POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

02.10.2025

Supply chain e Cybersecurity

Open Innovation Lombardia - Finlombarda

Giorgia Dragoni

Ricercatrice Senior e Direttrice
Osservatorio Cybersecurity & Data Protection
Osservatorio Digital Identity

giorgia.dragoni@polimi.it

Agenda

L’Osservatorio Cybersecurity & Data Protection

Il contesto di riferimento per la cybersecurity, tra minacce e spinta normativa

La gestione del rischio cyber associato alle terze parti (il rischio supply chain) nelle organizzazioni

L’evoluzione normativa e le implicazioni sulla gestione delle terze parti (DORA, NIS2, ecc.)

La mission e gli obiettivi dell'Osservatorio Cybersecurity & Data Protection

Mission: Comprendere e affrontare le principali problematiche della Cybersecurity e della Data Protection e supportare, attraverso la creazione e diffusione di conoscenza, le organizzazioni nel cogliere le opportunità della cybersecurity a difesa del proprio patrimonio informativo

RICERCA

Sviluppare una conoscenza approfondita del **mercato cybersecurity italiano e internazionale**, monitorando i percorsi di trasformazione **tecnologica e organizzativa** delle aziende e l'impatto della trasformazione digitale in temini di minacce e opportunità di cybersecurity

NETWORKING

Stimolare il **confronto pre-competitivo** tra decisori e C-Level della domanda, dell'offerta e delle istituzioni. Creare occasioni di interazione in cui **collaborare e sviluppare relazioni**

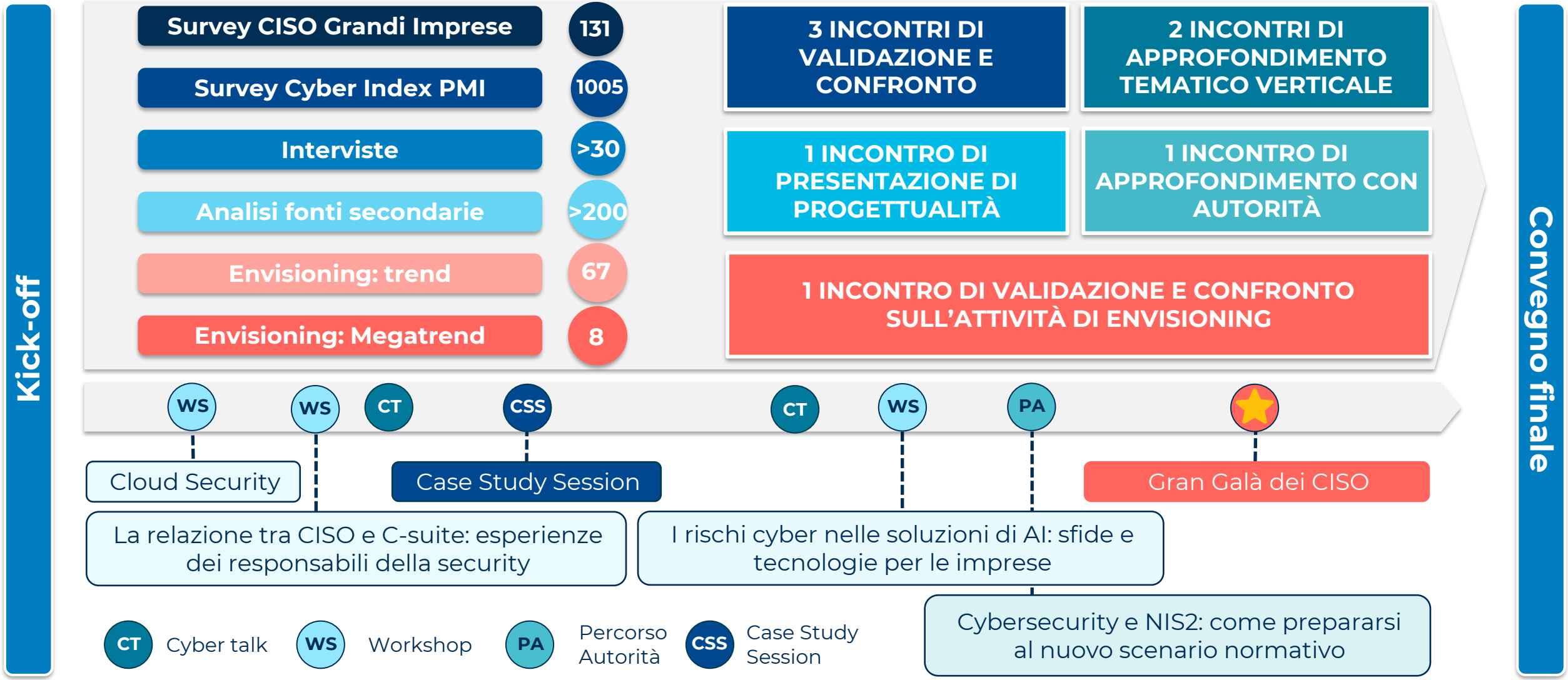
COMUNICAZIONE

Fare **chiarezza** sulle opportunità e diffondere buone pratiche, esperienze e cultura sulla cybersecurity, raggiungendo il più **ampio numero di persone** possibile

AGGIORNAMENTO

Mettere a disposizione il **know-how** unico e distintivo dell'Osservatorio tramite la produzione di output peculiari e modelli interpretativi originali

