cybersecurity è strutturata, ma l'attuazione resta parziale.**
  Nonostante la strategia formale di cybersecurity sia già molto diffusa, solo due organizzazioni su tre l'hanno pienamente implementata. La comprensione della strategia da parte del business e la disponibilità di risorse adeguate sono limitate, segnalando che manca ancora una piena integrazione della sicurezza nei processi aziendali.
- **La carenza di competenze è la principale criticità.**
  Il reperimento di personale qualificato è la difficoltà più segnalata, seguita dalla scarsa comprensione del valore della cybersecurity e dal limitato riconoscimento del ruolo del CISO.
- **L'evoluzione tecnologica, così come la situazione geopolitica, impongono un ripensamento della sicurezza.**

La trasformazione digitale e l'adozione di nuove tecnologie – in primis intelligenza artificiale, cloud e identity management – stanno ridefinendo le priorità della cybersecurity. Le tensioni internazionali e i vincoli normativi legati alla sovranità digitale stanno influenzando le decisioni su fornitori e tecnologie. Quasi quattro organizzazioni su dieci hanno già modificato le proprie scelte per effetto di fattori geopolitici, e oltre sei su dieci prevedono che tale impatto crescerà ulteriormente nei prossimi anni.

PRESENZA DI UN RUOLO DEDICATO (CISO) PER LA CYBERSECURITY



Fonte: Indagine "Il Ruolo del CISO 2025" di AssoCISO e TIG, settembre 2025

I RISULTATI DELL'INDAGINE

L'indagine ha coinvolto un campione composto in prevalenza da organizzazioni di grande dimensione che nel 94% dei casi dispone già di una strategia formale di cybersecurity, che nel 78% dei casi è stata anche approvata dai vertici. Tuttavia, il livello di implementazione resta incompleto: solo il 65% dichiara di averla pienamente attuata. Ancora più critico il livello di comprensione della strategia da parte del business (ritenuto buono solo nel 46% dei casi) e la disponibilità di risorse adeguate (36%). Il ruolo del CISO è ormai presente nel 61% delle organizzazioni coinvolte, mentre nei restanti casi la responsabilità della sicurezza è affidata ad altre figure, come il CIO (14%), il security manager (6%) o l'IT manager (6%). La presenza del CISO cresce proporzionalmente alla dimensione aziendale e risulta più diffusa nei settori finanza e utilities.

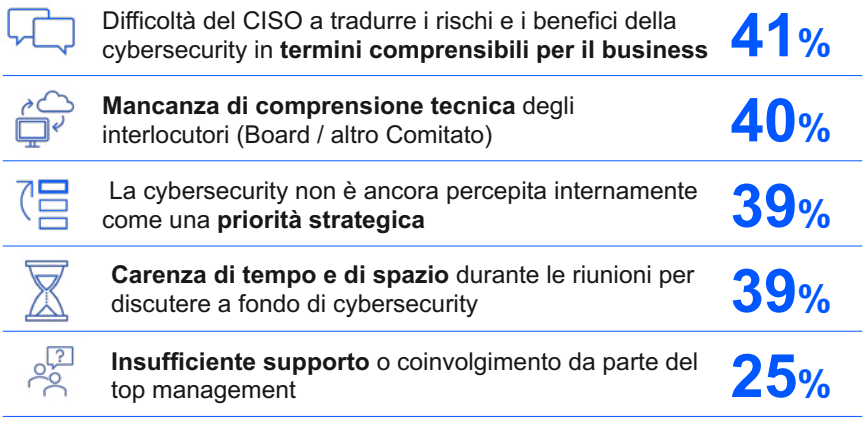
RESPONSABILITÀ E RELAZIONI CON IL VERTICE AZIENDALE

Nelle organizzazioni più strutturate, il CISO gestisce un portafoglio di attività ampio — dalla threat intelligence alla cloud security — mentre nelle realtà più piccole può trovarsi a coprire responsabilità afferenti tipicamente ad altri ruoli, come le funzioni di compliance. La comunicazione verso il CDA avviene in modo strutturato (su base trimestrale, semestrale o annuale) solo in 1 azienda su 2 (il 48% delle risposte). Negli altri casi, avviene solo su richiesta, in situazioni particolari, è disintermediata dal Comitato rischi o altri comitati, dal CIO o dal CSO, o anche non avviene mai.

LE PRINCIPALI CRITICITÀ PER IL CISO

Il **reperimento di personale qualificato** rappresenta oggi la difficoltà più sentita, indicata dal 57% dei rispondenti. Seguono la difficoltà di far comprendere il valore della cybersecurity (39%) e la scarsa valorizzazione del ruolo all'interno dell'organizzazione (38%). Solo al quarto posto, rispetto al passato, si colloca la mancanza di fondi adeguati (36%), segno di una maggiore attenzione ma ancora non sufficiente. Tra le richieste più ricorrenti per lavorare meglio, i CISO indicano appunto la necessità di ampliare e strutturare il team di sicurezza, ottenere maggior supporto dal top management, avere chiarezza su ruoli e responsabilità, budget adeguati e strumenti di automazione per ridurre il carico operativo. Rilevante anche la domanda di una **maggiore integrazione** con le altre funzioni aziendali. La comunicazione con il CDA è importante, ma comporta molte sfide (come mostra la figura successiva).

PRINCIPALI CRITICITÀ NELLA COMUNICAZIONE CON IL BOARD



Per **migliorare la comunicazione con il Board** il CISO deve ripensare il proprio linguaggio, abbandonare i tecnicismi, coinvolgere gli interlocutori e individuare i momenti opportuni

D. Quali sono le principali difficoltà che il CISO incontra nel comunicare efficacemente con il Board / Altro Comitato sulla cybersecurity?
Base: tutti i rispondenti (144)

Fonte: Indagine "Il Ruolo del CISO 2025" di AssoCISO e TIG, settembre 2025
ALTRO: Difficoltà a comunicare i miglioramenti raggiunti in ambito cybersecurity (mancanza di metriche condivise)

TRASFORMAZIONE DIGITALE E NUOVI TREND TECNOLOGICI

Le aziende italiane sono oggi impegnate in profondi processi di trasformazione digitale, che portano con sé anche la necessità di ripensare la cybersecurity. Secondo gli intervistati, il trend tecnologico destinato ad avere maggiore impatto in cybersecurity è **l'intelligenza artificiale**, seguita da migrazione al cloud, evoluzione dell'identity management e connettività degli oggetti. Il livello di automazione delle difese cyber — sia nei Security Operations Center (SOC) sia a livello architetturale — è giudicato buono: il 61% delle organizzazioni dichiara un grado di automazione "abbastanza o molto elevato".

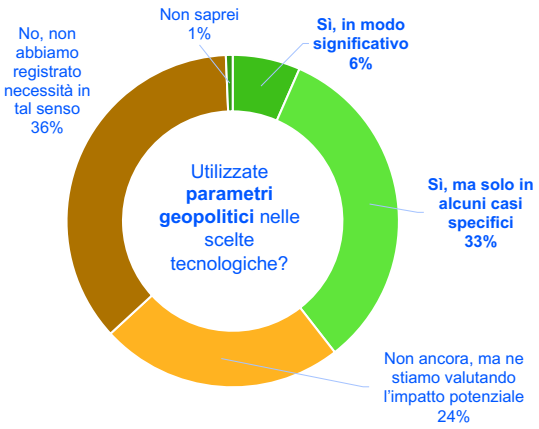
IDENTITÀ DIGITALI E COMPLESSITÀ DI INTEGRAZIONE

Le identità digitali sono oggi uno degli obiettivi primari degli attaccanti, e le organizzazioni si stanno attrezzando con misure specifiche per proteggerle. Tuttavia, il livello di adozione delle soluzioni di sicurezza per la gestione delle identità è fortemente variabile: molto più maturo nelle grandi aziende, ancora disomogeneo nelle realtà di minori dimensioni. Persistono inoltre diversi vincoli tecnologici, come la difficile integrazione tra sistemi legacy e soluzioni moderne, la complessità architetturale e la scarsa consapevolezza del personale. Anche la limitata automazione incide negativamente, mentre il costo delle soluzioni risulta oggi un ostacolo secondario.

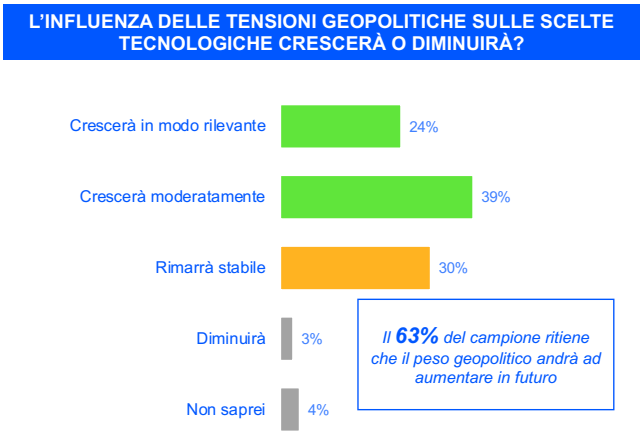
FATTORI GEOPOLITICI E SCELTE TECNOLOGICHE

In un contesto internazionale sempre più instabile, gli **aspetti geopolitici** influenzano in modo crescente le valutazioni su tecnologie e fornitori di cybersecurity. Le principali preoccupazioni riguardano le normative che impongono vincoli di scelta, la sovranità e localizzazione dei dati, le tensioni nelle aree chiave della supply chain, la dipendenza da tecnologie extra-UE, i rischi di backdoor o ingerenze statali e le sanzioni verso determinati vendor o Paesi. Ben il 39% delle organizzazioni dichiara di aver rivalutato o modificato le proprie scelte tecnologiche (vendor, servizi cloud, soluzioni di sicurezza) a causa di dinamiche geopolitiche, e il 63% prevede che questa influenza crescerà nei prossimi anni.

VALUTAZIONI GEOPOLITICHE NELLE SCELTE TECNOLOGICHE



D. La Sua organizzazione ha recentemente rivalutato o modificato le scelte tecnologiche (vendor, servizi, cloud, etc.) a causa di dinamiche geopolitiche?
Base: tutti i rispondenti (152)



D. Ritiene che nei prossimi 12-24 mesi l'influenza delle tensioni geopolitiche sulle scelte tecnologiche crescerà o diminuirà?
Base: tutti i rispondenti (152)

Fonte: Indagine "Il Ruolo del CISO 2025" di AssoCISO e TIG, settembre 2025

Far percepire al business l'importanza della cybersecurity

Intervista a **Andrea Succi**
CISO, Ferrari Group

Andrea Succi,
CISO, Ferrari Group

Con Andrea Succi abbiamo ragionato dell'evoluzione del ruolo del CISO, sempre più centrale nel supportare le aziende nei processi di trasformazione digitale. L'arrivo dell'AI crea un momento importante per il CISO, è un reale Game Changer. Oltre tutto, l'**AI è utilizzata da anni in cybersecurity**: chi si occupa di sicurezza ne conosce molto bene benefici e nuove opportunità, oltre che il rovescio della medaglia, ossia che possa essere utilizzata dagli attaccanti. Il compito del CISO diventa quindi quello di adottare un approccio proattivo, evidenziando fin dall'inizio – con una strategia Shift Left – le criticità dell'adozione dell'AI a supporto del business.

Come il CISO può puntare ad allinearsi alle esigenze del business?
Il primo passo per il CISO è comprendere a fondo il contesto di business in cui opera: ogni realtà ha le sue esigenze specifiche e le sue peculiarità che devono essere colte per costruire una strategia di sicurezza efficace. È essenziale capire quali sono le fonti di reddito, o che cosa chiede e di cosa necessita il cliente, non solo quello interno, come siamo abituati a considerare, ma soprattutto quello esterno, che sempre di più chiede sicurezza. In questo modo il CISO può capire come la sicurezza può diventare un valore aggiunto per i clienti. Oggi, infatti, servono sempre più prodotti e servizi sicuri, spinti anche da normative rilevanti come NIS2 e DORA. Questa crescente attenzione alla cybersecurity si riflette lungo l'intera filiera, con un aumento delle richieste di sicurezza in molti i settori. Le aziende stanno imparando che la sicurezza non è solo una necessità tecnica, ma un elemento strategico per costruire fiducia e competitività.
Le aziende hanno compreso che gli incidenti di sicurezza si verificano principalmente in tre situazioni: vulnerabilità tecniche, fattore umano – punti deboli che rientrano nel perimetro di azione dell'azienda e possono essere mitigati direttamente – o fornitori che non rispettano adeguati standard di sicurezza.
Oggi, per dimostrare di essere in grado di erogare prodotti e servizi sicuri, l'organizzazione deve dotarsi di team competenti sulla cybersecurity, **capaci di dialogare con i clienti e rafforzare la fiducia lungo la filiera**. In questo modo la sicurezza diventa rilevante per il business.
Il secondo passaggio, dopo aver capito come aiutare l'organizzazione e la supply chain a elevare la propria postura di sicurezza, è tradurla in azioni e iniziative concrete, sempre in **partnership con il business.** Questo vale anche al contrario: essendo l'organizzazione parte di una filiera è fondamentale coinvolgere i team di security fin dalle prime fasi del rapporto con i fornitori, per garantire che gli standard di sicurezza siano rispettati lungo tutta la catena.
Se vogliamo, il paradigma è diverso rispetto al passato: il ruolo del CISO oggi non è più quello di bloccare iniziative rischiose, ma **supportare l'organizzazione a bilanciare innovazione e sicurezza**. Il compito del CISO e del suo team diventa quello di aiutare, monitorare, dare linee guida. Serve un approccio **"Shift left",** coinvolgendo il CISO fin dall'inizio nel design (security-by-design) per integrare la sicurezza in modo efficace. In alcuni casi questo approccio porta a risultati molto interessanti, che permettono sia di migliorare l'esperienza del cliente, sia di renderlo più sicuro.

Pensiamo alle iniziative di trasformazione digitale e al passaggio al cloud: qual è il ruolo del CISO? Vale lo stesso discorso?

Spesso i CISO sono stati coinvolti tardi nei processi di adozione cloud, trovandosi così a gestire ambienti già operativi. Questo è il motivo per cui oggi, con l'arrivo dell'intelligenza artificiale, in tanti ci siamo mossi proattivamente.

Tornando al cloud, questo ci ha insegnato l'importanza di valutare fin da subito aspetti critici come resilienza e continuità operativa. Fortunatamente, molti provider cloud offrono già soluzioni robuste in termini di sicurezza infrastrutturale e ridondanza. Oggi il cloud computing è ormai centrale nell'IT e questo rende essenziale adottare le linee di guida di sicurezza specifiche: tecnologie come CASB (Cloud Access Security Broker), Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), Cloud Native Application Protection Platforms (CNAPP) permettono di monitorare centralmente vulnerabilità come le misconfiguration, l'assenza di MFA o patch mancanti, semplificando e centralizzando la gestione della sicurezza. Il cloud è un ambiente diverso, richiede specifici strumenti di gestione, ed essendo più esposto è anche più attaccabile: però ha sicuramente un trade off come la maggiore ridondanza e la migliore sicurezza infrastrutturale.

