Rapporto sulla Ricerca

Educazione alla sicurezza delle informazioni per le PMI - Liberare il potenziale, aumentare la consapevolezza

Funded by the Erasmus+ Programme of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

Numero del progetto: 2018-1-EN02-KA202-005218

Contenuti

1 Introduzione: Certificazione parziale nella sicurezza delle informazioni

La sicurezza delle informazioni è aumentata notevolmente di importanza negli ultimi anni. Con un'ondata di violazioni di dati, aziende tenute in ostaggio da attacchi malware a livello internazionale e l'uso strategico della guerra informatica come mezzo per estendere il potere politico in sfere straniere, la digitalizzazione non è più percepita solo come una soluzione di riscatto per le aziende in difficoltà, ma anche come una fonte vitale di rischio che merita vaste misure di protezione. I rischi sorgono in molti contesti, ma possono essere radicati in due ambiti: sul sito e cibernetico.

Sono necessari approcci olistici per affrontare la situazione di minaccia esistente e crescente. Di fronte a scenari di rischio diffusi e intangibili, gli individui, sia in ambito privato che aziendale, tendono a deprezzare l'importanza della rilevazione del rischio di sicurezza delle informazioni come mezzo di governance e gestione continua. Per ovviare a questa ampia mancanza di consapevolezza, che si trasmette dalla sfera pubblica al mondo aziendale, è necessario adottare misure di sensibilizzazione e formazione. Nel frattempo, le aziende hanno bisogno di capire come possono affrontare il tema della sicurezza delle informazioni con una strategia personalizzata, che si adatti alle proprie esigenze e al proprio budget. Per sostenere le aziende in questa sfida è stato condotto lo studio "Information Security Education for SMEs". Lo studio si è posto l'obiettivo di far luce sui bisogni di formazione e di personale delle PMI per trovare soluzioni alla persistente mancanza di lavoratori qualificati.

Il sottotitolo "Sbloccare il potenziale, aumentare la consapevolezza" fornisce quindi un suggerimento riguardo alla risorsa più importante: il personale presente nelle PMI. Molti dipendenti possiedono competenze e conoscenze acquisite nel corso della loro carriera, di cui spesso non sono nemmeno consapevoli. Infatti, l'acquisizione di apprendimenti non formali e informali, specialmente nei settori guidati dalla tecnologia e dall'innovazione, come la sicurezza dell'informazione, forniscono una ricchezza di risorse che possono essere raccolte attraverso la validazione e il riconoscimento delle competenze. Per facilitare il processo di riconoscimento, il team del progetto TeBeISi ha sviluppato unità di apprendimento e, con il supporto della presente indagine, fornisce strumenti e mezzi alle PMI per identificare i dipendenti adatti a assumere nuove responsabilità nel campo della sicurezza informatica.

Il progetto TeBeISi si sforza di contribuire alla pratica aziendale e di rispettare la realtà quotidiana delle PMI di tutta l'UE. Questo studio approfondisce la comprensione dei decisori, dei reclutatori e degli individui interessati nel campo della sicurezza delle informazioni e lo sviluppo delle risorse e dei requisiti della sicurezza delle informazioni e del personale di sicurezza delle informazioni nelle PMI. Per raggiungere questo obiettivo, lo studio è strutturato come segue: il capitolo due fornisce una panoramica sulla ricerca esistente sulla sicurezza delle informazioni nelle PMI e sui requisiti del personale, il capitolo tre fornisce il background della metodologia di ricerca TeBeISi e il contesto in cui questo studio è stato progettato, il capitolo 4 presenta i risultati del questionario quantitativo, il capitolo cinque illustra brevemente le linee guida più importanti per le PMI e, infine, il capitolo sei conclude con una prospettiva sugli sviluppi futuri.

2 Rassegna della letteratura

L'utilizzo dei sistemi informativi e delle tecnologie dell'informazione è diventato un prerequisito per il successo delle imprese in tutti i settori economici. Senza la tecnologia dell'informazione, lavorare con le informazioni non è solo inefficace ma anche impossibile (Hallová et al. 2019). Inoltre, la nostra dipendenza da questi sistemi aumenta ogni giorno. Tuttavia, con il rapido sviluppo delle moderne tecnologie e dei sistemi informativi, aumenta anche il potenziale di abuso (Smith, 2003; Leede et al., 2005; Kumar et al., 2011).

Nel mondo di oggi, in cui tutti gli individui e le aziende dipendono dalle tecnologie dell'informazione, la sicurezza delle informazioni e la protezione dei dati sono elementi importanti che richiedono particolare attenzione. A questo proposito, la direttiva dell'Unione Europea (UE) riguardante le misure per un elevato livello comune di sicurezza delle reti e dei sistemi informativi in tutta l'Unione e il regolamento generale sulla protezione dei dati (Kogenhop, 2020) sono fattori importanti. L'iniziativa normativa della Commissione europea riflette l'accresciuta necessità di una guida legislativa, poiché i rapidi sviluppi tecnologici e la globalizzazione hanno creato nuove sfide per la protezione dei dati e delle informazioni personali (Wilkinson, 2018).

Negli ultimi anni, nuove forme di tecnologia dell'informazione (ad esempio, sensori e dispositivi mobili) hanno drammaticamente ampliato ciò che può essere misurato e analizzato, ponendo sfide completamente nuove per la sicurezza e la privacy (Weber, 2010; Newell & Marabelli, 2015; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Lee, Cho & Lim, 2018). La possibilità che i clienti siano colpiti da problemi di sicurezza e privacy legati ai sistemi informativi rende queste sfide centrali per i professionisti del business (Sicari et al., 2015; Sicari et al., 2016). D'altra parte, i manager delle organizzazioni hanno bisogno di utilizzare i nuovi strumenti informatici per archiviare non solo i dati personali ma anche quelli riservati per rimanere competitivi nel 21° secolo. Nel frattempo, l'archiviazione dei dati su carta è obsoleta a causa del potenziale dell'archiviazione elettronica dei dati, le organizzazioni stanno adottando rapidamente le nuove tecnologie e l'archiviazione elettronica è diventata comune in molti paesi (McAfee, 2010).

La tendenza crescente verso l'archiviazione dei dati in formato elettronico, così come la crescente connettività di internet e la conseguente esposizione ai criminali informatici, ha portato allo sviluppo di requisiti specifici di protezione dei dati (McAfee, 2010). Le tecnologie di archiviazione dei dati devono avere misure di protezione dei dati e gli utenti che lavorano con i dati devono essere formati per capire i rischi di fuga di dati aziendali a persone non autorizzate. I leader delle organizzazioni devono essere consapevoli delle gravi conseguenze delle fughe di dati elettronici. Così come gli impiegati che non rispettano la sicurezza delle informazioni (Siponen, Mahmood & Pahnila, 2009), i manager delle organizzazioni che sono negligenti nell'acquisizione e gestione dei dati elettronici espongono le loro aziende a rischi e minacce (Northhouse, 2010). I manager devono esercitare attenzione e capacità di autocontrollo al fine di favorire l'azienda, soprattutto in termini di sicurezza dei dati (Guinote & Vescio, 2010). Una delle sfide chiave nella gestione della sicurezza delle informazioni è capire come i fattori organizzativi, individuali e tecnici si combinano per influenzare i risultati della sicurezza delle informazioni in un'organizzazione (Wilkinson, 2018).

Recenti ricerche mostrano che in molti casi, la fuga di dati elettronici nelle piccole aziende è il risultato di una inadeguate leadership e pratiche di gestione. I manager nelle

organizzazioni
prendono le decisioni più importanti e se i manager non affrontano adeguatamente le questioni informatiche, minacciano la sopravvivenza dell'azienda (Davies & Hertig, 2008). Un possibile fattore mitigante è stato proposto da Noguerol und Branch (2018), sostenendo che i manager aziendali possono influenzare positivamente il comportamento dei dipendenti nell'area della sicurezza dei dati favorendo un ambiente di lavoro sano e promuovendo le relazioni interpersonali.

Le aziende di tutte le dimensioni in tutto il mondo soffrono di una mancanza di sicurezza informatica, e molte di esse sono esposte alla criminalità informatica. Tuttavia, la fuga di dati elettronici è una preoccupazione soprattutto per le piccole imprese. Tra l'altro, le PMI hanno vincoli finanziari, manager a volte inefficaci, e una mancanza di attenzione ai dettagli che non sono direttamente legati al business (O'Rourke, 2003; Adamkiewicz, 2005; Goodwin, 2005; Baker & Wallace, 2007).

Nonostante la crescente minaccia di incidenti informatici dall'esterno, i dipendenti rimangono la principale causa di incidenti di sicurezza (Richardson, 2008; PwC, 2017). Le risorse umane all'interno dell'organizzazione possono essere più pericolose di quelle esterne all'organizzazione perché hanno familiarità con i sistemi informativi dell'organizzazione e accedono ai dati attraverso le loro normali attività lavorative (Herath & Rao, 2009a, 2009b; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Siponen & Vance, 2010). Le politiche di protezione delle informazioni dovrebbero garantire la sicurezza delle informazioni (Bulgurcu, Cavusoglu, & Benbasat, 2010), ma la ricerca mostra che molti incidenti di sicurezza sono causati da dipendenti che ignorano o non sono consapevoli delle politiche di sicurezza (Willison & Warkentin 2013, Path to Cyber Resilience, 2016).

Ricercatori e professionisti considerano sempre più la sicurezza informatica dei sistemi organizzativi come una questione socio-tecnica, che richiede approcci non solo tecnici ma anche manageriali (Burns, Roberts, Posey, Bennett, & Courtney, 2018). A causa dell'uso diffuso delle tecnologie informatiche nelle aziende, ai dipendenti viene spesso affidato l'accesso continuo alle informazioni e ai sistemi informativi aziendali per svolgere i propri compiti lavorativi. Nonostante questa maggiore flessibilità operativa, le organizzazioni sono meno in grado di monitorare il comportamento dei dipendenti con accesso a dati riservati (Herath & Rao, 2009). Pertanto, al fine di migliorare la protezione del prezioso patrimonio informativo delle organizzazioni nel contesto della proliferazione della tecnologia, la formazione preventiva dei dipendenti in materia di sicurezza delle informazioni è fondamentale per la sicurezza informatica delle organizzazioni (von Solms & von Solms, 2009; D'Arcy, Hovav & Galletta, 2009; Albrechtsen & Hovden, 2010; Puhakainen & Siponen, 2010; Karjalainen & Sipo-nen, 2011; Posey, Roberts, Lowry, Bennett & Courtney, 2013). La ricerca mostra che le organizzazioni identificano i programmi di sensibilizzazione dei dipendenti come una priorità assoluta nei loro budget per la sicurezza delle informazioni (PWC, 2015), e i dirigenti della sicurezza delle informazioni affermano che la formazione dei dipendenti è una delle attività più importanti necessarie per attuare una strategia di successo per la sicurezza delle informazioni e dei dati (van Zadelhoff, Lovejoy & Jarvis, 2014).Employee training is the most effective non-technical means of ensuring information security in organisations and preventing employees from disclosing sensitive information to unauthorised parties (Colwill, 2009; Peikari, Shah, & Lo, 2018).

La formazione può aumentare la conoscenza e la consapevolezza dei dipendenti delle minacce e delle conseguenze di una violazione della sicurezza e aiutare a prevenire tali incidenti (Kluge, 2007; D'Arcy Hovav & Galletta, 2009).

L'istruzione e la formazione dei dipendenti è un mezzo per le imprese per ridurre il rischio di violazioni della sicurezza interna (Burns, Roberts, Posey, Bennett & Courtney, 2015; Barlow, Warkentin, Ormond, & Dennis, 2018). È un prerequisito importante e ha un impatto positivo sul comportamento di sicurezza delle informazioni. Programmi di formazione dei dipendenti ben progettati possono contribuire a ridurre i rischi di sicurezza delle informazioni per un'azienda (Anderson & Agarwal, 2010; Liang & Xue, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; Johnston & Warkentin, 2010; Whitman & Mattord, 2012; Jenkins & Durcikova, 2013; Johnston, Warkentin & Siponen, 2015). Secondo i ricercatori (Gardner & Thomas, 2014; Posey, Roberts & Lowry, 2015), l'istruzione e la formazione continua dei dipendenti in materia di sicurezza dei dati e delle informazioni è un modo efficace per orientare il loro comportamento in materia di sicurezza delle informazioni e al rispetto delle politiche di sicurezza delle informazioni dell'organizzazione. I dipendenti con un'adeguata conoscenza della sicurezza delle informazioni sono in grado di prevenire minacce e attacchi, con conseguente aumento della riservatezza, integrità e disponibilità delle informazioni all'interno dell'organizzazione (Sabeeh & Lashkari, 2011). Si nota che a causa della natura dinamica delle minacce alla sicurezza delle informazioni e delle vulnerabilità, la formazione e l'istruzione dei dipendenti dovrebbero essere una pratica regolare e continua in un'organizzazione (Yoo et al., 2018; McConnell, 2020).

Mentre il trattamento dei dati personali è inevitabile per molte PMI, spesso non è il loro core business e non hanno sufficienti risorse umane o finanziarie per assicurare una corretta conformità. In particolare, le PMI non sono preparate ad adottare misure di sicurezza delle informazioni semplicemente perché non sono tenute ad avere una sicurezza delle informazioni documentata a causa delle loro piccole dimensioni (Kuusisto, & Ilvonen, 2003; Doherty, & Fulford, 2005). Le PMI sono per lo più consapevoli del GDPR, ma non hanno le risorse per conformarsi ai requisiti; non hanno la capacità organizzativa per implementare i requisiti del GDPR e la sicurezza delle informazioni all'interno della loro organizzazione. Le sfide più comuni per la protezione dei dati e la sicurezza delle informazioni affrontate dalle PMI includono: capire quali cambiamenti devono essere fatti per conformarsi; progettare e sviluppare nuovi processi e procedure relative al trattamento dei dati personali; la cultura del personale sull'importanza della protezione dei dati. Nonostante i numerosi pareri e linee guida sul GDPR emessi dalle autorità di regolamentazione e dagli esperti di protezione dei dati, manca una guida pratica, facile da capire e mirata per le PMI su come attuare la legislazione sulla protezione dei dati nella pratica (Jasmontaitė-Zaniewicz, Calvi, Nagy & Barnard-Wills, 2021). Si sottolinea che in particolare le PMI attualizzano la necessità di una formazione e di una consulenza mirata e specifica per il settore, basata su esempi e casi di studio che riflettono le specificità di queste organizzazioni (Barnard-Wills, Cochrane, Matturi, & Marchetti, 2019).

3 TeBeISi – Metodo ed Approccio

La sicurezza delle informazioni nelle PMI, per ora, è un argomento poco studiato e non si sa molto sulle esigenze e i requisiti delle PMI in tutta l'UE. Nel frattempo, gli obblighi legislativi sulla protezione dei dati (GDPR) hanno portato a un rapido aumento delle misure prese e della consapevolezza tra le PMI, la sicurezza delle informazioni è stata trattata da molte entità molto più come un "bello da avere" - e non è stata perseguita con molto sforzo o dedizione. L'introduzione dell'Information Security Management System, o la certificazione delle aziende e degli individui, si sta diffondendo lentamente nella cultura dei dipendenti e dei proprietari delle aziende. Tuttavia, è stato stabilito che tra i molti fattori che compongono la sicurezza dell'azienda, il fattore umano, cioè l'impiegato, la direzione e, infine, il responsabile della sicurezza delle informazioni, può fare la più grande differenza.

Il progetto TeBeISi si è posto l'obiettivo di fornire approfondimenti sullo stato della sicurezza dell'informazione nelle PMI e di approfondire le possibilità di formazione e istruzione per le PMI al fine di superare la carenza di personale qualificato.

