Summary | Tavolo Sicurezza Digitale 2026

Luglio 2026

Agenda

- Introduzione e Aree di Indagine
- Key Points e Insights

Introduzione e Aree di Indagine

Introduzione

La survey condotta da AUSED a maggio 2026, fornisce indicazioni sulla maturità della Cybersecurity in un ampio contesto multisettoriale italiano

Dati partecipanti

Numero Totale

101 Partecipanti totali operanti prevalentemente nel Reparto IT, ma anche Executive e Sales

Posizione Organizzativa

La maggior parte dei partecipanti occupa ruoli C-Level / Executive mentre completano il campione un numero più contenuto di figure junior

Informazioni sulle aziende dei partecipanti

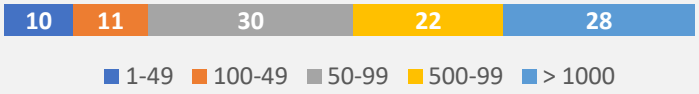
Area Geografica

Area 1: Piemonte, Val d'Aosta, Liguria, Lombardia	*61*
Area 2: Trentino-Alto Adige, Veneto, Friuli-Venezia Giulia, Emilia-Romagna	*28*
Area 3: Toscana, Umbria, Marche, Lazio, Sardegna	*12*

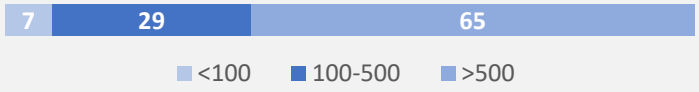
Settore

+10 Settori: Manifattura, Costruzione, Energia, Finanza, Sanità, Trasporto, Commercio, Amministrazione etc.

Fatturato (in Mln di €)



Numero Totale Dipendenti



Aree di Indagine

La survey esplora cinque aree di indagine identificate dal Tavolo AUSED come fattori chiave della maturità organizzativa in Cybersecurity nelle aziende intervistate

INGAGGIO, CONSAPEVOLEZZA E MATURITÀ AZIENDALE

***Consapevolezza** del **personale**, **chiarezza** delle **policy** e **commitment** della **direzione** nel promuovere una cultura della sicurezza*

COMPETENZE ED ORGANIZZAZIONE

Struttura organizzativa** della Cybersecurity, **posizionamento** del **CISO** e **gestione strategica** delle **competenze** e della **formazione

SCELTE TECNOLOGICHE

Maturità nella gestione vendor, integrazione** tra **perimetri** di **sicurezza** e **sistematicità** nella **validazione tecnica delle soluzioni

BUDGET E ASPETTI CONTRATTUALI

***Allocazione** del **budget**, classificazione tra costo operativo e investimento, e **pianificazione** pluriennale supportata da valutazioni economiche*

GOVERNANCE, RISK MANAGEMENT, COMPLIANCE E RESPONSABILITÀ

***Definizione** di **ruoli**, mappatura **delle dipendenze critiche**, **piani di continuità e incident response**, e integrazione tra funzioni*

Key Points e Insights

Ingaggio, Consapevolezza e Maturità Aziendale

Key Points

- La **cybersecurity** è percepita come **tema strategico per continuità operativa, reputazione e resilienza del business**, non più solo come ambito tecnologico
- **La consapevolezza del rischio cyber è in crescita, ma resta spesso teorica:** molte aziende faticano a tradurla in comportamenti sistematici e iniziative continuative
- Solo il **45%** delle organizzazioni **considera la cybersecurity una priorità strategica** supportata da **investimenti dedicati**; un ulteriore **30% ne riconosce l'importanza**, **ma senza risorse adeguate**
- **Le grandi imprese mostrano livelli di maturità superiori:** il 64% delle aziende > €1 mld di fatturato dichiara programmi continuativi di awareness, rispetto al 36% delle realtà più piccole
- **La sensibilizzazione è ancora disomogenea**: accanto a campagne strutturate, microlearning, video formativi e gamification, molte aziende si affidano a interventi occasionali
- **Il fattore umano resta un'area di vulnerabilità:** il 25% dei dipendenti è percepito come poco consapevole e solo il 55% dei test di phishing simulato produce risultati positivi
- **Le policy di sicurezza sono spesso poco efficaci sul piano operativo**: solo circa metà delle aziende dispone di policy formalizzate, aggiornate e facilmente accessibili