Dalla nostra survey "Cyber Risk Management 2025"[1] emerge che i responsabili cybersecurity sono più preoccupati per ambienti di cloud ibrido: ti ritrovi?

La **complessità è nemica della sicurezza** e aumenta ulteriormente negli scenari di cloud ibrido, dove bisogna gestire risorse distribuite su più ambienti (on-premises e multi-cloud). Banalmente la complessità rende più difficile mantenere tutto in sicurezza.

Gestire ambienti diversi richiede competenze specifiche spesso non disponibili internamente, aumentando la necessità di consulenze esterne. Nonostante ciò, il cloud offre vantaggi significativi come maggiore flessibilità e riduzione dei rischi legati alla shadow IT. Dato che le risorse inutilizzate si pagano, possono essere identificate più facilmente e quindi dismesse.

L'AI è un'innovazione dirompente di cui si parlerà moltissimo nei prossimi anni: quale impatto avrà sulla cybersecurity, e, dal punto di vista del CISO, come gestirne la sicurezza?

L'AI rappresenta una sfida complessa ma anche un'opportunità straordinaria per la cybersecurity. La prima preoccupazione di molti CISO quando hanno visto che cosa poteva fare è stata chiedersi: quali sono i rischi? cosa servirà fare per rendere sicuro questo nuovo oggetto che sicuramente mi ritroverò in azienda? Quando OWASP ha iniziato a sviluppare uno standard per la sicurezza dei modelli linguistici avanzati (LLM) due anni fa, ho deciso di partecipare attivamente come contributor per analizzarne i rischi principali – come prompt injection o data poisoning. Questo lavoro mi ha permesso di comprendere meglio sia le vulnerabilità che le potenzialità dell'AI.

Ancora prima che venisse rilasciato lo standard, ho coinvolto altri CISO per verificare se erano interessati ad approfondire il tema opposto: l'introduzione dell'AI in cybersecurity. Così a giugno 2023 ho co-fondato il collettivo "CISOs4AI"[2] per esplorare proprio queste opportunità.

1 https://www.theinnovationgroup.it/cyber-risk-management-survey-2025/?lang=it

2 https://cisos4ai.org/

L'obiettivo è **utilizzare l'AI per affrontare alcune delle sfide della cybersecurity** che ad oggi non stiamo vincendo, come la carenza di risorse umane qualificate. Per esempio, l'AI può analizzare grandi volumi di dati velocemente o automatizzare parzialmente la risposta agli incidenti. In futuro, grazie all'apprendimento continuo, sarà possibile sviluppare difese proattive capaci di individuare segnali deboli prima che si trasformino in minacce concrete. Ora CISOs4AI è composto da una quarantina di CISO o profili analoghi.

Come deve essere gestito l'arrivo dell'AI dal punto di vista della sicurezza e quale impatto avrà questa innovazione sul ruolo del CISO?

Dal punto di vista della sicurezza dell'AI stessa, alcuni rischi, come il prompt injection (gli utenti possono manipolare i sistemi di AI generativa fornendo input dannosi – i prompt, le domande – mascherati da prompt legittimi dell'utente) non possono essere completamente eliminati a causa della natura stocastica dei modelli generativi. Tuttavia, possono essere mitigati ed è per questo che esistono standard come OWASP. Non dimentichiamoci che a contorno dell'AI esistono componenti applicativi e infrastrutturali che sappiamo già come proteggere.

Il ruolo del CISO in questo contesto diventa quello di **agente del cambiamento**: non solo deve garantire la sicurezza dei progetti AI con un approccio di security-by-design, ma anche promuoverne l'adozione responsabile all'interno dell'organizzazione. In alcune aziende il CISO viene coinvolto anche per la definizione del business case dell'AI per la conoscenza che ha maturato. In molti casi siamo visti come un'autorità in azienda in tema di AI, considerando che è un tema piuttosto complesso, e spesso il CISO, che oltre a capirla, l'utilizza da anni in una serie di soluzioni di cybersecurity (di detection, mail security, anti-phishing e così via).

L'impatto sull'organizzazione è duplice: accanto ai rischi già evidenziati, si aprono opportunità per trasformare la cybersecurity, spostandola da una difesa reattiva a una prevenzione proattiva basata sull'identificazione dei pattern. Già oggi, alcune soluzioni AI integrate nei SOC affiancano gli analisti di primo livello, accelerando i processi decisionali e aumentando l'efficienza operativa.

L'intelligenza artificiale apre scenari rivoluzionari per il futuro della cybersecurity. Come CISOs4AI, immaginiamo un futuro in cui l'analisi predittiva, alimentata da enormi quantità di dati, permetterà di anticipare le minacce prima ancora che si manifestino. In questa prospettiva, l'AI potrebbe automatizzare in modo parziale o completo la risposta agli incidenti, riducendo drasticamente i tempi di mitigazione e rafforzando le difese aziendali. Grazie all'apprendimento continuo, l'AI sarà in grado di evolversi costantemente, adattandosi a minacce sempre più sofisticate e rispondendo alla sfida posta dalla continua trasformazione degli attacchi. La capacità di riconoscere nuovi pattern e individuare segnali deboli permetterà di anticipare le minacce emergenti, rivoluzionando il paradigma della sicurezza informatica: da una difesa reattiva a una prevenzione anticipativa. Questa visione non è ancora realtà, ma rappresenta la direzione verso cui stiamo andando. L'AI ha la potenzialità di cambiare il modo in cui proteggeremo le organizzazioni, e ridefinire il concetto stesso di resilienza digitale.

I vantaggi e le sfide di un approccio risk based

Camilla Bellini
Research & Content Manager, TIG - The Innovation Group

I lavori del tavolo sull'Integrated risk management (IRM) e sulla supply chain cybersecurity del CISO Panel di Roma dello scorso 27 maggio hanno preso il via con una domanda fondamentale: **"Che cos'è il rischio?"**. Andando oltre le definizioni standard, i partecipanti hanno trovato convergenza su un punto chiave: il rischio può e deve essere visto come un'opportunità.
Le recenti normative, in particolare NIS2 e DORA, sono state identificate come catalizzatori di questa visione, offrendo una leva per i professionisti della sicurezza nel parlare al business e indirizzare efficacemente programmi e investimenti.
Il contesto operativo attuale presenta complessità crescenti. Ad esempio, nella Pubblica amministrazione lo spostamento di dati nel cloud rappresenta una sfida significativa. **La sicurezza deve agire da abilitatore** per garantire la continuità operativa del business, evitando perdite che potrebbero impattare direttamente sui ricavi o sui servizi erogati.

LE OPPORTUNITÀ LEGATE A UNA CORRETTA GESTIONE DEL RISCHIO

Contrariamente a una visione puramente negativa, il rischio viene visto dai partecipanti del tavolo come un'opportunità e una leva per guidare investimenti, indirizzare sforzi e trasformare la percezione della sicurezza come abilitatore fondamentale di un business sicuro e resiliente.
In questo particolare momento, norme come NIS2 e DORA sono percepite come strumenti utili per elevare la sensibilità del top management e fornire un quadro di riferimento per la gestione del rischio. Il rischio deve essere considerato una

Un momento del CISO Panel di Roma, 27 maggio 2025

leva strategica per poter parlare con il business, ottenere investimenti e indirizzare programmi e iniziative. È fondamentale però parlare la lingua del business ("money on the table") per comunicare efficacemente le esigenze di sicurezza.
Inoltre, bisogna **superare la gestione "a silos" dei rischi** (cyber, finanziario, legale, operativo, ecc.) per adottare una visione integrata (Enterprise Risk Management - ERM): questo richiede collaborazione tra diverse funzioni aziendali (security, operation, application, legal, sales, procurement), la capacità di comunicare il rischio in un linguaggio comprensibile per il business e l'abilità del CISO nello stringere alleanze con le altre funzioni.
Se questi sono quindi i punti di forza di un approccio risk-based, dal tavolo sono anche emerse sfide e punti di attenzione.

LE CRITICITÀ DA CONSIDERARE

La mancanza di consapevolezza del rischio a tutti i livelli dell'organizzazione, in particolare nel top management nel settore sia pubblico sia privato, è un ostacolo significativo. La responsabilità deve partire dall'alto per far sì che si diffonda all'intera struttura. Un problema diffuso, in particolare nella PA, oltre alla insufficiente conoscenza è proprio la **mancanza di un inventario preciso degli asset** (sistemi, dati, informazioni). Senza conoscere cosa si deve proteggere, è impossibile prendere decisioni informate e quindi adottare una sicurezza basata sulla gestione del rischio. In risposta a questa esigenza, viene indicato nel tavolo la possibilità di ricorrere a simulazioni di scenari di rischio, che possono aiutare a far comprendere l'impatto reale di situazioni critiche al top management.
I partecipanti hanno poi sottolineato che il rischio e la sua rilevanza dipende molto dal singolo contesto del business, per cui la mission e la visione aziendale sono elementi fondamentali per valutare correttamente il rischio e prioritizzare le azioni. Dato che non è possibile proteggere tutto contemporaneamente, la prioritizzazione basata sul contesto e sugli obiettivi di business è fondamentale: è necessario identificare i sistemi e i processi critici che hanno il maggiore impatto sul business in caso di incidente.

INCLUDERE LA SUPPLY CHAIN E LE TERZE PARTI

Un elemento cruciale del rischio, evidenziato anche dalla NIS2, è quello legato alla **gestione delle terze parti e alla supply chain**. È vitale comprendere le loro attività, mettere in atto controlli e verificare che abbiano processi adeguati di gestione degli incidenti, poiché l'inefficienza di un fornitore può avere un impatto diretto sull'azienda stessa. Il processo virtuoso implica testare, contestualizzare, prioritizzare e formare. I framework di cybersecurity sono un ausilio per strutturare in modo virtuoso queste attività. Va ricordato che secondo la NIS2, la responsabilità sulla sicurezza rimane in capo alla propria entità anche quando si esternalizza o si usa un fornitore.
In conclusione, il panel ha sottolineato che il rischio deve essere visto come un'opportunità e una leva per il business, superando una visione puramente tecnologica. È fondamentale passare da una gestione a silos a una gestione integrata del rischio, coinvolgendo tutte le funzioni aziendali. La comunicazione efficace del rischio al business, traducendolo in impatti finanziari e operativi, è cruciale per ottenere supporto e investimenti. La consapevolezza, la responsabilità diffusa, la conoscenza degli asset e una solida gestione delle terze parti sono elementi chiave per una cybersecurity più efficace.

Sviluppare un modello NIS2 in ottica di multi-compliance

Intervento di **Valentina Frediani**
Founder e CEO di Colin & Partners

La normativa NIS2 ha assunto un ruolo centrale nelle strategie aziendali di cybersecurity, con particolare attenzione alla sua complementarità con altre regolamentazioni europee. Il processo di iscrizione all'ACN ha rappresentato una sfida per molte aziende, evidenziando la complessità degli adempimenti richiesti. Di questi temi ha parlato Valentina Frediani con un intervento sul tema "Sviluppare un modello NIS2 in ottica di multi-compliance", nel corso del Cybersecurity Summit 2025, lo scorso 20 marzo a Milano.

NIS2: LE PROSSIME SCADENZE E I PRINCIPI CARDINE

Un aspetto fondamentale riguarda le scadenze: dopo quella del 28 febbraio, una nuova fase tra il 15 aprile e il 31 maggio ha imposto l'obbligo di notificare il backup del punto di contatto e di caricare i dati di alcune figure chiave dell'azienda. Le successive date chiave sono il 31 dicembre per gli aspetti legali e aprile 2026 per quelli tecnologici. Tuttavia, la compliance non deve essere vista come un traguardo statico, ma come un processo dinamico che evolve insieme ai cambiamenti aziendali.
Uno dei principi cardine della NIS2 è **l'accountability**, ovvero la responsabilità non solo di rispettare la normativa, ma anche di integrare best practices nella gestione della cybersecurity aziendale. La regolamentazione offre l'opportunità di migliorare la governance e la sicurezza, superando un mero approccio burocratico.
Un tema particolarmente delicato riguarda poi l'**ambito dell'OT (Operational Technology) security**, dove spesso si riscontrano lacune nella preparazione e nella definizione delle procedure aziendali. Questo può generare conflitti interni e ambiguità decisionali, evidenziando la necessità di una governance strutturata della sicurezza informatica. La NIS2 obbliga i board aziendali a prendere coscienza di questi aspetti, sottolineando l'importanza di una visione integrata della cybersecurity.
A livello organizzativo, spicca il ruolo del punto di contatto, che non si limita a fungere da canale di notifica, ma deve anche garantire la compliance e la gestione degli aggiornamenti documentali. Tuttavia, la responsabilità finale rimane in capo ai soggetti designati dalla normativa.
Un'altra sfida significativa riguarda la supply chain, che deve adeguarsi ai requisiti della NIS2. Se da un lato la normativa impone nuove complessità, dall'altro offre un'opportunità: facendo leva sull'obbligatorietà della compliance, le aziende possono integrare i fornitori nelle strategie di sicurezza senza compromettere le relazioni professionali. Tuttavia, l'applicazione pratica presenta difficoltà, poiché alcuni fornitori potrebbero non essere pronti a investire nell'adeguamento richiesto.

LE AZIONI FONDAMENTALI PER L'ADEGUAMENTO NIS2

Un efficace percorso di adeguamento alla NIS2 deve tenere conto di diversi elementi fondamentali:

1. **Gestione della supply chain:** le aziende devono adottare un approccio differenziato, categorizzando i fornitori in base al tipo di servizio che offrono (es. data center, logistica) e adattando di conseguenza le richieste di sicurezza e responsabilità. Un modello uniforme non è efficace per una corretta gestione del rischio.

2. **Interdisciplinarità tra ruoli aziendali:** la cybersecurity non può essere considerata come un tema isolato. È essenziale un approccio integrato che coinvolga le diverse funzioni aziendali, come il DPO, il reparto legale e l'IT. Lavorare in silos riduce l'efficacia della sicurezza informatica e della compliance.
3. **Coinvolgimento delle risorse umane e formazione:** la sicurezza informatica non riguarda solo l'IT, ma deve coinvolgere anche il personale aziendale. La formazione continua è fondamentale per garantire la consapevolezza e la preparazione necessarie ad affrontare le minacce cyber.
4. **Compliance oltre la checklist:** il rispetto della normativa non può essere ridotto a un mero elenco di spunte. È necessario un approccio che tenga conto dei flussi aziendali, della gestione del rischio e delle risorse, con una visione strategica della compliance.
5. **Continuità operativa e sicurezza OT**: le aziende devono integrare le esigenze della cybersecurity con la gestione della continuità operativa, soprattutto in ambito OT. La sicurezza delle infrastrutture critiche non può essere trascurata.
6. **Integrazione tra tecnologia e politiche aziendali:** la cybersecurity e la compliance devono essere integrate nelle politiche aziendali in modo dinamico, considerando l'evoluzione delle nuove tecnologie, come l'intelligenza artificiale. Le strategie di sicurezza devono adattarsi ai cambiamenti tecnologici per garantire un'efficace protezione dei dati e delle infrastrutture.