3.1 Oggetto della Ricerca

L'agenda di ricerca su cui si è basato il progetto TeBeISi si radica principalmente in tre passi iterativi: primo, benchmarking delle pratiche comuni (IO1 e IO2), secondo, analisi dei bisogni (IO3) e sviluppo di strumenti adeguati e raccomandazioni per aziende, individui e istituzioni educative (IO4 e IO5). Analizzando la situazione del mercato, specialmente il ruolo delle certificazioni e degli strumenti esistenti nel contesto del riconoscimento delle competenze e della trasparenza. Dall'analisi dei requisiti, è stato sviluppato un processo che è rappresentato nella Figura 1.

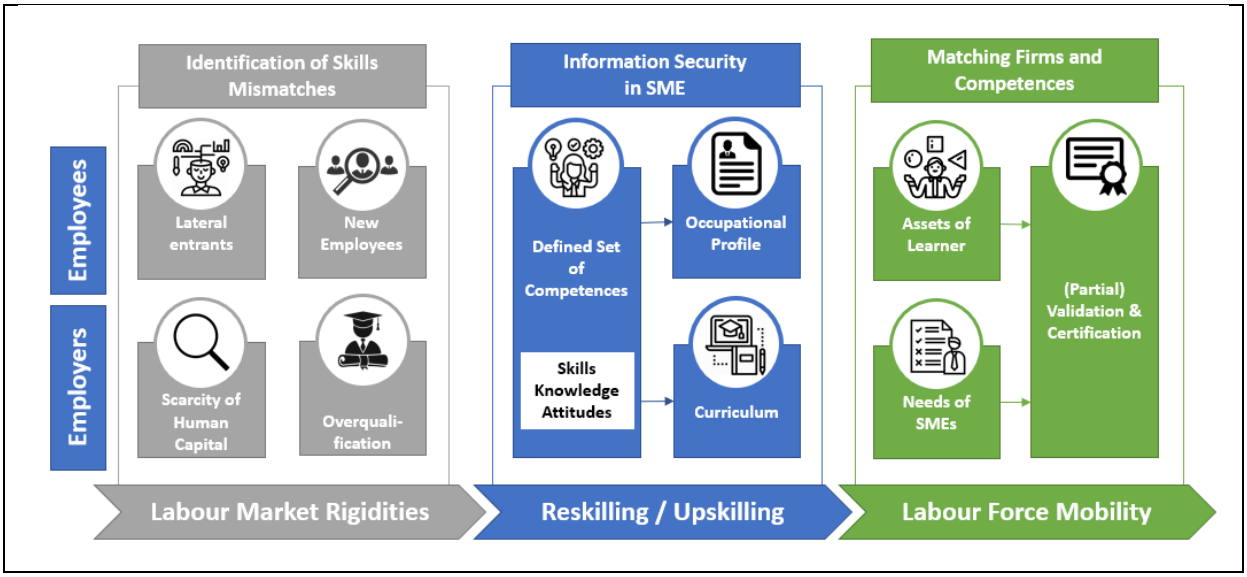


Figura 1: Una via d'uscita - La soluzione TeBeISi per superare il gap di competenze nel mondo della sicurezza informaticarket.

In breve, le attuali rigidità del mercato del lavoro possono essere descritte in due modi: da un lato, c'è semplicemente un basso numero di specialisti disponibili sul mercato. Questa scarsità si aggrava ulteriormente a causa del fatto che la maggior parte degli specialisti disponibili sono altamente qualificati - spesso troppo altamente, poiché diventano troppo costosi per le

nelle aziende sono simili a quelle dell'intero settore IT: molti collaboratori esterni stanno diventando attivi nel settore, e lavoratori completamente nuovi iniziano a impostare la loro carriera in questo promettente dominio. La soluzione sviluppata dal progetto TeBeISi parte quindi dall'analisi delle Competenze Conoscenze e abilità richieste nelle PMI, per costruire un curriculum specifico progettato intorno ai bisogni delle PMI.

È diventato evidente che, non solo dal punto di vista delle qualifiche, i bisogni delle PMI sono molto diversi da quelli delle grandi aziende, ed è per questo che il progetto suggerisce un profilo occupazionale diverso per tenere conto di queste differenze. Il profilo occupazionale e il programma di studi sono basati sulle competenze determinate tra le PMI. Infine, un check-up dei bisogni delle aziende e delle competenze dei dipendenti le aiuta a identificare i candidati idonei, che presentano una buona predisposizione per il lavoro nel campo della sicurezza dell'informazione e che sono desiderosi di riqualificarsi e proseguire la loro carriera in un nuovo campo. L'investimento nel personale esistente e la riqualificazione dei propri dipendenti sono quindi considerati come le possibilità più economiche per le aziende e i lavoratori per colmare il fabbisogno di competenze.

Il presente studio supporta questa problematica in diversi modi: In primo luogo, mira a identificare i requisiti da una prospettiva manageriale, considerando le strategie di assunzione, le posizioni aperte, la conoscenza della sicurezza delle informazioni e la cultura aziendale. In secondo luogo, si ri-valutano i requisiti tecnici, considerando specificamente le competenze sociali, ma anche quelle tecniche. In entrambi i contesti, gli elementi sono stati sviluppati attraverso una serie di interviste con esperti e focus group. Quindi, in terzo luogo, il questionario pre-inviato fornisce una conferma e una convalida tra colleghi dei risultati stabiliti attraverso un disegno di ricerca con metodo misto.

3.2 Metodo

Il progetto di ricerca con metodo misto che ha portato allo sviluppo dei profili di competenza e del programma di studi TeBeISi consiste in quattro elementi centrali, i cui risultati sono stati mescolati e utilizzati in modo iterativo durante l'implementazione del progetto In primo luogo, in una ricerca a tavolino, sono state analizzate le certificazioni e i profili professionali, producendo approfondimenti sulle com-petenze insegnate e sulle competenze tipiche dei professionisti che operano sul mercato. Tuttavia, questa ricerca è stata limitata dalla constatazione che solo a volte il caso specifico delle PMI è stato preso in considerazione, e che rimane poco chiaro cosa distingue le esigenze di base di una PMI e i requisiti più avanzati delle imprese più grandi. Perciò, l'enfasi è stata posta sull'osservazione dettagliata del contesto delle PMI, incluso il coinvolgimento di diversi stakeholder delle PMI (imprenditori, camere di commercio, ricercatori specifici ecc.), la valutazione della letteratura specifica delle PMI e l'analisi dei processi di certificazione specifici delle PMI e dei corsi disponibili nei paesi partner.

Attraverso una serie di interviste con esperti e focus group, condotti in Lituania, Italia, Germania e Polonia con datori di lavoro, dipendenti e fornitori di formazione, sono state analizzate le competenze dei professionisti della sicurezza delle informazioni. Dall'analisi qualitativa, sono state estratte informazioni approfondite sull'importanza delle competenze tecniche, metodologiche, sociali e personali, e sono stati identificati elementi specifici in ogni categoria. L'intera analisi è disponibile nel documento "Information Security Competences - a qualitative analysis of Expert Interviews on Knowledge and Skills of Professionals in Information Security".

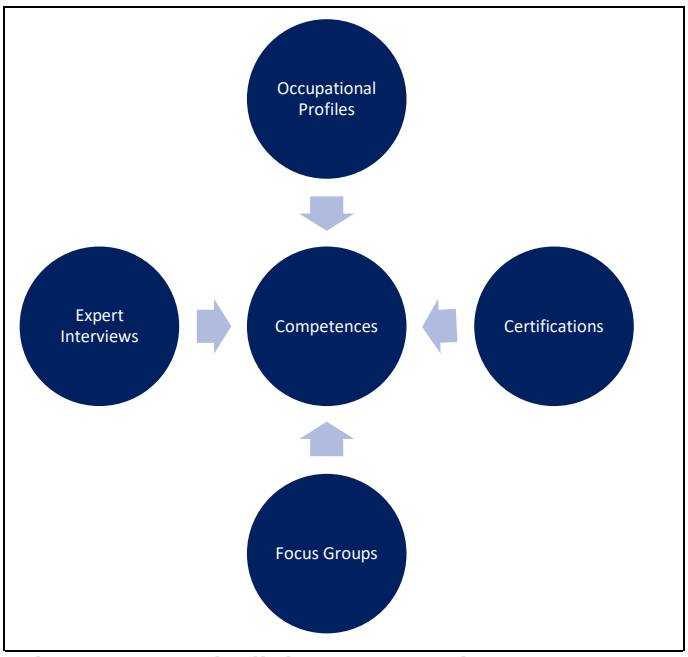


Figura 2: Agenda di ricerca TeBelSi

Gli elementi particolari identificati sono stati riformulati e raggruppati in unità di apprendimento secondo lo standard ECVET dei risultati dell'apprendimento (cfr. IO4). Nella presente indagine, queste unità sono state sottoposte a valutazione in termini di frequenza e importanza nelle aziende, in modo che i risultati finali forniscano indicazioni sulle priorità delle aziende e sui compiti più urgenti che devono essere affrontati.

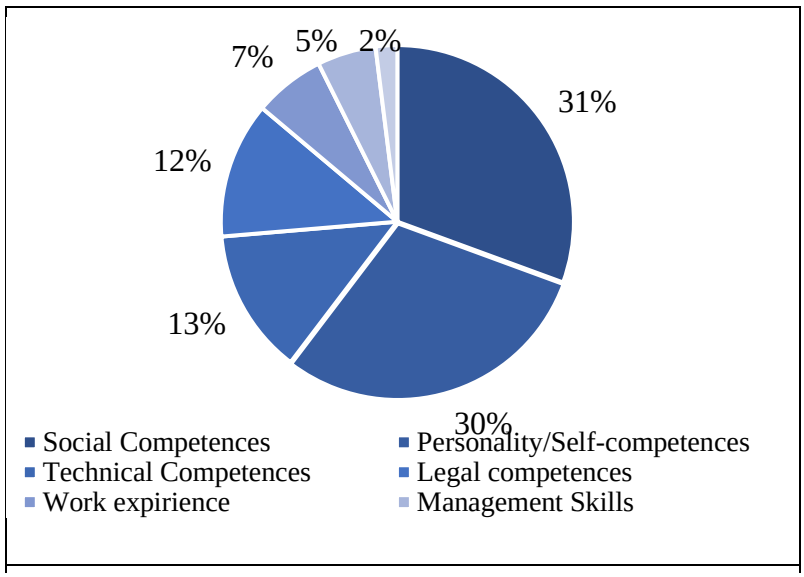


Figura 2. Competenze critiche di successo

4 Studio: Formazione ed addestramento alla gestione della sicurezza dell'informazione per le PMI

Nell'ambito del progetto, il gruppo che ha condotto TeBeISi ha realizzato l'indagine "Information Security Education for SMEs" con l'obiettivo di ottenere informazioni sulle pratiche attuali in materia di sicurezza dell'informazione nelle piccole e medie imprese, sulla necessità di conoscenze, abilità e competenze e sulle prospettive delle PMI nell'affrontare le sfide esistenti legate alla scarsa disponibilità di risorse. L'indagine sulla formazione alla sicurezza dell'informazione per le PMI ha lo scopo di identificare gli apprendimenti e le competenze in specifici sottocampi del settore professionale della sicurezza dell'informazione nel mondo delle piccole e medie imprese. L'indagine è stata condotta tramite Limesur-veyvey. In un periodo di circa 6 settimane 160 partecipanti, specialisti di sicurezza dell'informazione, proprietari e amministratori delegati di PMI, nonché esperti di selezione e IT hanno risposto all'indagine online diffusa nei paesi partner del progetto, principalmente Polonia, Germania, Lituania, Italia e Austria.

Lo studio si compone di due aspetti principali: da un lato, sono stati analizzati i requisiti dal punto di vista dei selezionatori, cioè i dipartimenti HR e i proprietari di aziende, concentrandosi sui principali aspetti che prendono in considerazione durante il processo di reclutamento. Dall'altro lato, ai dipartimenti IT e agli specialisti della sicurezza delle informazioni è stato chiesto di fornire il loro punto di vista sui requisiti tecnici e sul benchmarking delle competenze per i nuovi dipendenti del settore. Inoltre, ad entrambi gli indirizzi è stato chiesto di fornire informazioni sulla cultura aziendale e sui tratti di personalità dei dipendenti di successo. A tal fine, sono stati utilizzati gli item convalidati da Ingela et al. (2005) per la cultura aziendale e Ramos-Villagrasa et al. (2019) per le prestazioni lavorative. Per il questionario, le scale sono state ritrasformate in scale Likert a 5 punti. Ai partecipanti sono state presentate domande in base alla loro posizione. Il questionario è stato sviluppato nell'ambito dell'IO3 del progetto Te-BeISi ed è disponibile insieme ai restanti documenti di output del progetto.

4.1 Descrizione di Dati

La maggior parte delle aziende che hanno partecipato all'indagine appartiene al campo delle micro, piccole e medie imprese (più di tre quarti). Il quarto rimanente consiste di grandi imprese (5%), organizzazioni governative (6%) e non governative (8%). Quando necessario, sono stati considerati solo i valori per le PMI. La figura 4 mostra la distribuzione dei partecipanti totali secondo la dimensione dell'impresa. Per la definizione di dimensione dell'impresa, è stata utilizzata la definizione comune europea che rispetta il numero di dipendenti e il fatturato. (Commissione europea 2021).

Le imprese operano in diversi settori, come la salute umana e il lavoro sociale, l'istruzione o nel campo delle attività professionali, scientifiche e tecniche, secondo la classificazione NACE Rev. 2 (Eurostat 2008). Il 10% delle aziende opera nel settore dell'informazione e della comunicazione (Figura 5).

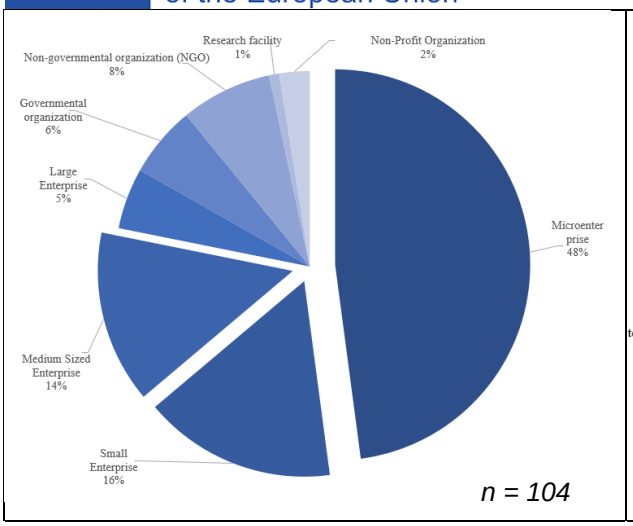


Figure 3: "Quali aziende partecipano al sondaggio?"

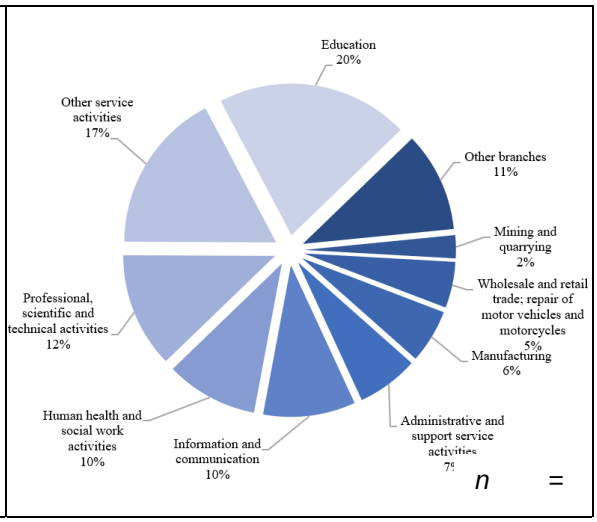


Figure 4: "In quale ramo dell'industria opera la sua azienda?"