Le attività e le metodologie dell'Osservatorio nell'edizione 2024



Agenda

L’Osservatorio Cybersecurity & Data Protection

Il contesto di riferimento per la cybersecurity, tra minacce e spinta normativa

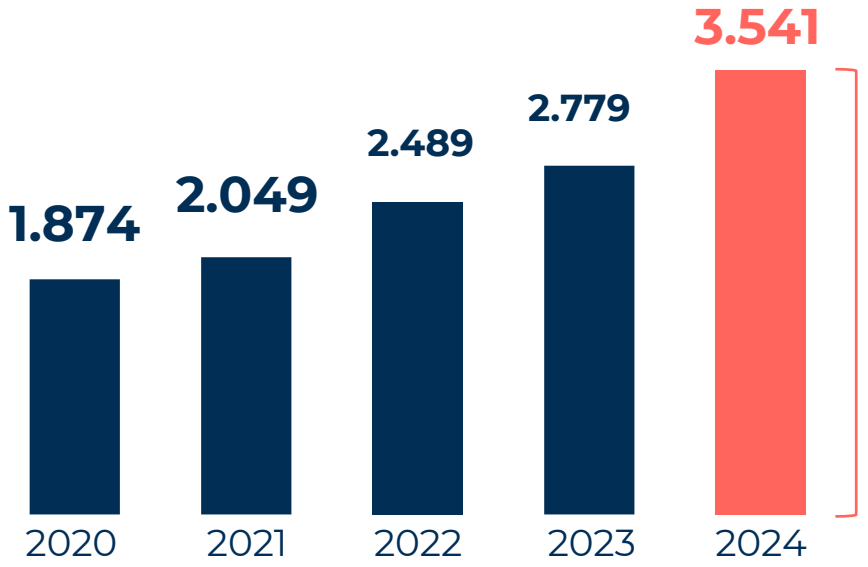
La gestione del rischio cyber associato alle terze parti (il rischio supply chain) nelle organizzazioni

L’evoluzione normativa e le implicazioni sulla gestione delle terze parti (DORA, NIS2, ecc.)

Lo scenario della minaccia

- **Sofisticazione della tecnologia (quantum computing ed AI)**
- **Attacchi su larga scala e nuovi target profittevoli**

Incidenti gravi di dominio pubblico dal 2020 al 2024 (vista globale)



35% Attacchi verso organizzazioni in **America**

30% Attacchi verso organizzazioni in **Europa**

10% Attacchi verso organizzazioni in **Italia**

© Clusit - Rapporto 2025 sulla Sicurezza ICT in Italia

Quale impatto avrà il cambiamento degli **equilibri geopolitici** sulla **distribuzione geografica** e sulla matrice degli attacchi?

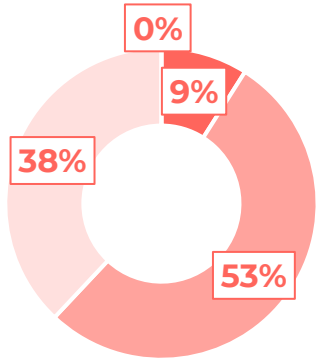
Gli attacchi gravi a livello italiano

Anche in Italia si evidenzia un **aumento degli attacchi (+15% rispetto al 2023),** ma diminuisce la percentuale di attacchi con severity «Critica»

Tra il 2022 e il 2024 il numero di attacchi gravi in Italia è quasi raddoppiato

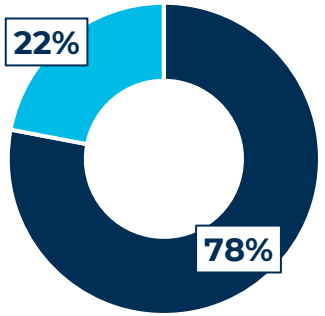
Incidenti gravi di dominio pubblico dal 2018 al 2024 (vista sull'Italia)

Severity



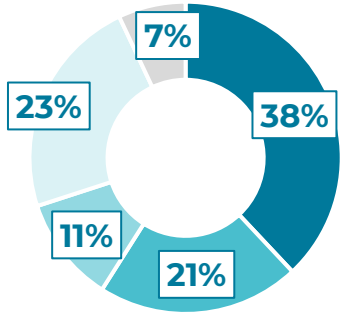
- Critica
- Alta
- Media
- Bassa

Tipologia



- Cybercrime
- Hacktivism

Tecniche



- Malware
- DDoS
- Phishing
- Altro
- Sconosciuto

Lo scenario normativo

La normativa torna a giocare un ruolo centrale nell'indirizzare scelte aziendali e investimenti

L'**adeguamento normativo** rappresenta la **priorità** in ambito cybersecurity per le grandi organizzazioni **a livello europeo**

Survey European Digital Tech Watch 2024 – Campione: 1.021 grandi organizzazioni

NIS 2 - *Network and Information Security*

- Ampliamento del perimetro dei settori critici
- Definizione di un livello comune di resilienza

Una tra le più importanti iniziative giuridiche per ***numero di imprese coinvolte*** *dopo il GDPR*

Oltre 26.000 aziende si sono registrate alla piattaforma ACN!

DORA - *Digital Operational Resilience Act*

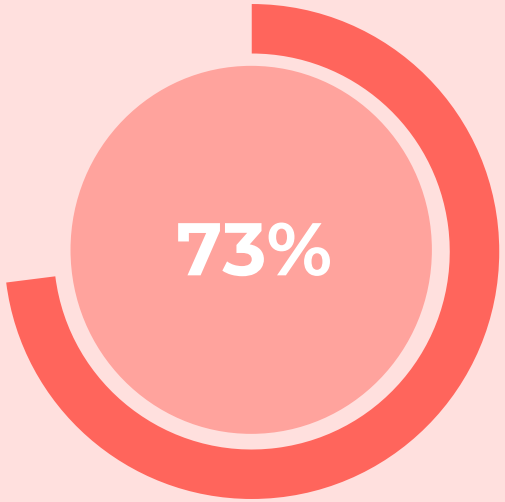
Tracciamento di importanti ***novità sull'approccio integrato alla gestione del rischio cyber***

Cyber Resilience Act

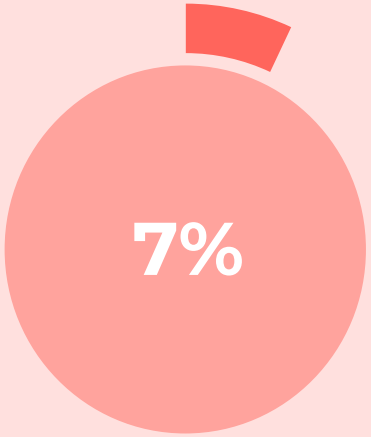
Redistribuzione *(parziale)* ***dei rischi cyber*** *lungo la filiera digitale*

La situazione delle organizzazioni italiane

ATTACCHI VERSO LE GRANDI ORGANIZZAZIONI ITALIANE



Aziende che hanno **subito almeno un attacco** nel 2024



Aziende che hanno subito **attacchi cyber che hanno richiesto interventi onerosi** per la gestione e la mitigazione

