UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

Cyber Risk Self Assessment

Autovalutazione del livello di Sicurezza Informatica delle PMI

Report 2020

cini Cybersecurity National Lab

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

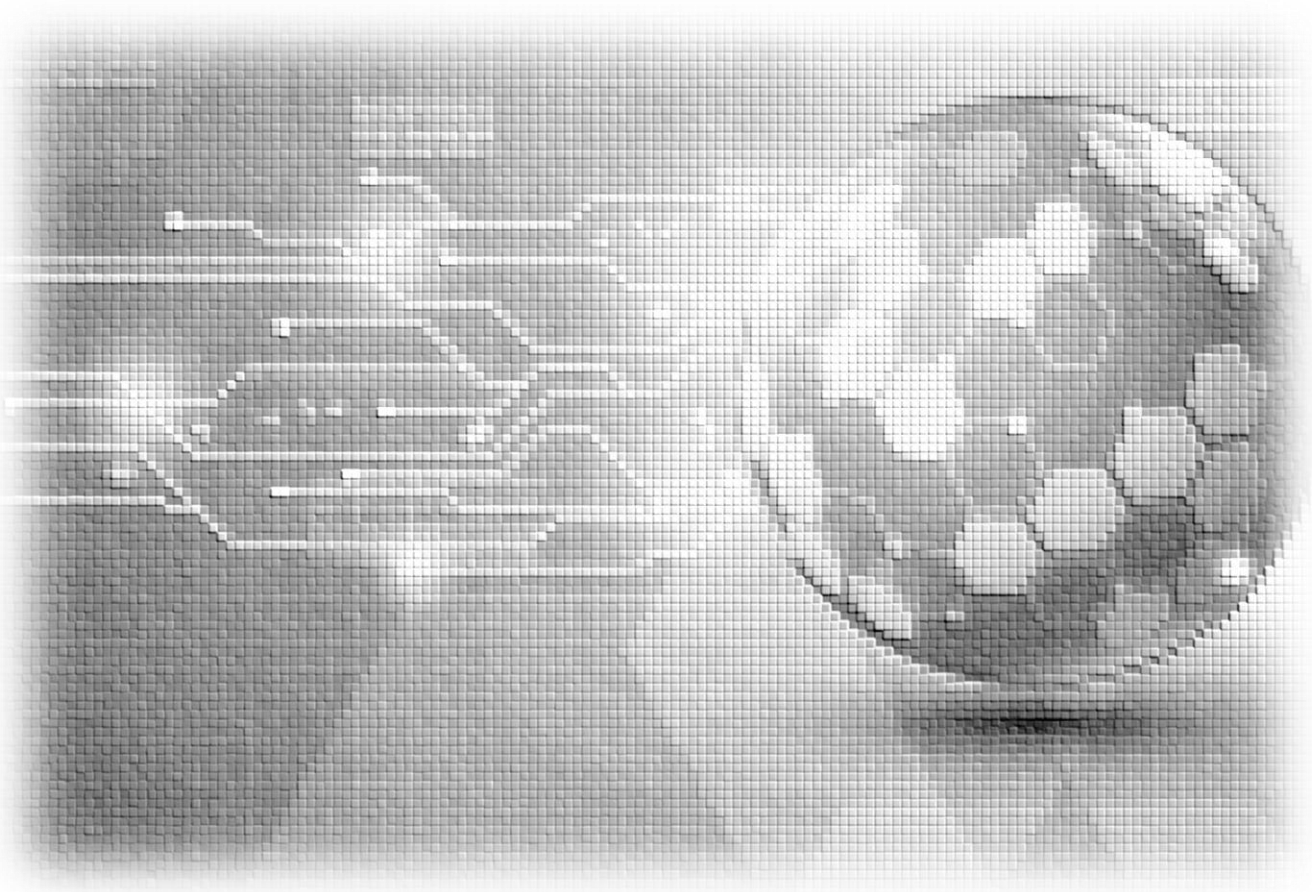
UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

cini Cybersecurity National Lab

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA

Cyber Risk Self Assessment

Autovalutazione del livello di Sicurezza Informatica delle PMI



Responsabili del Progetto

Rocco Mammoliti POSTE ITALIANE SPA, *Sezione IT Unindustria, Cybersecurity*
Aniello Gentile ENEL SPA, *Sezione IT Unindustria, Cybersecurity*

Progetto promosso da

Vittoria Carli, *Presidente Sezione Information Technology, Unindustria*

in collaborazione con

Francesco d'Angelo, *Presidente Sezione Comunicazioni, Unindustria*

Elaborazioni a cura di

Matteo Giacalone, POSTE ITALIANE SPA
Vincenzo Caserta, CAPGEMINI ITALIA SPA
Luigi Martino, UNIVERSITA' DI FIRENZE, *Laboratorio Nazionale di Cybersecurity*
Marco Angelini, UNIVERSITA' LA SAPIENZA, *CIS Sapienza, Laboratorio Nazionale di Cybersecurity*
Gabriele Oliva, UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA
Roberto Setola, UNIVERSITA' CAMPUS BIO-MEDICO DI ROMA

Hanno collaborato nel Gruppo di lavoro :

Marco Massenzi, TELECONSYS SPA
Vincenzo Bianchini, TECNOLOGIE E COMUNICAZIONI SRL
Ascenzo Asseri, TIM SPA
Paolomaria Innocenzi, TIM SPA
Marco Francola, GFX SRL
Antonio Amati, ALMAVIVA SPA
Roberto Casini, BT ITALIA SPA
Michele Onorato, WESTPOLE SPA

Si ringraziano tutti i membri del Consiglio Direttivo della Sezione IT di Unindustria - Unione degli Industriali e delle imprese di Roma Frosinone Latina Rieti Viterbo, per gli stimoli ed i contributi ricevuti

CONTENTS

Prefazione

Alzare il livello di sensibilizzazione e consapevolezza sui rischi derivanti dal mondo cyber e le opportunità di investire nell'innalzamento del livello di cybersecurity è un approccio necessario che ciascun Paese deve affrontare oggi per aumentare la sua resilienza verso attacchi informatici che provengono da gruppi di cyber-criminali sempre più organizzati e avanzati.

L'incremento della sensibilizzazione richiede, tra l'altro, la disponibilità di strumenti che, in modo semplice e intuitivo, permettano di misurare il livello di "preparazione" (readiness) di ciascuno, sia in funzione del proprio ruolo all'interno dell'organizzazione/istituzione cui appartiene, sia come "semplice" cittadino. Anche in questo campo, come peraltro in moltissimi altri quando si parla di cybersecurity, è necessaria una forte sinergia e una stretta cooperazione e condivisione di risorse, dati e informazioni tra tutti i soggetti, siano essi pubblici o privati.

Questo lavoro si colloca esattamente in questo filone ed è il risultato di una iniziativa congiunta tra il Laboratorio Nazionale Cybersecurity del CINI (https://cybersecnatlab.it) e Unindustria, mirata a misurare il livello di readiness delle PMI italiane. I dati in esso raccolti e analizzati costituiscono un primo importante tassello di un progetto più ambizioso al fine di garantire un'adeguata diffusione della sicurezza cyber per l'intero Sistema Paese.

In particolare, il progetto promosso da Unindustria svolge un ruolo di promotore e catalizzatore di numerose altre iniziative analoghe rivolte a obiettivi diversi in tutte le varie Regioni e nei domini verticali più diversificati.

Paolo Prinetto

Direttore del Laboratorio Nazionale Cybersecurity del CINI

INTRODUZIONE

Le **Piccole e Medie Imprese** rappresentano la spina dorsale ed un prezioso *humus* per la crescita economica, sociale e culturale del Paese.
Per tale crescita, la trasformazione digitale con la conseguente digitalizzazione dei servizi e dei processi produttivi, costituisce un fattore critico di successo, che permette di cogliere ed affrontare al meglio le sfide offerte dalla globalizzazione e dalla rivoluzione informatica.
In questo scenario, diventa essenziale per ogni Azienda garantire adeguati livelli di sicurezza informatica, in linea con l'andamento tecnologico a livello internazionale, in quanto l'esposizione ai rischi informatici e cyber rappresenta un fattore ineludibile, in continua evoluzione, senza confini e capace di infliggere danni incommensurabili alle realtà non protette.
Risulta pertanto essenziale e strategico, al fine di salvaguardare il business dell'impresa, il know-how, la reputazione, i servizi digitali e la sicurezza dei dati dei propri Clienti, avere piena conoscenza del livello di preparazione e maturità di cybersecurity della propria Azienda, capace di indicare gli eventuali punti di miglioramento per poter raggiungere un livello di protezione adeguato ed in linea con gli standard e le best practice internazionali.
Il **progetto Cyber Risk Self-Assessment** è stato sviluppato dalla Sezione Information Technology di **Unindustria**, sulla scia dell'esperienza simile sviluppata da Assolombarda, in coordinamento con le Sezioni Comunicazioni e Sicurezza, e con la collaborazione scientifica del **Laboratorio Nazionale di Cybersecurity del CINI** e **dell'Università Campus Biomedico di Roma.** I risultati di questo progetto, insieme alle future iniziative, sono a disposizione del Sistema Paese per garantire una migliore protezione sotto il profilo cyber e della sicurezza informatica delle PMI italiane, a garanzia e tutela delle loro competenze, dei loro prodotti e del loro know-how.