Per l'indagine, era importante conoscere il tipo di attività dei partecipanti nell'azienda, cioè o esperti di IT e sicurezza delle informazioni o CEO / selezionatore in una PMI, poiché le responsabilità funzionali che coinvolgono la sicurezza delle informazioni cambiano. Secondo le loro risposte, ai partecipanti sono state mostrate diverse domande nel sondaggio. Come si può vedere nella figura 4 e nella figura 5, due terzi dei partecipanti lavorano come direttore generale o nel reparto risorse umane. Questo gruppo ha risposto a domande relative alla cultura aziendale, alle competenze in azienda, alla formazione in azienda o alle tecnologie utilizzate in azienda..

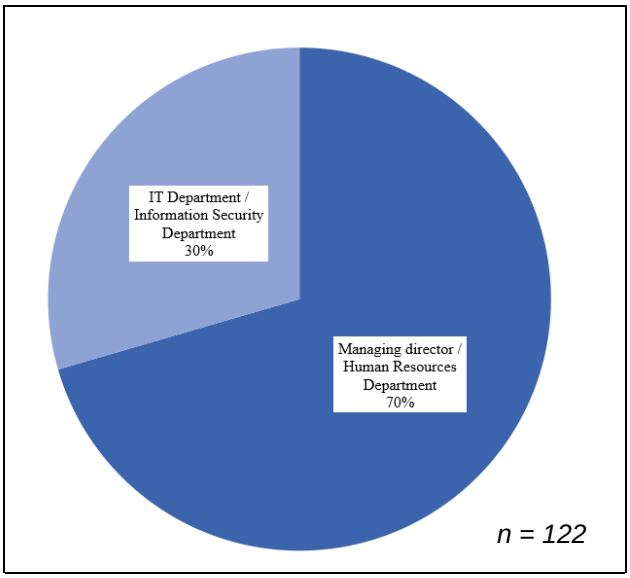


Figura 5: "Quale è il tuo ruolo in azienda?"

Agli intervistati del settore IT o della sicurezza informatica, invece, sono state poste domande incentrate sulle loro prestazioni lavorative, sui tratti della personalità e su domande relative alla gestione dell'IT nell'azienda. Questa distinzione è stata fatta per tenere conto delle diverse prospettive sulla sicurezza dell'informazione, con un'attenzione manageriale da parte dei proprietari dell'azienda e un'attenzione tecnica da parte degli esperti di sicurezza dell'informazione.Considerando l'origine degli intervistati, quasi la metà dei partecipanti appartengono ad aziende Italiane. Inoltre, le aziende sono anche originarie di Lituania, Germania, Polonia, Austria e Repubblica Ceca (Figura 6). Infine, una breve panoramica sulla distribuzione dei sessi: C'è una leggera maggioranza di partecipanti di sesso maschile, con 38 di sesso femminile su 102 partecipanti (Figura 8). Sfortunatamente, la dimensione e la distribuzione dei partecipanti non ha permesso di comparare i paesi o il genere, cosa che deve essere presa in considerazione quando si interpretano i risultati. Tutti i grafici che seguono illustrano sia un confronto tra PMI che tra non PMI. Se non indicato diversamente, solo le risposte delle PMI sono state accettate nell'analisi.

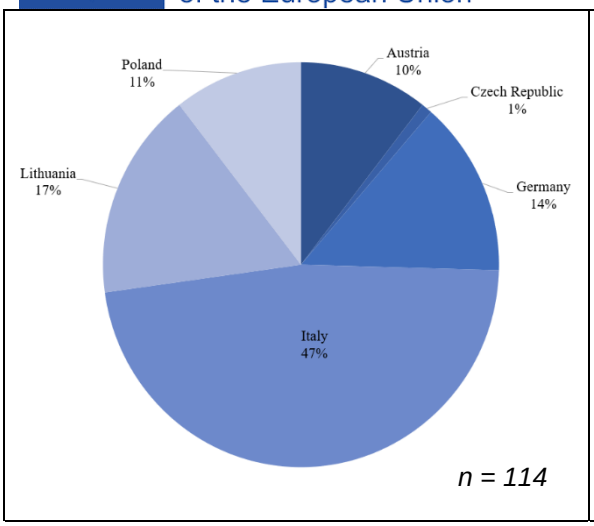


Figura 6: "In quale paese opera principalmente la tua azienda?"

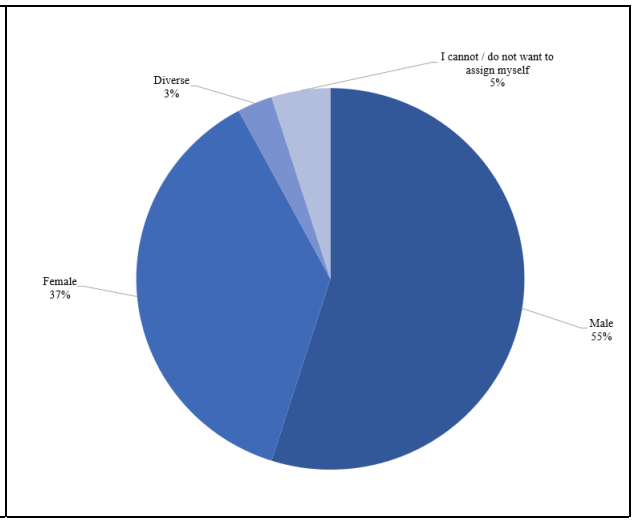


Figura 7: "Com'è la distribuzione dei sessi?"

4.2 Analisi

La parte principale dell'indagine può essere differenziata in due gruppi: aspetti manageriali e tecnici della sicurezza delle informazioni nelle PMI. Mentre il primo aspetto comprende i capitoli 4.2.1 Cultura aziendale, 4.2.2 Competenze nell'azienda, 4.2.3 Sicurezza delle informazioni nelle PMI e 4.2.4 Sicurezza delle informazioni nell'azienda: requisiti del personale, il secondo comporta domande specifiche sulle competenze nel capitolo 4.2.4 Sicurezza delle informazioni nell'azienda: requisiti del personale, 4.2.5 Autovalutazione delle competenze, 4.2.6 Personalità (Big Five) e 4.2.7 Performance lavorativa

4.2.1 Cultura Aziendale

Al fine di rivelare le differenze tra le aziende che hanno implementato misure di sicurezza dell'informazione rispetto a quelle che non l'hanno fatto, la cultura aziendale è stata identificata come un aspetto cruciale che separa le aziende l'una dall'altra. Di conseguenza, il primo passo per i partecipanti è stato quello di caratterizzare la cultura aziendale stessa. Per analizzare la cultura aziendale sono state usate le brevi scale suggerite da Jöns et al. (2005), usando una scala Likert a 5 punti con 1 e 5 come estremi.

In questo contesto, agli intervistati è stato chiesto di descrivere le loro aziende secondo le caratteristiche "Strategia", "Struttura", "Leadership" e "Cooperazione". Per queste caratteristiche, gli autori hanno sviluppato 18 domande, illustrate nella tabella 1. Come si può vedere di seguito, esiste una differenza significativa negli approcci tra i 18 item. Bisogna quindi dire che alcuni degli argomenti sono formulati positivamente e altri negativamente. Di conseguenza, un confronto diretto non dà risultati immediati e significativi. Ancora più importante, l'aggregazione delle categorie ai quattro aspetti menzionati sopra deve essere

considerata in questo contesto.

Question	N	Mean	Std. Dev.	Var.	Kurtosis	Std. Err.
The company is highly customer-oriented.	83	4.37	0.79	0.63	3.34	0.52
The company is open towards innovations.	83	4.19	0.82	0.67	1.73	0.52
The company is highly quality-oriented.	84	4.13	0.97	0.93	0.47	0.52
The company is characterised by team orientation.	84	3.96	0.94	0.88	0.98	0.52
The company is highly performance-oriented.	83	3.96	0.94	0.89	1.30	0.52
Managers place great trust in the employees.	82	3.91	0.77	0.60	-0.19	0.53
Employees place great trust in the managers.	84	3.87	0.89	0.79	1.32	0.52
Employee information has a high priority.	82	3.76	0.90	0.80	-0.57	0.53
Employees are involved in decision-making.	82	3.67	0.99	0.99	0.29	0.53
Conflicts are addressed openly in the company.	83	3.55	0.93	0.86	0.12	0.52
The company is strongly hierarchically organised.	84	2.94	1.25	1.57	-0.98	0.52
The company has a bureaucratic management style.	84	2.64	1.09	1.20	-0.82	0.52
The relationship between employees is characterised by competition.	84	2.52	1.11	1.24	-0.56	0.52
When mistakes and problems occur in the company, first of all culprits are sought.	84	2.26	1.03	1.06	-0.27	0.52
The leadership style in the firm is authoritarian.	83	2.24	1.11	1.23	-0.52	0.52

Tabella 1 "Per favore, indichi in che misura le seguenti caratteristiche descrivono l'azienda per cui lavora o l'organizzazione per cui lavora".

Le summenzionate caratteristiche possono essere distinte per strategia, struttura, leadership e cooperazione. Gli autori definiscono queste categorie come segue: L'orientamento al cliente, l'apertura verso le innovazioni, un alto orientamento alla qualità e alle prestazioni fanno parte del campo della strategia. Per quanto riguarda la struttura aziendale è importante sapere se l'azienda ha uno stile di gestione burocratico e se l'azienda è fortemente organizzata gerarchicamente. L'ultimo punto porta alla prossima categoria leadership. All'interno di questa area, lo stile di leadership, la priorità dell'informazione dei dipendenti e il coinvolgimento dei dipendenti nel processo decisionale giocano un ruolo significativo. Inoltre, i partecipanti sono coinvolti se si verificano errori e problemi nell'azienda. Infine, argomenti come l'orientamento al lavoro di squadra, la fiducia dei dipendenti verso i manager, la gestione dei conflitti in azienda e la relazione tra i dipendenti fanno parte della categoria cooperazione.

Come mostra la figura 9, le aziende nell'indagine hanno un orientamento strategico relativamente alto, un basso grado di struttura gerarchica e un basso grado di leadership direttiva. Si nota che le aziende che non fanno parte del settore delle PMI hanno un valore leggermente più alto nel campo della struttura. Si può supporre che soprattutto le grandi aziende sono più organizzate gerarchicamente rispetto alle piccole e medie imprese. Per quanto riguarda la strategia, la leadership e la cooperazione si possono osservare solo differenze marginali tra le PMI e le non PMI.

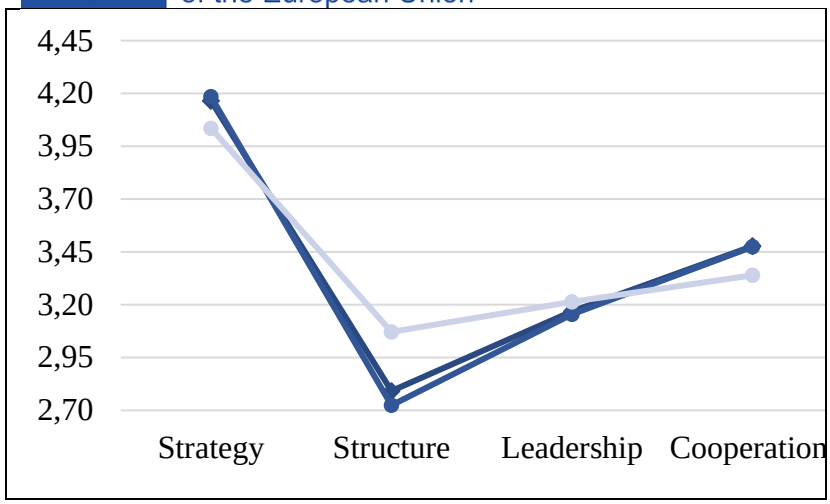


Figure 8: Caratteristiche raggruppate nelle seguenti categorie "Strategia, Struttura, Leadership, Cooperazione" - tutte le aziende

Per quanto riguarda la domanda iniziale di questa parte dell'indagine, si può notare che esiste una leggera differenza nel grado di cooperazione, strategia e leadership, che è maggiore nelle aziende che hanno adottato misure di sicurezza dell'informazione rispetto alle aziende che non l'hanno fatto.

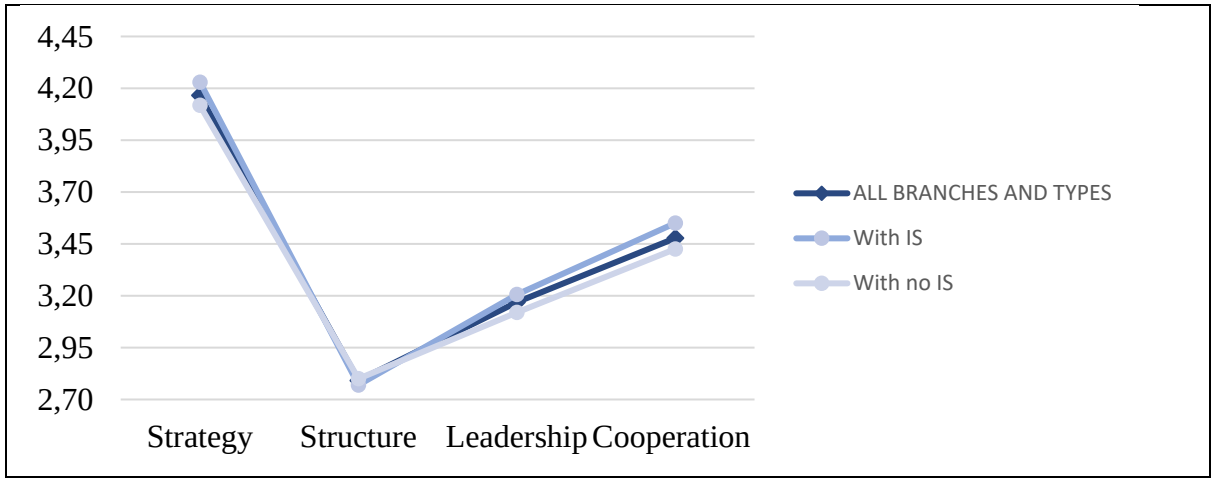


Figura 10: Caratteristiche raggruppate nelle seguenti categorie "Strategia, Struttura, Leadership, Cooperazione" - aziende che hanno una strategia di sicurezza delle informazioni e aziende che non ce l'hanno

4.2.2 Competenze nell'azienda

Nell'ambito dell'indagine, è stato un punto focale ottenere approfondimenti sulle competenze più importanti nel campo della sicurezza delle informazioni che i dipendenti dovrebbero avere quando lavorano in una PMI. Agli intervistati è stato chiesto di dare un'occhiata più da vicino alla strategia di sicurezza dell'informazione nella loro azienda e ai compiti che sono particolarmente rilevanti. La tabella 2 mostra una panoramica dei diversi compiti e attività. L'importanza della particolare attività è misurata tra "5 - molto importante" e "1 - per niente",

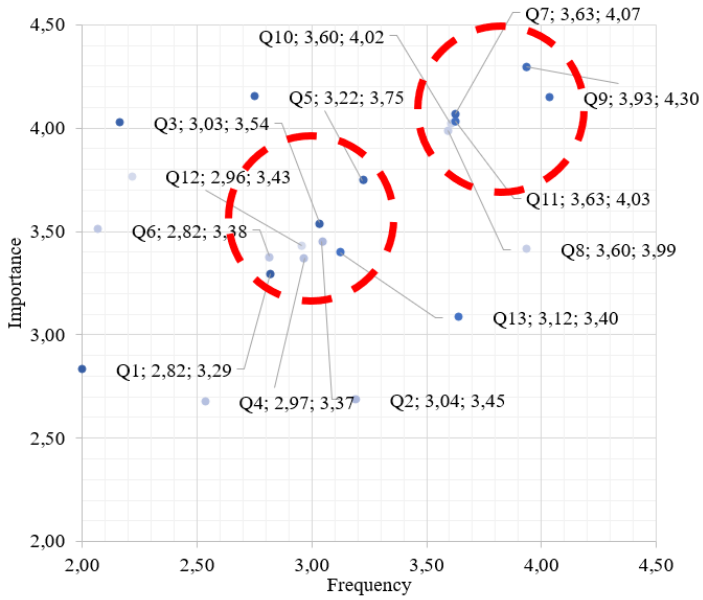
e la frequenza tra "5 - molto spesso" e "1 - mai".