PRINCIPALI FATTORI DI RISCHIO

Fattore umano — **75%**

Obsolescenza infrastrutturale — **73%**

Azioni malevole di cybercriminali — **59%**

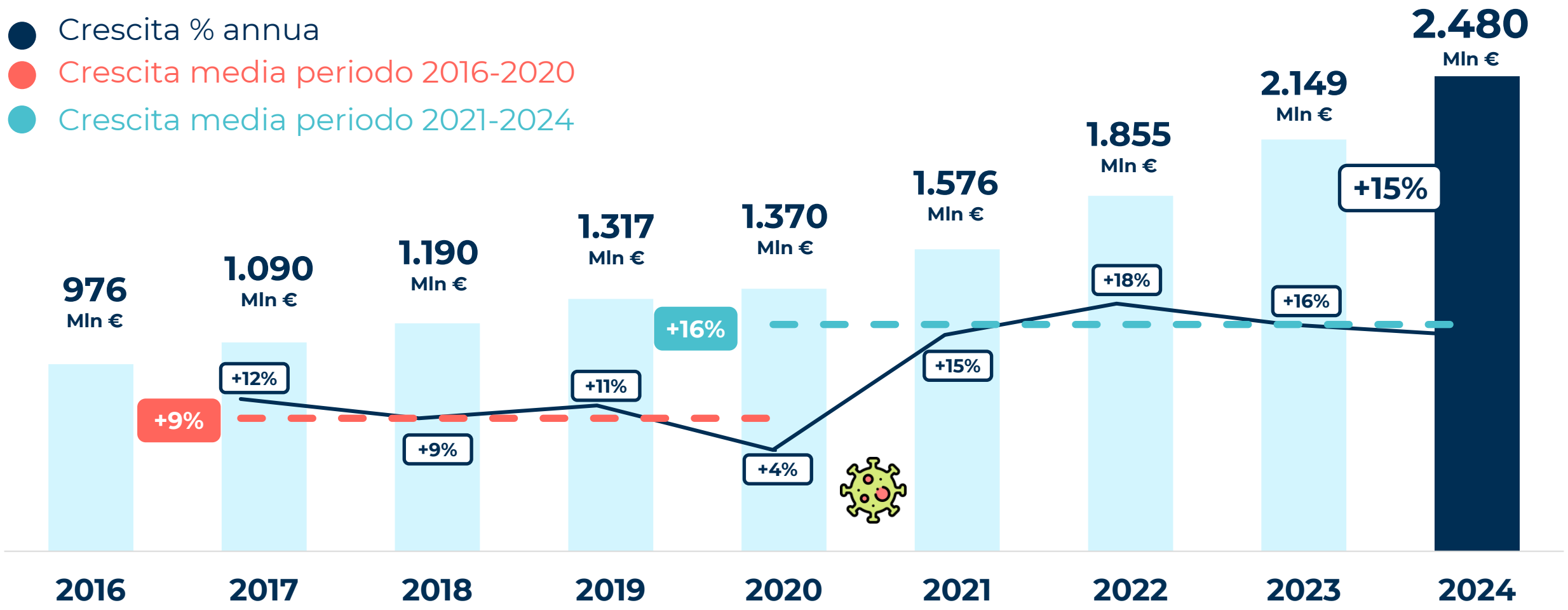
•
•
•

Utilizzo spontaneo di AI da parte del business — **33%**

Campione Survey CISO: 131 Grandi Organizzazioni

La spesa in cybersecurity: il mercato 2024

Sebbene in lieve rallentamento, le crescita del mercato cybersecurity si mantiene su una **media costante del 15% dal post pandemia.** Il mercato si consolida, ma resta strategico investire in sicurezza digitale



Agenda

L’Osservatorio Cybersecurity & Data Protection

Il contesto di riferimento per la cybersecurity, tra minacce e spinta normativa

La gestione del rischio cyber associato alle terze parti (il rischio supply chain) nelle organizzazioni

L’evoluzione normativa e le implicazioni sulla gestione delle terze parti (DORA, NIS2, ecc.)

Con **rischio cyber** si intende qualsiasi rischio di **perdita finanziaria**, **interruzione** o **danno alla reputazione** di un'organizzazione a causa di **guasti dei suoi sistemi informatici**.

Institute of Risk Management

Nuove minacce e sfide tecniche

Costante **aumento degli attacchi** e **sofisticazione** delle tecnologie a disposizione dei cybercriminali

Rischio operativo

A differenza di qualche anno fa, i rischi di cybersecurity hanno un **impatto reale sulla performance aziendale**

Evoluzione normativa

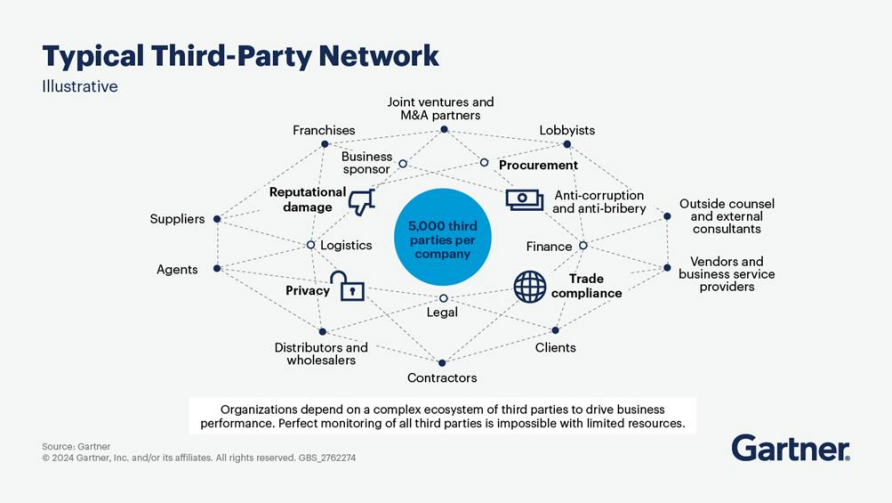
Forte richiamo all'attenzione ai **rischi e alla gestione degli stessi**, agli incidenti e agli effetti negativi

Il rischio associato alle terze parti

Cosa si intende per terze parti?

"A third party is any entity that the organization has **a contractual relationship with**."

Il rischio si estende anche alle **quarte parti**, che sono subappaltatori o fornitori di servizi aggiuntivi ingaggiati da terze parti.