In conclusione, l'adozione della NIS2 rappresenta una sfida, ma anche un'opportunità per rafforzare la sicurezza aziendale e migliorare la governance. Un approccio sistemico, che integri la cybersecurity, la compliance legale e le politiche aziendali, è essenziale per garantire la resilienza a lungo termine. La chiave per il successo risiede nella formazione continua, nella gestione del rischio e nel monitoraggio costante delle minacce, con un occhio sempre attento all'evoluzione normativa e tecnologica.

RIVEDI QUI
LA SESSIONE

NIS2, quale l'approccio corretto?

Orazio Mardente
Business Development – Soluzioni Risk & Compliance, Cybersel

Con il decreto legislativo 4 settembre 2024, n. 138, l'Italia ha recepito nell'ordinamento nazionale la direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione, abrogando la precedente direttiva.
Il Decreto ("NIS2") coinvolge, solo in Italia, circa 20.000 soggetti, molto eterogenei per settore, dimensione, rilevanza (viene fatta una distinzione tra settori altamente critici e critici, e tra soggetti essenziali ed importanti) e maturità pregressa in ambito sicurezza delle informazioni-cybersecurity.
Questo comporta che un approccio univoco per gestire la conformità e per elevare la propria postura di sicurezza informatica (sia in termini di predisposizione di

un framework procedurale idoneo, che di effettiva attuazione) non sia possibile.
È però necessario, prendendo esempio da esperienze pregresse in altri contesti (si veda l'ambito DORA), implementare alcuni principi comuni, validi in generale per tutti i soggetti interessati, da applicare secondo un principio di proporzionalità e gradualità (in base all'effettiva esposizione ai rischi di sicurezza), con un approccio volto al miglioramento continuo:

- **Coinvolgimento del Management e degli Organi Direttivi:** è fondamentale che la NIS2 (e i temi di sicurezza informatica che si porta dietro) sia percepita come rilevante, non solo ai fini della conformità, ma come vantaggio competitivo per il business;
- **Condivisione organizzativa:** la NIS2 deve diventare un "tema" aziendale e non riguardare solo gli addetti ai lavori o un numero ristretto di funzioni/risorse (CISO, Punto di contatto, Risk Management e Compliance);
- **Gestione di un approccio "risk based"**;
- **Identificazione, raccolta e gestione** di tutti dati/informazioni rilevanti ai fini di poter realizzare KPI e KRI che permettano all'organizzazione di prendere decisioni volte alla corretta gestione del rischio (accettazione, mitigazione, eliminazione, trasferimento).

Partendo da questa impostazione (da cui deriverà la "strategia" aziendale) si procederà a quanto richiesto dalla direttiva, ovverosia alla definizione di policy e procedure chiare, relative alle misure di sicurezza da adottare (mediante assessment/gap analisys tra quanto in essere e quanto necessario). In base all'esperienza Cybersel è importante inoltre avere strumenti informatici "abilitanti", che permettano la reale applicazione e la gestione operativa e di controllo delle misure di sicurezza implementate per gli aspetti di gestione del rischio, della continuità operativa, della gestione incidenti, della catena di fornitura, delle vulnerabilità, ...
Questi strumenti devono avere **funzionalità specifiche per i vari ruoli aziendali:** Management, business owner (funzioni di I livello), Subject Matter Espert, funzioni di controllo di II e III livello (Risk Management, Compliance, Internal Audit).
Solo in questo modo sarà possibile avere processi conformi, ma sostenibili e gestibili da parte dell'organizzazione, massimizzando efficacia ed efficienza, riducendo attività manuali a basso valore aggiunto ed errori.
Un fenomeno interessante e altamente virtuoso che si sta sviluppando in alcune organizzazioni è quello di **tenere conto della normativa** (applicandola in termini di approccio e misure di sicurezza), pur non essendo soggetti vigilati.
Questa situazione si sta riscontrando in varie situazioni: quando all'interno di un Gruppo solo alcune società risultano essere in perimetro NIS2, ma si decide di estendere l'applicazione a tutte le Società del Gruppo "rilevanti"; quando si è fornitori di soggetti in perimetro NIS2 o DORA; quando si matura la convinzione che la **sicurezza delle informazioni sia un aspetto di vantaggio competitivo**, di reputazione e di mitigazione del rischio; su specifici processi "critici".
Non è facile prevedere se si tratti di un fenomeno "isolato" per pochi o se sarà la strada (auspicabile) verso cui tutti tenderanno. Sicuramente è prevedibile che le normative si evolveranno e si estenderanno come perimetro nel tempo, così come (e questo sta già avvenendo) il numero di incidenti di sicurezza informatica coinvolgerà sempre più soggetti (la ormai fatidica frase: non è più una questione di "se", ma di "quando").
Chi sta applicando questo approccio "virtuoso" si troverà avvantaggiato (come è già accaduto nel passato), in un contesto che inevitabilmente diventerà sempre

più complesso e interconnesso (la mia sicurezza dipende anche da come viene gestita dai soggetti a cui sono collegato). In conclusione: pensare che la sicurezza delle informazioni sia importante per una organizzazione "solo" perché si è soggetti ad una nuova normativa/regolamentazione è alquanto riduttivo, così come non gestirla con adeguata priorità "solo" perché le scadenze previste non sono a breve termine. Occorre cogliere l'opportunità e attivare la sensibilizzazione aziendale – poi i benefici saranno evidenti per tutti, anche per i più scettici e/o meno attenti.

Cybersecurity: più che una questione di numeri, una sfida di competenze

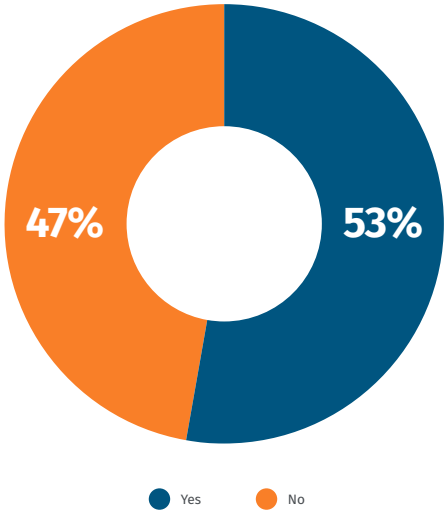
A cura della **Redazione**

Da anni si parla di "carenza di talenti" nel mondo della cybersecurity. Ma il nuovo rapporto di SANS Institute e GIAC per il 2025 (2025 Cybersecurity Workforce Research Report di SANS e GIAC) capovolge la prospettiva: non è tanto un problema di scarsità di professionisti, quanto di **allineamento tra competenze richieste e profili disponibili**. In altre parole, servono meno "teste in più" e più persone con le giuste capacità. E le aziende che stanno affrontando meglio la sfida sono quelle che hanno capito che, per costruire team cyber solidi, serve una visione strategica sul talento.

DALLA QUANTITÀ ALLA QUALITÀ: CERCARE LE GIUSTE COMPETENZE

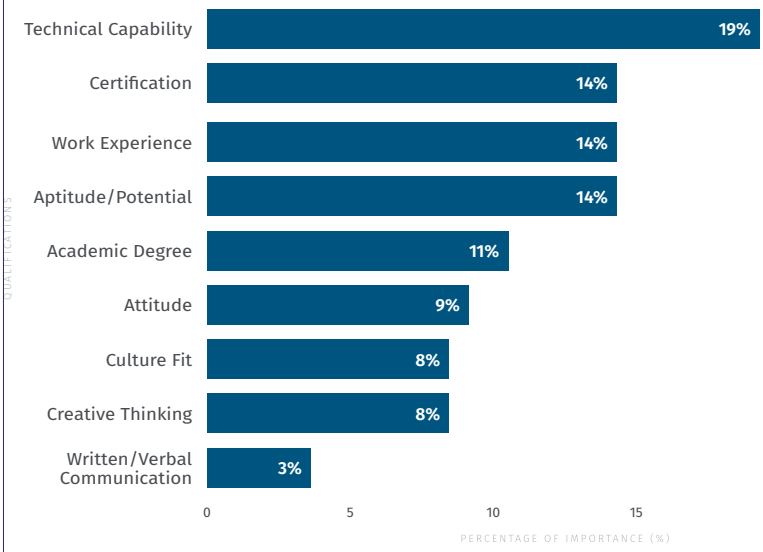
Secondo la ricerca, che è basata sulle risposte di 3.400 professional a livello globale (per il 75% dell'ambito cybersecurity e per il 25% dell'area HR), il 52% delle

BIGGEST STAFFING CONCERN: QUANTITY VS. FIT



Fonte: 2025 Cybersecurity Workforce Research Report di SANS e GIAC

RANKING HIRING QUALIFICATIONS: ALL REGIONS



Fonte: 2025 Cybersecurity Workforce Research Report di SANS e GIAC

organizzazioni segnala come sfida principale "non avere il personale giusto", contro il 48% che lamenta "non avere abbastanza personale". Un cambio di paradigma: conta di più la **qualità delle competenze** che la quantità delle risorse.
Non è un caso che la **capacità tecnica** sia oggi il primo criterio di valutazione dei candidati, seguita da certificazioni professionali specifiche. Ma l'esperienza pregressa o il titolo di studio non bastano più: si cercano persone **adattabili, curiose, capaci di comunicare e risolvere problemi**. Le cosiddette *power skills*, considerate sempre più decisive nei processi di selezione.

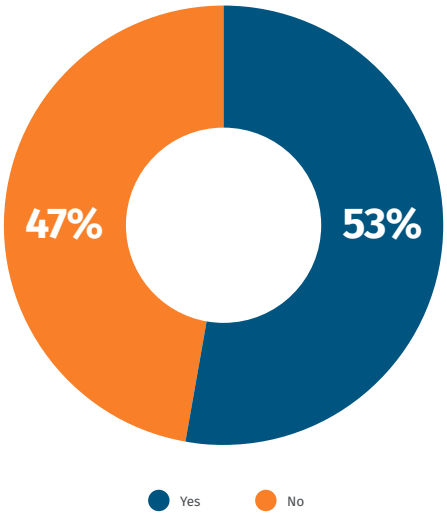
HR E CYBERSECURITY: UNA NUOVA ALLEANZA

Un'altra novità importante è la crescente collaborazione tra le **Risorse Umane** e i team di sicurezza. In molte realtà, gli HR business partner sono integrati nei team cyber, partecipano ai processi di selezione e vengono formati sulle tecnologie e i framework di sicurezza per comprendere meglio i profili cercati. Strumenti come il framework NICE (americano) o l'ECSF (europeo) stanno favorendo la creazione di un **linguaggio comune** tra chi cerca e chi valuta il talento cyber, standardizzando ruoli e competenze.

FORMAZIONE CONTINUA E CRESCITA INTERNA: LA CHIAVE PER ATTRARRE E TRATTENERE TALENTI

Oltre il 55% delle aziende ha attivato programmi strutturati di formazione per il personale di cybersecurity. Molte adottano l'approccio **"grow your own"**: formare risorse interne ad alto potenziale, anche senza esperienza specifica nel settore. In Europa, cresce l'apertura verso profili non convenzionali – insegnanti, psicologi, infermieri – che mostrano spirito d'adattamento e capacità comunicative.
Un elemento ricorrente nelle aziende più avanzate è la **cultura del mentoring**: chi ha un mentore ha 5 volte più probabilità di avanzare di carriera. E realtà come Airbus o United Airlines investono in veri e propri ecosistemi di crescita professionale, tra accademie interne, conferenze di settore, laboratori pratici e percorsi di certificazione.

DO YOU USE THE NICE OR ECSF FRAMEWORK FOR DEVELOPING JOB REQUIREMENTS?



Fonte: 2025 Cybersecurity Workforce Research Report di SANS e GIAC

CERTIFICAZIONI: UNA GARANZIA PER AZIENDE E CLIENTI

La **validazione delle competenze** attraverso certificazioni formali è diventata uno standard di settore. Il 65% delle organizzazioni le richiede per audit o consulenze, e il 58% le usa per decisioni di assunzione o promozione. Le certificazioni danno credibilità ai professionisti e rassicurano anche i clienti sulla solidità dei team.

AMBIENTE E CULTURA: IL FATTORE UMANO AL CENTRO

Un altro pilastro per attrarre e trattenere talenti è la **cultura del lavoro**. Il valore più apprezzato dai professionisti cyber? "Lavorare bene in un team". Le aziende che offrono flessibilità, fiducia e ambienti sfidanti – più che solo stipendi alti – hanno più successo nel trattenere le persone.
Il lavoro da remoto è ormai una norma per molti (42% lavora da casa almeno tre giorni a settimana) e modelli innovativi come la settimana corta o gli orari flessibili stanno guadagnando terreno.

NON SOLO RETENTION: VALORIZZARE ANCHE CHI SE NE VA

Alcune aziende, come Santander, adottano una visione matura anche sul turnover: se un professionista cresce internamente e poi ottiene un ruolo prestigioso altrove, è comunque un successo. Significa che l'organizzazione sa **sviluppare talenti di valore**. Altre, come Airbus, puntano a creare ambienti talmente stimolanti da far scegliere alle persone di rimanere.

IN CONCLUSIONE, SARANNO VINCENTI LE STRATEGIE PIÙ INNOVATIVE PER UN CONTESTO IN CONTINUA EVOLUZIONE

La gestione dei talenti nella cybersecurity è diventata una vera e propria **disciplina strategica**. Non basta più assumere: occorre capire quali competenze servono, formare chi ha potenziale, creare ambienti di lavoro motivanti e costruire un'identità culturale forte.
Anche le normative – come NIS2, DORA, SEC o CMMC – stanno spingendo verso modelli più strutturati nella definizione dei ruoli e nella convalida delle competenze. Chi saprà muoversi in questa direzione, potrà contare su team più resilienti, motivati e capaci di affrontare le sfide complesse del mondo digitale.

"Possiamo confermare che questa tendenza si sta affermando anche in Italia – spiega il Responsabile SANS Manlio Longinotti – dove c'è ancora molto da fare per quanto riguarda la cultura della formazione in sicurezza informatica. Le organizzazioni virtuose che ciclicamente propongono ai team i nostri training specialistici unitamente alle certificazioni GIAC, sono consapevoli che il valore di questi progetti va oltre l'aggiornamento professionale dei singoli ed una migliore postura di sicurezza e capacità di individuazione e risposta alle minacce. Investire sulle persone in questo modo infatti rende le aziende più attrattive e competitive in un settore dove il networking fra professionisti e la fame di competenze nuove sono fra i valori principali su cui basare una solida strategia di talent acquisition".