Question	Code
Analysis of business processes and preparation of strategic reports on data protection and information security	Q1
Track and report on changes inside and outside the organisation that affect the organisation's security strategy	Q2
Write company policies on the systematic handling of certain information and data	Q3
Develop recommendations for equipment to be procured, taking into account the company's information security and data protection requirements	Q4
Carry out (information) activities to raise employees' awareness of safety risks in their daily work and to spread safety awareness among the workforce	Q5
Create training plans for the company to regularly train employees on information security and data protection	Q6
Install firewall and anti-virus software Carrying out updates and applying elementary methods to check the security of the software used in the company and preparing appropriate documentation	Q7
Securing mobile devices, communication channels and data storage through passwords or other means of authentication	Q8
Carrying out routine data backups and applying proper conduct methods in accordance with the GDPR to data processing in the company	Q9
Set up administrator accounts and restrict access rights among staff according to the security levels set	Q10
Establish passwords for individual staff access and a secure storage and recovery process	Q11
Create policies and processes for the occurrence of any claims	Q12
Coordinating the needs of managers and employees of the company and providing both parties with information and insights from the company	Q13

Tabella 2: "Compiti e attività nel campo della sicurezza dell'informazione"

La figura 11 mostra i risultati in una tabella incrociata (la frequenza è visualizzata sull'asse x; l'importanza è visualizzata sull'asse y). In generale, nessuna delle attività menzionate mostra un basso grado di importanza o frequenza. Tuttavia, due gruppi di attività possono essere chiaramente distinti, uno con una disposizione ad alta frequenza e importanza, l'altro a media frequenza e importanza. I gruppi sono stati cerchiati in rosso nella figura sottostante.

Il primo gruppo di competenze indica valori alti sia in frequenza che in importanza. A questo gruppo appartengono le competenze relative a "test di sicurezza", "codifica", "gestione delle password" e "controllo di accesso basato sui ruoli". All'interno di questo gruppo, la "gestione dei dati", vale a dire l'esecuzione di backup di routine dei dati e l'applicazione di metodi di condotta adeguati secondo il GDPR al trattamento dei dati, è caratterizzata dal valore complessivo più alto per quanto riguarda l'importanza e la frequenza (Q9: 3,93; 4,30). D'altra parte, le attività nel campo della "gestione dei processi/ degli stakeholder/ della conformità", " acquisto di ICT", "sensibilizzazione e influenza", e "istruzione e formazione" possono essere raggruppate insieme. Tutte le competenze sono considerate piuttosto importanti, la frequenza, tuttavia, non si può dire che sia particolarmente alta. Gli intervistati classificano il campo "gestione dei processi" come meno importante e meno frequente. Quest'area riguarda l'analisi dei processi aziendali e la preparazione di rapporti strategici sulla protezione dei dati e la sicurezza delle informazioni. Tuttavia, il valore di 2,82 mostra che l'argomento riceve sicuramente attenzione nelle aziende.



Learning Units	Code
Process Management	Q1
ICT Risk Management	Q2
Compliance Management	Q3
ICT Procurement	Q4
Sensitization and influencing	Q5
Education and Training	Q6
Security Testing	Q7
Encoding	Q8
Data Management	Q9
Role based access control	Q10
Password Management	Q11
Business Continuity Management	Q12
Mediation and Stakeholder management	Q13

Figura 9: Competenze nell'azienda – Risultati

La figura riportata di seguito si concentra sull'analisi delle competenze nelle PMI (Figura 12). I dati descrivono la differenza d'importanza tra PMI e non PMI: più un valore è vicino allo zero, minore è la differenza. Pertanto, i valori più grandi comportano differenze maggiori. I valori positivi indicano che le competenze sono più importanti e usate frequentemente nelle PMI, mentre i valori negativi rappresentano il contrario. Tutte le competenze già menzionate possono essere trovate nella tabella incrociata. Per quanto riguarda la descrizione degli assi, bisogna fare attenzione: In questo caso, l'asse x mostra l'importanza; l'asse y mostra la frequenza. Si può menzionare che la gestione dei dati del dominio è considerata più importante e più frequentemente utilizzata anche nelle PMI. La figura 11 ha già mostrato l'alta importanza della gestione dei dati (vedi Q9). Il seguente aspetto è particolarmente interessante nel contesto della certificazione parziale nella sicurezza dell'informazione: Il codice Q6 descrive le competenze e le attività nell'istruzione e nella formazione. Come mostra la Figura 12, il codice Q6 può essere trovato nel campo, che è caratterizzato da competenze che sono

meno importante e meno utilizzato nelle PMI. La creazione di piani di formazione per formare regolarmente i dipendenti sulla sicurezza delle informazioni e la protezione dei dati è ovviamente meno importante per le PMI. Si dimostra che tutte le competenze sono abbastanza importanti (media > 3.3) e usate frequentemente (media > 2.8). Le competenze più importanti e più frequentemente utilizzate sono i compiti abituali dell'amministratore di sistema medio, ad esempio la creazione di backup, l'installazione di software antivirus e firewall o la creazione di password individuali.

4.2.3 Sicurezza Informatica nelle PMI

In questa sezione gli intervistati rispondono a domande più dettagliate relative alla sicurezza dell'informazione nelle loro aziende. La questione da esaminare riguarda le ragioni che hanno impedito all'azienda di investire nel miglioramento della sicurezza delle informazioni

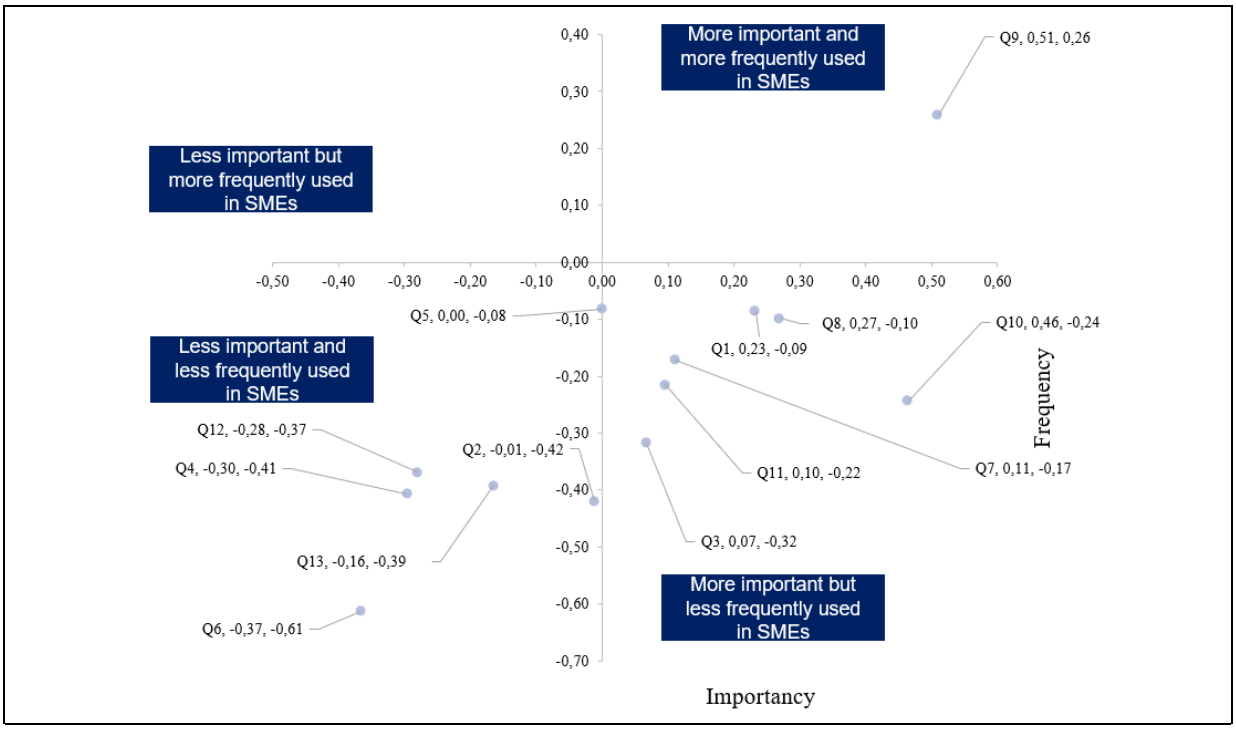


Figura 10: Analisi delle competenze della PMI

(Figura 13). I partecipanti qui sono solo quelli che hanno selezionato la PMI come tipo di azienda.

Come mostrato nella figura seguente, la ragione principale è che non ci sono abbastanza risorse finanziarie nelle aziende (più del 30% degli intervistati ha dato questo motivo). Inoltre, la mancanza di offerte da parte dei fornitori di servizi è anche un aspetto importante per quanto riguarda il problema degli investimenti nel campo della sicurezza dell'informazione. Da un lato, circa il 15 % ha dichiarato che questo problema non si applica nella sua azienda, o le aziende sono riuscite a coprire le loro necessità: un aspetto che può essere considerato abbastanza positivo. D'altra parte, quasi un terzo dei partecipanti non percepisce alcuna necessità o piuttosto nessuna priorità e dichiara che altri temi sono stati più importanti finora. Un punto abbastanza serio che dimostra che il tema della sicurezza delle informazioni non è ancora centrale in tutte le aziende. Infine, l'aspetto riguardante il personale disponibile sembra giocare un ruolo piuttosto meno importante. Solo circa 4 partecipanti hanno indicato una relazione tra la mancanza di personale e il problema dell'investimento nella sicurezza dell'informazione.

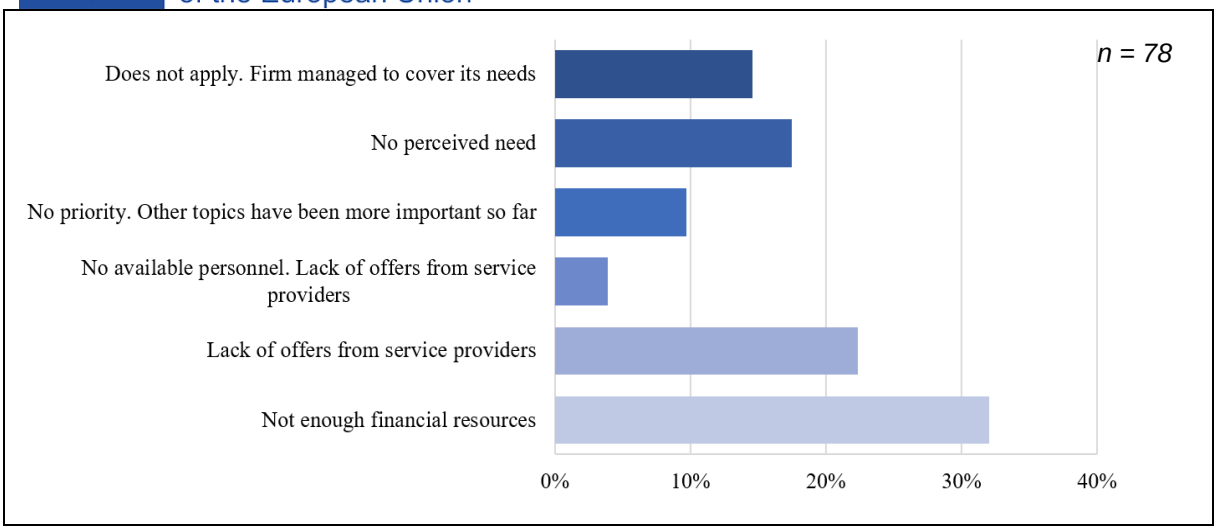


Figura 11: "Quali ragioni hanno impedito alla sua azienda di investire nel miglioramento della sicurezza delle informazioni fino ad oggi?"

Gli intervistati sottolineano l'importanza di particolari tipi di istruzione necessari per la sicurezza delle informazioni in azienda. In questo contesto è stato chiesto che tipo di istruzione o formazione è necessaria/ utile/ ecc. per un dipendente incaricato di garantire la sicurezza delle informazioni in un'azienda. Va detto che c'è una differenza tra competenze o formazioni necessarie ("must-have") e competenze o formazioni utili ("nice-to-have"). La figura 14 mostra una grande importanza per quanto riguarda l'esperienza sul lavoro. Quasi la metà dei partecipanti vede questo punto come "must-have". Inoltre, la formazione interna o la formazione continua è anche rilevante e utile. In generale, si può vedere che gli intervistati preferiscono avere un dipendente con esperienza piuttosto che con istruzione. Tutti i programmi di studio non classici sono solo un po' meno indispensabili e più importanti di tutti i tipi di istruzione universitaria.

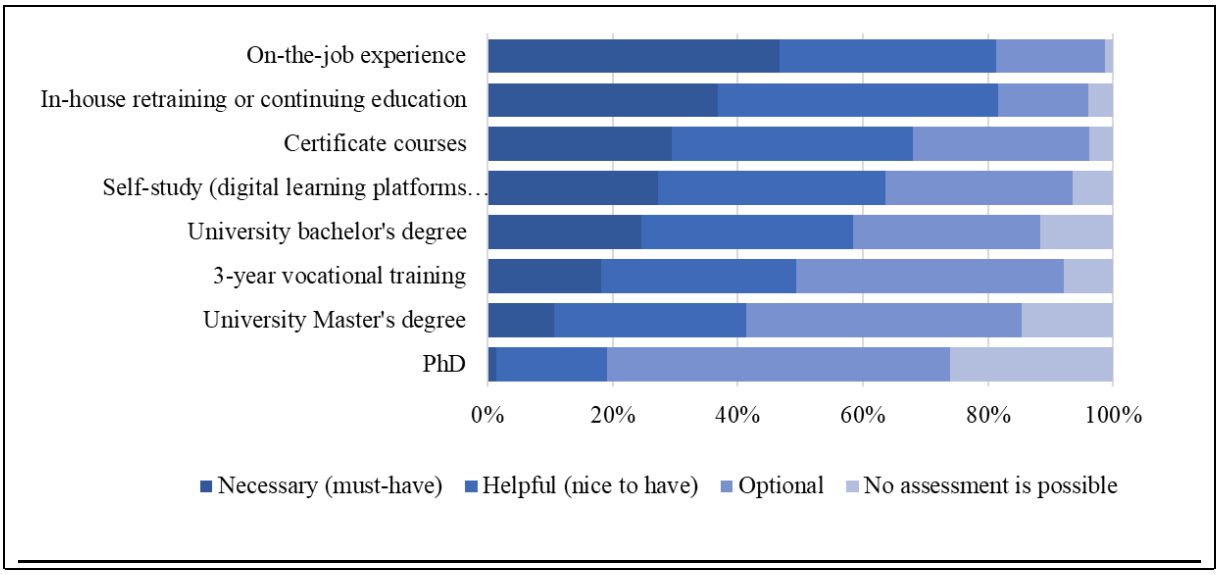


Figura 14: "In base alla sua esperienza, che tipo di istruzione o formazione è necessaria/utile/facoltativa per un dipendente incaricato di garantire la sicurezza delle informazioni nella sua organizzazione?

Nell'ambito del sondaggio sono state chieste agli intervistati anche le possibili opzioni per aumentare la sicurezza delle informazioni (Figura 15). L'opportunità di aumentare la qualificazione dei dipendenti è la più apprezzata ed è stata scelta per quasi il 50% del totale.

L'altra opzione è l'acquisto di un servizio di terzi, che è stato scelto il 30% delle volte. Tuttavia, la creazione e il ricoprimento di una nuova posizione o la copertura dei rischi attraverso l'assicurazione non è così popolare.