Quali sono i rischi associati alle terze parti?

Le relazioni con terze parti spesso implicano:

- **l'accesso a informazioni privilegiate** come i dati dei clienti e i sistemi interni, il che le rende **potenziali punti di ingresso per gli attacchi informatici**
- **punti di accesso da remoto** riservati alle terze parti, con **privilegi elevati**, potenzialmente sfruttabili da soggetti malintenzionati per il compimento di attacchi cyber

Il rischio associato alle terze parti: tipologie di attacchi e possibili conseguenze

MINACCE CYBER «TRADIZIONALI»

Minacce e vettori di attacco tradizionali (es. business email compromise, phishing, botnet, ransomware…) che sfruttano l'**anello debole** della filiera per fare breccia a cascata nell'organizzazione

MINACCE ALLA CATENA DI FORNITURA

Modifiche irregolari ai prodotti/servizi in fase di produzione o distribuzione (es. software malevolo installato in un sistema e poi distribuito o componente alterato)

Data breach e divulgazione di dati riservati

Danni reputazionali

Perdite economiche

Interruzione delle attività

Qualche esempio di attacchi supply chain: il rischio terze parti in pratica

SolarWinds

Un sofisticato attacco cyber contro SolarWinds, avvenuto tramite l'iniezione di una backdoor nel processo di distribuzione degli aggiornamenti della piattaforma Orion, ha permesso a un gruppo di cybercriminali - probabilmente sostenuto dal governo russo - di spiare per mesi e trafugare dati ai danni delle organizzazioni della filiera, tra cui agenzie governative e aziende di alto livello in tutto il mondo (oltre 18.000 vittime)

Dicembre 2020

Kaseya

Nel «più grande attacco ransomware della storia», il collettivo di cybercriminali REvil ha colpito un software di Kaseya, società che fornisce sistemi di monitoraggio e gestione remota della rete, propagandosi a cascata su decine di clienti. REvil ha annunciato di aver compromesso oltre 1 milione di dispositivi, chiedendo 70 milioni di dollari di riscatti

Luglio 2021

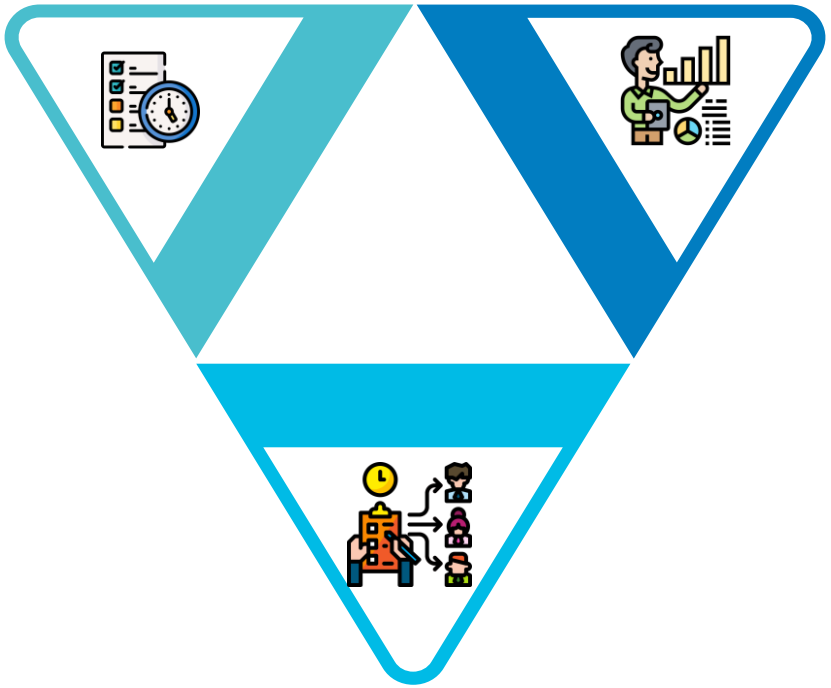
Gli aeroporti di Heathrow, Bruxelles e Berlino Brandeburgo

Un attacco ransomware ai danni di Collins Aerospace, fornitore di sistemi di check-in e imbarco, ha reso inutilizzabili chioschi self-service e terminali automatici per la gestione delle operazioni di check-in, stampa delle carte d'imbarco e bag-drop, causando ritardi, code e cancellazioni in alcuni tra i principali aeroporti europei

Settembre 2025

Aumento dell'esposizione al rischio

Il **40%** delle organizzazioni vede la partecipazione a una **filiera strategica** come fattore che ne aumenta l'esposizione al rischio



Ricorso a un Third Parties Security Manager

Il **40%** delle organizzazioni ha introdotto un **ruolo ad hoc** per la gestione della sicurezza delle terze parti

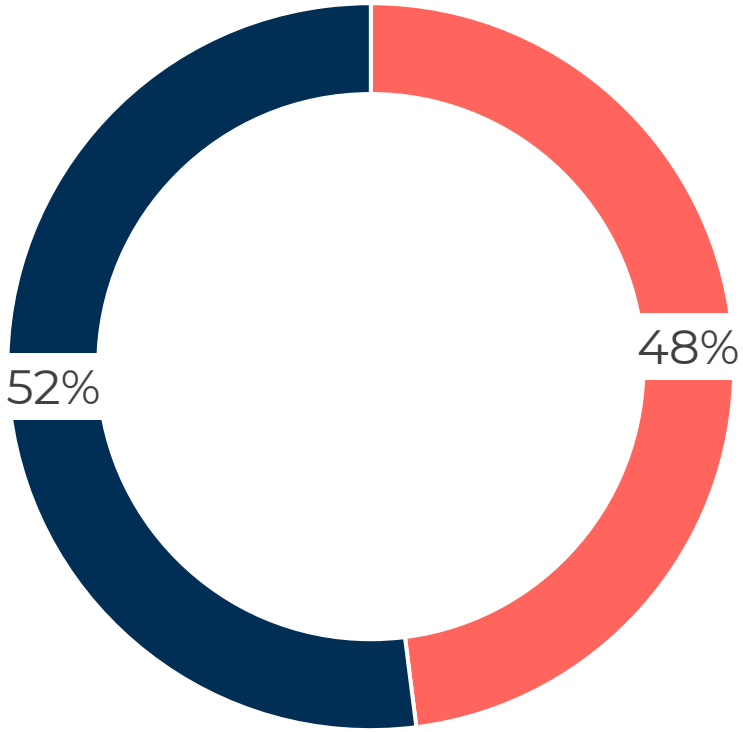
Impatto sul modello di gestione della sicurezza