3 Cyber resilienza e incident response

Comunicare il valore della cybersecurity per ottenere investimenti

Elena Vaciago
Research Manager, TIG - The Innovation Group

Convincere il top management a investire in cybersecurity resta una delle sfide più complesse per chi si occupa di sicurezza informatica. In molte aziende, il tema viene ancora percepito come un centro di costo, difficile da giustificare in termini di ritorno sull'investimento. Dal dibattito del tavolo di lavoro "Cyber Resilienza e Incident Response" del CISO Panel di Roma è emerso che la chiave per superare questa impasse è saper comunicare il valore della sicurezza in modo strategico, collegandola direttamente agli obiettivi di business e alla resilienza complessiva dell'organizzazione.

OLTRE LA LOGICA DELLA PAURA: DALLA MINACCIA ALL'OPPORTUNITÀ

Tradizionalmente, la cybersecurity è stata presentata come una forma di protezione contro i rischi: un'assicurazione, necessaria ma poco tangibile, utile solo "nel caso in cui succeda qualcosa". Questo approccio, basato sulla logica della paura, fatica però a ottenere l'attenzione e il sostegno dei vertici aziendali. Al contrario, è sempre più importante inquadrare la sicurezza come un **abilitatore di business**, capace di aprire nuovi mercati, garantire la continuità operativa e accrescere la fiducia di clienti e stakeholder.
Per esempio, ottenere la conformità a norme come la direttiva europea NIS2 o a standard settoriali può rappresentare un vantaggio competitivo. In alcuni casi, è addirittura un requisito indispensabile per lavorare con determinati clienti, in particolare nel settore pubblico o in ambiti regolamentati. In quest'ottica, la cybersecurity smette di essere un costo e si trasforma in una leva di crescita e posizionamento.

PARLARE IL LINGUAGGIO DEL BUSINESS

Uno dei passaggi fondamentali per ottenere finanziamenti è tradurre il bisogno tecnico in valore economico. Questo significa saper spiegare al management, con dati e scenari concreti, qual è l'impatto di un eventuale incidente in termini di business: perdita di produttività, danni reputazionali, sanzioni, esclusione da gare o partnership strategiche. Lo storytelling e l'uso di use case reali possono aiutare a rendere la minaccia più comprensibile.
Un'azienda che ha vissuto un attacco informatico, poi, è spesso più propensa a investire perché ha già sperimentato direttamente le conseguenze di una cattiva preparazione. Ma per chi non ha (ancora) vissuto episodi simili, simulazioni ed esercitazioni sono strumenti essenziali per "toccare con mano" il rischio e valutare concretamente le vulnerabilità organizzative.

SIMULARE PER CAPIRE (E CONVINCERE)

Le **esercitazioni pratiche** rappresentano uno strumento sempre più efficace per far emergere le lacune, costruire consapevolezza, ottenere l'attenzione della direzione e giustificare il budget, in quanto permettono di far "toccare con mano" i rischi. Sono stati menzionati diversi tipi di escitazioni cyber, come i Tabletop Exercises rivolti al top management; i Cyber Drills, simulazioni che coinvolgono

l'intera azienda (non solo IT/Cyber), incluse funzioni come legale, procurement, comunicazione; i Cyber Range, esercitazioni più tecniche, spesso su piattaforme che simulano o clonano l'infrastruttura reale. Anche la frequenza varia (trimestrali, annuali, a sorpresa). In generale, le esercitazioni servono a misurare il gap tra il comportamento atteso (basato su policy/procedure) e la risposta reale. Questo gap evidenzia la necessità di piani d'azione e giustifica le richieste di nuovi investimenti. Nella discussione è stato citato il beneficio legato all'uso di framework come MITRE e soprattutto Tiber (originario del settore finanziario ma applicabile altrove) per strutturare queste simulazioni. È stato anche osservato che la NIS2 include le esercitazioni tra i requisiti di base.
Strumenti strutturati come il **framework Tiber** permettono di pianificare simulazioni complesse, coinvolgere le funzioni di business e identificare percorsi inusuali che un attaccante potrebbe sfruttare. Il valore di questi test risiede nella loro capacità di evidenziare le conseguenze operative e reputazionali di un attacco, e nel supportare la definizione di piani d'azione basati sull'evidenza.
Nella discussione è stato anche affrontato il **ruolo della tecnologia** nell'Incident Response: si è discusso di SOAR (Security Orchestration, Automation, and Response) per l'automazione della gestione e del contenimento degli incidenti. È emerso il tema dell'Intelligenza Artificiale (AI), vista come un potenziale supporto cruciale, specialmente nella fase di analisi: l'AI può infatti aiutare gli analisti a velocizzare l'individuazione delle cause di vulnerabilità o comportamenti anomali, correlare dati e arricchire le informazioni. Nelle architetture più evolute, agenti AI possono persino superare il concetto tradizionale di SOAR. Infine, è stato menzionato il concetto di "Shift Left" come un progetto importante per integrare i controlli di sicurezza nelle prime fasi dello sviluppo software (pipeline CI/CD), con l'obiettivo di ottenere un Security-by-design effettivo su vasta scala. Questo richiede però una stretta collaborazione tra security e team IT.

LA COMPLIANCE COME ALLEATO

Anche la normativa può giocare un ruolo positivo nel facilitare l'approvazione di investimenti. La direttiva NIS2, per esempio, ha introdotto obblighi più stringenti, rendendo il **Board direttamente responsabile** delle scelte in materia di cybersecurity. In molti casi, ciò ha contribuito a elevare il tema a livello strategico e ad accelerare il rilascio dei budget necessari. Va ricordato infatti che investimenti etichettati come funzionali alla compliance sono spesso percepiti come prioritari e diventano più facilmente approvabili. Tuttavia, permane il rischio è che la compliance sia vissuta come un semplice adempimento formale. Per evitare questo, è fondamentale legare il rispetto delle norme a una visione più ampia, che veda la sicurezza come strumento per garantire la continuità operativa e la competitività dell'azienda.

IL RUOLO DEL TOP MANAGEMENT

Il coinvolgimento diretto del top management nelle attività di pianificazione, esercitazione e risposta agli incidenti è cruciale. Manager e membri del Board devono essere messi nelle condizioni di comprendere a fondo il rischio, partecipando attivamente ai momenti decisionali e formativi. Solo così si può costruire una cultura condivisa della resilienza.
Organizzare corsi dedicati, sviluppare analisi strategiche basate sulla Business Impact Analysis (BIA), coinvolgere le funzioni non tecniche nelle simulazioni: tutte queste azioni aiutano a integrare la cybersecurity nella governance aziendale, rendendo più naturale la discussione sul budget e più trasparente la relazione tra investimento e valore.

Il ruolo cruciale delle prove informatiche

Paolo Dal Checco
Consulente Informatico Forense e Professore dell'Università di Torino

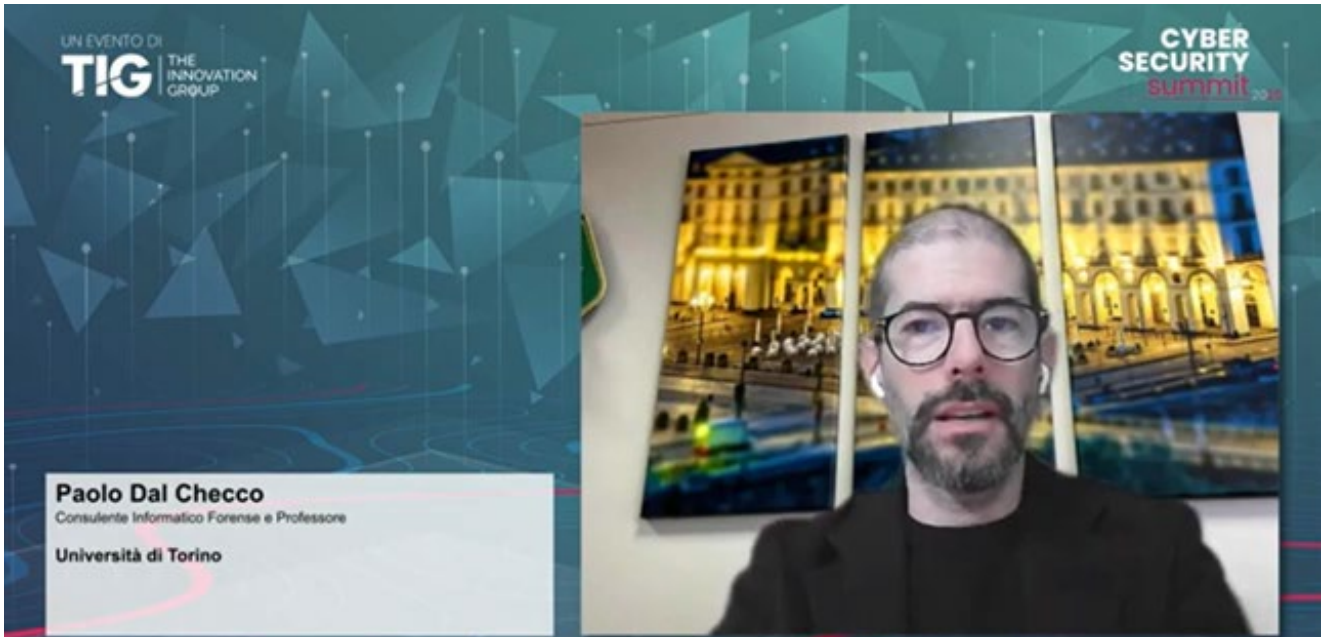
In un'epoca in cui il crimine informatico è in continua espansione, le prove digitali sono diventate sempre più fondamentali nelle indagini legali. Paolo Dal Checco, uno dei consulenti più esperti in Italia nel campo della forensic IT, approfondisce l'importanza delle prove informatiche e la loro gestione, con un focus particolare sul loro utilizzo post-incidente.

LE PROVE INFORMATICHE: UN NUOVO TIPO DI "PROVA" LEGALE

Dal Checco spiega che **le prove informatiche sono essenziali in contesti legali** dove è necessario difendersi da accuse o individuare chi accusare. Cosa distingue le prove digitali da quelle tradizionali? «Nel mondo tradizionale, i chimici analizzano la materia fisica e i balistici esaminano le armi: nel mondo digitale le prove sono anch'esse digitali», afferma Dal Checco. Le prove informatiche vanno infatti acquisite, clonate (ove possibile) e documentate in modo da poterle poi utilizzare in tribunale, così come accade con il campione di sangue in un'indagine criminologica.
L'analisi delle prove raccolte è un passaggio cruciale, che però in un primo momento riguarda più un'«evidenza digitale» piuttosto che una vera e propria «prova». Solo successivamente, durante il dibattimento, queste evidenze diventano prove legali vere e proprie.

LA NORMATIVA ITALIANA E LE CRITICITÀ NELL'ACQUISIZIONE DELLE PROVE

In Italia, la legislazione in materia di prove informatiche è ancora parzialmente arretrata, risale alla **Legge 48 del 2008**. «Questa legge è ormai obsoleta», sottolinea Dal Checco. Essa regolamenta principalmente l'acquisizione delle prove da parte delle forze dell'ordine, ma anche da parte di consulenti privati e aziende. Il prin-



Un momento dell'intervento di Paolo Dal Checco, Consulente Informatico Forense e Professore dell'Università di Torino, al Cybersecurity Summit 2025 di Milano

cipio cardine è che le prove informatiche non devono essere alterate durante la loro acquisizione. È fondamentale che chi gestisce le prove in ambito informatico le tratti con la stessa cura e attenzione con cui un investigatore tratterebbe una scena del crimine, preservando l'integrità delle evidenze per evitare che possano essere compromesse.
Uno degli errori più comuni, secondo Dal Checco, è che **le prove sono compromesse o cancellate** durante la fase di reazione all'incidente, quando i sistemi sono ripristinati o reinstallati senza le dovute precauzioni per conservare le tracce utili.

LA PREPARAZIONE NELLE FASI DI INCIDENT RESPONSE

Il consulente forense fa notare che uno degli errori frequenti nelle fasi di incident response è la **sottovalutazione dell'importanza della conservazione delle prove.** «Quando arriviamo in azienda dopo un attacco informatico, spesso scopriamo che i sistemi sono stati già reinstallati, che molte tracce sono state cancellate o sovrascritte, e ciò che rimane è insufficiente per una ricostruzione completa dell'accaduto», racconta Dal Checco. La preparazione nell'affrontare un incidente informatico dovrebbe includere anche la gestione delle prove, un elemento che troppo spesso viene trascurato in favore di misure di sicurezza immediate.

L'IMPATTO DELLA NIS2 SULLA GESTIONE DELLE PROVE INFORMATICHE

Un tema che ha animato il Summit è quello delle implicazioni della Direttiva NIS2. Dal Checco ha recentemente contribuito con un parere tecnico alla Camera dei deputati, in cui ha evidenziato come la legislazione europea non presti sufficiente attenzione alla fase di acquisizione delle prove. «Le aziende colpite da un attacco informatico sono chiamate a comunicare cosa è successo, le misure adottate, e i danni subiti. Ma manca una sezione specifica che indichi l'importanza della gestione delle prove durante l'incidente», afferma Dal Checco.
Secondo l'esperto, sarebbe importante che le aziende riportassero anche le fasi di digital forensics adottate per conservare e cristallizzare le prove. «Includere la gestione delle prove informatiche nel processo di risposta all'incidente non è solo una questione di dovere verso le autorità, ma anche una forma di autodifesa», aggiunge. La documentazione accurata delle attività di acquisizione delle prove potrebbe infatti rappresentare una prova di buona fede nel caso in cui si voglia dimostrare di aver fatto tutto il possibile per prevenire o mitigare l'attacco.

LA BLOCKCHAIN E LA SICUREZZA NELLE CRIPTOVALUTE

Un altro aspetto interessante affrontato da Dal Checco riguarda il mondo delle criptovalute, in particolare la gestione delle prove in caso di attacchi. L'esperto cita l'esempio del recente data breach di Bybit, per un ammontare di 1,46 miliardi di dollari. La blockchain, grazie alla sua natura immutabile, fornisce una solida base di prove digitali, rendendo la gestione delle transazioni criptate particolarmente interessante. «Nel caso di Bybit, gli esperti forensi hanno ricostruito l'attacco analizzando i timestamp dei file e altre tracce digitali», spiega Dal Checco.
La sicurezza delle criptovalute, purtroppo, non è infallibile. L'attacco a Bybit è stato possibile grazie a una tecnica di phishing che ha ingannato la piattaforma, portando a transazioni fraudolente. Le indagini sono state condotte grazie all'informatica forense, che ha permesso di identificare gli indirizzi coinvolti e rispondere alle domande cruciali su come e chi ha perpetrato l'attacco.