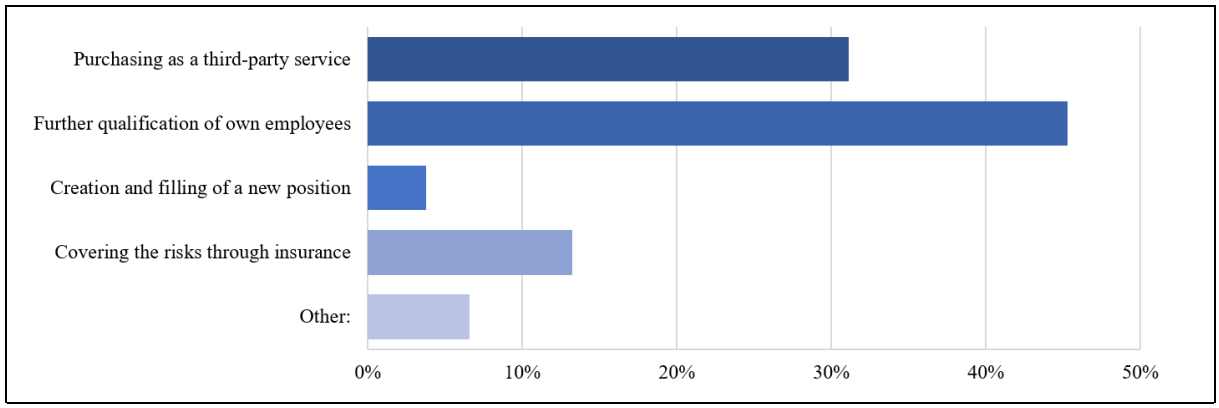


Figura 15: Possibili opzioni per aumentare la sicurezza delle informazioni

Lo studio per quanto riguarda la sicurezza dell'informazione nelle PMI mostra che c'è una mancanza di finanziamenti e di servizi di terze parti nel campo della sicurezza dell'informazione - è la ragione principale riguardante il problema dell'investimento nella suddetta area. Questo è particolarmente importante perché gli intervistati vogliono utilizzare un servizio di terzi per migliorare la sicurezza delle informazioni nella loro azienda. A causa della mancanza di finanziamenti e di offerta sul mercato dei servizi di sicurezza, sembra che i nostri intervistati preferiscano migliorare le qualifiche dei loro dipendenti per mantenere il livello accettabile di sicurezza delle informazioni. Questo è in linea con i requisiti formativi: gli intervistati preferiscono assumere qualcuno con esperienza piuttosto che con istruzione.

4.2.4 Sicurezza Informatica nell'azienda: caratteristiche personali

Un altro punto che è stato analizzato nell'ambito dell'indagine è il bisogno del personale per quanto riguarda la sicurezza informatica nell'azienda. A tal fine sono state analizzate non solo le differenziazioni tra le PMI e le non PMI, ma anche le diverse situazioni delle imprese in relazione all'esistenza di incidenti di sicurezza informatica. Soprattutto quest'ultimo fornisce un quadro chiaro dei cambiamenti di atteggiamento delle aziende verso la sicurezza informatica e la spesa per la sicurezza informatica. L'esistenza di incidenti di sicurezza informatica è mostrata nella figura 16.

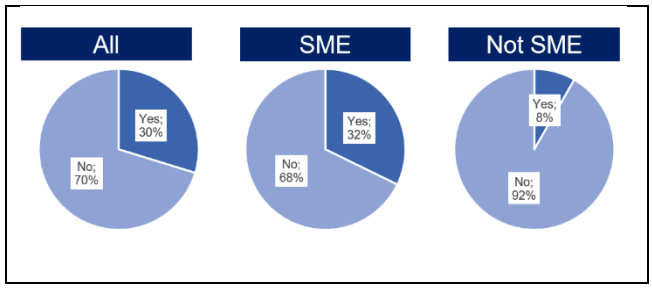


Figura 12: "Sei a conoscenza di incidenti, o rischi, in ambito di sicurezza informatica avvenuti negli ultimi due anni?

Al fine di capire meglio la realtà del personale nelle aziende, è stato chiesto agli intervistati quanti impiegati occupano attualmente con il principale obiettivo di lavoro riguardante la sicurezza informatica, e quanti impiegati prevedono di impiegare nei prossimi anni. Risulta evidente che c'è normalmente un dipendente che è formalmente responsabile della sicurezza delle informazioni nella maggior parte delle

aziende. Anche nelle non-PMI sono di solito non più lavoratori responsabili di questo settore di attività (Figura 17). Sopra è mostrato se c'è personale impiegato, sotto si possono vedere i numeri equivalenti delle imprese che hanno risposto alla prima domanda.

Inoltre è stato chiesto quante posizioni aperte nella sicurezza dell'informazione ci sono nell'azienda. Come mostra la figura 18, circa il 50 % degli intervistati ha risposto che attualmente non ci sono posizioni aperte nella sicurezza dell'informazione nella loro impresa. Se si considera la comparsa di un incidente di sicurezza dell'informazione (IS) si può notare un forte aumento delle posizioni create. Tra le imprese che non hanno avuto un incidente di sicurezza dell'informazione (NO IS), circa il 90% non ha una posizione specifica per la sicurezza dell'informazione. Questo numero si riduce a solo il 20% rispetto alle aziende che hanno avuto un incidente. Numeri comparabili sono stati riportati per l'esistenza di più di una

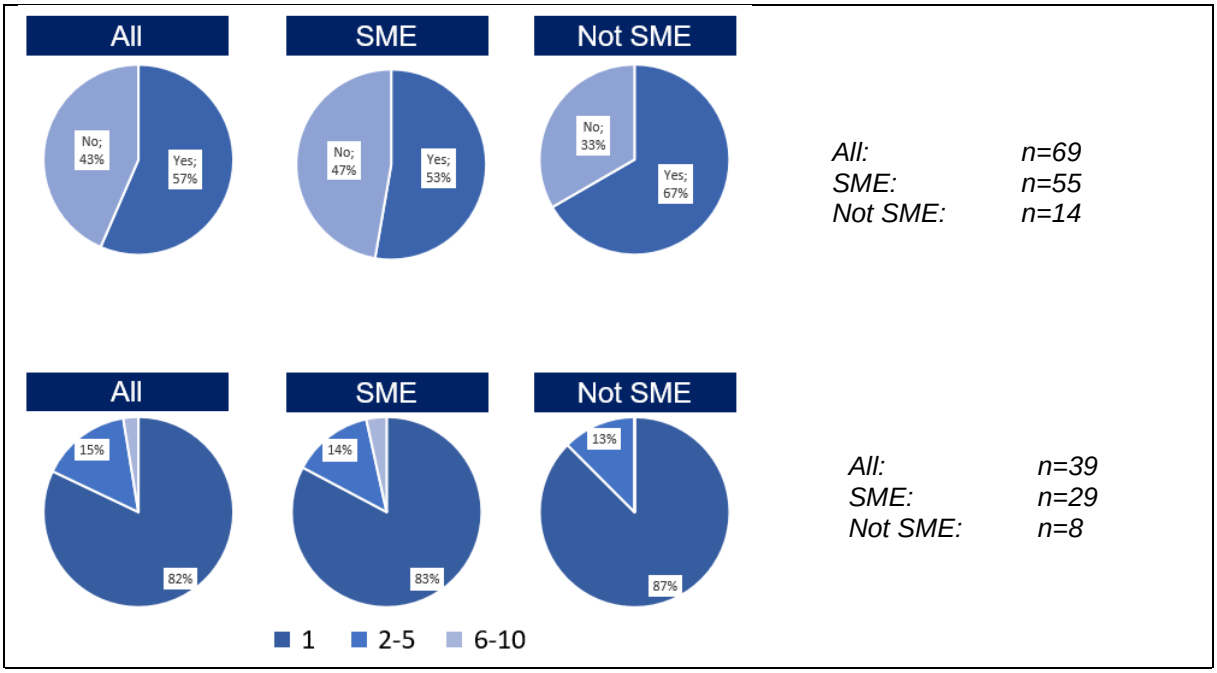


Figura 17: "Ci sono dipendenti nella sua azienda che sono formalmente responsabili della sicurezza delle informazioni? (sopra) - Se sì, quanti?" (sotto)

posizione, illustrando l'iniziativa che le aziende prendono dopo un attacco.

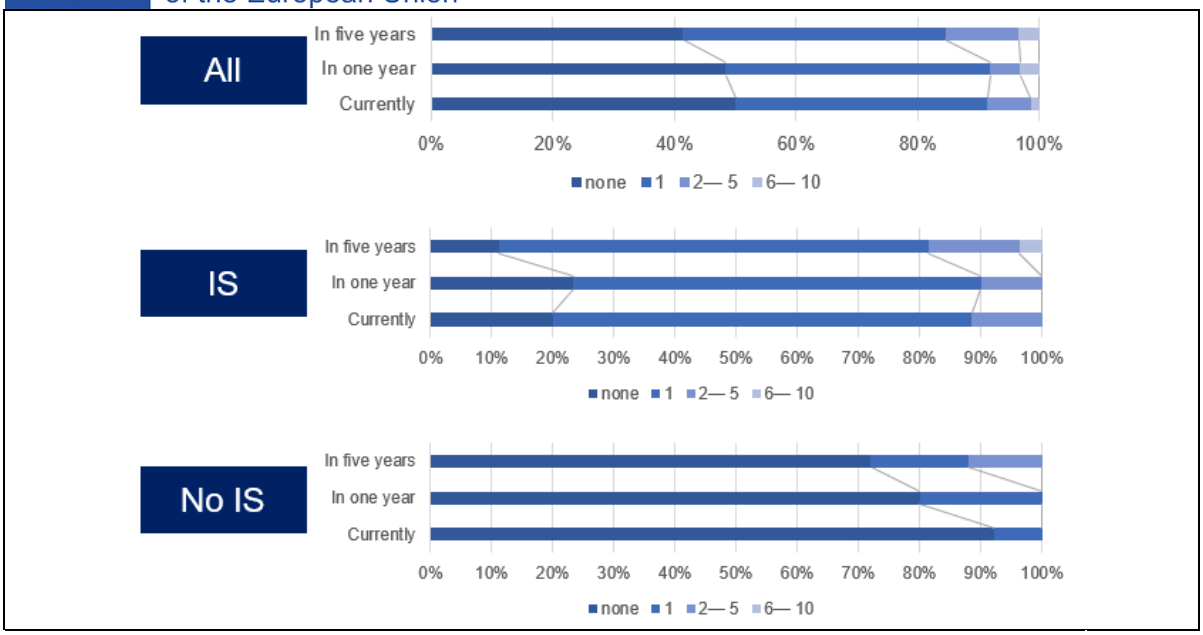


Figura 18: "Quante posizioni aperte per la sicurezza delle informazioni ci sono nella sua azienda?

In questo contesto, agli intervistati è stato chiesto ulteriormente come affrontano i bisogni di risorse umane nella sicurezza dell'informazione fino ad ora. La figura 20 mostra che soprattutto le non-PMI danno grande importanza al perfezionamento dei dipendenti. Se si considerano le PMI, si può notare che l'acquisto di servizi di "sicurezza dell'informazione" da fornitori terzi equivale all'incirca a un'ulteriore formazione dei dipendenti. L'assunzione di nuovi dipendenti, al contrario, è meno significativa per le aziende. Si può concludere che, in generale, lo sviluppo delle capacità interne e l'ulteriore formazione dei propri dipendenti è considerata la soluzione più adatta per la maggior parte delle aziende. Tuttavia, c'è un rischio per la validità dei dati riportati, che diventa evidente quando si considerano le aziende che hanno avuto un incidente di sicurezza delle informazioni e quelle che non l'hanno avuto. Come si può vedere nella figura 21, la voce "nessuna misura" diminuisce dal 31% (la più frequentemente citata) tra le imprese che non hanno avuto un incidente di sicurezza dell'informazione al solo 10% (la meno citata) tra le imprese che hanno avuto un incidente di sicurezza dell'in-

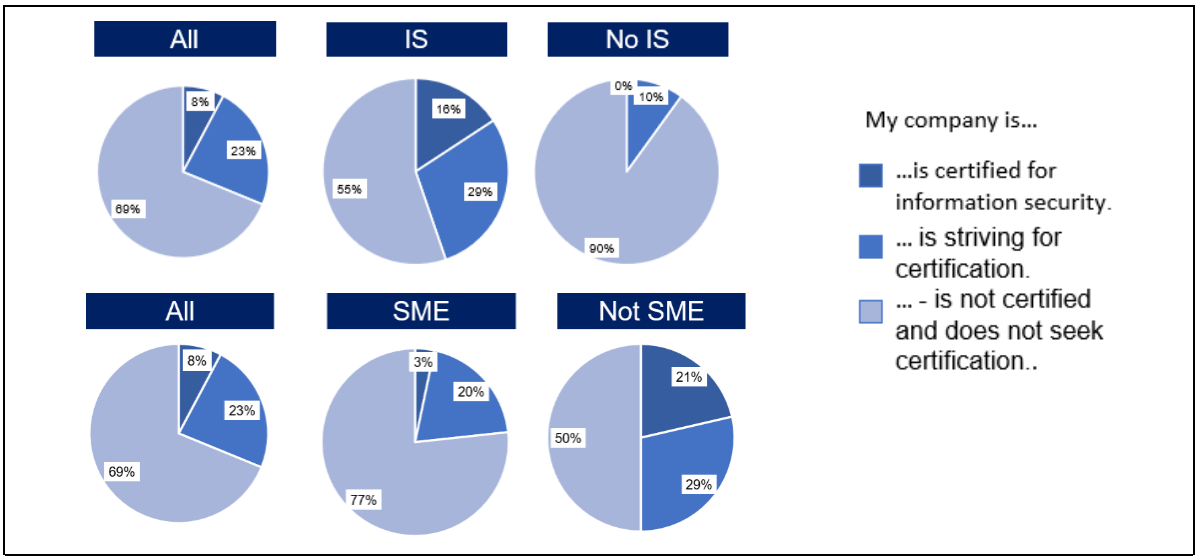


Figura 19: Certificazione aziendale per la sicurezza delle informazioni

formazione.

Numeri analoghi possono essere osservati dall'esistenza di certificazioni tra le PMI e le non-PMI, così come tra le imprese con un incidente di sicurezza dell'informazione. Mentre le certificazioni sono appena evidenti tra le PMI (3 %), sono completamente assenti tra le PMI senza un incidente di sicurezza dell'informazione. Per le imprese che hanno avuto un incidente, i numeri sia per le certificazioni esistenti che per quelle pianificate aumentano significativamente.