Il **71%** delle organizzazioni ritiene che il rischio supply chain avrà un **impatto rilevante** sul modello di gestione della cybersecurity nei **prossimi 3 anni**

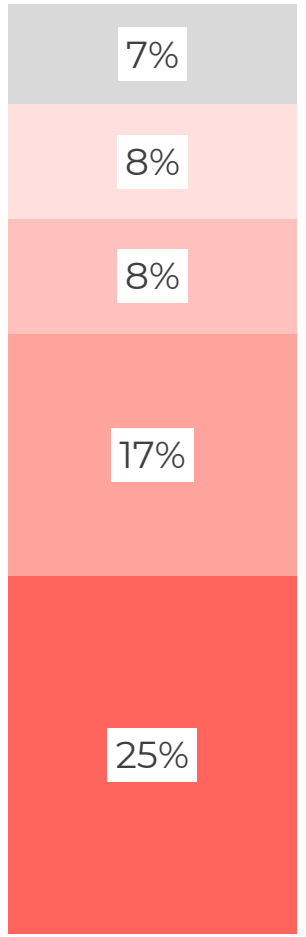
Campione Survey CISO: 112 Grandi Organizzazioni

Il rischio cyber associato alle terze parti nelle PMI

Quota di imprese che partecipa a filiere critiche



- Opera all'interno di filiere critiche
- Non opera all'interno di filiere critiche

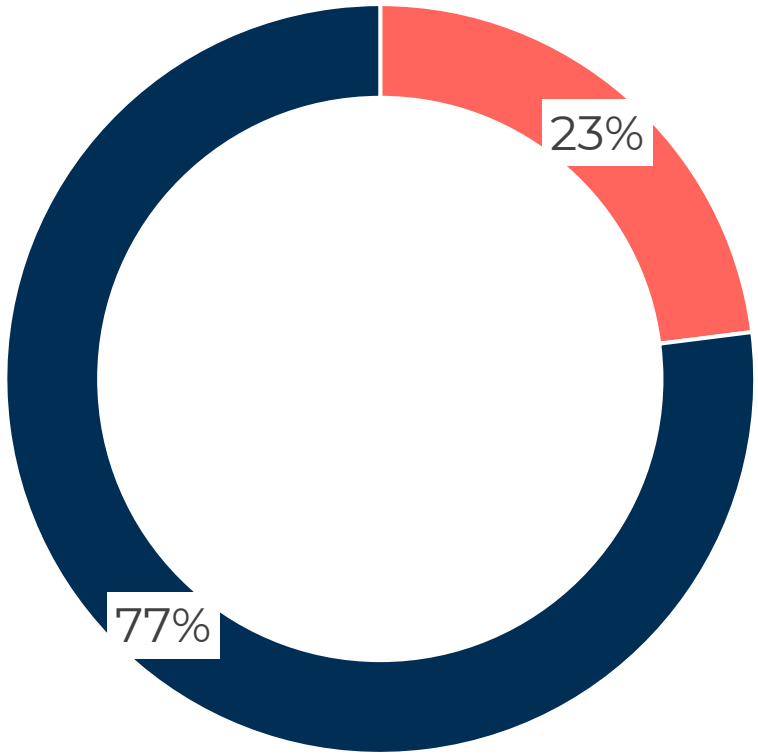


- La filiera si estende in Paesi con instabilità geopolitica
- Sedi e/o impianti all'estero
- Relazioni con infrastrutture critiche
- Relazioni con la Pubblica Amministrazione
- Relazioni con multinazionali o imprese con più di 1.000 addetti

Campione Cyber Index PMI: 1.005 PMI

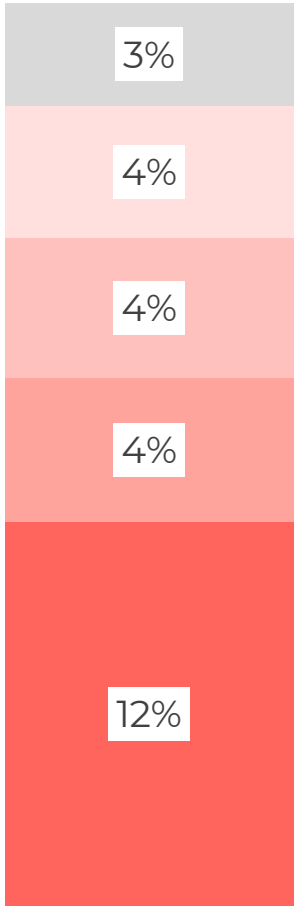
Il rischio cyber associato alle terze parti nelle PMI