Insights

- ❑ **La cultura cyber non** risulta ancora **pienamente integrata** nei comportamenti quotidiani e **nelle decisioni manageriali** della maggior parte delle aziende coinvolte
- ❑ **Il principale gap** riguarda la **capacità di rendere la cybersecurity sistematica, misurabile e continuativa**, superando un approccio ancora episodico alla formazione e alla sensibilizzazione
- ❑ **La maturità cyber dipende** sempre meno dalla sola tecnologia e sempre più dalla **capacità di coinvolgere in modo continuativo persone**, **management e funzioni aziendali**

Competenze ed Organizzazione

Key Points

- È emersa una **maturità in crescita sul piano tecnologico**, ma resta caratterizzata da criticità organizzative e di sviluppo delle competenze
- **La governance cyber è ancora largamente centralizzata e dipendente dall'IT:** circa il 55% delle organizzazioni affida la gestione della cybersecurity alla capogruppo
- **Solo il 20% delle aziende opera con un modello autonomo supportato da linee guida comuni,** confermando una forte concentrazione delle responsabilità cyber a livello corporate
- Il **modello operativo** prevalente è **misto**: circa il **50% delle aziende combina risorse interne** e **servizi esternalizzati**
- **Nelle iniziative di OT Security, la governance è affidata prevalentemente all'IT**, circa nel 55% dei casi, evidenziando una **limitata integrazione tra funzioni ICT e Operations**
- **Il ruolo del CISO/Security Manager risulta ancora spesso collocato all'interno dell'organizzazione IT** e non sempre dotato di autonomia e visibilità coerenti con la rilevanza strategica della cybersecurity
- La formazione continua resta poco strutturata: il **55% delle aziende utilizza formazione spot**, circa il 25% percorsi di breve termine e solo il 20% programmi strutturati su orizzonti di 1-2 anni
- **Le certificazioni professionali sono ancora poco valorizzate**: l'81% delle aziende non richiede certificazioni specifiche ai professionisti cyber

Insights

- ❑ La **cybersecurity** spesso **ancora considerata come funzione operativa** da gestire, più che come capacità strategica da sviluppare
- ❑ **La centralizzazione a livello corporate favorisce standardizzazione e controllo**, ma può limitare la rapidità di risposta a minacce o esigenze locali
- ❑ **Il gap principale è nella gestione delle competenze** con formazione spot, e scarso ricorso alle certificazioni rendono difficile costruire capacità cyber solide
- ❑ Con l'aumentare della complessità aziendale, il **CISO evolve da figura tecnica a ruolo multidisciplinare**, con responsabilità di business, compliance, ICT e security

Scelte Tecnologiche

Key Points

- **Le aziende** adottano molti strumenti cyber, ma **non sempre dispongono di una vera architettura integrata e interoperabile**
- **La difesa cyber è spesso costruita** come una collezione di prodotti acquistati **per esigenze contingenti, più che come un sistema coerente e governato**
- **Il portafoglio vendor risulta ancora frammentato**: il 46% delle aziende non ha una strategia di consolidamento o si limita a censimenti sporadici dei tool
- **Solo il 6% monitora il portafoglio tecnologico** con KPI di efficienza e revisione continua
- **Il 42% delle aziende gestisce ancora i perimetri IT, OT, Web e Marketing come silos** o con una condivisione dei log solo embrionale
- **La mappatura delle competenze interne guida raramente le scelte tecnologiche**: il 58% sceglie la tecnologia per funzionalità, valutando le competenze solo dopo l'acquisto o formando in modo reattivo
- **La selezione delle soluzioni resta spesso "sulla carta"**: il 53% sceglie su brand, prezzo, requisiti dichiarati o demo non strutturate.
- **Solo il 7% testa le soluzioni in ambiente reale o controllato** tramite Red Teaming, penetration test o metriche di efficacia
- **L'interoperabilità è ancora trattata come opzionale**: solo il 12% rende le API aperte un requisito mandatorio e bloccante

Insights

- ❑ **Molte organizzazioni** acquistano tecnologia di sicurezza, ma **non progettano ancora la difesa cyber come architettura coerente, misurata e sostenibile**
- ❑ **La frammentazione dei vendor e dei perimetri aumenta la complessità operativa** e rischia di ridurre l'efficacia complessiva della protezione
- ❑ **Il gap principale riguarda l'allineamento tra tecnologia, competenze e capacità operative**: strumenti avanzati non generano valore se non sono realmente gestibili dai team
- ❑ **La validazione tecnica resta debole**: senza test in ambiente reale, le aziende rischiano di selezionare soluzioni efficaci "sulla carta" ma non adeguate al proprio contesto operativo