1 PMI E CYBER SECURITY

l'Italia con il suo tessuto economico ed aziendale costituito in gran parte di PMI è uno dei Paesi più esposti al rischio ed alla minaccia cyber. In particolare, il Sistema di *intelligence* italiano fa notare che: "l'attività a protezione del know-how tecnologico e innovativo delle imprese italiane ne ha registrato la persistente esposizione ad iniziative di spionaggio industriale, specie con modalità cyber agevolate dalla digitalizzazione pressoché integrale dei processi produttivi e più pervasive nei confronti delle piccole e medie imprese".[1]

Questo assunto evidenzia l'interazione esistente tra minaccia cyber (capace di pervadere l'intero tessuto economico del Paese) e la continua necessità di mantenere sicuri i sistemi informatici delle aziende. In aggiunta a ciò, emerge che la minaccia informatica è sempre di più affiancata al rischio sistemico dovuto dalla percezione - ancora troppo diffusa - che la cyber security sia da intendere come una spesa, invece che un investimento.

Tale situazione è stata validata anche dalle osservazioni e dalle evidenze empiriche emerse durante la ricerca effettuata per il progetto Cyber Risk Self-Assessment. In particolare, come illustrato dai grafici presenti in questo report, dalla comparazione di tutti *cluster* di riferimento (Commitment Aziendale; Livello di Esposizione e Maturità Tecnologica) è emerso che le PMI italiane, a differenza delle Grandi Aziende, scontano un basso livello di consapevolezza rispetto ai rischi, alle minacce e anche alle opportunità relative alla cyber security.

I grafici mettono in evidenza quindi un trade-off negativo. Infatti, benché vi sia un'elevata interdipendenza tra Grandi Aziende e PMI, queste ultime hanno minore capacità di comprendere la portata dei rischi cyber, mettendo così a rischio l'intera struttura della *supply chain*. Questo basso livello di consapevolezza, affiancato alla elevata necessità di informatizzazione dei processi produttivi, implica un'esposizione crescente dell'intero Sistema Paese ai pericoli provenienti dal mondo digitale. Risulta quindi di particolare importanza stabilire una collaborazione continua e sinergica tra Istituzioni e imprese al fine di raggiungere una piena "consapevolezza sui temi delle minacce all'economia e al Sistema Paese, specie nella dimensione cyber".[2]

La rilevanza strategica dell'infrastruttura digitale e della *supply chain* è emersa, in modo evidente, soprattutto in occasione della pandemia Covid-19. In tale occasione infatti, "l'ambiente digitale" si è rilevato indispensabile per garantire la "business continuity", attraverso le attività aziendali svolte da remoto (c.d. *smart working*). Allo stesso tempo, l'elevata esposizione digitale delle attività produttive e aziendali condotte "da casa" ha aumentato i rischi cyber dovuti a un basso livello di sicurezza degli strumenti informatici delle nuove postazioni lavorative.

In linea con tali premesse, il **Progetto Cyber Risk Self-Assessment** mira a valutare lo "stato di preparazione cyber" del tessuto economico e produttivo del Paese, attraverso un'analisi approfondita della postura delle PMI nei confronti delle dinamiche informatiche e cyber.

Il **fine ultimo** è di duplice portata: da un lato lo studio si pone l'obiettivo di **dedurre osservazioni scientifiche rispetto alla preparedness delle PMI** nel contesto di riferimento, al fine di proporre strumenti, processi e modelli organizzativi in grado di affrontare l'andamento della minaccia cyber. Dall'altro, grazie agli indicatori forniti dalla survey è possibile **estrapolare delle informazioni chiave per i decisori politici e aziendali** al fine di emanare apposite *policies* sui fabbisogni specifici delle PMI italiane rispetto al cyber risk, con l'obiettivo di favorire la diffusione della sicurezza informatica in Italia.

[1] Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla Politica dell'Informazione per la Sicurezza 2019* https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2020/03/RELAZIONE-ANNUALE-2019-4.pdf

[2] Ibidem

2 IL PROGETTO

Il Progetto trae origine dalla riconosciuta centralità del ruolo rivestito dalle Piccole e Medie Imprese per il Paese, cuore pulsante e prezioso humus per la crescita economica, sociale e culturale. Per tale crescita, la trasformazione digitale con la conseguente digitalizzazione dei servizi e dei processi produttivi, rappresenta ormai un fattore critico di successo, che permette di cogliere ed affrontare al meglio le sfide offerte dalla globalizzazione.

In questo scenario, diventa essenziale per ogni Azienda garantire adeguati livelli di sicurezza informatica, in linea con lo stato dell'arte a livello mondiale, in quanto l'esposizione ai rischi informatici ed al cyber risk è una urgenza sempre più attuale, in continua evoluzione, senza confini e capace di infliggere danni di varia natura alle realtà non protette.

Il Progetto si pone come obiettivo generale quello di valutare il livello di sicurezza ed esposizione delle PMI ai rischi cyber, valutarne i fabbisogni in termini generali e, conseguentemente, aumentarne consapevolezza e capacità di tutela del patrimonio aziendale.

- Maggiore Consapevolezza e stato dell'arte delle PMI in ambito Sicurezza Informatica
- Misurazione Statistica del livello di Rischio Cyber delle PMI, clustering e identificazione dei Fabbisogni
- Strumenti e Servizi di Sicurezza Informatica «Made In Italy» utili per una migliore protezione

Il Progetto si articola dunque nelle seguenti macro fasi:

3 CYBER SECURITY SURVEY

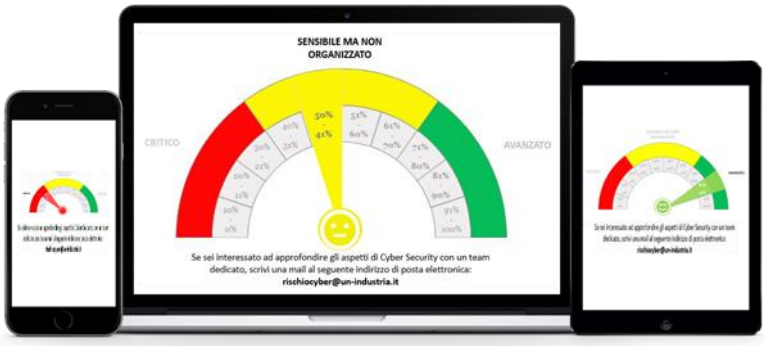
La Cyber Security Survey è un questionario che si compone di 32 domande suddivise tra domande di carattere generale sull'organizzazione della società ovvero fatturato annuo, numero di dipendenti, forma societaria ecc. e domande di carattere tecnico/organizzativo.

Le domande di carattere generale hanno lo scopo di posizionare l'Azienda tra Micro, Piccola, Media, Grande Azienda secondo quanto definito dall'Articolo 2 del decreto ministeriale del 18/04/2005 [5]:

> *"1. La categoria delle microimprese, delle piccole imprese e delle medie imprese (complessivamente definita PMI) è costituita da imprese che:*
>
> *a) hanno meno di 250 occupati, e*
>
> *b) hanno un fatturato annuo non superiore a 50 milioni di euro, oppure un totale di bilancio annuo non superiore a 43 milioni di euro.*
>
> *2. Nell'ambito della categoria delle PMI, si definisce piccola impresa l'impresa che:*
>
> *a) ha meno di 50 occupati, e*
>
> *b) ha un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro.*
>
> *3. Nell'ambito della categoria delle PMI, si definisce microimpresa l'impresa che:*
>
> *a) ha meno di 10 occupati, e*
>
> *b) ha un fatturato annuo oppure un totale di bilancio annuo non superiore a 2 milioni di euro."*

La compilazione della Cyber Security Survey da parte delle Aziende è anonima al fine di non profilare le Aziende che rispondono rispetto all'output della Survey e di conseguenza rendere più autentiche le risposte.

La Survey, disponibile al seguente link https://it.surveymonkey.com/r/95JBQW9, fornisce un output immediato sullo stato della sicurezza della PMI.