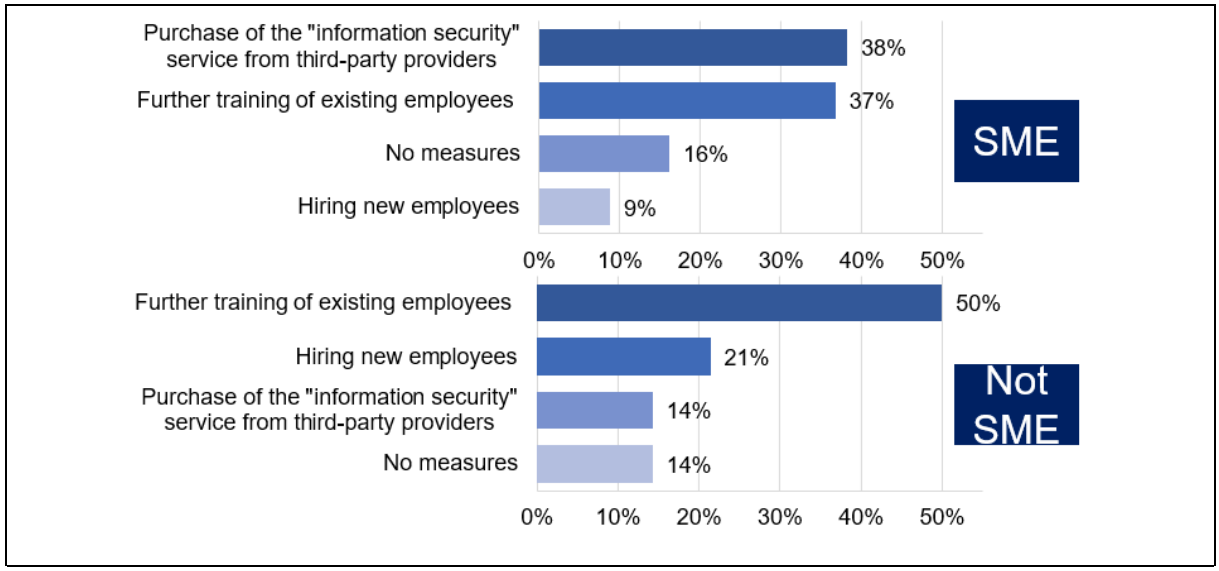


Figura 20: "Come state affrontando finora il fabbisogno di risorse umane nel campo della sicurezza informatica?"

Considerando lo scopo di questo sondaggio, non è solo importante capire la situazione delle certificazioni e degli investimenti, ma anche le misure già intraprese per affrontare le sfide della sicurezza informatica. Come si vede nella figura sottostante, due terzi degli intervistati hanno risposto negativamente a questa domanda. Tuttavia, questo significa anche che circa il 30% ha risposto in modo affermativo. Considerando i risultati della figura 18 e della figura 21, la sensazione è che le imprese si attivino solo dopo un attacco. Non solo le aziende vedono la necessità di creare una posizione equivalente a tempo pieno, ma cercano anche di approfondire le possibilità di migliorare la loro sicurezza delle informazioni con qualsiasi mezzo. Si può concludere che il sentimento esistente tra i professionisti della sicurezza dell'informazione e la comunità della sicurezza dell'informazione, "imparare dal dolore" è una descrizione accurata della realtà nella maggior parte delle aziende. La comprensione di prendere misure acute e di investire risorse nei dipendenti cresce il più delle volte dopo un attacco - quando il danno è già fatto.

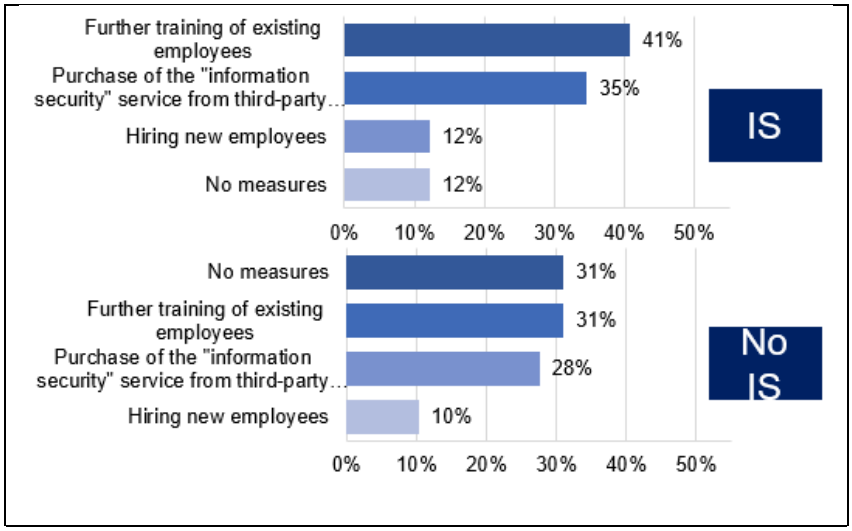


Figura 21: "Come state affrontando finora il fabbisogno di risorse umane nel campo della sicurezza informatica?" - IS e No IS

4.2.5 Auto valutazione delle competenze

Nell'ambito dell'indagine è stato chiesto agli intervistati di valutare se stessi per quanto riguarda le attività di istruzione e formazione in materia di sicurezza delle informazioni. Avevano a disposizione una scala da "0 - nessuna esperienza", "1 - conoscenza generale", "2 - conoscenza generale più esperienza pratica", "3 - conoscenza teorica avanzata" a "4 - conoscenza teorica avanzata più esperienza pratica". La figura seguente mostra che la password e i dati gestionali sono stati spesso menzionati. Questo include per esempio stabilire le password o eseguire i backup di routine dei dati. Dai valori ottenuti sono state prese le medie ed elencate nella figura sottostante. Mentre gli intervistati in media si sentono più esperti nella gestione delle password, nella gestione dei dati e nell'istruzione e formazione, meno fiducia è stata espressa riguardo alla garanzia di rispetto delle norme, alla codifica e alla sensibilizzazione dei dipendenti.

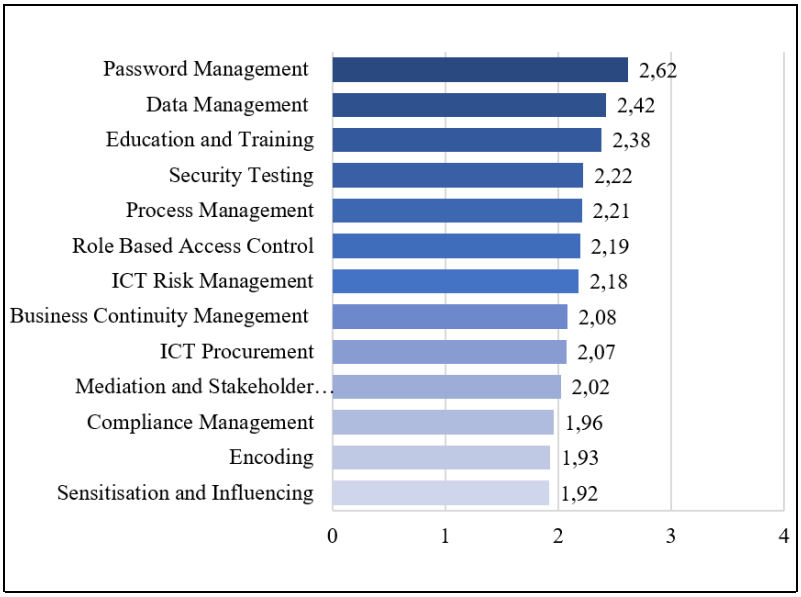


Figura 22: "Per favore, valuta te stesso: Quali delle seguenti attività di istruzione e formazione puoi svolgere?"

Personalità (Big Five)

Nel corso di molte discussioni con gli esperti, è diventato chiaro che il lavoro della sicurezza delle informazioni richiede requisiti speciali ai professionisti riguardo alle loro abilità sociali. Tuttavia, è diventato evidente che nella maggior parte dei casi, è implicito anche il riferimento alle caratteristiche personali. A questo proposito, l'"atteggiamento corretto" non si limita alla relazione con i dipendenti nell'ambito del posto di lavoro, ma la condotta in generale considerando la propensione dei tratti caratteriali. È quindi un'intenzione di questa indagine fare luce sulla propensione dei tratti caratteriali e sulle prestazioni lavorative tra gli esperti di sicurezza informatica. I risultati possono essere visti come un'indicazione delle precondizioni favorevoli per i nuovi candidati al posto di lavoro. A tal fine, sono stati impiegati i cinque tratti di personalità Big five (Rammstedt et al. 2013), che forniscono un modello a cinque fattori di raggruppamento dei tratti di personalità. Secondo questo modello, i seguenti cinque fattori di base descrivono la maggior parte dei tratti di personalità in modo dicotomico, dove ogni tratto comporta due estremi:

Dimensione	Punteggi più alti	Punteggi più bassi
Apertura	inventiva/curiosa	coerente/cauta
Coscienziosità	efficiente/organizzato	stravagante/disattento
Estroversione,	amante del divertimento, attivo, appassionato	riservato, solitario, tranquillo, sobrio
Relazionalità	Affettuoso, aggregante, loquace	Critico/razionale
Emotività	passivo, insensibile	resiliente, ottimista

Tavola 3: Dimensioni dei Big-5.

Il BFI-10 è una scala di 10 item che misura i tratti sopra menzionati. Questa scala è stata specificamente sviluppata per essere breve e progettata per situazioni in cui gli intervistati sono pochi in termini di tempo. Ogni scala BFI-10 consiste di un item con punteggio vero e uno con punteggio falso, ad esempio, per ottenere la misura dell'apertura, il valore della domanda sei viene estratto dal valore della domanda dieci. Più alto è il risultato, più una persona è inventiva/curiosa.

Nr.	Items	Polarità	Sotto scale
1	Sono piuttosto riservato.	-	Apertura
2	Io ho fiducia negli altri e credo che le persone siano buone.	+	Relazionalità
3	Sono piuttosto tranquillo e tendo alla pigrizia.	-	Coscienziosità
4	Io sono piuttosto rilassato ed affronto bene lo stress .	-	Emotività
5	Io ho pochi interessi artistici.	-	Apertura
6	Sono estroverso e socievole.	+	Estroversione
7	Io tendo a criticare gli altri.	-	Relazionalità
8	Completo accuratamente i compiti.	+	Conscienziosità
9	Io divento nervoso facilmente.	+	Emotività
10	Io possiedo una immaginazione fervida	+	Apertura

Tabella 4: Struttura BFI-10

Dagli istogrammi sottostanti si può dedurre che tra tutti gli intervistati, le persone tendono ad essere efficienti/organizzate piuttosto che stravaganti/imprudenti (vedi coscienziosità). Le risposte sono distribuite positivamente anche nell'apertura; possiamo vedere che più intervistati si identificano come inventivi/curiosi piuttosto che coerenti/cauti (vedi apertura). Gli intervistati sono quasi equamente distribuiti tra le definizioni di estroversione, con una marginale indulgenza positiva, cioè gli intervistati sono considerati più estroversi/energici che solitari/riservati (in misura molto limitata). La situazione opposta può essere osservata per l'emotività e la relazionalità. In questo caso gli intervistati sono più resilienti/confidenti e critici/razionali piuttosto che sensibili/nervosi e amichevoli/compassionevoli rispettivamente. L'indulgenza generale può essere vista nella Figura 24.

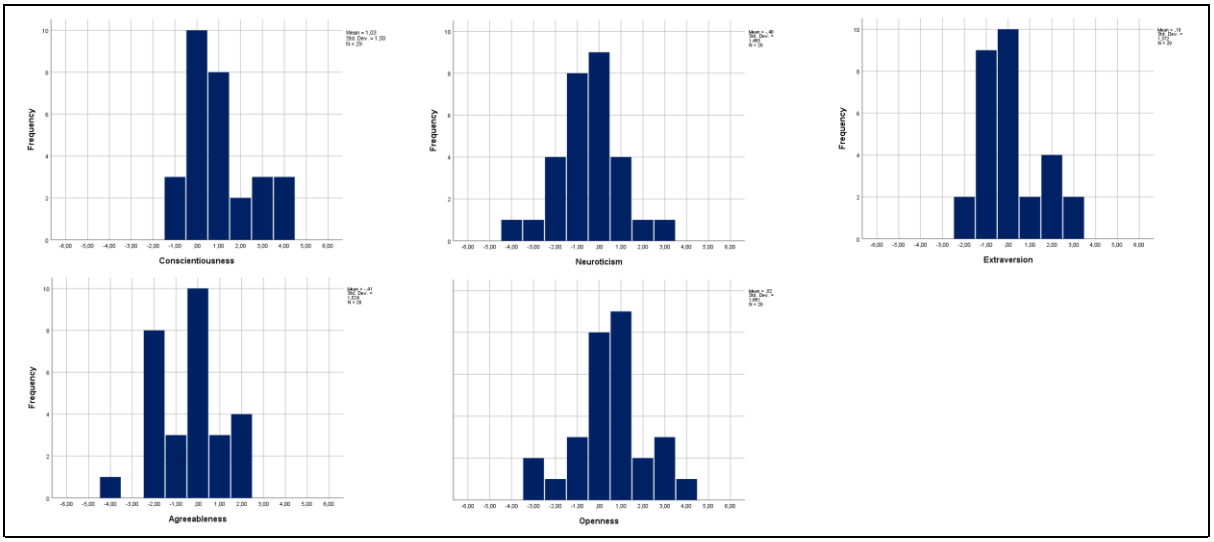


Figura 23: Istogrammi Big-Five osservati per i professionisti della sicurezza delle informazioni.

Dalla clemenza si possono dedurre diverse ipotesi cruciali sui tratti caratteriali degli esperti di sicurezza dell'informazione. Il fattore più dominante è il valore positivo per la coscienziosità, che implica forti disposizioni verso una condotta efficiente e organizzata. I valori negativi per l'emotività sostengono il pensiero degli esperti, che la resilienza e la fiducia nel proprio lavoro giocano un ruolo importante. Inoltre, gli esperti possono essere caratterizzati per essere coerenti e cauti (apertura), critici e razionali (gradevolezza) e in misura limitata riservati (estroversione).

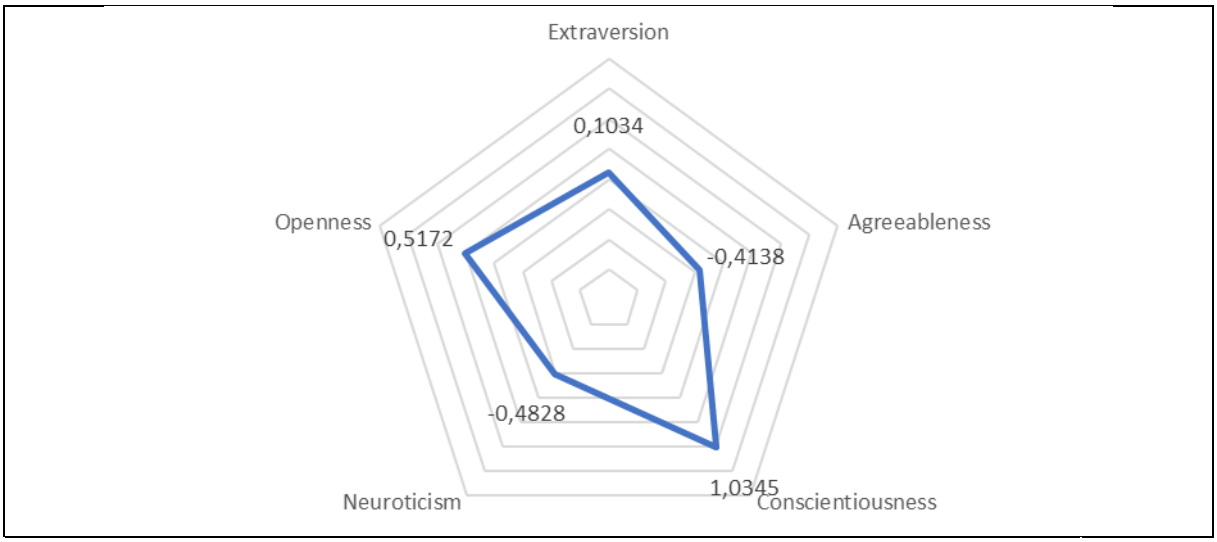


Figura 24: Big-Five, confronto dei valori medi

Come possiamo vedere dalla matrice di pesi mostrata nella tabella 5, in generale, tutti gli item mostrano il loro valore più alto sul fattore corrispondente, in linea con le ipotesi. Questo depone a favore della validità dell'approccio nel nostro caso.