Pressioni subite da stakeholders esterni



- Ha subito pressioni
- Non ha subito pressioni

Tipologia di stakeholder

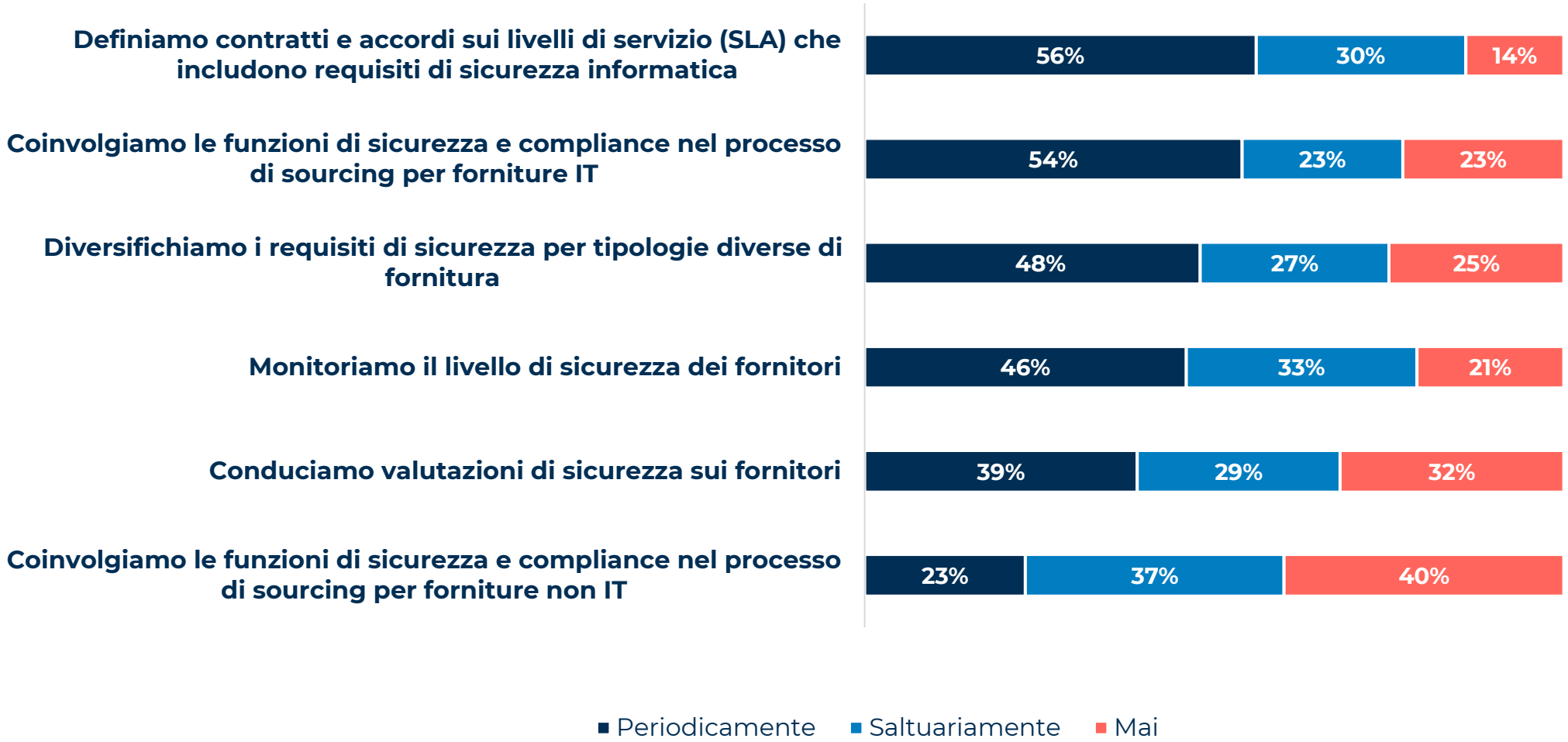


- Organizzazioni governative o regolatorie
- Istituti di credito
- Aziende della filiera
- Dipendenti
- Clienti

Campione Cyber Index PMI: 1.005 PMI

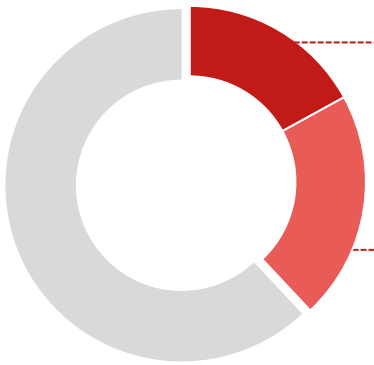
Come fronteggiare il rischio: le azioni messe in campo dalle grandi organizzazioni

Quali azioni stanno mettendo in campo le organizzazioni e con quale frequenza?



Campione Survey CISO: 131 Grandi Organizzazioni

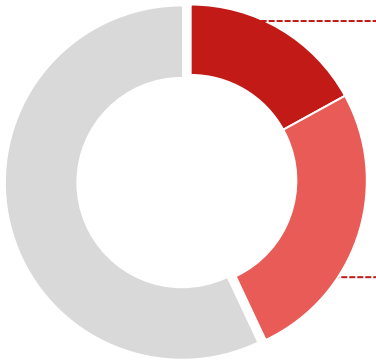
Come fronteggiare il rischio: le azioni messe in campo dalle PMI



17% Monitoriamo periodicamente il livello di sicurezza di tutti i fornitori con cui l'azienda si relaziona

21% Monitoriamo saltuariamente il livello di sicurezza di alcuni fornitori considerati più rilevanti

VALUTAZIONE DELLE TERZE PARTI



17% Definiamo clausole formali per regolamentare responsabilità, accessi, attività di monitoraggio e richiediamo certificazioni a fornitori e partner

26% Non abbiamo definito clausole formali ma richiediamo certificazioni a fornitori e partner