Budget e Aspetti Contrattuali

Key Points

- **Le aziende riconoscono l'importanza della cybersecurity**, ma **faticano a tradurla in modelli economici e contrattuali maturi**
- **La spesa cyber resta contenuta**: la maggioranza investe tra 0,1% e 0,5% del fatturato, con prevalenza della fascia 0,1–0,2%
- **Molte organizzazioni**, soprattutto PMI, **hanno bassa confidenza sulla spesa effettiva**, segnale di scarsa tracciabilità e governance finanziaria
- **Il budget è spesso allocato per inerzia o in modo reattivo**, **guidato da urgenze**, **audit o incidenti**, più che da priorità di rischio condivise
- **La spesa ricade prevalentemente in Opex**, risultando più esposta a rinegoziazioni annuali e alla percezione di costo da contenere
- **La pianificazione resta limitata** con circa il 45% definisce la spesa solo annualmente, mentre solo il 29% la collega a roadmap pluriennali di rischio
- **Le valutazioni economiche sono deboli**: il 40% stima l'impatto solo qualitativamente e il 35% non basa le decisioni su valutazioni economiche
- **L'85% non dispone di KPI strutturati** per misurare e controllare la spesa cyber
- **I presidi contrattuali risultano ancora parziali** con circa il 50% che include SLA, obblighi e supporto incident solo per parte dei fornitori rilevanti
- **Il 40% copre contrattualmente meno della metà dei fornitori critici** e il 45% ha solo avviato la mappatura delle dipendenze critiche

Insights

- ❑ **Il tema centrale non è solo quanto si spende, ma come la spesa cyber viene governata,** giustificata**, pianificata** e **raccontata al vertice aziendale**
- ❑ **La cybersecurity resta spesso percepita come costo operativo ricorrente,** più che come portafoglio di investimenti governati e collegati a priorità di rischio
- ❑ L'assenza di classificazione della spesa, KPI e modelli quantitativi rende **difficile costruire business case solidi e difendere gli investimenti davanti a CFO e CdA**
- ❑ **La fragilità contrattuale** e la **limitata copertura dei fornitori critici amplificano il rischio**, soprattutto in uno scenario regolatorio in cui cresce la responsabilità sulla supply chain

Governance, Risk Management, Compliance e Responsabilità

Key Points

- **La governance cyber mostra un divario tra consapevolezza e operatività**: piani, ruoli e presidi esistono, ma non sempre sono verificati o pienamente attuati
- **Solo il 26% delle organizzazioni ha raggiunto una maturità operativa nella definizione di ruoli e responsabilità** tra funzioni chiave
- Il **50% delle aziende non ha ancora avviato iniziative strutturate sulla definizione di ruoli e responsabilità** tra IT, OT, CISO e Business
- **La mappatura delle dipendenze critiche è ancora limitata**: solo il 17% delle aziende l'ha implementata o ottimizzata, mentre il 57% è in fase iniziale o non ha avviato attività
- **L'Incident Response Plan esiste nel 76% delle organizzazioni**, ma è stato testato solo nel 45% dei casi e condiviso con il management nel 54%
- **Il Business Continuity Plan è presente nell'84% delle organizzazioni**, ma risulta testato solo nel 38% dei casi
- **Il 74% delle aziende dichiara di avere una catena decisionale formalizzata per la gestione degli incidenti gravi**, ma **spesso non** è **esercitata né condivisa con** le funzioni **business** non-IT
- **La gestione dei fornitori critici resta parziale** con il 53% delle aziende che copre meno della metà dei fornitori critici o non ha previsto obblighi contrattuali specifici
- **Solo il 17% ha contratti strutturati** con obblighi chiari, SLA e supporto operativo su tutti o quasi tutti i fornitori rilevanti

Insights

- La governance cyber delle aziende partecipanti appare in una **fase di transizione**: molti presidi non sono ancora tradotti in capacità operative realmente verificabili
- **Il principale gap riguarda il passaggio da "piano esistente" a piano esercitato:** IRP e BCP non testati generano un falso senso di sicurezza in caso di crisi reale
- **L'incertezza su ruoli, responsabilità e catena decisionale può rallentare la risposta agli incidenti**, soprattutto quando devono essere coinvolte funzioni IT, OT, CISO, Business e management
- Senza mappatura delle dipendenze e contratti strutturati, i **fornitori critici** rischiano di **non** essere realmente **governabili durante un incidente**