Le domande della Survey sono elencate nella tabella seguente:

COD.	DOMANDA
A1.1	Organizzazione dell'azienda - Tipologia di azienda
A1.2	Organizzazione dell'azienda - Anni di attività dell'azienda
A1.3	Organizzazione dell'azienda - N° sedi dell'azienda
A1.4	Organizzazione dell'azienda - Provincia della sede operativa principale
A2.1	Dimensione dell'azienda - Numero di dipendenti dell'azienda
A2.2	Dimensione dell'azienda - Fatturato medio annuo nell'ultimo triennio
A3	Selezionare la sezione di appartenenza a UNINDUSTRIA / attività prevalente
A4	La tua azienda ha un reparto interno che cura gli aspetti di Cyber Security?
A5	Nella tua azienda vengono censiti i sistemi e gli apparati fisici in uso (dispositivi mobili, computer, server, etc.)?
A6	I server della tua azienda dove sono collocati?
A7	Le applicazioni della tua azienda (acquistate e/o sviluppate internamente) sono utilizzate da:
A8	Per la sicurezza delle applicazioni della tua azienda vengono acquistati prodotti/servizi?
A9	Nella tua azienda è previsto l'accesso alle applicazioni aziendali da parte di personale in mobilità (tramite App su smartphone/tablet)? Se si, sono previste azioni finalizzate a prevenire possibili rischi?
A10	Nella tua azienda il personale accede a sistemi esterni (di clienti per manutenzione, di committenti per condivisione dati, etc.)? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
A11	Puoi indicarci il principale strumento di approvvigionamento di servizi/prodotti di sicurezza della tua azienda?
A12	Ritieni che nella tua azienda ci sia una adeguata consapevolezza rispetto agli impatti connessi alle problematiche legate ai rischi di sicurezza informatica?
A13	Quale ritieni sia per la tua azienda il budget annuo adeguato da destinare alla protezione contro le minacce informatiche?
A14	Sei interessato ad approfondire il tema della sicurezza informatica?
B1	L'azienda è inserita in una filiera "sensibile" per le minacce cyber (energia, sanità, finance, etc.)?

COD.	DOMANDA
B2	I processi aziendali necessitano di accesso a internet per poter funzionare? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
B3	I prodotti dell'azienda possono essere (o saranno) connessi a Internet? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
B4	I servizi dell'azienda richiedono connessione a internet? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
B5	È prevista una politica di aggiornamento del software/firmware dei dispositivi utilizzati nell'azienda?
B6	È prevista una politica di aggiornamento del software/firmware dei dispositivi utilizzati nell'azienda da remoto?
B7	I prodotti dell'azienda possono essere impiegati in sistemi/applicazioni critiche (sistemi che in caso di malfunzionamento possono provocare morte o gravi rischi alle persone, perdita o grave danneggiamento di mezzi e materiali, gravi danni ambientali, danno economico)?
B8	È previsto un controllo di qualità certificato ed una fase di collaudo per tutti i prodotti/servizi dell'azienda?
B9	L'azienda utilizza software di protezione (antivirus, antimalware, etc.) regolarmente aggiornato su tutti i dispositivi?
B10	Nell'ultimo biennio è stato effettuato un corso di formazione sulla cyber security al personale non tecnico? (es riconoscere allegati e-mail maligni, utilizzare solo software autorizzato, etc.)?
B11	Escludendo software antivirus ed eventuale formazione del personale, l'azienda ha investito parte del budget dello scorso anno in attività relative alla sicurezza informatica?
B12	Utilizzate soluzioni di backup delle informazioni mantenuti fisicamente separati e periodicamente testati?
B13	L'azienda ha subito nel corso dell'ultimo biennio attacchi informatici?
B14	Il controllo di qualità considera anche la sicurezza informatica?

Le domande di carattere tecnico si suddividono nelle seguenti **macro-categorie**:

4 CYBER SECURITY SCORE (CSS)

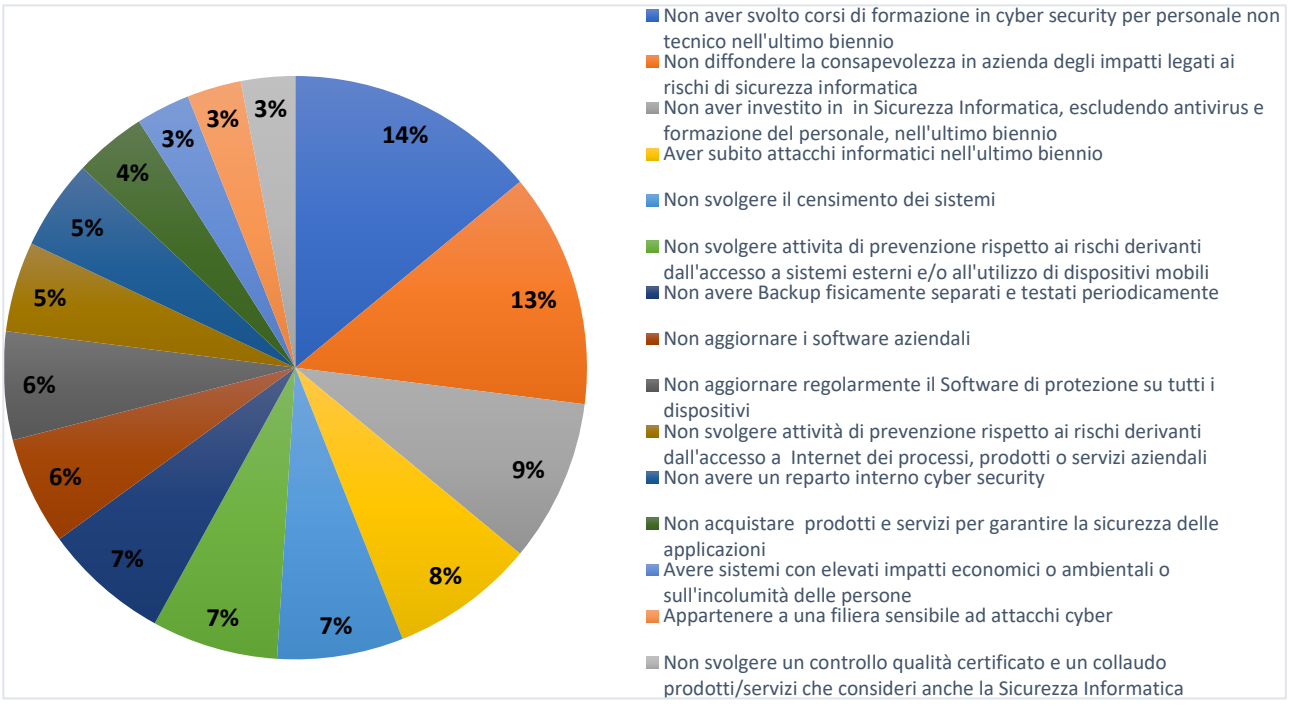
Oltre ad un output immediato che viene fornito dalla Cyber Security Survey a conclusione della compilazione del questionario, si calcola un indicatore denominato Cyber Security Score (CSS) che misura il grado di maturità dell'Azienda nella gestione delle tematiche di Cyber Security.

Il CSS varia da 0 a 1 e viene calcolato associando dei pesi alle domande che compongono la Survey.

Il peso alle domande è stato valutato applicando una metodologia descritta in appendice che ha richiesto l'intervista a esperti della Cyber Security appartenenti sia al mondo aziendale che a quello accademico.

> Per far fronte alla oggettiva difficoltà di quantificare il peso di ciascun fattore, nel presente studio ci si è avvalsi dell'esperienza di esperti, scelti tra Security Manager ed esponenti del mondo accademico;

La seguente tabella riporta i valori numerici associati a ciascun fattore, ottenuti tramite la metodologia Sparse Analytic Hierarchy Process (SAHP) [1,2,3] sulla base delle informazioni ottenute dagli esperti.



Si può notare come i tre fattori caratterizzati dai pesi più alti siano:

- "**Non aver svolto corsi di formazione in cyber security** per personale non tecnico nell'ultimo biennio "(circa 0,137)
- "**Non diffondere la consapevolezza in azienda degli impatti** legati ai rischi di sicurezza informatica "(circa 0,125)
- "**Non aver investito in Sicurezza Informatica**, escludendo antivirus e formazione del personale, nell'ultimo biennio" (circa 0,09);

tali fattori ricadono in una dimensione di **Commitment Aziendale** ed hanno complessivamente un peso di oltre il 37% sull'indicatore CSS.

5 ANALISI DEI DATI

186 AZIENDE	Nel corso del 2019 e del primo semestre del 2020, sono state raccolte **186 risposte** da Aziende appartenenti a diversi settori merceologici e a diversificate tra Micro, Piccola, Media e Grazie Azienda.

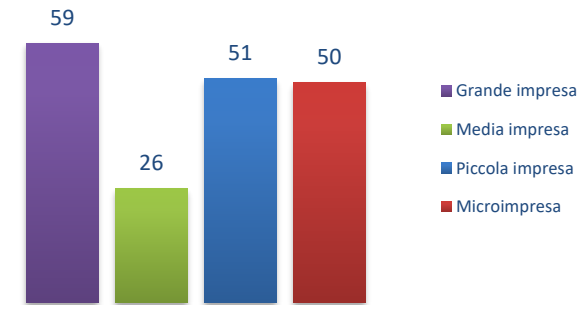
I parametri considerati più significativi al livello di analisi, e per questo coinvolti nello studio, sono:

- Tipologia d'azienda e/o Settore aziendale
- Fatturato
- Numero di dipendenti
- CSS Pesato
- Budget di sicurezza desiderato
- Città
- Anni di Attività

Di seguito si illustrano i risultati principali derivanti dalle analisi svolte.