GESTIONE DELLE TERZE PARTI

Agenda

L’Osservatorio Cybersecurity & Data Protection

Il contesto di riferimento per la cybersecurity, tra minacce e spinta normativa

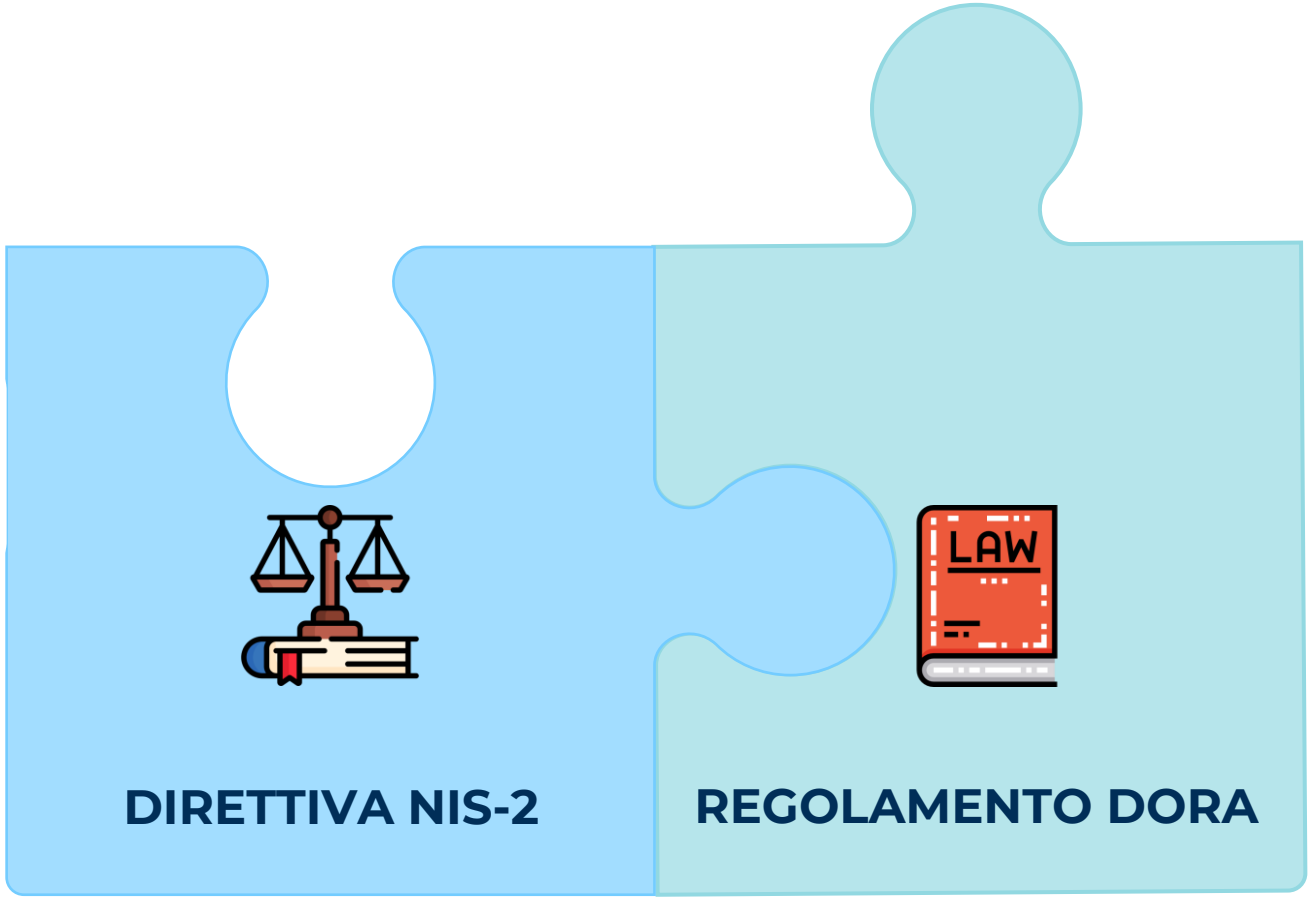
La gestione del rischio cyber associato alle terze parti (il rischio supply chain) nelle organizzazioni

L’evoluzione normativa e le implicazioni sulla gestione delle terze parti (DORA, NIS2, ecc.)

L’evoluzione normativa in ambito cyber

Entrata in vigore a **gennaio 2023**

Recepita in Italia dal **Decreto Legislativo n. 138 del 4 settembre 2024**



Pubblicato in **Gazzetta ufficiale** dell’Unione Europea a **dicembre 2022**

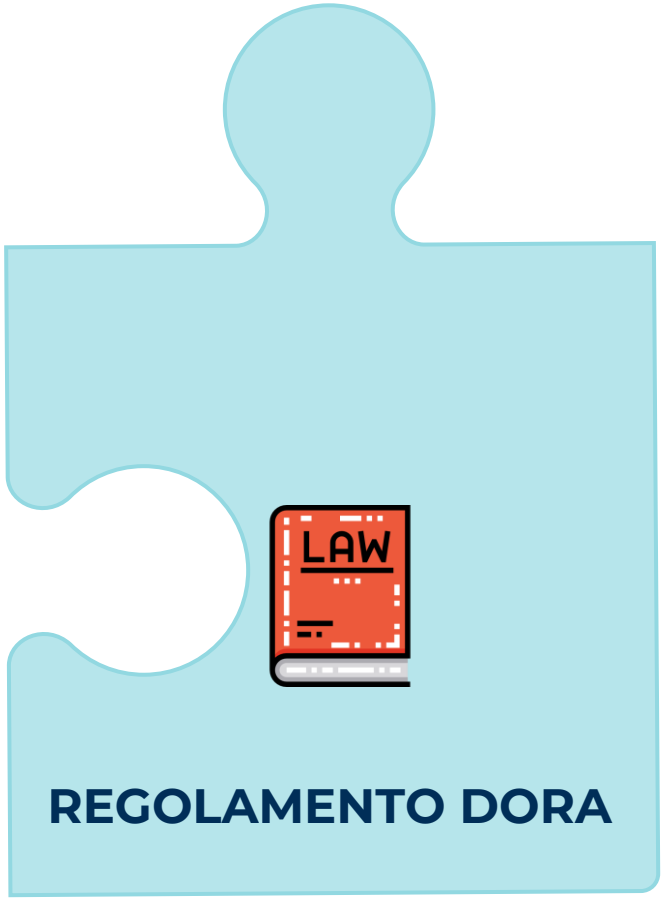
Applicabile dal **17 gennaio 2025**

Il regolamento DORA: implicazioni sulla gestione delle terze parti

Si applica agli **operatori del mondo finanziario** e ai **fornitori di servizi ICT**

Introduce, tra gli altri, gli **obblighi** di:

- Adottare un piano di **governance e organizzazione interna**
- Implementare un piano per la **gestione dei rischi informatici** (anche a livello di filiera)
- Creare appositi **registri informativi** con le informazioni sulle terze parti ICT
- **Classificare gli incidenti** connessi ai fornitori ICT e le minacce informatiche
- **Test di resilienza** (vulnerability assessment, penetration test) **periodici** che coinvolgono anche le terze parti
- Prevedere **protocolli di info-sharing**



WHO

Parlamento Europeo e Consiglio Europeo

WHEN

17 gennaio 2023

WHY

Superare i limiti riscontrati nella NIS1, così da poter garantire un livello comune elevato di cybersicurezza all'interno dell'Unione Europea

WHAT

- **Riduce la discrezionalità** degli Stati Membri;
- **Assicurare uniformità** tra Stati Membri in termini di **misure di sicurezza previste e risorse diponibili alle autorità di controllo;**
- **Rafforzare la condivisione di informazioni** fra Stati Membri

I PUNTI CHIAVE

- **Nuovi soggetti essenziali e importanti**
- **Criterio di dimensionamento**
- **Gestire i rischi** di cybersecurity **nelle catene di approvvigionamento e nelle relazioni con i fornitori**
- **Notifica incidenti per fasi**: preallarme entro 24 ore; notifica entro 72 ore, relazione finale entro 1 mese
- **Sanzioni** definite a discrezione del singolo Stato Membro

Il D. Lgs. 138 di recepimento della NIS 2

WHO

Governo Italiano, ACN

WHEN

Obbligo di registrazione entro il **28 febbraio 2025**

Obblighi di notifica incidenti a partire dal **1° gennaio 2026**

WHY

Recepire la direttiva NIS 2 a livello nazionale

WHAT

- **Notifica degli incidenti** al CSIRT Italia (ACN)
- **Rafforzamento delle misure di difesa cyber con misure tecniche, operative ed organizzative**, come analisi dei rischi, formazione sul tema cyber, uso di MFA, procedure di gestione incidenti, etc.

