AZIENDA OSPEDALIERO UNIVERSITARIA PISANA

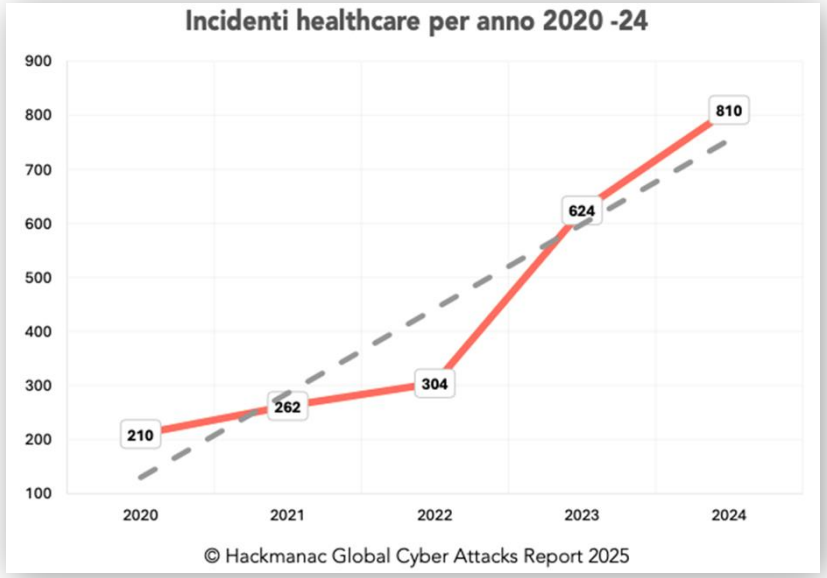
SST Azienda USL Toscana nord ovest
Servizio Sanitario della Toscana

La consapevolezza degli operatori delle aziende USL Toscana Nord-Ovest e Azienda Ospedaliera Universitaria Pisana (AOUP) in materia di cyber-sicurezza

Alessandro Stefanini - alessandro.stefanini@unipi.it*
Ettore Pieruccini - ettore.pieruccini@phd.unipi.it*
Davide Aloini, Elisabetta Benevento, Federico Niccolini, Gianluca Dini, Martina Neri

Il presente lavoro è stato finanziato dall'Università di Pisa per mezzo dei fondi «PRA – Progetti di Ricerca di Ateneo» – n. Progetto PRA_2022_87, dal Titolo «Valutazione della Consapevolezza e della Preparazione alla Cyber-sicurity nel settore sanitario.

Introduzione



Negli ultimi anni, si è registrato un aumento per **numero** e **severità** degli attacchi hacker nel settore sanitario, in Italia e nel Mondo.

***Perché** il settore sanitario è particolarmente bersagiato?*

- Alto valore dei dati sanitari
- Propensione a pagare i riscatti
- Vulnerabilità dei sistemi digitalizzati
- Scarsa formazione del personale

Come prevenire gli attacchi informatici?

Sono **due** le risorse principali per affrontare il tema della sicurezza informatica sul luogo di lavoro:

Sistemi informatici

Operatori Aziendali

Come prevenire gli attacchi informatici?

Sono **due** le risorse principali per affrontare il tema della sicurezza informatica sul luogo di lavoro:

Sistemi informatici

Operatori Aziendali

OBIETTIVO DELLA RICERCA

Investigare la **consapevolezza** degli operatori sanitari in materia di **cyber-sicurezza.**

*Come è stata concettualizzata la **consapevolezza** degli operatori riguardo al tema della sicurezza informatica?*

Attraverso la relazione tra la loro **conoscenza** e il loro **comportamento**, suddivisi secondo 5 aree di analisi:

- **Gestione delle Password**
- **Utilizzo di Internet e delle email**
- **Gestione dei dispositivi personali**
- **Identificazione e Gestione degli incidenti informatici**
- **Gestione dei dati**

Metodologia di raccolta dati

Per investigare, quindi, la conoscenza e il comportamento degli operatori sanitari in materia di cyber-sicurezza, è stato distribuito un **questionario a risposta multipla** a tutti i lavoratori delle due organizzazioni sanitarie in analisi.

- Composto da **41 domande**
- Distribuito **via mail** a tutti gli operatori di USL TNO e AOUP
- **1363 risposte complete** registrate
- Partecipazione degli operatori su base **volontaria**
- Tasso di risposta pari a circa il 10% per entrambe le organizzazioni
- **Privacy** dei rispondenti garantita
- Il **campione** di rispondenti riflette in modo **coerente la composizione demografica** dell'azienda e del settore sanitario

Analisi qualitativa delle risposte: Gestione delle Password

In generale, gli operatori mostrano **buone pratiche di cybersecurity nella gestione delle password**, diversificandole tra i vari account e mantenendole nascoste, senza condividerle con amici, parenti o colleghi.