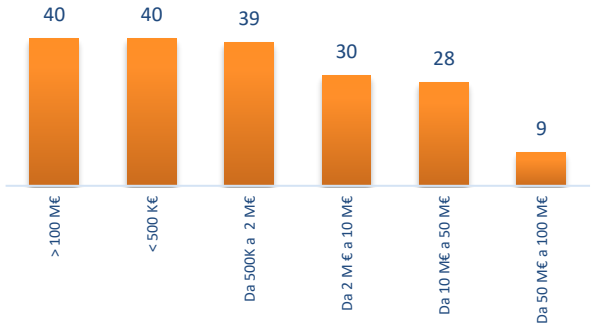
5.1 DATI GENERALI DELLE AZIENDE

TIPOLOGIA DI IMPRESA



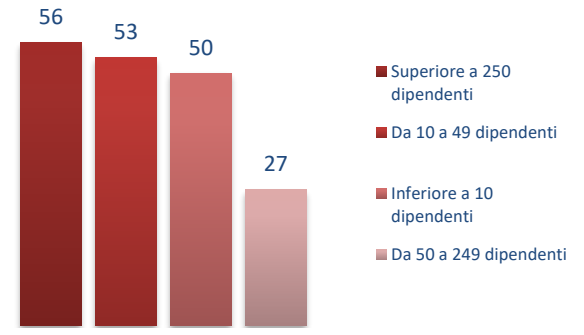
Il grafico evidenzia che sul totale delle 186 risposte, circa il 68% (127 su 186) sono relative a PMI.

FATTURATO



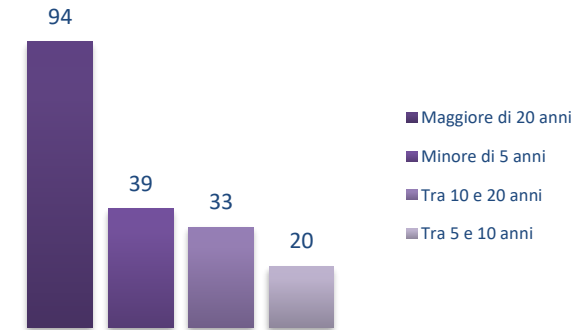
Il grafico mostra la distribuzione del numero di risposte alla Survey in relazione al fatturato annuo.

NUMERO DI DIPENDENTI



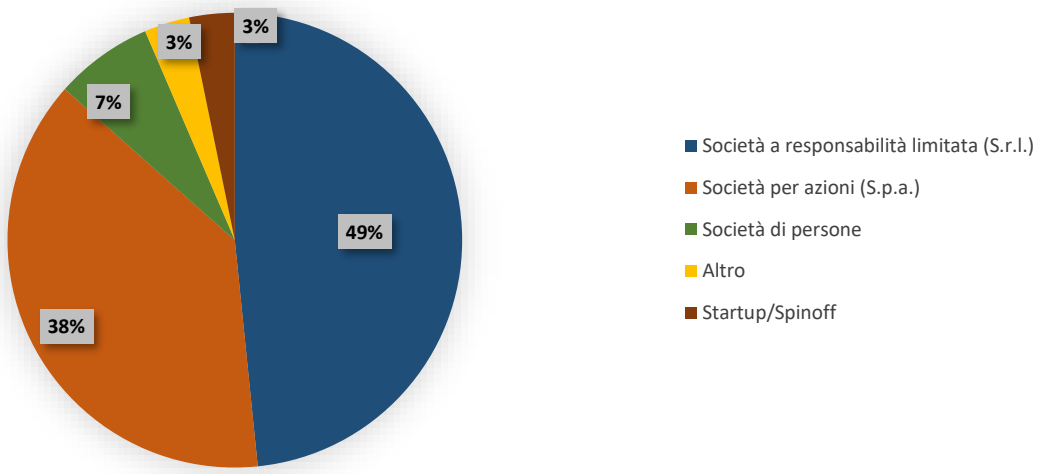
Il grafico mostra la distribuzione del numero di risposte alla Survey in relazione al numero di dipendenti.

ANNI DI ATTIVITA'



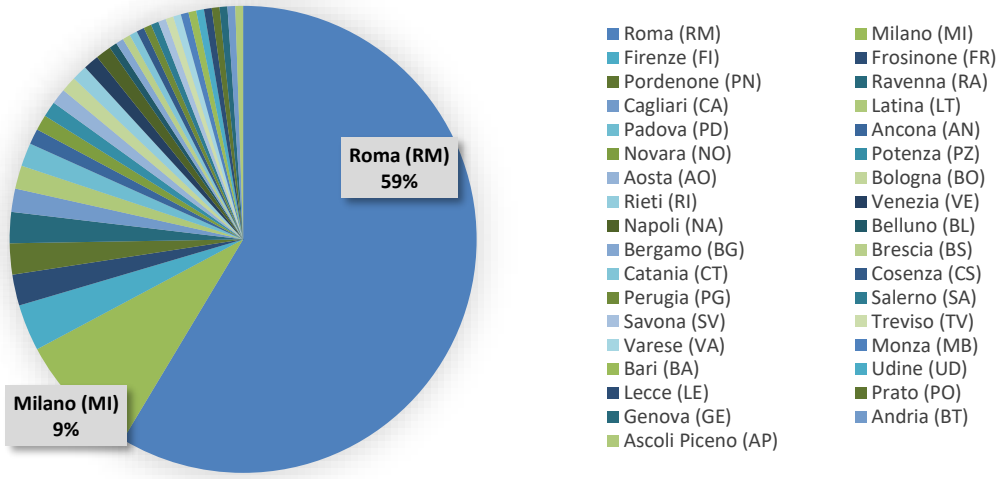
Il grafico mostra la distribuzione del numero di risposte alla Survey in relazione agli anni di attività dell'azienda. Dal grafico si evince che le risposte alla Survey sono pervenute principalmente da società che sono presenti sul mercato da più di 20 anni.

TIPOLOGIA DI SOCIETA'



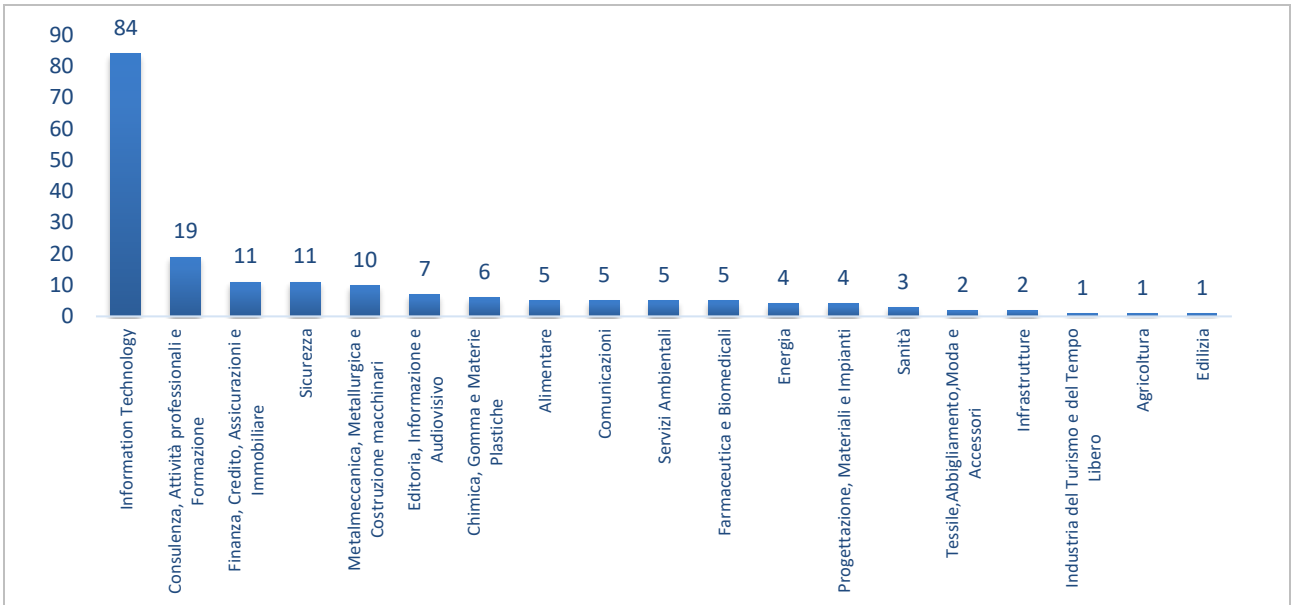
Il grafico mostra la distribuzione del numero di risposte alla Survey in relazione alla tipologia di società. Dal grafico si evince che le risposte alla Survey sono pervenute principalmente da forme societarie quali Società a Responsabilità limitata (49%) e Società per azioni (38%).