PUNTI CHIAVE

- **Circa 25mila nuovi soggetti** che si aggiungono a quelli già interessati dalla Direttiva NIS
- **Soggetti essenziali e importanti** per il Paese perché forniscono servizi critici
- **Coinvolte anche le PMI** che risultano **d'importanza strategica** per il **paese** (es. Fornitori di reti pubbliche, identificati ai sensi della Direttiva RCE, unici fornitori di servizi essenziali, fornitori sistemici della catena di approvvigionamento di soggetti essenziali, etc...)
- **Autoregistrazione** al **portale ACN** da parte delle **aziende** che rientrano nei parametri di soggetti **Essenziali ed Importanti**
- **Obblighi di rafforzamento** in **proporzione al Rischio Cyber**

Gli ambiti di applicabilità

DIMENSIONE

- **Medie imprese**
- **Grandi imprese**
- **Piccole e micro imprese solo** se hanno un **ruolo chiave** per la società, l'economia o settori e servizi che **rientrino nell'ambito di applicazione**

SETTORE MERCEOLOGICO

- Gli Operatori di Servizi Essenziali diventano **Soggetti essenziali** (Allegato I)

- **Soggetti importanti** (Allegato II). Sono compresi i Fornitori di Servizi Digitali

TERRITORIALITÀ

- Società che **prestano i loro servizi o svolgono le loro attività all'interno dell'Unione Europea**

Principio di proporzionalità degli obblighi

Più sono critici i settori, maggiori saranno gli obblighi:
Settori altamente critici → obblighi elevati
Settori critici → obblighi intermedi
Settori ordinari → obblighi di base

I settori merceologici coinvolti dal D. Lgs. 138

SETTORI AD ALTA CRITICITÀ

- Energia
- Trasporti
- Settore bancario
- Infrastrutture dei mercati finanziari
- Settore sanitario
- Acqua potabile
- **Acque reflue** NEW
- **Infrastrutture digitali** NEW
- **Gestione dei servizi TIC** NEW
- **Pubblica Amministrazione** NEW
- **Spazio** NEW

NEW SETTORI CRITICI

- Servizi postali e di corriere
- Gestione dei rifiuti
- Fabbricazione produzione e distribuzione di sostanze chimiche
- Produzione, trasformazione e distribuzione di alimenti
- Fabbricazione (dispositivi medici, computer e prodotti di elettronica e ottica, apparecchiature elettriche, macchinari autoveicoli, rimorchi, mezzi di trasporto)
- Fornitori di servizi digitali
- Ricerca

Le fasi della normativa NIS2

RECEPIMENTO (febbraio 23 - metà ottobre 24)	Avvio informale di alcuni tavoli settoriali Adozione definitiva in CDM (7 agosto) **Pubblicazione in Gazzetta Ufficiale (1° ottobre)** **Entrata in vigore (16 ottobre)**
PRIMA FASE ATTUATIVA (metà ottobre 24 – metà aprile 25)	[ACN e Autorità di settore] Avvio formale di tutti i tavoli settoriali **[Soggetti] Censimento e registrazione dei soggetti (entro febbraio 2025)** [ACN e Autorità di settore] **Adozione dell'elenco dei soggetti NIS e notifica (aprile 2025)** [ACN] **Elaborazione e adozione degli obblighi di base (aprile 2025)***
SECONDA FASE ATTUATIVA (metà aprile 25 – metà aprile 26)	[**Soggetti**] **Implementazione obblighi di base (termine per notifiche di incidente 01/2026)** [ACN] Monitoraggio e supporto dell'implementazione obblighi di base [ACN] Elaborazione e adozione del modello di categorizzazione delle attività e dei servizi [ACN] **Elaborazione e adozione degli obblighi a lungo termine (aprile 2026)**
TERZA FASE ATTUATIVA (da metà aprile 26)	[**Soggetti**] **Completamento dell'implementazione obblighi di base (termine per misure di sicurezza 10/2026)** [Soggetti] Categorizzazione delle attività e dei servizi [Soggetti] Implementazione degli obblighi a lungo termine

*La scadenza per completare la trasmissione delle informazioni da parte dei soggetti NIS all'Autorità nazionale competente è stata prorogata dal 31 maggio al 31 luglio 2025

Fonte: Agenzia per la Cybersicurezza Nazionale

La direttiva NIS-2: le implicazioni sulla gestione delle terze parti

NIS2 richiede che le entità coperte **valutino e gestiscano i rischi che possono derivare dall'intera supply chain**, inclusi fornitori di servizi, cloud, hosting, partner IT. L'idea è che anche se la terza parte non è direttamente soggetta alla norma, la sua vulnerabilità può impattare l'ente in scope

Obblighi contrattuali e clausole con fornitori
È previsto che nei contratti con terze parti ci siano clausole che prescrivano requisiti di sicurezza specifici: protezione dei dati, misure tecniche e organizzative, obblighi di reporting, diritto di audit

Monitoraggio e verifica continua
Oltre ad ottenere impegni contrattuali, è richiesto che ci sia un processo per verificare che le terze parti rispettino questi obblighi, tramite audit, controlli, monitoraggio continuo

Mappatura / classificazione di fornitori / terze parti
È necessario identificare le terze parti, classificarle in base al rischio che comportano per l'ente, valutare la loro criticità, complessità, impatto

Obblighi di reporting / obblighi di segnalazione incidenti
Se ci sono incidenti che coinvolgono o sono causati da terze parti, gli enti devono includerli nei loro obblighi di notifica

POLIMI SCHOOL OF MANAGEMENT | osservatori.net digital innovation

02.10.2025

Supply chain e Cybersecurity

Open Innovation Lombardia - Finlombarda