La principale criticità emersa è legata alla memorizzazione delle password: molti operatori le tengono **annotate su supporti cartacei**, facilmente accessibili a terzi non autorizzati.

Analisi qualitativa delle risposte: Uso di Internet e delle email

Gli operatori hanno mostrato **buone pratiche** e consapevolezza **nella gestione di email e navigazione web**, dichiarando di controllare i mittenti delle email lavorative ricevute, e di verificare la sicurezza e autenticità dei siti web che navigano durante le attività lavorative.

Non tutti riconoscono a pieno quanto sia rischioso per la sicurezza dei dati interni all'organizzazione **accedere agli account di lavoro tramite reti esterne** non sicure.

Analisi qualitativa delle risposte: Gestione dei dispositivi personali

La maggior parte degli operatori utilizza i **dispositivi aziendali per svolgere attività lavorative**, come scambio di email, accesso agli account lavorativi, e navigazione sui siti web aziendali.

La criticità principale risiede nella consapevolezza ancora parziale dei rischi legati all'uso improprio di **dispositivi personali per lo scambio di dati e informazioni aziendali**.

Analisi qualitativa delle risposte: Gestione degli incidenti informatici

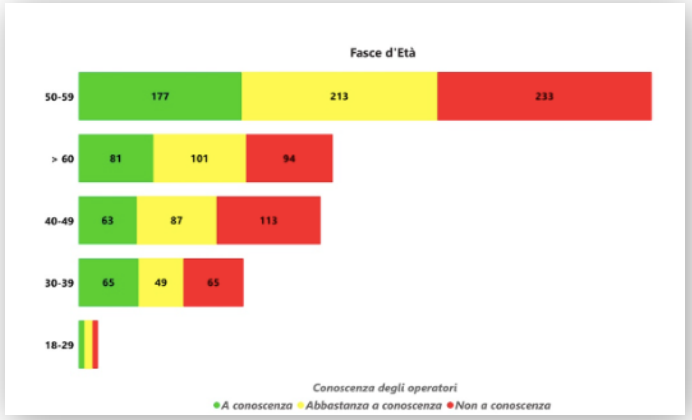
La maggior parte dei rispondenti **non** è **in grado di riconoscere un incidente informatico** e non conosce le procedure aziendali per gestirlo o segnalarlo correttamente.

Analisi qualitativa delle risposte: Gestione di dati e informazioni

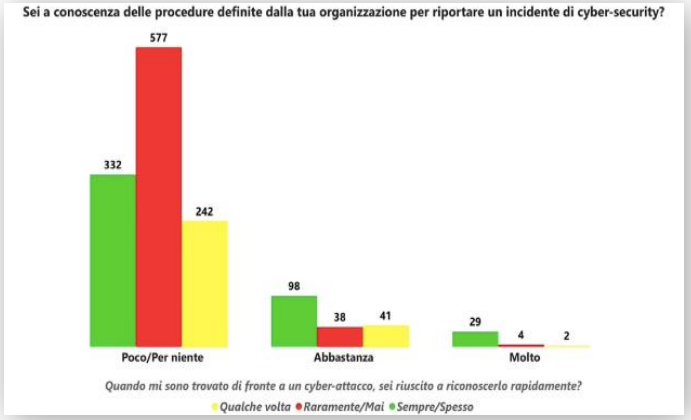
Gli operatori mostrano buone pratiche e consapevolezza nella gestione dei **dati sensibili** condivisi in azienda, sia in termini di comportamento che di conoscenza delle corrette procedure per la loro **protezione**, **salvataggio** e **trasferimento**.

Risultati più rilevanti

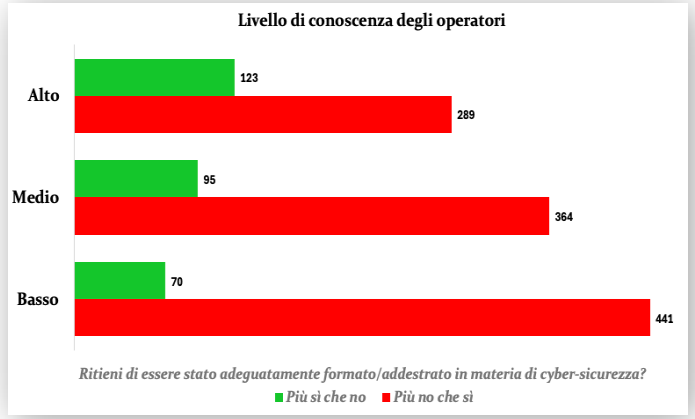
Dall'analisi incrociata delle risposte emergono tre evidenze principali:



Il profilo demografico non influisce sulla consapevolezza: conoscenze e comportamenti in materia di sicurezza informatica risultano omogenei tra età, genere, ruolo, anzianità e titolo di studio.