DISTRIBUZIONE GEOGRAFICA



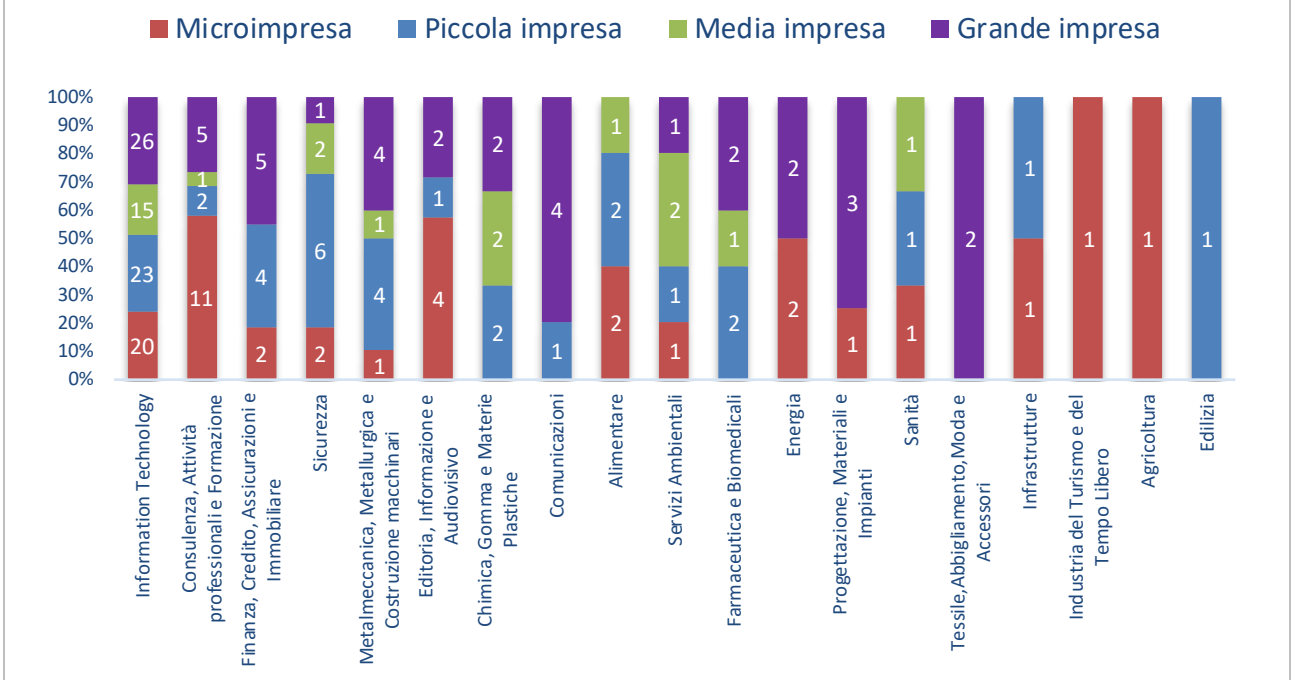
Il grafico mostra la distribuzione del numero di risposte alla Survey in relazione alla distribuzione geografica.
Dal grafico si evince come la partecipazione al progetto sia pervenuta da diverse città italiane ma, tuttavia, vi è una presenza predominante di Roma (59%) avendo l'iniziativa avuto origine nell'ambito di Unindustria. Obiettivo per le prossime rilevazioni è estendere la Survey a livello nazionale in modo omogeneo.

SETTORE DI APPARTENENZA



Il grafico mostra la distribuzione del numero di risposte alla Survey in relazione al settore di appartenenza. Dal grafico si evince come la partecipazione al progetto sia pervenuta principalmente dalla sezione Information Technology (84 su 186) avendo l'iniziativa avuto origine nell'ambito della sezione IT di Unindustria.

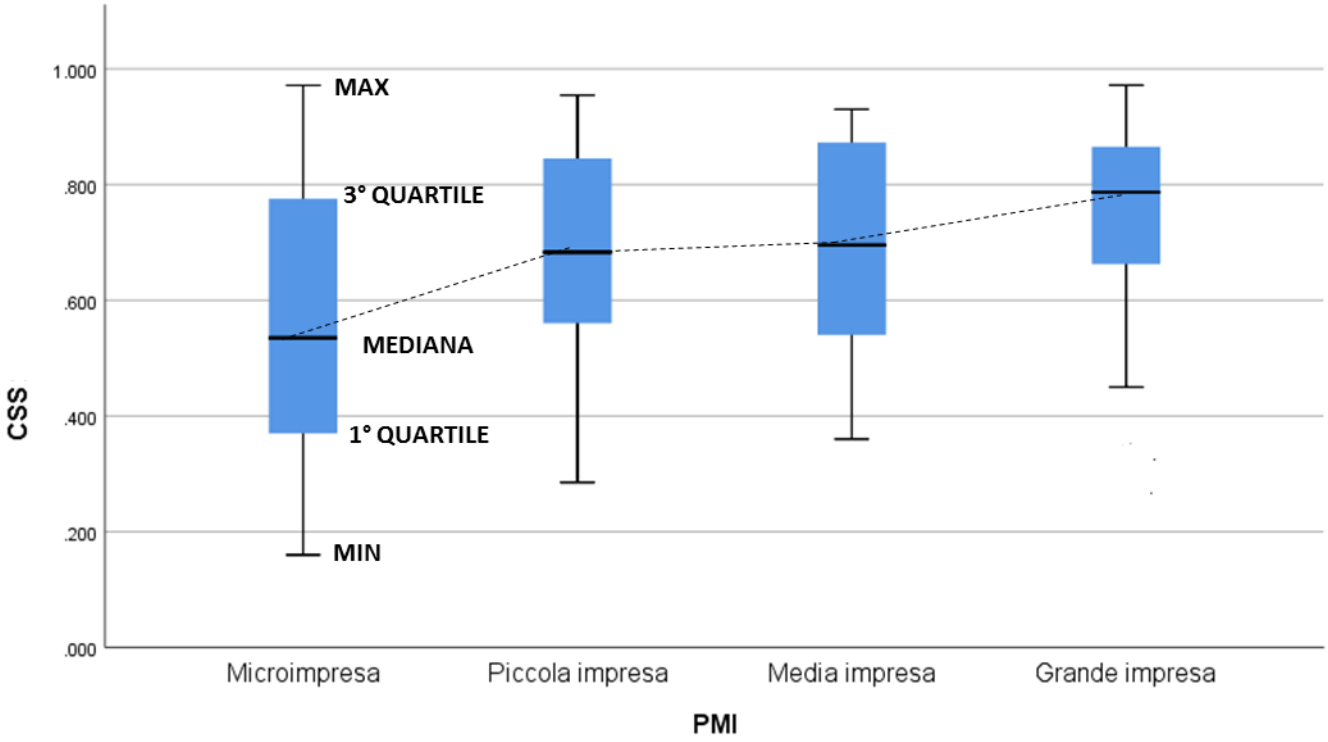
SETTORE DI APPARTENENZA E TIPOLOGIA



Il grafico mostra la distribuzione del numero di risposte alla Survey in relazione al settore di appartenenza e alla tipologia aziendale.
Per il settore Information Technology si evidenzia una equa ripartizione della compilazione della Survey tra le diverse tipologie aziendali.

5.2 CSS E DIMENSIONE SOCIETARIA

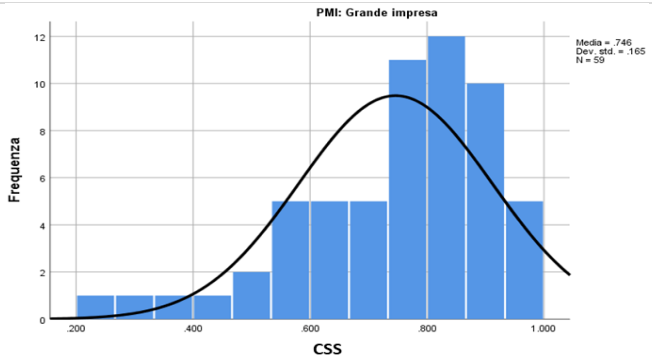
In questa sezione si analizza la relazione che intercorre fra l'indice di Cyber Security Score (CSS) e la dimensione societaria.



A tal fine, il boxplot della figura sopra riportata fornisce un colpo d'occhio sulla distribuzione statistica del valore del CSS nelle micro, piccole, medie e grandi imprese; nello specifico, per ciascuna tipologia di impresa, il grafico riporta cinque numeri di sintesi (minimo, 1° quartile (Q1), mediana, 3° quartile (Q3), massimo) che descrivono le caratteristiche salienti della distribuzione. Il rettangolo del boxplot ha come estremi inferiore e superiore rispettivamente Q1 e Q3. La mediana divide la scatola in due parti. La variabilità minima e massima si ottiene congiungendo Q1 al minimo e Q3 al massimo.
La figura mostra chiaramente come la mediana del CSS cresca sensibilmente al crescere della dimensione societaria. Inoltre, si osserva come la distanza tra i valori massimo e minimo si stringano al crescere della dimensione societaria, suggerendo che la Cybersecurity readiness sia non solo maggiore nelle imprese più strutturate, ma anche soggetta a minori variazioni.