Item	E	A	C	N	O
Mi vedo come una persona riservata	**,411***	0.067	0.212	-0.264	-0.169
Mi vedo come uno generalmente fiducioso	**-,422***	**-,572****	-0.054	-0.081	0.210
Mi vedo come uno tendenzialmente pigro.	-0.163	0.138	**-,597****	0.097	0.294
Mi vedo come uno rilassato che affronta bene lo stress.	0.193	0.039	0.113	**-,379***	-0.233
Mi vedo come uno che ha poschi interessi artistici.	-0.101	-0.006	**-,375***	0.089	**,670****
Mi vedo come persona estroversa e socievole.	**-,635****	**-,401***	-0.194	0.067	0.095
Mi vedo come uno che cerca difeti negli altri	0.091	**,538****	-0.154	0.283	-0.026
Mi vedo come uno preciso nel lavoro.	0.281	0.039	**,566****	-0.335	-0.264
Penso di essere uno che diventa nervosa facilmente.	-0.137	0.350	-0.271	**,678****	0.000
Penso di possedere un fervida immaginazione.	0.191	0.267	0.175	-0.137	**-,493****

Tabella 5: "Test di validità: Correlazione tra elementi e gruppi"

Gli intervistati riservati si considerano rilassati. Credono anche di fare un lavoro accurato e di avere un'immaginazione fervida. Gli intervistati che si sono segnati come generalmente fiduciosi, sono anche più estroversi e socievoli. Gli intervistati pigri hanno pochi interessi artistici, sono estroversi e socievoli, ma trovano anche difetti negli altri. Quelli rilassati pensano di fare un lavoro accurato e hanno un'immaginazione attiva. Quelli che tendono a trovare difetti con gli altri si innervosiscono facilmente e si vedono come qualcuno che ha un'immaginazione attiva. Infine, gli intervistati "scrupolosi" hanno un'immaginazione attiva.

4.2.6 Prestazione lavorativa

Questa parte si basa sull'Individual Work Performance Questionnaire (IWPQ). L'IWPQ è una scala di 18 item sviluppata da Ramos-Villagrasa et al. (2019) per misurare le tre dimensioni principali della performance lavorativa:

- Attenzione al compito (5 items)
- prestazione in un determinato contesto (8 Items)
- comportamento lavorativo controproducente (5).

Tutti gli elementi hanno un periodo di richiamo di tre mesi e una scala di valutazione a 5 punti (da 0 = raramente a 4 = sempre per il compito e la prestazione contestuale; e da 0 = mai a 4 = spesso per il comportamento lavorativo controproducente). Per i comportamenti controproduttivi, la scala comporta una polarità negativa, in modo che i valori più bassi sono più desiderabili, in quanto ciò si traduce in minori comportamenti controproduttivi in generale. I rispettivi valori sono illustrati nella Figura 25 alla Figura 27, il profilo finale combinato nella Figura 28.

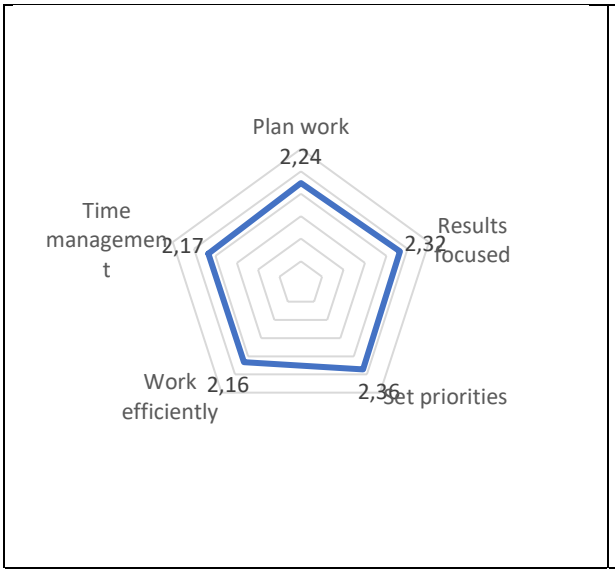


Figura 13: Attenzioine al compito

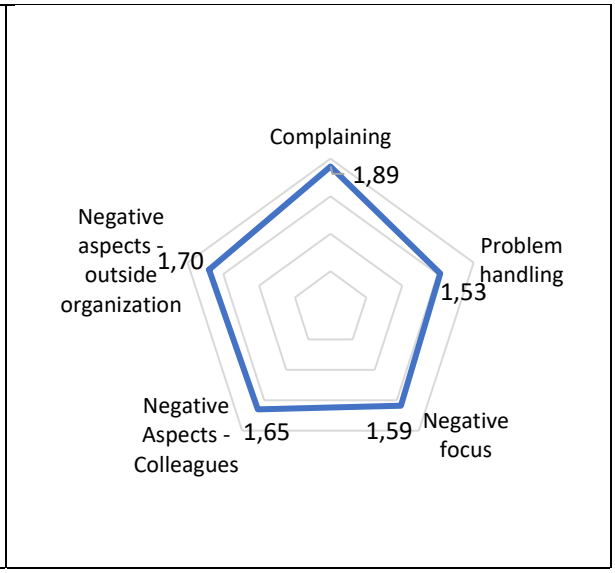


Figura 14: Comportamenti controproducenti

Si nota che i partecipanti dispongono di un basso punteggio per i comportamenti controproducenti, confermando il risultato del test BIG.5 che la resilienza e l'alto tasso di tolleranza sono aspetti importanti per il lavoro di un professionista della sicurezza delle informazioni. Guardando nelle singole categorie, i fattori più importanti sono "l'aggiornamento delle conoscenze relative al lavoro" (2,32) e la "partecipazione attiva" tra le prestazioni contestuali, una debole "attenzione agli aspetti negativi del lavoro" (1,59) e un forte orientamento alla "gestione dei problemi" (1,53) tra i comportamenti controproducenti e un'alta attenzione alla "definizione delle priorità" (2,36) e "focalizzata sui risultati" (2,32 nell'attenzione al compito.

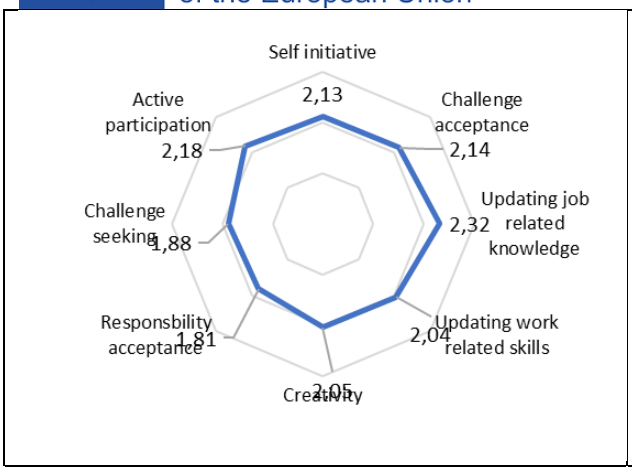


Figura 15: Performance in un determinate con-testo

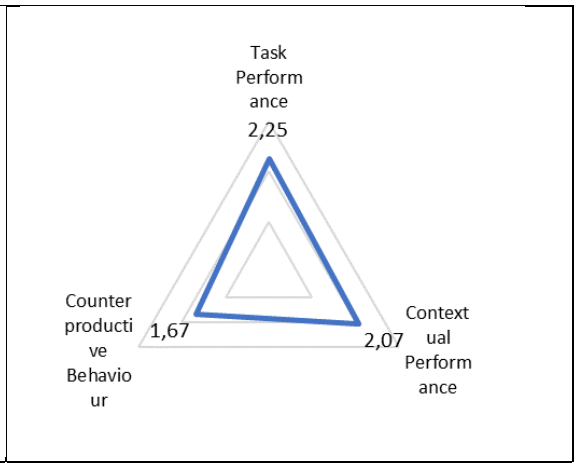


Figura 16: IWPQ risultati per espertio di ITS

Come mostrato nella Figura 28, la misura per l'attenzione al compito è più alta delle altre misure, e la misura per la prestazione in un determinato contesto è più alta di quella per il comportamento controproducente. Questi risultati sono in linea con gli studi precedenti. Tuttavia, l'attenzione al compito è significativamente più bassa rispetto ai risultati di base di altri articoli, indicando problemi in questo campo - le misure più alte per il comportamento controproduttivo confermano questa constatazione. La misura per la performance contestuale è anche inferiore a quella di altri studi, ma non in modo significativo.

In conclusione, possiamo dire che i partecipanti del campo dell'IT e della sicurezza dell'informazione sono meno produttivi di quelli solitamente osservati negli studi pertinenti.

4.3 Riepilogo

Tutto sommato, lo studio fornisce importanti approfondimenti sulla sicurezza informatica nelle PMI. Per quanto riguarda la situazione sul mercato del lavoro e la capacità nelle aziende, va detto che in più del 50 % delle aziende non c'è nessun dipendente formalmente responsabile della sicurezza informatica. Se i partecipanti hanno risposto affermativamente, nella maggior parte dei casi solo un dipendente è responsabile di questo settore di attività. Guardando lo sviluppo delle offerte di lavoro si possono osservare pochi cambiamenti. Una frazione delle aziende creerà da sei a dieci posti di lavoro nel settore della sicurezza dell'informazione nei prossimi cinque anni.

I risultati confermano il principio del "learning by pain", vale a dire che prima che le aziende si impegnino in attività di sicurezza deve verificarsi un incidente. Questa affermazione è sostenuta dai risultati coerenti riguardanti le certificazioni, la creazione di posizioni specifiche e in generale le misure adottate in materia di sicurezza informatica.

Per quanto riguarda il tipo di formazione richiesto si può sottolineare la grande importanza dell'esperienza professionale. Quasi la metà dei partecipanti ha dichiarato che questo è particolarmente importante. In generale, gli intervistati preferiscono avere un dipendente con esperienza piuttosto che con istruzione. Alla luce dell'attuale scarsità di possibilità di assunzione sul mercato del lavoro, le aziende considerano l'ulteriore qualificazione dei dipendenti esistenti come l'opzione più fattibile per coprire il bisogno di risorse umane.

Infine, una valutazione dei tratti caratteristici tramite il test della personalità Big 5 e l'IWPQ, sono stati identificati importanti profili degli impiegati che possono essere individuati tra i nuovi impiegati da inserire nel settore. Una forte disposizione di resilienza in entrambi i test,

soprattutto una routine di lavoro organizzata e un approccio critico e analitico sono stati determinati come elementi distintivi per gli specialisti della sicurezza informatica.

5 Linee guida per le PMI

La protezione dei dati e la sicurezza delle informazioni hanno acquisito una rilevanza significativa man mano che l'applicazione delle ICT è diventata più intensa nei processi organizzativi e gestionali all'interno delle PMI. La pressione delle PMI per gestire meglio la sicurezza delle informazioni e la protezione dei dati deriva da diverse cause. In primo luogo, il processo e la gestione dei dati nelle PMI sono diventati altamente dipendenti dall'infrastruttura ICT. Secondo, la legislazione che riguarda la privacy e la protezione dei dati è stata rafforzata e codificata in modo più dettagliato. In terzo luogo, la consapevolezza pubblica sul diritto alla privacy e la responsabilità per l'uso dei dati personali è aumentata. Diversi incidenti di fuga di dati in tutto il mondo hanno anche giocato un ruolo nel rendersi conto che la sicurezza delle informazioni è una questione prioritaria quando si usano i servizi digitali. Le PMI sono state interessate dalla digitalizzazione in misura minore rispetto alle grandi imprese. Tuttavia, una parte significativa di esse lavora con documenti digitali personali. Alcune delle PMI gestiscono dati sensibili. Tutti questi fattori gettano le basi per una migliore regolamentazione e garanzia della sicurezza delle informazioni e della protezione dei dati nelle PMI. Il regolamento aggiornato dall'Unione europea ha lasciato alcune PMI in difficoltà nel trovare o preparare personale adatto che possa soddisfare i requisiti più severi per la sicurezza delle informazioni e la protezione dei dati.

1 L'implementazione del GDPR ha portato a cambiamenti significativi nelle pratiche di gestione dei record digitali e fisici per le PMI. Alcune organizzazioni non avevano un'infrastruttura fisica e digitale adeguata per soddisfare i nuovi requisiti. Nella maggior parte dei casi il periodo di transizione prima dell'attuazione del GDPR è stato utilizzato per compensare le carenze infrastrutturali. Una delle azioni più tangibili per le PMI è quella di verificare le condizioni dell'infrastruttura fisica e correggere le carenze che impediscono di soddisfare i requisiti per una corretta sicurezza informatica e la garanzia di protezione dei dati nell'organizzazione. In primo luogo, c'è bisogno di un documento interno che definisca le procedure e i regolamenti relativi alla sicurezza informatica e alla protezione dei dati (comprese le regole aziendali vincolanti se l'organizzazione trasferisce i dati in paesi non UE). In secondo luogo, ci devono essere limitazioni di accesso fisico ai record fisici (armadietti, casseforti, aree ad accesso limitato). Il personale deve essere informato sulle procedure relative alla gestione dei dati (restrizioni alla divulgazione delle informazioni, tenere i registri chiusi dall'accesso pubblico, politiche di consenso all'uso dei dati, password e posto di lavoro security policies, user rights management).

2 Gli interessati (clienti) devono essere informati sulle pratiche di gestione dei dati nelle aree in cui i loro dati vengono utilizzati. I clienti hanno bisogno di concedere l'accesso ai dati personali, e di essere informati sul diritto di chiedere la correzione dei dati relativi, opporsi al trattamento, ritirare il consenso all'accesso ai dati, presentare un reclamo, chiedere la cancellazione dei record, opporsi alle transazioni di dati con altri soggetti di gestione dei dati.

3 Un'altra area in cui le PMI riscontrano incoerenze con i regolamenti sulla sicurezza delle informazioni e la protezione dei dati è la raccolta di dati che non dovrebbero essere raccolti o immagazzinati dati vengono solitamente raccolti a seguito di processi di flussi di lavoro obsoleti. In alcuni casi, i dati sono legati a sistemi informativi o altre misure di identificazione digitale. Per evitare questi casi le PMI dovrebbero concentrarsi sulla conservazione della quantità minima di dati necessari e cancellare i dati se il loro scopo d'uso è irrilevante. I dati

esistenti dovrebbero essere conservati e gestiti sulla base di algoritmi e procedure trasparenti. Politiche di sicurezza come "scrivania pulita" o "schermo bloccato" dovrebbero essere considerate come predefinite nelle PMI.

4 La quarta linea guida è legata alla qualità dell'istruzione e della certificazione. L'analisi della letteratura e le storie dirette dei dipendenti delle PMI rivelano che per le piccole e medie organizzazioni la certificazione non è il modo ottimale per scegliere i candidati che potrebbero lavorare con informazioni private. Il criterio principale è la conoscenza e le competenze che riguardano l'ICT e il settore legale, così come altre abilità sociali più interdisciplinari. Le PMI di solito non hanno risorse adeguate per assumere specialisti ben addestrati per mantenere l'infrastruttura informativa. Inoltre, i campi di attività delle varie PMI variano molto. Questo crea un problema in cui i corsi di formazione universali o i certificati non dotano i dipendenti di conoscenze specifiche, applicabili in ambiti ristretti. Le PMI richiedono corsi di formazione applicabili praticamente e basati su scenari con esempi di situazioni reali. Uno dei modi per garantire che queste informazioni siano disponibili è quello di documentare i processi all'interno dell'organizzazione e poi condividere le esperienze attraverso reti professionali o eventi comunitari. In alternativa, le PMI potrebbero avviare una cooperazione con gli istituti di istruzione superiore che potrebbero analizzare scientificamente i casi arricchendo il corpo di conoscenze esistenti in ambiti specifici.

5 L'ultima linea guida è legata alle incoerenze o imperfezioni dei regolamenti legali. Per alcune istituzioni, le limitazioni allo scambio di informazioni e dati personali possono essere un serio onere per garantire gli interessi dei loro clienti. Per esempio, una casa di riposo ha un residente costante che non ha più membri della famiglia. In caso di emergenza il residente viene portato all'ospedale, l'istituzione attuale non dà informazioni private a terzi (compresa la casa di riposo). Se il cliente viene trasferito in un altro ospedale, la casa di riposo deve fare le proprie indagini per trovare il suo residente. In questo caso entrambe le istituzioni obbediscono alla legge, ma la situazione crea delle lacune legali che devono essere corrette. Le PMI dovrebbero avviare la correzione o l'avvio di norme giuridiche (attraverso i rappresentanti politici) che coprano tali questioni.