RIVEDI QUI
LA SESSIONE

Resilienza cibernetica e risposta agli incidenti: pilastri fondamentali per la sicurezza digitale

Paolo Cecchi
Senior Sales Director Mediterranean Region, SentinelOne

Nell'attuale panorama digitale, in continua evoluzione e sempre più interconnesso, le minacce informatiche rappresentano una realtà costante e in crescita. Ogni giorno, aziende, organizzazioni governative e singoli individui sono bersaglio di attacchi sofisticati, dal ransomware al phishing, dalle violazioni di dati al sabotaggio delle infrastrutture critiche.
In questo contesto, la semplice prevenzione non è più sufficiente; è imperativo adottare un approccio più olistico che includa la **resilienza cibernetica** e una robusta **risposta agli incidenti**.

COS'È LA RESILIENZA CIBERNETICA?

La resilienza cibernetica può essere definita come la capacità di un'organizzazione di resistere, riprendersi e adattarsi a fronte di attacchi informatici, interruzioni o guasti del sistema.
Non si tratta solo di prevenire gli attacchi, ma anche di minimizzare l'impatto di quelli che riescono a superare le difese, garantendo la continuità delle operazioni e la protezione dei dati essenziali.

Un'organizzazione cyber-resiliente è in grado di:

- **Anticipare:** Identificare e comprendere le potenziali minacce e vulnerabilità.
- **Proteggere:** Implementare controlli di sicurezza robusti per prevenire gli attacchi.
- **Rilevare:** Monitorare costantemente i sistemi per individuare attività sospette o attacchi in corso.
- **Rispondere:** Agire rapidamente e in modo coordinato per mitigare l'impatto di un incidente.
- **Ripristinare:** Recuperare i sistemi e i dati compromessi nel minor tempo possibile.
- **Apprendere:** Analizzare gli incidenti per migliorare continuamente le difese e i processi.

La resilienza cibernetica non è un obiettivo da raggiungere, ma un processo continuo di valutazione, miglioramento e adattamento. Richiede una cultura aziendale che ponga la sicurezza al centro, con il coinvolgimento di tutti i livelli, dal consiglio di amministrazione ai dipendenti.

L'IMPORTANZA DELLA RISPOSTA AGLI INCIDENTI

La **risposta agli incidenti** è una componente cruciale della resilienza cibernetica. Per quanto un'organizzazione possa essere preparata, è statisticamente probabile che prima o poi subisca un incidente di sicurezza. La velocità e l'efficacia con cui un'organizzazione risponde a un attacco possono fare la differenza tra un inconveniente gestibile e una catastrofe aziendale.

Un piano di risposta agli incidenti ben strutturato dovrebbe includere le seguenti fasi:

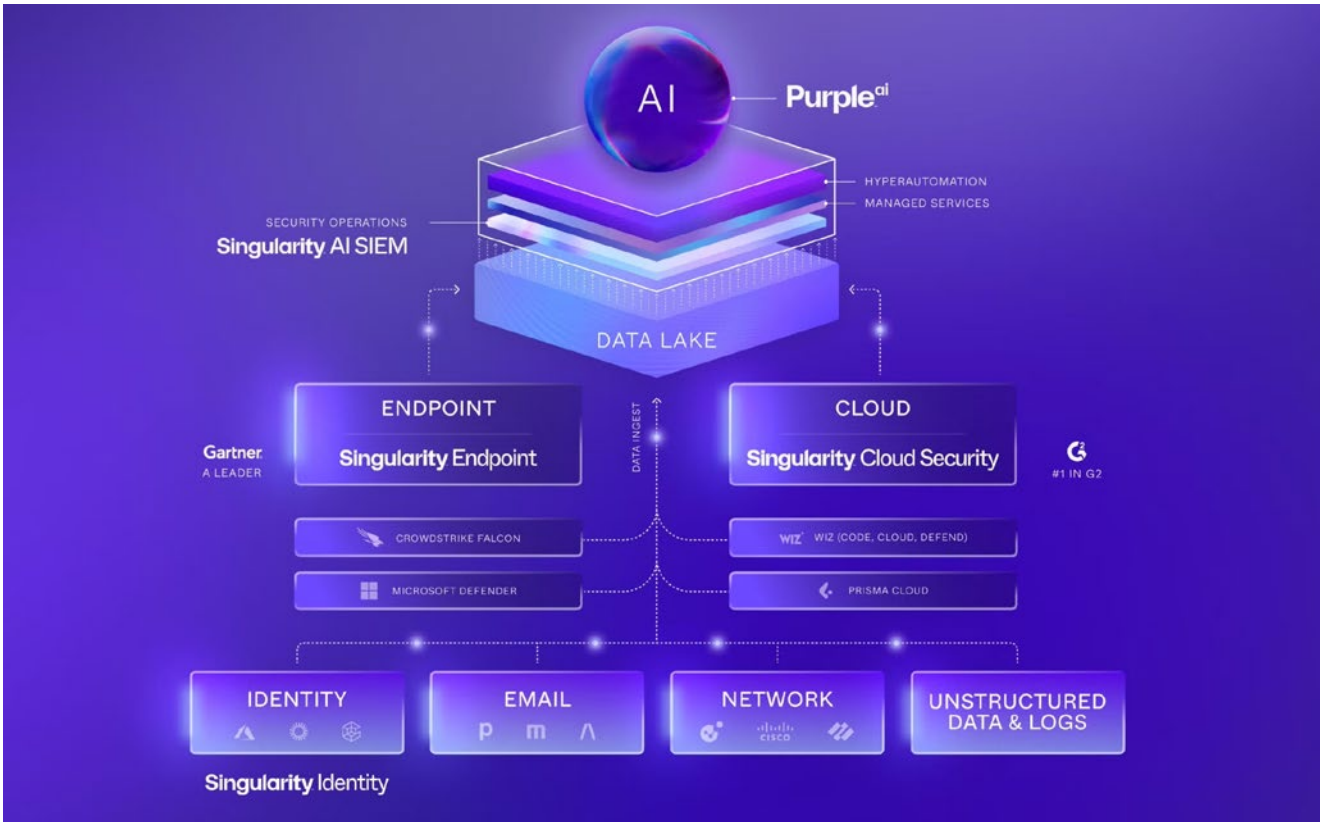
1. **Preparazione:** Creazione di un team di risposta agli incidenti (CSIRT o CERT), definizione di ruoli e responsabilità, sviluppo di procedure, formazione del personale, creazione di toolkit e piattaforme di analisi forense.
2. **Identificazione:** Rilevamento precoce dell'incidente attraverso sistemi di monitoraggio, alert e segnalazioni.
3. **Contenimento:** Isolamento dei sistemi compromessi per impedire che l'attacco si diffonda ulteriormente. Questo può includere la disconnessione di dispositivi, la segmentazione della rete o il blocco di indirizzi IP malevoli.
4. **Eradicazione:** Rimozione della causa dell'incidente, come malware, backdoor o account compromessi.
5. **Ripristino:** Ripristino dei sistemi e dei dati a uno stato operativo sicuro e funzionale, preferibilmente da backup puliti.
6. **Post-Incidente (Lezioni Apprese):** Analisi approfondita dell'incidente per comprendere come è avvenuto, quali vulnerabilità sono state sfruttate e cosa può essere migliorato per prevenire futuri attacchi. Questa fase è fondamentale per il ciclo di miglioramento continuo della resilienza.

BENEFICI DI UN APPROCCIO INTEGRATO

Adottare un approccio integrato che combini la resilienza cibernetica con una solida strategia di risposta agli incidenti porta a numerosi benefici:

- **Minimizzazione dei danni:** Riduzione dell'impatto finanziario, operativo e reputazionale degli attacchi.

La piattaforma Singularity di SentinelOne



- **Continuità aziendale:** Garanzia che le operazioni critiche possano continuare o essere ripristinate rapidamente.
- **Conformità normativa:** Rispetto delle normative sulla protezione dei dati (es. GDPR) e dei requisiti di sicurezza.
- **Miglioramento della fiducia:** Aumento della fiducia di clienti, partner e stakeholder.
- **Apprendimento e miglioramento continuo:** Capacità di adattarsi e rafforzare le difese a fronte di nuove minacce.

In conclusione, la resilienza cibernetica e la risposta agli incidenti non sono più optional, ma componenti essenziali di una strategia di sicurezza digitale moderna. Investire in queste aree significa non solo proteggere le risorse digitali, ma anche salvaguardare la reputazione, la fiducia e, in ultima analisi, il futuro di qualsiasi organizzazione nell'era digitale.
La piattaforma Singularity di SentinelOne rappresenta una risposta innovativa a queste sfide. Si tratta di una piattaforma di cybersecurity alimentata da intelligenza artificiale, che integra protezione, rilevamento e risposta automatica su endpoint, workload cloud, container e identità, il tutto gestito da una console unica e intuitiva. L'integrazione di servizi evoluti MDR, DFIR e Watch Tower aumenta la capacità di anticipare e contenere minacce emergenti. In questo modo, le organizzazioni possono rafforzare la propria cyber resilienza, prevenendo interruzioni e minimizzando i rischi operativi e finanziari.

4 OT/IOT cybersecurity e rischi legati alla supply chain

CYBERSECURITY INDUSTRIALE: UNA PRIORITÀ CON MOLTE SFIDE APERTE

Elena Vaciago
Research Manager, TIG - The Innovation Group

STATO DELL'ARTE DELLA CYBERSECURITY NEL SETTORE MANIFATTURIERO

Roundtable con **Luca Moroni**, Co-Founder, CSA Cyber Security Angels
Luigi Mina, Head of Cyber Security Architecture & Engineering, Eni
Pier Luigi Vanti, ICT & Industry 4.0 Corporate Director, IMA
Oronzo Lucia, Coordinatore Scientifico del Comitato Scientifico, SPS Italia

SICUREZZA OT: COMPLESSITÀ DEGLI AMBIENTI E CICLI DI VITA LUNGHISSIMI SONO LA VERA SFIDA

Giancarlo Calzetta
Research & Content Manager, TIG - The Innovation Group

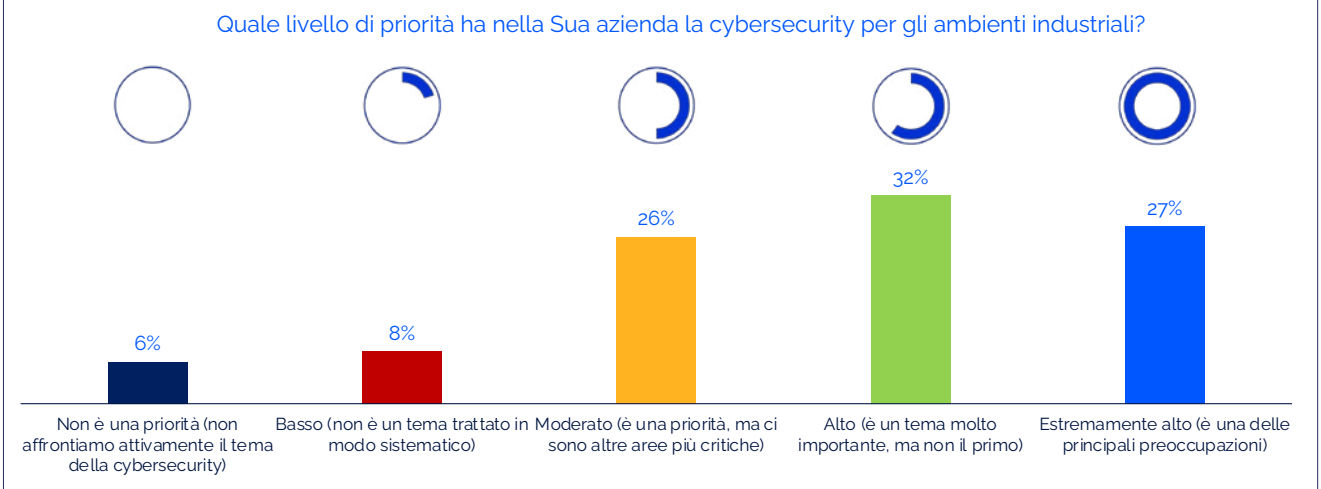
Cybersecurity industriale: una priorità con molte sfide aperte

Elena Vaciago
Research Manager, TIG - The Innovation Group

La cybersecurity in ambito industriale si sta finalmente guadagnando l'attenzione che merita. Spinta dall'evoluzione normativa (NIS2, IEC 62443, CRA e altre), sempre più aziende riconoscono l'importanza della protezione degli ambienti OT/ICS come fattore critico per garantire resilienza e continuità operativa. L'indagine "Smart Manufacturing Survey 2025"[1] di marzo 2025 (realizzata da TIG - The Innovation Group, in collaborazione con SPS Italia, ContactValue e Made Competence Center) ha indagato la maturità delle aziende italiane (intervistando un campione di 94 realtà industriali del Paese) nel percorso verso l'Industria 4.0.

Sono state analizzate le tendenze dell'adozione di strategie Data driven legate alla raccolta di informazioni provenienti dalla fabbrica (IoT, oggetti connessi); dell'uso attuale e prospettico dell'intelligenza artificiale nei processi produttivi; dei punti di attenzione per la cybersecurity e per la Transizione 5.0 verso sostenibilità ambientale e responsabilità sociale. Riportiamo di seguito i risultati con riferimento all'adozione di misure e processi di cybersecurity specifici per gli ambienti industriali.
Secondo i risultati della survey, il **59% delle imprese considera la sicurezza informatica una priorità alta o estremamente alta.** Solo un'esigua minoranza (6%) – composta esclusivamente da realtà di piccole e medie dimensioni – non affronta attivamente il tema. Il **34% la ritiene una priorità moderata o bassa**, segno che, pur riconoscendone la rilevanza, molte aziende sono ancora concentrate su altre urgenze.