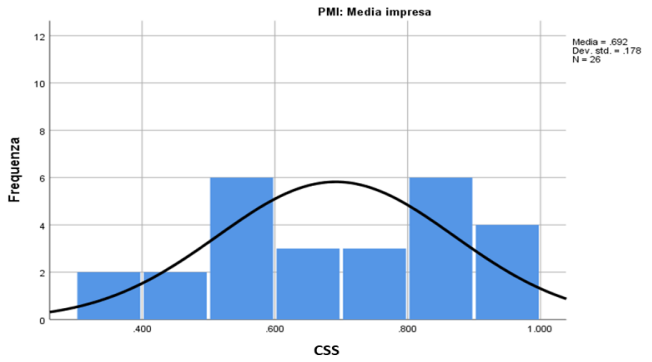
Di seguito è rappresentata la distribuzione del "CSS" per Micro, Piccola, Media e Grande Impresa. Nel grafico vengono evidenziati gli indicatori di centralità del CSS, tra cui la moda, ovvero il valore che si manifesta con maggiore frequenza, e la mediana, ovvero il valore centrale tra i dati numerici.

GRANDE IMPRESA



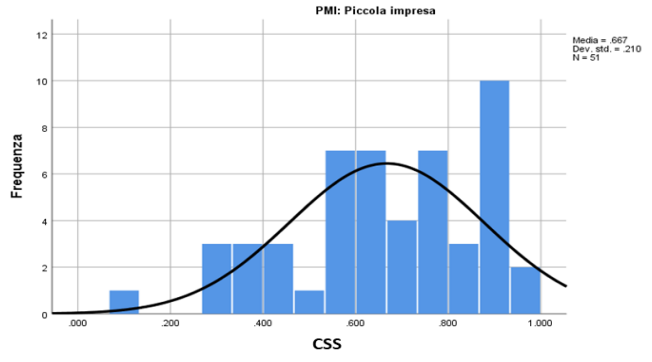
MEDIA	.74610
MEDIANA	.78683
MODALITA'	.895
DEVIAZIONE STD	.165476
VARIANZA	.027
MINIMO	.240
MASSIMO	.972

MEDIA IMPRESA



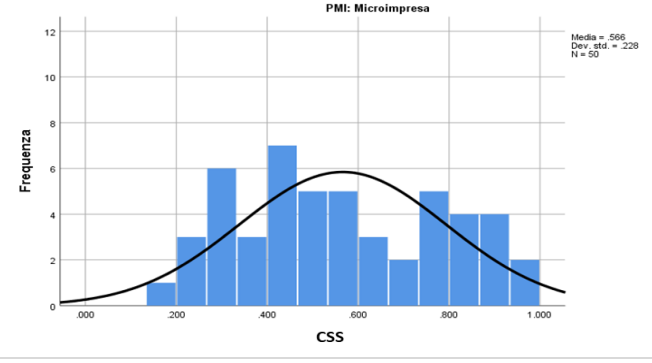
MEDIA	.69173
MEDIANA	.69555
MODALITA'	.875
DEVIAZIONE STD	.178236
VARIANZA	.032
MINIMO	.360
MASSIMO	.930

PICCOLA IMPRESA



MEDIA	.66698
MEDIANA	.68314
MODALITA'	.910
DEVIAZIONE STD	.210313
VARIANZA	.044
MINIMO	.070
MASSIMO	.954

MICROIMPRESA



MEDIA	.56591
MEDIANA	.53500
MODALITA'	.589
DEVIAZIONE STD	.227605
VARIANZA	.052
MINIMO	.160
MASSIMO	.971

5.3 CSS e Clustering Analysis

Al fine di validare l'intuizione che la dimensione societaria sia fortemente connessa al CSS, si è provveduto a implementare una procedura di clustering dei dati relativi alle aziende considerate.

Nello specifico, si è scelto di considerare i **seguenti fattori:**

- ANNI: età dell'azienda
- DIPENDENTI: numero di dipendenti
- FATTURATO
- PRESENZA REPARTO CYBERSECURITY: si è scelto di assegnare valore 1 alle aziende con un reparto dedicato alla cybersecurity e 0 altrimenti
- BUDGET DI SICUREZZA DESIDERATO
- CSS

Utilizzando la tecnica di clustering C-Means, che consente di dividere i dati in C gruppi senza specificare ipotesi a priori sul significato semantico di tali gruppi, si è provveduto a dividere i dati in C=2,3 e 4 gruppi. Inoltre, per ogni scelta del parametro C, il metodo fornisce un valore "medio" del gruppo, che può essere utilizzato come "rappresentante". Si riportano nelle tabelle seguenti i rappresentanti ottenuti per C=2,3,4; le figure riportano anche una percentuale di appartenenza delle aziende a ciascun gruppo, che può essere interpretata come una sorta di dimensione dei gruppi.

ANNI	DIPENDENTI	FATTURATO	PRESENZA REPARTO CYBERSECURITY	BUDGET DI SICUREZZA DESIDERATO	CSS	NUMEROSITÀ DEL GRUPPO
11.98	35.15	5.71 M€	0.40	20.98k€	0.60	56%
22.47	258.61	107.06M€	0.95	113.18k€	0.76	44%

Rappresentanti nel caso di C=2 gruppi

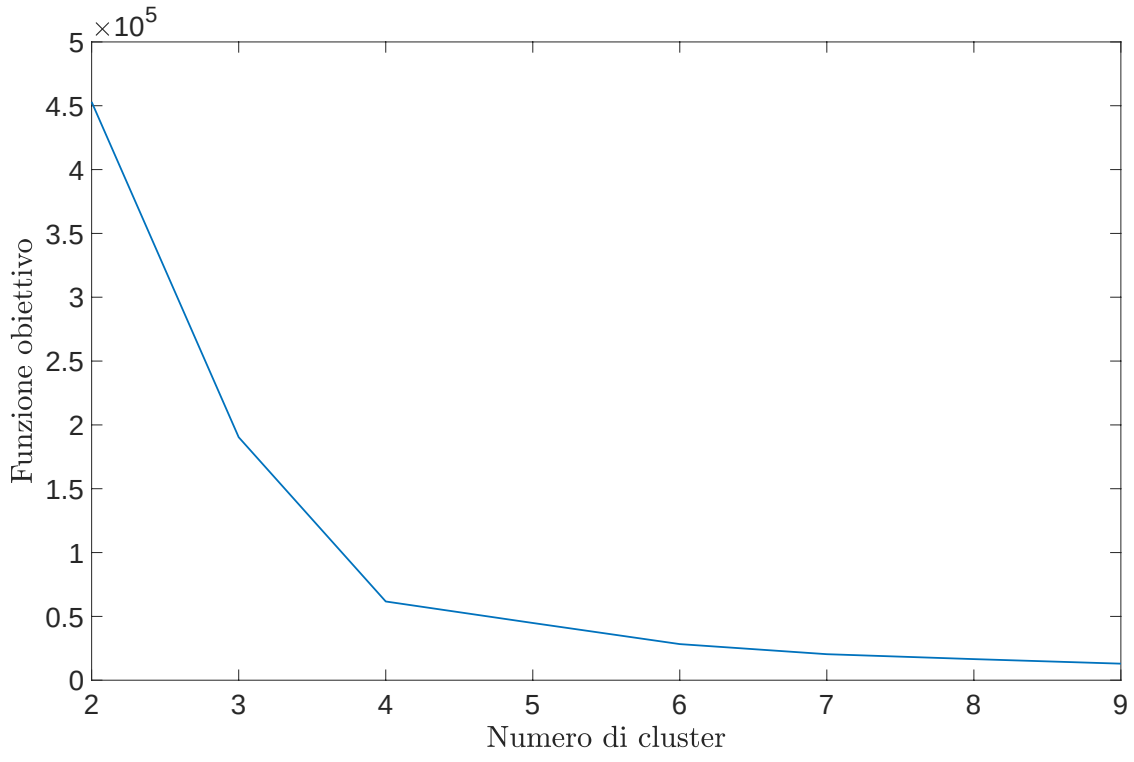
ANNI	DIPENDENTI	FATTURATO	PRESENZA REPARTO CYBERSECURITY	BUDGET DI SICUREZZA DESIDERATO	CSS	NUMEROSITÀ DEL GRUPPO
11.38	28.57	4.70 M€	0.05	15.79k€	0.51	34.26%
15.13	62.76	10.77M€	0.95	36.24k€	0.75	34.86%
23.51	292.72	134.31M€	0.98	132.45k€	0.78	30.88%

Rappresentanti nel caso di C=3 gruppi

ANNI	DIPENDENTI	FATTURATO	PRESENZA REPARTO CYBERSECURITY	BUDGET DI SICUREZZA DESIDERATO	CSS	NUMEROSITÀ DEL GRUPPO
11.03	25.08	4.03M€	0.02	14.35k€	0.49	28.03%
5.82	29.77	4.10M€	0.95	22.25k€	0.73	22.21%
22.81	107.85	20.96M€	0.94	52.76k€	0.76	23.37%
23.84	297.34	141.93M€	0.99	138.67k€	0.78	26.39%