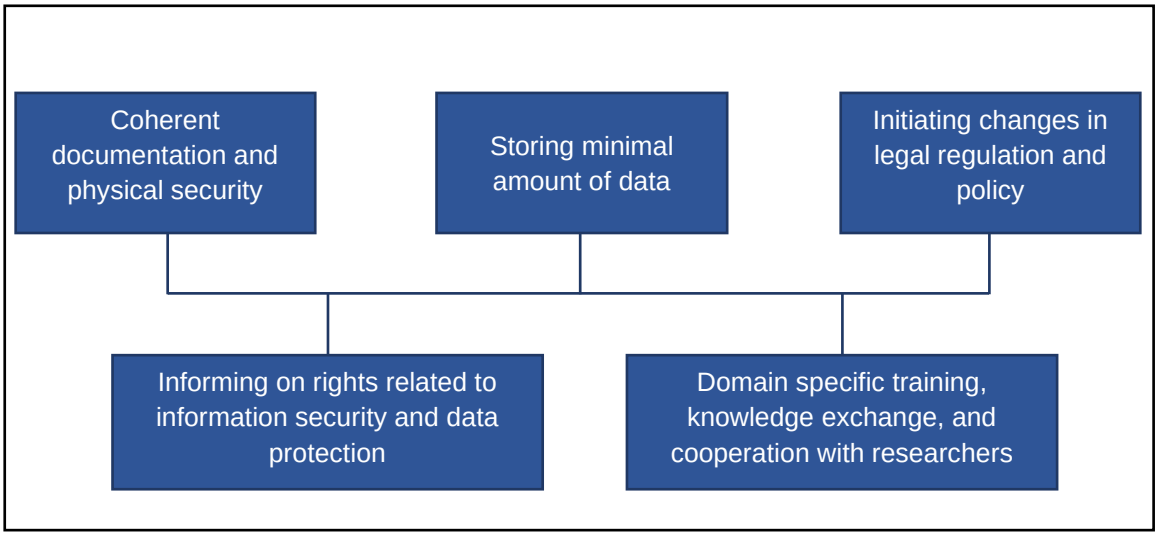


Figura 29: Linee guida basate su problemi comuni che le PMI affrontano nella sicurezza delle informazioni e nella protezione dei dati

6 Prospettive e raccomandazioni

Durante la realizzazione del progetto TeBeISi, le attività hanno rivelato che il bisogno di formazione sulla sicurezza informatica e la protezione dei dati personali per le piccole e medie imprese e le istituzioni sociali è alto. Queste organizzazioni spesso affrontano costi finanziari elevati per assumere un professionista della protezione dei dati, quindi spesso queste funzioni sono assegnate a un altro dipendente. L'obiettivo è quello di rispettare i requisiti del GDPR e garantire la protezione dei dati personali sia dei clienti che dei dipendenti dell'azienda. Il progetto ha anche dimostrato che la formazione sulla sicurezza informatica e la protezione dei dati personali è relativamente costosa e che le PMI sono molto felici di ricevere gratuitamente una formazione di qualità sull'uso del GDPR (formazione sostenuta dal progetto Erasmus plus) e di migliorare le competenze del personale nelle aree della sicurezza informatica e della protezione dei dati personali.

Il questionario sviluppato durante il progetto ha permesso ai dipendenti delle piccole e medie imprese di valutare le loro competenze esistenti nel campo della sicurezza delle informazioni e della protezione dei dati personali. Il programma di studi creato durante il progetto dà alle parti interessate la possibilità di scegliere la formazione appropriata. I partner associati, le PMI, le istituzioni educative e le autorità pubbliche hanno espresso interesse a continuare il percorso del progetto TeBeiSi e a costruire sui risultati del progetto in iniziative future. Pertanto, i partner del progetto prevedono di continuare le attività congiunte e di sviluppare e testare un pacchetto di formazione in tutti i paesi partner del progetto durante il prossimo progetto.

Le attività del progetto implementate permettono di raccomandare alle aziende di prestare maggiore attenzione alla comunicazione interna e alla formazione (sia organizzando corsi di formazione nelle aziende che inviando i dipendenti ai corsi di formazione). Tutti i dipendenti, specialmente quelli che entrano in contatto diretto con i dati personali nell'ambiente di lavoro, dovrebbero essere consapevoli dei requisiti di protezione dei dati, essere costantemente formati su cosa sono i dati personali, come riconoscerli, cosa può e non può essere fatto con i dati personali. È anche necessario fare una valutazione realistica dei requisiti per la raccolta dei dati personali, cioè mantenere un fondo di surplus, necessario solo per i dati personali raccolti. Le piccole e medie imprese così come le istituzioni di servizi sociali dovrebbero valutare l'impatto del GDPR e identificare le aree problematiche, il che consentirebbe di avere tempo per la formazione e la sensibilizzazione dei dipendenti.

Si suggerisce inoltre che le aziende eseguano prima un audit dei dati personali che raccolgono e detengono, al fine di identificare su quali operazioni di trattamento dei dati concentrarsi. Questo aiuterebbe a rivelare quali processi relativi alla gestione dei dati personali e alla sicurezza delle informazioni richiedono ulteriore attenzione e competenze del personale da migliorare. Dal questionario condotto si può dedurre che le PMI sono più a loro agio con gli investimenti formativi sui dipendenti esistenti, producendo il trade-off più conveniente per quanto riguarda le risorse necessarie e la sicurezza.

7 Letteratura

Adamkiewicz, S. L. (2005). *The correlation between productivity and the use of information security controls in small businesses.* Dissertation Abstracts International, 66(03), 1541B. (UMI No. 3167184).

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. Anintervention study. *Computers & Security, 29*(4), 432–445. doi: 10.1016/j.cose.2009.12.005

Anderson, C. L. & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Baker, W. H., & Wallace, L. (2007). Is information security under control? *IEEE Security & Privacy,* 5, 36-44. doi:10.1109/MSP.2007.11.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems*, *19*(8), 689–715. doi: 10.17705/1jais.00506

Barnard-Wills, D., Cochrane, L., Matturi, K. & Marchetti, F. (2019). *Report on the SME experience of the GDPR*. https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. doi: 10.2307/25750690

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. *Decision Sciences*, *49*(6), 1187–1228. doi:10.1111/deci.12304

Burns, A.J., Roberts, T.L., Posey, C., Bennett, R.J., & Courtney, J.F. (2015). Assessing the role of security education, training, and awareness on insiders' security related behavior: An expectancy theory approach. *Proceedings of the IEEE 48th Hawaii International Conference on Systems Sciences, HI.* doi:10.1109/HICSS.2015.471

Colwill C. (2009). Human factors in information security: the insider threat–who can you trust these days? Information Security Technical Report, *14*(4),186–96. doi:10.1016/j.istr.2010.04.004

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security counter measures. *Journal of Business Ethics*, *89*(1),59–71. doi:10.1007/s10551-008-9909-7

D'Arcy, J., Hovav, A, Galletta, D. (2009). User awareness of security counter measures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98. doi: 10.1287/isre.1070.0160

Davies, J. S., & Hertig, A. C. (2008). *Theory and practice of asset protection. Security, supervision and management*. Burlington, MA: Elsevier.

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal, 18*, 20-38.

Easttom, C. (2006).
Computer security fundamentals. Upper Saddle River, NJ: Prentice Hall.

Path to Cyber Resilience: Sense, Resist, React. EY's 19th Global Information Security Survey 2016-17. https://www.ey.com/Publication/vwLUAssets/EY-giss-india/$FILE/EY-giss-india.pdf

Eurostat (2008): NACE Rev. 2. Online verfügbar unter https://ec.europa.eu/eurostat/de/web/nace-rev2, zuletzt geprüft am 08.07.2021.

European Comission (2021): SME definition - Internal Market, Industry, Entrepreneurship and SMEs. Online verfügbar unter https://ec.europa.eu/growth/smes/sme-definition_en, zuletzt aktualisiert am 30.08.2017, zuletzt geprüft am 08.07.2021.

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*. New York, NY: Elsevier.

Goodwin, B. (2005, February 14). *Big guns target supply chain threat. Computer Weekly*. http://www.computerweekly.com/.

Guinote, A., & Vescio, K. T. (2010). *The social psychology of power*. New York, NY. The Gilford Press.

Hallová, M., Polakovič, P., Šilerová, E., & Slováková, I. (2019). Data Protection and Security in SMEs under Enterprise Infrastructure. *Agris On-Line Papers in Economics & Informatics*, *11*(1), 27–33. doi:10.7160/aol.2019.110103

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. doi: 10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. doi: 10.1057/ejis.2009.6

Yoo, C.W., Sanders, G.L., & Cerveny, R.P. (2018). Exploringthe influence of flow and psychological ownership on security education, training, and awareness effectiveness and security compliance. *Decision Support Systems*, *108*, 107-118. doi: https://doi.org/10.1016/j.dss.2018.02.009

Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R. & Barnard-Wills, D. (2021). *The GDPR Made Simple(r) for SME's*. doi: 10.46944/9789461171092

Jenkins, J. L. & Durcikova, A. (2013). What, I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior. *Proceedings of the International Conference on Information Systems*. AIS. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.661.9290&rep=rep1&type=pdf

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34(*3), 549-566. doi: 10.2307/25750691

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134. doi: 10.25300/MISQ/2015/39.1.06

Jöns, Ingela; Hodapp, Markus; Weiss, Katharina (2005): Kurzskala zur Erfassung der Unternehmenskultur. Online verfügbar unter http://psydok.psycharchives.de/jspui/handle/20.500.11780/349.

Karjalainen, M., & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555.

Kluge, EH. (2007). Secure e-health: managing risks to patient health data. International Journal of Medical Informatics**,** *76* **(**5–6**)**, 402-406**.** doi: 10.1016/j.ijmedinf.2006.09.003

Kogenhop, G. (2020). Tooling for optimal resilience. *Journal of Business Continuity & Emergency Planning*, *13*(4), 352–361.

Kumar, V., Batista, L. & Maull, R. (2011). The Impact of Operations Performance on Customer Loyalty. *Service Science*, *3*(2), 158-171. doi:10.1287/serv.3.2.158

Kuusisto, T., & Ilvonen, I. (2003). Information Security Culture in Small and medium size enterprises. *Frontiers of e-business research*, 431-439.

Lee, J. K., Cho, D., & Lim, G. G. (2018). Design and validation of the Bright Internet. *Journal of the Association for Information Systems*, 19(2), 63-85.

Leede, J. & Looise, J. K. (2005). Innovation and HRM: Towards an integrated framework. *Creativity and Innovation Management, 14* (2), 108-117. doi: 10.1111/j.1467-8691.2005.00331.x.

Leilanie Del Prado-Lu, J. (2005). *Gender, information technology, and health*. Quezon City, Philippines: The University of the Philippines Press.

Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413.

McAfee, I. (2010). *A good decade for cyber crime*. http://www.mcafee.com/ca/resources/reports/rp-good-decade-for-cyber crime.pdf.

McConnell, J. P. (2020). *UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases Challenges on Heuristics and Biases*. https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2127&context=gscis_etd.

Mohjel Eghdam, A., Khameneh, S., Hasankhni, H, Moghadam, S., Zamanzadeh V. (2013). Nurses' performance on Iranian nursing code of ethics from Patients' perspective. *26*(84),1–11. doi: 10.5681/jcs.2013.027

Newell, S., & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of datification. *The Journal of Strategic Information Systems, 24*(1), 3-14. doi: 10.2139/ssrn.2644093

Noguerol, L. O., & Branch, R. (2018). Leadership and Electronic Data Security within Small Businesses: An Exploratory Case Study. *Journal of Economic Development, Management, IT, Finance & Marketing*, *10*(2), 7–35.

Northouse, P. G. (2010). *Leadership: Theory and practice* (5th ed.). Thousand Oaks, CA: Sage.

O'Rourke, M. (2003). Cyber attacks prompt response to security threat. *Risk Management, 50*(1), 8.

Peikari, H. R., T., R.,
Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. *BMC Medical Informatics & Decision Making*, *18*(1), 1–13. doi:10.1186/s12911-018-0681-z

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of asystematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189–1210. doi: 10.25300/MISQ/2013/37.4.09

Posey, C., Roberts, T., & Lowry, P.B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179–214. Doi: 10.1080/07421222.2015.1138374

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quar-terly*, *34*(4), 757–778. doi: 10.2307/25750704

Rammstedt, Beatrice; Kemper, Christoph J.; Klein, Mira Céline; Beierlein, Constanze; Kovaleva, Anastassiya (2013): A Short Scale for Assessing the Big Five Dimensions of Personality. 10 Item Big Five Inventory (BFI-10). In: GESIS - methoden, daten, analyse 7 (2), S. 233–249.

Ramos-Villagrasa, Pedro J.; Barrada, Juan R.; Fernández-del-Río, Elena; Koopmans, Linda (2019): Assessing Job Performance Using Brief Self-report Scales: The Case of the Individual Work Performance Questionnaire. In: Revista de Psicología del Trabajo y de las Organizaciones 35 (3), S. 195–205. DOI: 10.5093/jwop2019a21.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). In: Official Journal of the European Union L 119, S. 1–88.

Richardson, R. (2008). *CSI computer crime and security survey*. http://www.cse.msstate.edu/~cse6243/ readings/CSIsurvey2008.pdf.

Sabeeh, A., and Lashkari, A. H. (2011). *Users' Perceptions on Mobile Devices Security Awareness in Malaysia.* International Conference for Internet Technology and Secured Transactions, Abu Dhabi: IEEE, 428-435.

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things*. Information Systems Frontiers*, *18*(4), 665-677.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. doi: doi.org/10.1016/j.comnet.2014.11.008

Siponen, M., & Vance, A.O. (2010). Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterly*, *34*(3), 87–502.

Siponen, M., Mahmood, M., & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145-147. doi: 10.1145/1610252.1610289

Smith, M. (2003). Business process design: correlates of success and failure. *The Quality Management Journal, 10* (2) 38-49. doi: 10.1080/10686967.2003.11919062.

The European Parliament and the Council of the European Union (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed 31st January, 2020).

The European Parliament and the Council of the European Union (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 31st January, 2020).

van Zadelhoff, M., Lovejoy, K., & Jarvis, D. (2014). *Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment*. https://www.ibm.com/smarterplanet/us/en/centerforappliedinsights/article/ciso_insights.html.

von Solms, S. H., & von Solms, R. (2009*). Information security governance*. NewYork, NY: Springer.

Weber, R. H. (2010). Internet of Things: New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. doi: 10.1016/j.clsr.2009.11.008

Whitman, M.E., & Mattord, H.J. (2012). *Principles of Information Security* (4thed.). Boston, MA: Course Technology.

Wilkinson, G. (2018). General Data Protection Regulation: No silver bullet for small and medium-sized enterprises. *Journal of Payments Strategy & Systems*, *12*(2), 139–149.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *Management Information Systems Quarterly*, *37* (1): 1–20. doi:10.25300/MISQ/2013/37.1.01

Rapporto di ricerca

Ringraziamo i co-autori ed editors

Simon Rath

Prof. Irena Žemaitaitytė

Mgr. Agata Katkonienė

Assoc. Prof. Marius Kalinauskas

Prof. Odeta Merfeldaitė

Assoc. Prof. Asta Railienė

Ivan Kharitonov

Teresa Rauenbusch

Certificazione parziale nel campo professionale della sicurezza informatica - TeBeISi

Finanziato dal programma Erasmus+ dell'Unione Europeahttps://information-security-in-sme.eu/.