IL 59% DELLE AZIENDE CONSIDERA LA CYBERSECURITY UNA PRIORITÀ ALTA O ESTREMAMENTE ALTA



Fonte: SMART MANUFACTURING Survey 2025, MARZO 2025

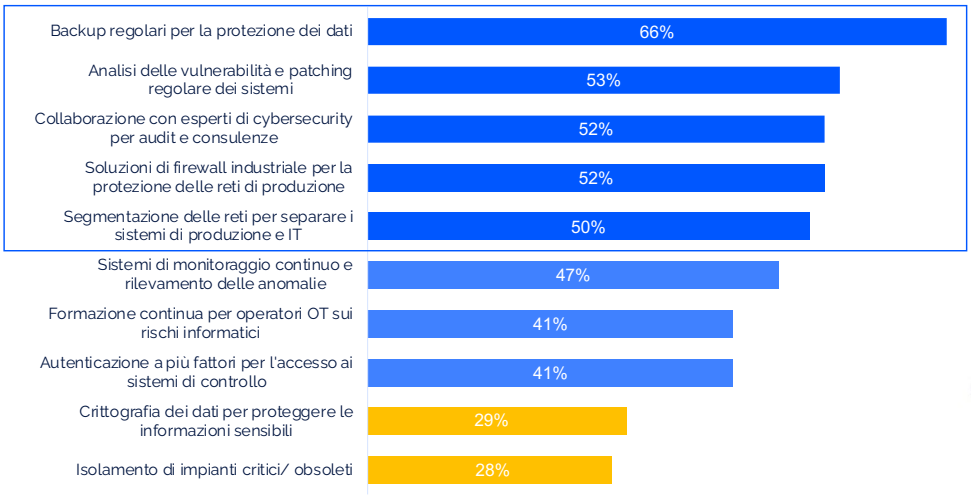
1 https://www.theinnovationgroup.it/smart-manufacturing-survey-2025/?lang=it

LE MISURE PIÙ ADOTTATE: DAI BACKUP AI FIREWALL INDUSTRIALI

Le tecnologie di difesa sono sempre più diffuse, anche se la loro adozione varia sensibilmente in base alla dimensione dell'azienda. Tra le misure più comuni spiccano:

- **Backup regolari** (66%): segnale di attenzione alla resilienza e alla continuità operativa.
- **Analisi delle vulnerabilità e patching** (53%): approccio proattivo al rischio, anche se con margini di miglioramento.
- **Firewall industriali** (52%) e **segmentazione delle reti** (50%): fondamentali per proteggere gli ambienti OT da intrusioni esterne.
- **Monitoraggio continuo delle anomalie** (47%): pratica utile, ma che potrebbe essere potenziata con soluzioni avanzate di threat detection.

QUALI MISURE DI SICUREZZA HA ADOTTATO LA SUA AZIENDA PER PROTEGGERE GLI AMBIENTI INDUSTRIALI DALLE MINACCE INFORMATICHE?



Fonte: SMART MANUFACTURING Survey 2025, MARZO 2025

Permangono tuttavia significative aree di miglioramento:

- La **collaborazione con esperti esterni riguarda solo il 52% delle aziende.**
- Appena il **41% investe in formazione continua per il personale operativo**, nonostante l'errore umano resti uno dei principali vettori di attacco.
- Solo il **28% isola gli impianti obsoleti o critici**, lasciando esposti sistemi legacy potenzialmente vulnerabili.
- Solo il **12% delle aziende utilizza l'intelligenza artificiale per la sicurezza OT**.
- Il **3% non adotta alcuna misura di sicurezza**, un dato allarmante in un contesto sempre più interconnesso e a rischio.

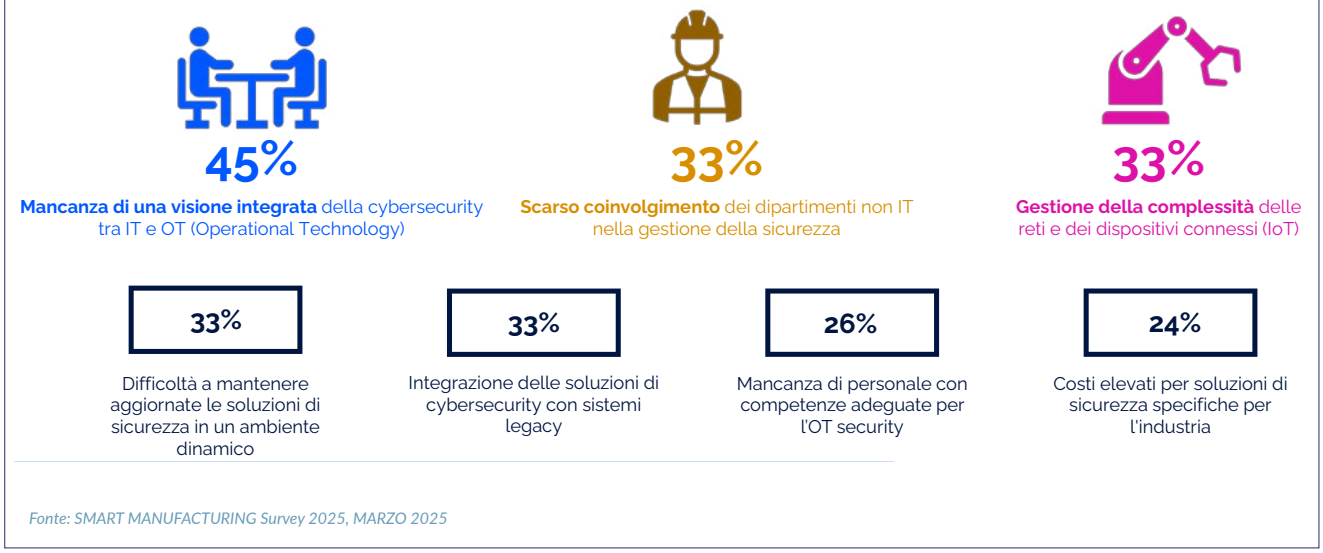
LE PRINCIPALI SFIDE: INTEGRAZIONE IT-OT, COMPLESSITÀ E COMPETENZE

La strada verso una cybersecurity industriale realmente efficace è ancora irta di ostacoli. La **mancanza di una visione integrata tra IT e OT** è la criticità più citata (45%), insieme allo **scarso coinvolgimento dei dipartimenti NON IT nella gestione di questi aspetti (33%)**: un disallineamento che può minare la sicurezza complessiva dell'intero ecosistema produttivo.

Seguono altri nodi critici:

- **Complessità operativa** (33%): l'integrazione con sistemi legacy, la gestione di reti IoT complesse e l'aggiornamento continuo delle tecnologie rappresentano sfide concrete.
- **Carenza di competenze** (26%): la scarsità di figure specializzate in OT security rallenta lo sviluppo di strategie efficaci.
- **Costi elevati** (24%) e **incertezza nella valutazione del rischio** (17%) completano il quadro delle difficoltà più sentite.

QUALI PRINCIPALI SFIDE CI SONO NELL'IMPLEMENTARE SOLUZIONI DI CYBERSECURITY PER GLI AMBIENTI INDUSTRIALI?



Fonte: SMART MANUFACTURING Survey 2025, MARZO 2025

In sintesi, il tema della cybersecurity industriale è ormai riconosciuto come cruciale, ma rimane molto lavoro da fare per tradurre questa consapevolezza in un'effettiva protezione degli impianti produttivi. Le aziende con un approccio moderato o basso (una percentuale ancora elevata, il 34% dai risultati della survey) potrebbero essere più vulnerabili agli attacchi cyber, soprattutto ransomware e attacchi alla supply chain. La necessità di formazione e investimenti in cybersecurity OT rimane un aspetto chiave per colmare il gap tra consapevolezza e azione concreta.

L'ambito della cybersecurity industriale è caratterizzato dalle seguenti tendenze:

- **Convergenza IT-OT.** L'evidente necessità di un approccio integrato indica una spinta verso la convergenza di IT e OT, con conseguenze significative in termini di gestione e coordinamento delle risorse tecnologiche e umane.
- **Evoluzione delle minacce.** La complessità crescente degli ambienti industriali, con un maggior numero di dispositivi IoT e sistemi legacy, implica un aumento della superficie d'attacco e la necessità di strategie di sicurezza più dinamiche.
- **Investimenti e innovazione.** Le sfide legate ai costi e alla formazione suggeriscono che le aziende dovranno investire maggiormente in soluzioni innovative e in programmi di aggiornamento continuo per mantenere un livello adeguato di protezione.

- **Implicazioni strategiche.** La mancanza di coinvolgimento dei reparti non IT e la visione frammentata della cybersecurity impongono un ripensamento della governance aziendale, orientato verso una gestione integrata e multidisciplinare della sicurezza.

L'integrazione tra sicurezza IT e OT sta diventando sempre più strategica, con l'adozione di misure tecniche come firewall, segmentazione di rete e autenticazione multifattore. **Le normative come NIS2 potrebbero incentivare l'adozione di soluzioni più avanzate**, come AI e threat intelligence per il rilevamento delle anomalie. **Il fattore umano resta però un elemento critico**, suggerendo la necessità di investire di più nella formazione del personale OT. Superare il gap IT-OT, investire nella formazione e adottare un approccio strutturato alla sicurezza saranno i prossimi passi obbligati per costruire un'industria davvero resiliente e sicura. L'indagine dimostra l'esigenza di investire in:

- **Formazione e sviluppo**. Investire in programmi di formazione specifici per OT security potrebbe colmare il gap di competenze.
- **Soluzioni integrate.** Sviluppare e adottare piattaforme che facilitino l'integrazione di IT e OT potrebbe migliorare la resilienza complessiva.
- **Innovazione tecnologica.** Incentivare soluzioni flessibili e scalabili che possano integrarsi con sistemi legacy rappresenta un'opportunità per rafforzare la cybersecurity industriale.

Stato dell'arte della cybersecurity nel settore manifatturiero

Roundtable con **Luca Moroni**, Co-Founder, CSA Cyber Security Angels
Luigi Mina, Head of Cyber Security Architecture & Engineering, Eni
Pier Luigi Vanti, ICT & Industry 4.0 Corporate Director, IMA
Oronzo Lucia, Coordinatore Scientifico del Comitato Scientifico, SPS Italia

La cybersecurity nel settore manifatturiero sta vivendo un momento di profonda trasformazione. Non più un tema ristretto a pochi esperti, la sicurezza informatica applicata agli ambienti operativi **(OT – Operational Technology)** è ormai riconosciuta come una preoccupazione elevata per la maggior parte delle aziende. È quanto emerso con forza dalla Roundtable dedicata alla cybersecurity nel manifatturiero, svoltasi lo scorso 2 aprile nell'ambito dello Smart Manufacturing Summit 2025[2].

I DATI RIVELANO UN CAMBIO DI PASSO, MA NON PER TUTTI

Secondo la survey, il 60% delle aziende intervistate considera la OT security una **preoccupazione alta o molto alta**. Un dato significativo che testimonia un netto cambiamento rispetto al passato. Tuttavia, l'interesse e l'adozione di misure di sicurezza mostrano profonde differenze dimensionali. Le grandi aziende sono molto attente, mentre **le piccole e alcune medie considerano ancora la**

2 https://www.theinnovationgroup.it/events/smart-manufacturing-summit-2025/?type=0&lang=it

OT security una priorità bassa o nulla. Questo gap crea gravi vulnerabilità nelle filiere produttive, che possono essere esposte a rischi se i partner più piccoli non si adeguano. L'adozione di misure di cybersecurity in ambito industriale ricalca quelle dell'IT, ma i livelli di implementazione si attestano attorno al **50-60% per le pratiche più diffuse**. Un dato allarmante emerso dalla survey è la **bassissima posizione occupata dalla formazione** (41% dei rispondenti) nella classifica delle misure adottate, aspetto solitamente ai primi posti nel mondo IT.

LA SFIDA PRINCIPALE: INTEGRARE IT E OT

Al primo posto tra le sfide percepite dalle aziende vi è la **mancanza di una visione integrata della cybersecurity tra IT e OT**. Nonostante gli ambienti stiano diventando sempre più unificati ("un tutt'uno"), una gestione unitaria, spesso guidata dall'IT, è ancora difficile da realizzare, anche a causa delle difficoltà nel coinvolgere adeguatamente il personale OT. Altre problematiche cruciali includono la complessità intrinseca degli ambienti industriali, le difficoltà nel mantenere le misure di sicurezza, l'integrazione di soluzioni disparate e la **carenza di personale specializzato**. Quest'ultima colpisce maggiormente le piccole imprese, mentre le difficoltà di integrazione preoccupano di più le grandi, probabilmente per via della maggiore complessità dei loro impianti.

LE VOCI DAL CAMPO: ESPERIENZE E STRATEGIE A CONFRONTO

La roundtable ha quindi dato voce a esperti del settore per approfondire queste tematiche.

Luca Moroni, Co-Founder di CSA Cyber Security Angels, ha presentato CSA come una community di "security by sharing" per aziende finali. Ha sottolineato l'impatto del **nuovo Regolamento Macchine**, già legge e in vigore da gennaio 2027, che introduce concetti di cybersecurity e AI nella progettazione delle macchine. Moroni ha evidenziato la necessità di **formare il personale "di campo"**, poiché spesso i fornitori non sono preparati sulla cybersecurity o lo sono solo su richiesta, e l'introduzione degli aspetti di sicurezza comporta costi che l'acquirente deve esigere. Ha concordato sulla mancanza di visione integrata IT/OT come sfida principale, suggerendo che sia l'OT a portare le proprie competenze nei comitati di cybersecurity. Ha inoltre posto l'accento sulla **supply chain come fattore chiave di rischio**, spesso causa di incidenti, e sulla mancanza di fornitori che introducano la sicurezza in modo proattivo.

Un momento della Roundtable Cybersecurity nello Smart Manufacturing Summit del 2 aprile 2025

Luigi Mina, Head of Cyber Security Architecture & Engineering di Eni, ha descritto il programma di OT security di Eni, avviato nel 2016-2017 in un contesto di grande diversificazione degli ambienti a livello mondiale. L'approccio è stato basato sull'**analisi del rischio** specifica per ciascun impianto, data l'impossibilità di applicare standard internazionali direttamente a impianti datati. Le misure privilegiate sono state il **monitoraggio passivo**, per ottenere visibilità rapida con basso impatto, e la **segregazione di rete**, essenziale data la rischiosità della comunicazione libera tra IT e OT. Eni gestisce IT e OT security sotto un'unica direzione per garantire il dialogo consapevole tra i due mondi. Tra le sfide, Mina ha citato il supporto dei fornitori, la **cultura e la formazione**, considerate fondamentali, l'eterogeneità dell'IoT e l'uso dell'AI anche da parte dei cyber criminali.
Pier Luigi Vanti, ICT & Industry 4.0 Corporate Director di IMA, ha portato la prospettiva di un costruttore di impianti. L'approccio alla cybersecurity OT di IMA è nato nel 2016 dall'esigenza di **servitizzazione delle macchine**, basata su connettività e raccolta di dati. L'ostacolo principale è stata la **paura dei clienti riguardo alla cybersecurity** nel connettere le macchine, specie al cloud. La soluzione è stata una **segregazione elevatissima** che consentisse solo la **raccolta unidirezionale dei dati** (principalmente diagnostici/ legati alla produttività delle macchine), mitigando così il rischio di violazione. IMA ha poi esteso il monitoraggio anche alla cybersecurity sui gateway, suggerendo che le strutture IT dei clienti gestiscano queste anomalie. Vanti ha menzionato normative come la **IEC 62443** e l'esperienza con la **certificazione ISO 27001** per la sicurezza IT. Ha sottolineato come i framework normativi aiutino a scoprire vulnerabilità "soft" sottovalutate, come la **formazione e sensibilizzazione degli utenti finali**, una delle vulnerabilità più frequenti e difficili da mitigare.
Oronzo Lucia, Coordinatore Scientifico del Comitato Scientifico di SPS Italia, ha offerto la visione del comitato di SPS Italia, nato per raccogliere esperienze e fornire indicazioni, in particolare per le realtà manifatturiere italiane più piccole. Lucia, con un background nel manifatturiero/automazione, ha riconosciuto la validità delle competenze sia IT che OT. Ha notato che la connettività, spinta da Industria 4.0, è stata a volte voluta dai clienti senza piena consapevolezza dei potenziali rischi, richiedendo poi ai costruttori di dover informare gli utilizzatori finali. Ha introdotto il concetto di **Security-by-design**, cruciale come la Safety by Design, per affrontare la sicurezza fin dall'inizio del ciclo di vita del prodotto. Il comitato di SPS Italia sta producendo **documenti e podcast ("Tech'nGo")**[3] con "pillole" informative sintetiche sulla cybersecurity. Le indicazioni includono un panorama delle **normative** (Regolamento Macchine, NIS2) e dei **framework implementativi** (IEC 62443, ISO 27000 series).