Rappresentanti nel caso di C=4 gruppi

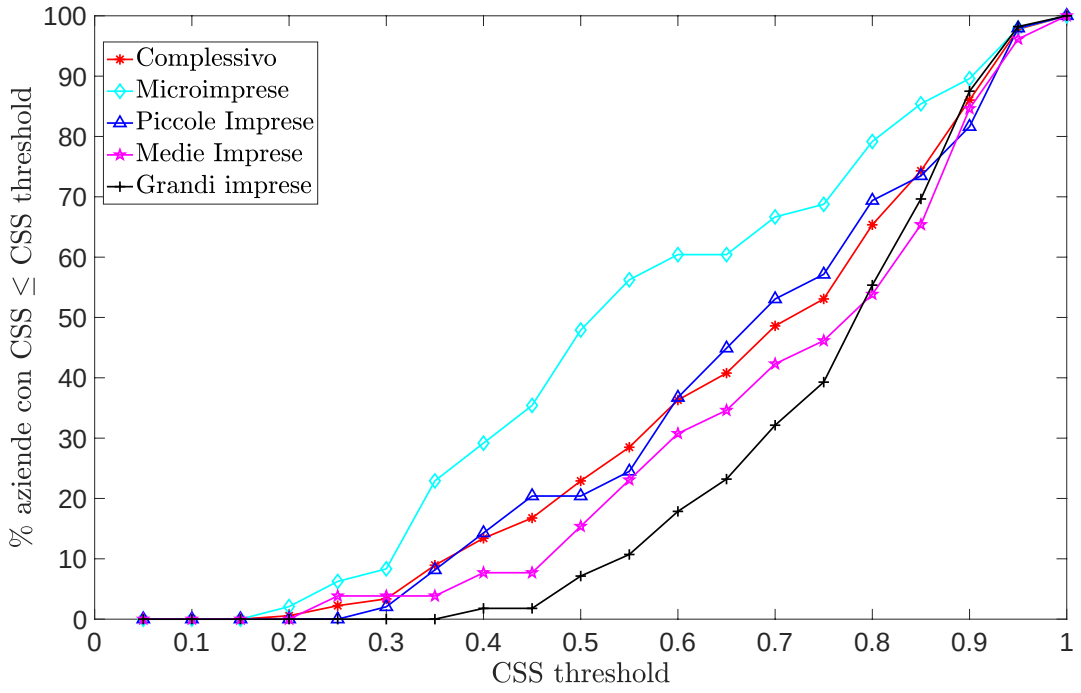
Dall'analisi delle tabelle precedenti si evince come la tecnica di clustering C-Means produca gruppi caratterizzati sia da dimensioni societarie (in base ad anni, numero di dipendenti e fatturato) che da valori dell'indice CSS crescenti, contribuendo a validare l'ipotesi che il CSS sia fortemente connesso alla dimensione societaria.
Allo scopo di confermare ulteriormente l'ipotesi che la dimensione societaria sia la metrica più importante per il CSS, è stata svolta un'analisi di tipo clustering K-Means. Nello specifico sono state analizzate le domande del questionario relative alla dimensione aziendale, ma non il CSS.
Si è scelto inoltre di non fissare un numero di gruppi a priori, ma di selezionarlo automaticamente in base alla struttura dei dati. Applicando la tecnica K-Means facendo variare il numero di gruppi tra 2 e 9, si è valutata la "qualità" del cluster, espressa dai valori numerici riportati nella figura seguente (minore il valore, maggiore la qualità). Al fine di scegliere un numero di gruppi specifico si evidenzia come la procedura automatica abbia comportato la scelta di un K=4 di gruppi (lo stesso numero di gruppi ottenuto considerando micro, piccola media e grande impresa), che corrisponde al "gomito" della funzione, ovvero al punto che corrisponde al massimo miglioramento della qualità dei cluster rispetto al raggruppamento ottenuto per il valore immediatamente inferiore di K; tale euristica è prassi comune per orientare la scelta automatica del numero di gruppi.



Successivamente è stato analizzato in dettaglio il caso di k=4 gruppi. Nello specifico, nella seguente tabella, si riporta per ogni gruppo i valori di media, mediana e moda dell'indice CSS medio minimo e massimo; si noti come, nonostante il CSS non sia stato impiegato per costruire i gruppi, ci sia una chiara relazione tra dimensione societaria e gruppi. In particolare, si osserva che ordinando i gruppi per ciascuno di tali indici singolarmente si ottiene lo stesso ordinamento. Inoltre, considerando la moda, si osserva un fenomeno di polarizzazione: i gruppi 0 e 1 sono caratterizzati da valori decisamente bassi, mentre i gruppi 2 e 3 presentano valori nettamente maggiori.

Cluster	Media CSS	Mediana CSS	Moda CSS	Dimensione in %
0	0.62	0.62	0.16	54.19%
1	0.70	0.71	0.45	9.50%
2	0.72	0.78	0.87	14.53%
3	0.78	0.81	0.89	21.78%

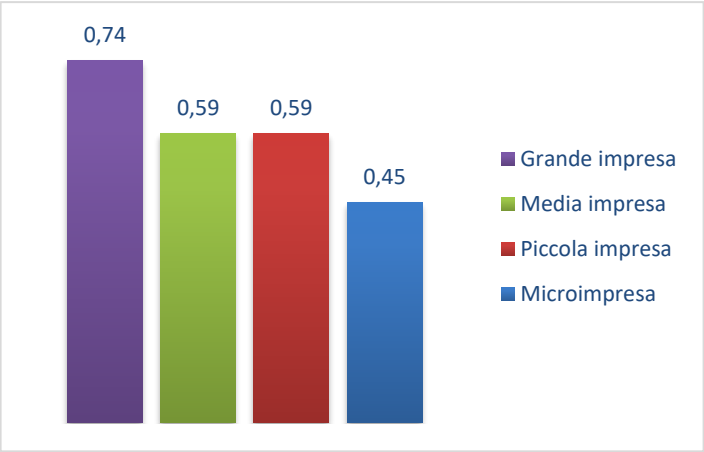
Il grafico successivo rappresenta una distribuzione cumulativa del CSS considerando le imprese sia complessivamente che per dimensione societaria. Dall'analisi del dato complessivo (curva rossa), da cui si evince che solo il 22.91% delle aziende ha un CSS<0.5 e meno del 4% inferiore a 0.3, ovvero il CSS è in generale elevato nelle aziende considerate.
Per quanto riguarda le diverse dimensioni di impresa, si osservano risultati inversamente proporzionali alla dimensione societaria. Nello specifico, la curva relativa alla grande impresa (in nero) riporta valori nettamente inferiori alle altre (ad es. solo il 7.13% delle aziende mostra un CSS<0.5). Si osserva inoltre come la micro impresa (curva azzurro chiaro) riporti valori considerevolmente maggiori del valore complessivo (ad esempio, la percentuale di medie aziende con CSS<=0.5 è del 47.92%, ovvero più del doppio della curva complessiva e circa 6.7 volte più delle grandi imprese). Si noti infine come le piccole imprese (in blu) abbiano risultati simili al dato aggregato, mentre la media impresa (in magenta) mostri valori intermedi tra quelli aggregati e quelli corrispondenti alla grande impresa.



Nel complesso, le analisi svolte supportano la tesi che il CSS sia fortemente correlato con la dimensione societaria.

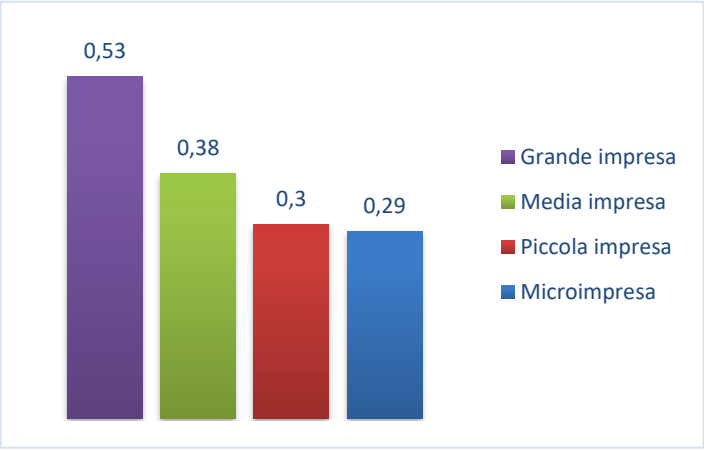
5.4 CSS E CATEGORIE DOMANDE

COMMITMENT AZIENDALE



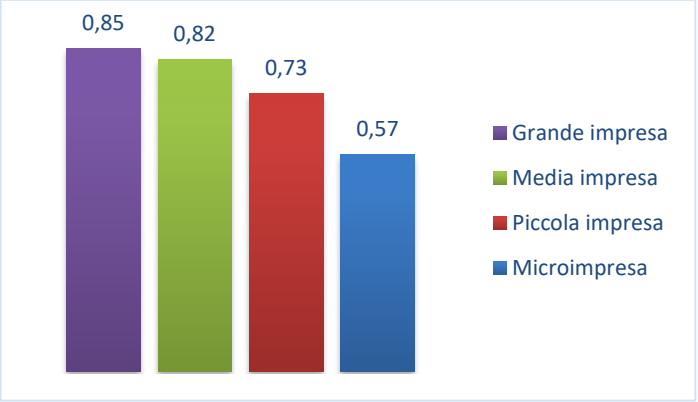
Il grafico illustra come il CSS associato alle domande relative al **commitment aziendale** sulle tematiche di cyber security in termini di **risorse, budget e awareness** decresca con il diminuire della dimensione societaria. Come verrà esposto nelle conclusioni è pertanto fondamentale porre particolare enfasi alle tematiche di commitment aziendale per le PMI e microimprese.