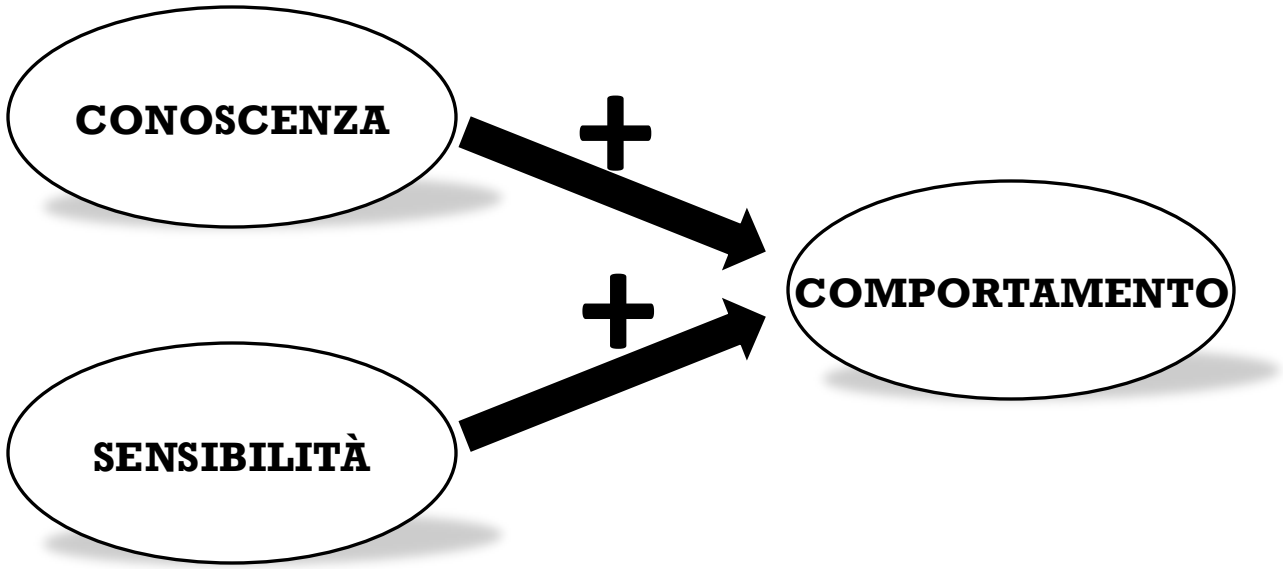


La formazione aziendale mostra un impatto positivo, poiché chi possiede maggiori conoscenze in ambito cyber dichiara di aver ricevuto una formazione adeguata.



Gli **operatori non riconoscono né sanno gestire un attacco informatico**. Sarebbe utile potenziare la formazione sulla gestione degli incidenti informatici per rafforzare la resilienza aziendale.

Risultati più rilevanti



L'analisi di *regressione lineare* fatta sulle risposte ha dato luce alle seguenti evidenze:

- Gli operatori con **maggiori conoscenze** sui cyber-rischi mostrano anche **comportamenti più sicuri** nelle pratiche quotidiane.
- Questo risultato conferma che **conoscenza e comportamento sono strettamente collegati**, evidenza spesso discussa ma raramente dimostrata con dati empirici.
- Inoltre, tra operatori con lo stesso livello di conoscenza, **chi** si dichiara **più sensibile** e attento al tema della sicurezza informatica **presenta comportamenti più sicuri**.

Conclusioni

- Complessivamente, è stato rilevato un **buon livello di consapevolezza degli operatori** circa i rischi informatici aziendali: gli operatori si sono dimostrati attenti e interessati alla problematica.

- L'area di interesse più **critica** per la cyber-sicurezza dell'organizzazione è la **gestione degli incidenti informatici**: la scarsa preparazione in materia impatta la vulnerabilità informatica azindale.

- Gli operatori dichiarano un forte interesse per migliorare la loro preparazione in materia di cyber-sicurezza. Un percorso di **formazione** mirato risulterebbe adegato **per tutti gli operatori**, indipendentemente da età, ruolo, e livello di istruzione.

- Gli **operatori più sensibili** al tema della sicurezza informatica, a parità di livello di conoscenza, tendono a **performare in maniera più cyber-sicura**.

AZIENDA OSPEDALIERO UNIVERSITARIA PISANA

SST Azienda USL Toscana nord ovest
Servizio Sanitario della Toscana

La consapevolezza degli operatori tecnico-sanitari delle aziende USL Toscana Nord-Ovest e Azienda Ospedaliera Universitaria Pisana (AOUP) in materia di cyber-sicurezza

GRAZIE PER L'ATTENZIONE!