CONCLUSIONI

In conclusione, la roundtable ha confermato che la cybersecurity nel manifatturiero è una priorità crescente, ma la strada verso una protezione efficace e diffusa è ancora lunga. L'integrazione IT/OT, la preparazione dei fornitori, la formazione del personale e un approccio Security-by-design sono elementi chiave per affrontare le sfide di un ambiente industriale sempre più connesso e regolamentato.

RIVEDI QUI
LA SESSIONE

3 https://www.spsitalia.it/it/dettaglio-prodotto/5480/tech-n-go--cybersecurity

Sicurezza OT: complessità degli ambienti e cicli di vita lunghissimi sono la vera sfida

Giancarlo Calzetta
Research & Content Manager, TIG - The Innovation Group

Il mondo dell'infrastruttura IT combatte le minacce informatiche da molto tempo e i numerosi attacchi ransomware che flagellano le imprese negli ultimi anni ha portato il tema della cybersecurity all'attenzione dei consigli d'amministrazione che ne riconoscono l'importanza. Purtroppo, nel mondo dell'OT non funziona allo stesso modo, come è emerso dalle discussioni di un tavolo di lavoro specifico sull'OT Security nel corso dell'evento di TIG - The Innovation Group "CISO Panel 2025" a Roma lo scorso 27 maggio.
Tradizionalmente, le macchine impegnate nella produzione facevano parte di un mondo a sé, **separato e poco integrato con il resto dell'azienda.** Questo ha, nel tempo, generato una gran quantità di inefficienze, ma anche un contesto in cui gli attacchi cyber erano più complessi da portare a segno. Con l'avvento dell'industria 4.0 e degli IoTs, le cose sono cambiate e adesso la situazione è difficile. Da una parte c'è un ecosistema di hardware, software e umano poco attrezzato per resistere ai criminali, dall'altro l'enorme quantità di opportunità a cui si potrebbe accedere sfruttando a dovere la connettività e i dati che ne derivano.

IL CONTESTO DELLA SUPPLY CHAIN E LE SPECIFICITÀ OT

Nonostante le differenze tra mondo IT e OT, i CISO sono d'accordo nel riconoscere come una delle principali superfici di attacco una vecchia conoscenza dei piani di resilienza: la supply chain. Questa, infatti, nelle statistiche raccolte da associazioni e report figura sempre come il veicolo di circa **un terzo degli attacchi informatici**. Non è un caso che il tema sia trattato in maniera attenta da normative recenti come NIS2 e il Codice degli Appalti del 2024, oltre che da standard internazionali come ISO 27001. Secondo gli esperti, però, nel contesto Operational Technology, questo aspetto assume una gravità ancora maggiore. Le tecnologie OT, a differenza di quelle IT, si caratterizzano per cicli di vita estremamente lunghi e provengono spesso da mondi produttivi storicamente meno sensibili alle tematiche cyber, con un forte ritardo nell'adozione di pratiche di sicurezza.

LE PRINCIPALI SFIDE NELLA GESTIONE DELLA SICUREZZA OT

Indipendentemente dal settore merceologico, le organizzazioni che gestiscono device OT e IoT affrontano tre macro-problemi fondamentali. In primo luogo, la **governance di questi oggetti non sempre ricade sotto le direzioni IT**, bensì sotto altre direzioni interne che potrebbero essere meno sensibili alle tematiche cyber e, giustamente, sono maggiormente focalizzate sulla continuità del servizio. Questo disallineamento può portare a lacune nella gestione della sicurezza. In secondo luogo, i device OT si trovano spesso in una **porzione di rete vasta e distribuita, insufficientemente segregata** sia al proprio interno che verso il mondo IT classico.
Negli ultimi anni abbiamo assistito a una crescente convergenza verso il mondo IT e, in particolare, verso il cloud, amplificando i punti di contatto e le potenziali vulnerabilità. Infine, il **governo dei fornitori,** soprattutto per quanto concerne le manutenzioni, avviene tramite processi che possono essere considerati meno severi di quelli ottimali. Questa mancanza di controllo rigoroso può mettere a repen-

taglio non solo il business, ma anche la sicurezza delle persone. Molte aziende, inoltre, al loro interno non sono ancora riuscite a calare la cybersecurity in tutti i processi e capita che il CISO venga coinvolto tardivamente, con conseguente aggravio di costi e tempi sulle operazioni da compiere. Un esempio classico è quello delle flotte, che descrive più in generale cosa spesso succede per l'approvvigionamento di IoT. La gara viene preparata e indetta dall'ufficio competente senza pensare che all'interno di ogni veicolo oggi è presente un modem che rappresenta un punto di vulnerabilità da gestire.

STRATEGIE DI MITIGAZIONE E ADEGUAMENTO NORMATIVO

Di fronte alla scadenza della NIS2 (ottobre 2026), che classifica molti di questi oggetti all'interno dei perimetri critici, emerge l'urgenza di colmare il **significativo divario tra il mondo tecnologico corporate (IT) e quello di produzione (OT)**, come evidenziato da qualsiasi risk assessment. Le aziende stanno implementando con immediatezza azioni di mitigazione che riguardano l'infrastruttura, i processi e gli aspetti contrattuali.

"Molti asset tecnologici presenti nelle infrastrutture legacy di organizzazioni pubbliche e private rientrano nei loro rispettivi perimetri critici e, di conseguenza, si collocano nella fascia alta dei sistemi da proteggere secondo la direttiva NIS2" ha commentato Valerio Visconti, Group CISO di Autostrade per l'Italia, Cyber Coach del tavolo di lavoro "Cyber Resilienza e IT / OT Supply Chain Security" del CISO Panel di Roma.

Sul fronte infrastrutturale, si sta procedendo con una **segregazione molto spinta** che include non solo la rete, ma anche elementi critici come Active Directory separate, sistemi di Identity Access Management (IAM) e Privilege Access Management (PAM) distinti. Dal punto di vista dei processi, è fondamentale adottare **procedure di OT Change diverse da quelle di IT Change**, riconoscendo la priorità della continuità del servizio nel mondo OT. Ad esempio, mentre un sistema aziendale come un SAP può essere fermato per manutenzione senza conseguenze catastrofiche, un sistema di controllo industriale richiede finestre temporali di patching molto più ampie e una tolleranza minima ai fermi.

Per le tecnologie più datate, dove la riscrittura da zero non è economicamente sostenibile a causa dei costi o del fatto che i sistemi sono ancora nel pieno del loro ciclo di vita, si introducono **tecnologie di mitigazione come il virtual patching**. Un altro aspetto cruciale è il blocco del "backlog" attraverso **processi di approvvigionamento Secure-by-design**. Tutti i nuovi progetti, sia che riguardino nuovi device OT su vasta scala, sia che implichino integrazioni tra IT e OT, devono partire con un focus spinto sulla cybersecurity, poiché sistemare tali tecnologie in corsa è spesso impossibile o eccessivamente oneroso e ogni giorno perso nell'attuare adesso questa politica corrisponde a lustri o decenni di sicurezza non ottimale. Infine, è essenziale esercitare pressione sul legislatore affinché i produttori di device OT assumano una postura cyber adeguata, possibilmente attraverso certificazioni basate su norme internazionali come la ISA/IEC 62443.

L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE E LA NECESSITÀ DI GOVERNANCE

L'Intelligenza Artificiale (AI) è già ampiamente utilizzata in progetti cross-settoriali, spesso per la **diagnostica e il monitoraggio che impiegano device OT e IoT come fonti di dati**. Tuttavia, il recente **boom della Generative AI** ha reso evidente la necessità di una governance più rigorosa per questi progetti. L'utilizzo di data model non adeguatamente controllati presenta rischi significativi, non solo

in termini di diffusione incontrollata di dati verso l'esterno, ma anche a causa di fenomeni come le allucinazioni che possono **impattare direttamente il servizio o, indirettamente, la sicurezza delle persone**. È quindi imperativo stabilire una governance completa dell'AI, che copra l'utilizzo da parte degli utenti aziendali, la gestione dei data model nei nuovi progetti e anche l'integrazione con l'IT classica. In conclusione, la protezione dell'ambiente OT richiede un approccio olistico che integri strategie infrastrutturali, procedurali e contrattuali, con un'attenzione particolare alla supply chain, all'integrazione della security in tutti i processi aziendali, all'adozione da subito di politiche di Security-by-design e all'innovazione responsabile nell'uso delle tecnologie emergenti come l'intelligenza artificiale.

IL RUOLO DEL TOP MANAGEMENT

Il coinvolgimento diretto del top management nelle attività di pianificazione, esercitazione e risposta agli incidenti è cruciale. Manager e membri del board devono essere messi nelle condizioni di **comprendere a fondo il rischio**, partecipando attivamente ai momenti decisionali e formativi. Solo così si può costruire una cultura condivisa della resilienza.
Organizzare corsi dedicati, sviluppare analisi strategiche basate sulla Business Impact Analysis (BIA), coinvolgere le funzioni non tecniche nelle simulazioni: tutte queste azioni aiutano a **integrare la cybersecurity nella governance aziendale,** rendendo più naturale la discussione sul budget e più trasparente la relazione tra investimento e valore.

5 Il futuro è oggi: cybersecurity e innovazione

QUANTUM COMPUTING E CYBERSECURITY: LA CORSA È INIZIATA

Intervento di **Noemi Ferrari**
Co-Fondatrice & Chief Technology Officer di Quantum Ket

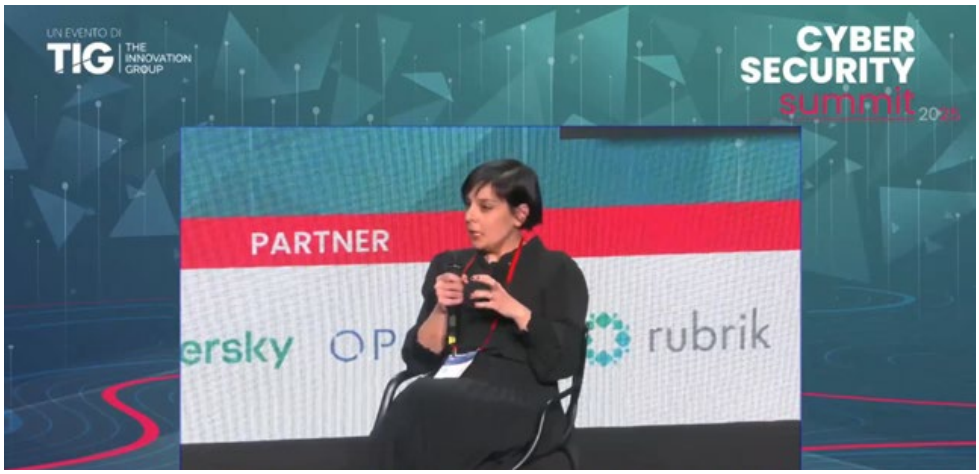
LA SFIDA DELLA SICUREZZA NEL CLOUD IBRIDO E NEL MULTI-CLOUD

Elena Vaciago
Research Manager, TIG - The Innovation Group

Quantum computing e cybersecurity: la corsa è iniziata

Intervento di **Noemi Ferrari**
Co-Fondatrice & Chief Technology Officer di Quantum Ket

Noemi Ferrari è intervenuta al Cybersecurity Summit 2025 dello scorso 20 marzo a Milano con un intervento molto interessante sul tema "Cosa succederà alla crittografia con il quantum computing?".
Il futuro della sicurezza informatica è già qui. O, per dirla con le parole di Noemi Ferrari, "il quantum computing è già realtà". CTO e cofondatrice della startup Quantum Ket, Ferrari guida l'innovazione italiana nel campo delle tecnologie quantistiche con uno sguardo pragmatico e, allo stesso tempo, entusiasta. Le abbiamo chiesto di spiegarci a che punto siamo davvero con il quantum computing, quali impatti avrà sulla crittografia e come le organizzazioni possono prepararsi.



Un momento dell'intervento di Noemi Ferrari, Co-Fondatrice & Chief Technology Officer di Quantum Ket al Cybersecurity Summit 2025 di Milano

DALLA FISICA NUCLEARE ALLA SICUREZZA QUANTISTICA

Fisica nucleare di formazione, Ferrari ha iniziato la sua carriera ai Laboratori Nazionali del Gran Sasso studiando la materia oscura. Ma è nella sicurezza che ha trovato la sua missione. Con Quantum Ket, oggi lavora allo sviluppo di tecnologie quantistiche applicate, in particolare, alla cybersicurezza.
"Abbiamo contribuito alla prima strategia quantistica europea," racconta. "E ora stiamo lavorando anche a quella italiana." Una leadership tutta italiana, che dimostra come anche startup giovani possano giocare un ruolo da protagoniste in un campo dominato da colossi globali.

DI COSA PARLIAMO QUANDO PARLIAMO DI TECNOLOGIE QUANTISTICHE?

La meccanica quantistica – quella branca della fisica che studia il comportamento delle particelle su scala microscopica – è alla base di una nuova ondata tecnologica, definita da molti come la seconda rivoluzione quantistica. Oggi siamo in grado, infatti, di manipolare attivamente questi stati quantistici e sviluppare tecnologie su questa base. Da questo nuovo paradigma derivano tre ambiti principali:

- Quantum computing
- Quantum sensing
- Quantum communication.

Guardiamo al primo: possiamo definirlo come un nuovo paradigma dell'informatica, che sfrutta la meccanica quantistica per affrontare problemi che i computer classici non riescono a risolvere. Un **computer quantistico** non è semplicemente una versione più potente di un computer tradizionale, è un oggetto completamente diverso, basato su una fisica differente.
Il bit classico può essere 0 oppure 1, mentre il **qubit**, l'unità fondamentale dell'informazione quantistica, può essere contemporaneamente 0 e 1 grazie al principio di sovrapposizione.
Se il primo ha attirato l'attenzione mediatica per il suo potenziale dirompente, il secondo è oggi il più maturo: **sensori di precisione estrema** stanno già trovando applicazioni in difesa, automotive e finanza. "Utilizzando la meccanica quantistica, siamo riusciti a realizzare sensori di precisione straordinaria, con accuratezze superiori di ordini di grandezza rispetto a quelli tradizionali" ha detto Ferrari. Ma è il terzo – la comunicazione quantistica – a rappresentare forse l'aspetto più strategico per la sicurezza.
"È vero che le tecnologie quantistiche hanno ancora problemi di stabilità e sono sensibili ai disturbi, ma nel caso dei sensori, proprio nel 2023 si è registrato un salto qualitativo. Oggi possiamo dire con certezza che funzionano anche in ambienti reali, non solo in laboratorio" sottolinea Ferrari.

IL QUANTUM COMPUTING È UNA MINACCIA PER LA CRITTOGRAFIA?

"La risposta è sì," afferma senza mezzi termini Ferrari. "Tra i problemi che il quantum computing riesce a risolvere ci sono quelli su cui si basa la crittografia attuale. Già dal 1994, con l'algoritmo di Shor, sappiamo che un computer quantistico potrà violare questi sistemi. Oggi i computer quantistici esistono, ma non sono ancora pienamente "fault tolerant". Tuttavia, c'è stata una forte accelerazione. Fino a un anno fa si pensava che ci volessero 15 anni; ora parliamo di 7 o addirittura meno. Pensate che l'attivazione delle testate nucleari si basa proprio su questi algoritmi. Il rischio è concreto. La Russia, per esempio, ha annunciato un investimento di 700 milioni di dollari solo per il 2025 sul quantum computing".

LE CONTROMISURE: PQC E QKD

Come proteggersi da questo scenario? Le contromisure si stanno già delineando lungo due linee:

- **Post-Quantum Cryptography (PQC):** algoritmi classici progettati per resistere ad attacchi quantistici, su cui il NIST americano ha definito i primi standard ufficiali ad agosto 2024;
- **Quantum Key Distribution (QKD):** sistemi basati su proprietà fisiche inviolabili.

"Questi algoritmi già esistono. Noi, ad esempio, ne abbiamo uno già commercializzato" rivela Ferrari. "Ma la tempistica è tutto: non ci si può permettere di aspettare. Negli Stati Uniti, ad esempio, il governo ha chiesto ufficialmente alle aziende di iniziare la migrazione, dopo che ad agosto 2024 il NIST si è pronunciato sugli algoritmi standard da adottare".

UN'INFRASTRUTTURA ANCORA IN DIVENIRE

Nonostante le promesse, le sfide restano. I computer quantistici sono rumorosi, instabili, richiedono temperature estremamente basse e sono sensibili ai disturbi ambientali. Ma anche su questo fronte si registrano progressi.

Altro nodo critico è l'infrastruttura di rete: senza ripetitori quantistici, una vera "internet quantistica" non è ancora possibile. Ma i governi stanno investendo, e saranno probabilmente i primi a utilizzare queste tecnologie in contesti reali.

RIVEDI QUI
LA SESSIONE

IL FUTURO? È GIÀ COMINCIATO

Per Ferrari, non si tratta più di futuro remoto: "Oggi ci sono approcci ibridi ispirati alla computazione quantistica che possono già essere eseguiti su computer classici. Chi parte oggi, sarà pronto domani."

La sfida della sicurezza nel cloud ibrido e nel multi-cloud

Elena Vaciago
Research Manager, TIG - The Innovation Group

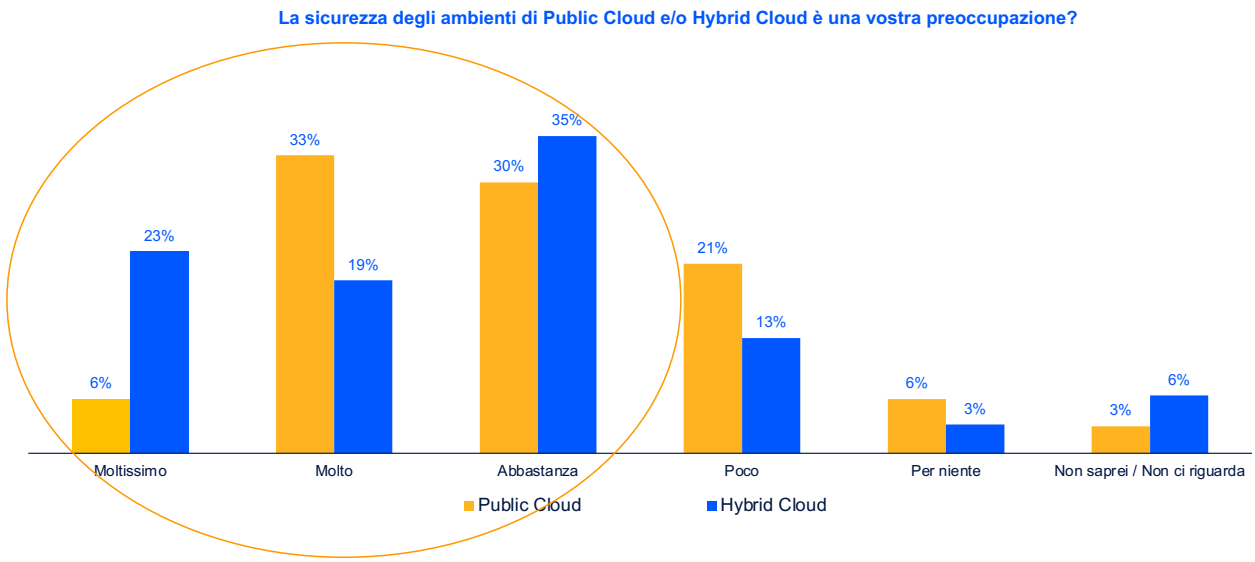
La transizione verso ambienti IT sempre più distribuiti, che combinano infrastrutture on-premise con molteplici piattaforme cloud (Public e Private), presenta sfide significative, in particolare sul fronte della sicurezza. È quanto emerso con forza durante la tavola rotonda "Zero Trust e Hybrid Multi-cloud security" al Cybersecurity Summit 2025, lo scorso 20 marzo a Milano.
La discussione ha evidenziato come la realtà IT attuale sia caratterizzata da un mix di ambienti on-prem, public e private cloud, una configurazione che si prevede continuerà anche nei prossimi anni, forse con una maggiore prevalenza del Public Cloud. Questa coesistenza definisce l'aspetto "Hybrid" della sicurezza trattata nella sessione.

LA PERCEZIONE DELL'INSICUREZZA DEL CLOUD È DIFFUSA NELLE AZIENDE ITALIANE

Come emerge dalla survey "Cyber Risk Management 2025"[1] di TIG e CSA – Cyber Security Angels, la preoccupazione per la sicurezza del cloud è alta, con il 70% delle aziende preoccupate per il Public cloud e un dato leggermente superiore (77%) per l'Hybrid cloud. Questo sottolinea come il tema della sicurezza nel cloud sia una questione concreta e sentita.
Un aspetto cruciale emerso è la notevole complessità della **sicurezza del cloud**, con una lunga lista di problematiche, tra cui interfacce/API mal configurate e la difficoltà nel rilevare l'utilizzo "ombra" del cloud.
Con l'adozione di configurazioni multi-cloud sempre più diffuse, le sfide per i responsabili della sicurezza si moltiplicano. Tra le principali, spiccano la necessità di competenze specifiche per ogni singolo cloud, la protezione dei dati e della privacy su tutti gli ambienti, l'integrazione di soluzioni di sicurezza eterogenee, la comprensione delle opzioni di integrazione dei servizi dei vari provider e la gestione dei costi crescenti.

1 https://www.theinnovationgroup.it/cyber-risk-management-survey-2025/?lang=it

LA SICUREZZA DEL PUBLIC CLOUD È UNA PREOCCUPAZIONE PER IL 70% DELLE ORGANIZZAZIONI, DELL'HYBRID CLOUD PER IL 77%



Fonte: Cyber Risk Management 2025 Survey, Gennaio 2025

ESPERIENZE DAL CAMPO: ZERO TRUST E MICRO-SEGMENTAZIONE

Andrea Angeletta, CISO di Aria, ha confermato che i risultati della survey rispecchiano pienamente le preoccupazioni riscontrate nel loro progetto di cloud transformation per la Pubblica Amministrazione. Aria ha adottato un approccio multi-cloud ibrido che include l'utilizzo di diversi public cloud. Fin dall'inizio, la scelta è stata quella di applicare un approccio Zero Trust "abbastanza spinto, abbastanza paranoico". Un punto critico affrontato è stata la protezione dei dati dei cittadini lombardi di fronte alla possibilità che i Cloud Service Provider potessero essere obbligati ad accedere ai dati. Questo ha portato a un intenso lavoro sulla cifratura e sulla conservazione delle chiavi in ambito nazionale. Sono stati implementate protezioni per i punti di ingresso nei tenant cloud per **mitigare i rischi derivanti da API mal configurate** che potrebbero consentire accessi diretti a dati e infrastrutture.

La gestione di cloud diversi, ognuno con il proprio gergo tecnico, rappresenta una difficoltà tangibile. Per uniformare la gestione e l'osservabilità, dove possibile, sono state privilegiate soluzioni *Cloud Independent* per funzioni critiche come il controllo dei flussi tra i workload, sebbene non sempre sia stato fattibile a causa di problemi di compatibilità. Tuttavia, l'osservabilità è stata mantenuta convogliando i log su piattaforme in grado di trattarli in modo uniforme.

Un elemento cardine dell'**approccio Zero Trust** scelto è stata la micro-segmentazione, considerata fondamentale per prevenire movimenti laterali, specialmente con dati sanitari. L'implementazione è descritta come un "lavoro enorme" e non banale, richiedendo una conoscenza analitica dei flussi applicativi, spesso difficile da ottenere con applicazioni datate e non documentate. Questo ha comportato lunghi periodi di osservazione, censimento e mappatura dei flussi per permettere solo quelli strettamente necessari.

LA COMPLESSITÀ DEI WORKLOAD E IL COSTO DEL LOCK-IN

Pier Paolo Bortone, Cybersecurity Director di Italiaonline, ha approfondito il concetto di workload come qualsiasi servizio o applicazione che sfrutti risorse cloud, sottolineandone la complessità derivante dalle diverse attività e dalle specifiche esigenze di sistema e rete. Ha discusso la complessità aggiuntiva dovuta al dialogo tra workload diversi, descrivendo inoltre la sfida di rendere i workload Cloud Agnostic per evitare il lock-in del vendor. Sviluppare componenti *Cloud Agnostic* è un investimento notevole, stimato come 8 volte più costoso rispetto a un componente Cloud Specifico: questo perché i workload sono spesso legati alla tecnologia cloud che meglio si adatta a loro (es. AWS per transazionali, Google/Azure per elaborazione dati), rendendo il lock-in "molto forte".
Secondo Bortone, l'**approccio alla trasformazione cloud** o ai nuovi progetti deve basarsi su un modello e una strategia fortemente legati al business. Questa strategia deve considerare costi (variabili vs. fissi, prevedibilità on-prem vs. consumo cloud), controllo, e soprattutto la necessità di competenze per gestire ambienti ibridi con tecnologie Cloud diverse. Ha evidenziato la maggiore esposizione al rischio e l'aumento della superficie d'attacco quando si porta un servizio in Cloud, rendendolo più esposto e richiedendo connettività tra data center e cloud.

IL RUOLO DELL'IT, CHE DEVE "DARE BUON ESEMPIO"

Francesco Cantoni, IT Manager di Arco Spedizioni, ha scherzosamente osservato che l'IT è "bravo a crearsi problemi da solo". La migrazione cloud ha messo in luce l'importanza di **evitare il lock-in**. Ha sollevato dubbi sui vantaggi dell'approccio ibrido dal punto di vista dei costi, confrontando il costo noto della gestione multi-cloud con il costo "sconosciuto" del lock-in. La tendenza attuale è l'utilizzo di diversi provider (Public e Private) per mantenere le "porte aperte".
Dopo l'entusiasmo iniziale per il cloud, si è capito che non era intrinsecamente sicuro e che i workload, sia on-prem che in cloud, necessitano di protezione, forse in modo ancora più stringente nel cloud. Strumenti come l'MFA (Multi-Factor Authentication) e il Conditional Access sono stati definiti basilari e fondamentali per migliorare la security posture di questi ambienti. È cruciale poi che il reparto IT dia il buon esempio, superando la "pigrizia" nell'implementare misure di sicurezza come l'MFA o l'uso di account dedicati. L'MFA, nonostante possa sembrare un "fastidio", è considerata fondamentale oggi, dato che **le password sono un componente di sicurezza obsoleto.**
La metodologia Zero Trust è strettamente legata al superamento dell'inerzia dell'IT, nell'applicare il principio del minimo privilegio, concedendo accessi solo allo stretto necessario. Nel multi-cloud, il numero di fornitori esterni che richiedono accesso aumenta, rendendo essenziale per l'azienda governare i propri dati e accessi, anche scontrandosi con resistenze interne o esterne. Queste pratiche sono oggi considerate delle best practice fondamentali.

RIVEDI QUI
LA SESSIONE

I PARTNER 2025

Ringraziamo i Partner del Cybersecurity Program 2025 di TIG - The Innovation Group

Cybersel SentinelOne

Gli appuntamenti del Cybersecurity Program 2026 di TIG

Il **CYBERSECURITY program 2026** di TIG - The Innovation Group affronterà, nel corso dell'intero anno, i principali punti di attenzione nell'Agenda del CISO, ossia come rispondere a esigenze di cyber resilienza e sovranità digitale, compliance, cloud security, incident response, supply chain security, threat intelligence, protezione di dati, reti, accessi, oggetti connessi.

Obiettivo del CYBERSECURITY program di TIG - The Innovation Group è quello di fare costantemente il punto sullo stato dell'arte della Cybersecurity e della Cyber Resilienza del Paese, partendo dall'analisi dello stato dell'arte della maturità delle sue realtà pubbliche e private per quanto riguarda la gestione del rischio cyber, le più attuali tendenze, opportunità e problematiche.

Nel 2026, il CYBERSECURITY program si compone dei seguenti appuntamenti:

CISO Summit *residenziale*

26 e 27 marzo

Baveno, *Grand Hotel Dino del Lago Maggiore*

3 incontri **CISO Panel** *in presenza*

maggio	**settembre**	**ottobre**
Roma	Milano	Padova