LIVELLO DI ESPOSIZIONE



Il grafico illustra come il CSS associato alle domande relative al **livello di esposizione** sia maggiore per le grandi aziende rispetto alle micro e PMI. Risulta quindi evidente che si deve tenere in debita considerazione l'interdipendenza esistente tra PMI e Grandi Aziende nella **Supply Chain** per cui problematiche di cyber security per le PMI si possono ripercuotere immediatamente anche sulle grandi aziende.

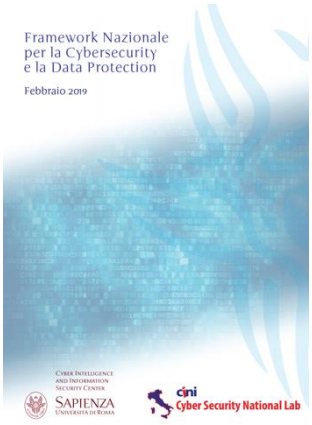
MATURITÀ TECNOLOGICA



Il grafico illustra come il CSS associato alle domande relative alla **maturità tecnologica** delle aziende sia maggiore per le grandi imprese e cresca all'aumentare della dimensione societaria. ciò è e determinato principalmente dalla maggiore possibilità di investire in prodotti e servizi di cyber security da parte delle grandi aziende rispetto a quelle più piccole.

6 FRAMEWORK NAZIONALE PER LA CYBERSECURITY E RACCOMANDAZIONI PER LE PMI

Pubblicato per la prima volta nel 2015 e aggiornato nel 2019 per includere tematiche legate alla protezione dei dati personali, Il Framework Nazionale per la Cybersecurity e la Data Protection [6] si è affermato nel tempo come lo strumento per valutare il rischio di esposizione ad attacchi cyber sul territorio italiano.



Al fine di rendere i risultati del cybersecurity survey descritti nelle precedenti sezioni interpretabili alla luce delle funzioni, category e sub-category del framework, e così costituire una base per una prima valutazione dell'esposizione al rischio, è stata iniziata una attività di mapping tra le domande del questionario e gli elementi del Framework. Questa attività è partita dai 15 controlli essenziali di sicurezza listati nel 2016 dal CIS-Sapienza nel relativo documento [7], da cui sono state estratte 4 function (Identify, Protect, Detect, Respond), 8 category e 17 sub-category. In particolare le singole domande del cybersecurity survey sono state singolarmente mappate su una o più delle 17 sub-category, fornendo anche un punteggio in merito all'attinenza.

Dall'analisi del mapping ottenuto e dei punteggi rilevati nella survey, possiamo notare già in questa fase alcuni elementi di interesse:

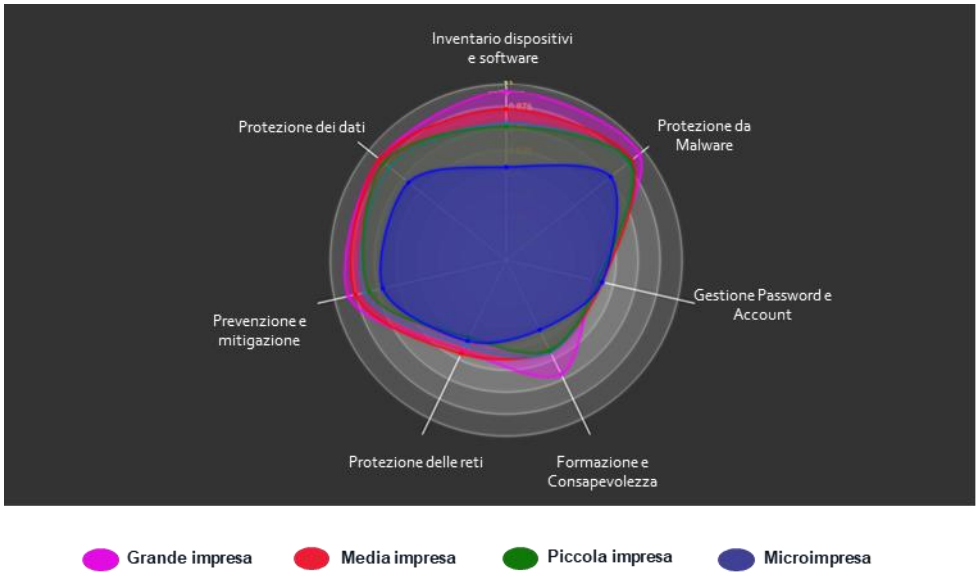
- Come esempio di mapping relativo al Commitment Aziendale, le domande A12 ("Ritieni che nella tua azienda ci sia una adeguata consapevolezza rispetto agli impatti connessi alle problematiche legate ai rischi di sicurezza informatica?") e B10 ("Nell'ultimo biennio è stato effettuato un corso di formazione sulla cyber security al personale non tecnico? (es riconoscere allegati e-mail maligni, utilizzare solo software autorizzato, ecc)") sono state legate con la sub-category PR.AT-1 ("Tutti gli utenti sono informati e addestrati"). Questo mapping permette di valutare meglio il grado di attenzione rispetto a consapevolezza cyber e training (category del Framework PR.AT – Awareness and Training)
- Come esempio di mapping relativo al livello di esposizione, la domanda B9 è stata legata alla sub-category del Framework PR.PT4 ("Le reti di comunicazione e controllo sono protette"). Da questa si evince l'attenzione verso la protezione dei canali di comunicazione interni ed esterni all'azienda, in particolare anche alla luce dell'aumento della modalità di lavoro da remoto (smart working). Il legame permette di andare ad individuare ulteriori aree di indagine, avvalendosi anche di altre sub-category legate alla stessa category PR.PT (Protective Technology)
- Come esempio di mapping relativo alla Maturità Tecnologica/Organizzativa, la domanda B12 relativa alla gestione dei backup è legata alla sub-category PR.IP-4 ("I backup delle

informazioni sono eseguiti, amministrati e verificati periodicamente"), così come la domanda B13 in materia di attacchi informatici è legata alla category DE.CM (Detect – Continous Monitoring) che prevede di monitorare lo stato di sicurezza per identificare possibili attacchi.

L'analisi sui controlli essenziali, ed espressamente delle Tematiche di sicurezza in cui essi sono organizzati, ha inoltre consentito di identificare gli ambiti in cui le PMI sono risultate più carenti dal punto di vista della sicurezza. Le Tematiche di sicurezza mappate sono le seguenti:

- **Inventario dispositivi e software**
- **Protezione da malware**
- **Gestione password e account**
- **Formazione e consapevolezza**
- **Protezione dei dati**
- **Prevenzione e mitigazione**
- **Protezione delle reti**

La seguente figura mostra il livello di maturità sulle singole Tematiche di sicurezza:



Nella rappresentazione, oltre alla conferma del diverso livello di maturità delle imprese in relazione alla dimensione aziendale, si evince come "Gestione password e account", "Formazione e consapevolezza" e "Protezione delle reti" rappresentino degli ambiti critici per la sicurezza delle aziende.

Vengono di seguito riportati informazioni e raccomandazioni tratti dal sopracitato documento dedicato ai controlli essenziali [7] al fine di fornire ulteriori dettagli per le Tematiche di sicurezza emerse come critiche:

- Gestione password e account
  - Complessità della password: *almeno 12 caratteri che contengano almeno un numero e un carattere non alfanumerico e che non contengano termini noti del vocabolario o informazioni facilmente riconducibili all'utente;*

- *Corretta educazione degli utenti nell'uso delle password: es. non utilizzare mai due volte una stessa password e conservarla in modo sicuro evitando la proliferazione di documenti non protetti contenenti liste di credenziali o appunti facilmente accessibili da chiunque;*
- *Impedire condivisione delle utenze: è necessario che l'azienda imponga un corretto uso delle utenze, impedendo la condivisione delle stesse tra più persone e proteggendo gli accessi, siano essi locali o remoti, attraverso opportune tecnologie (es. canali cifrati).*

- Formazione e consapevolezza
  - È necessario sensibilizzare e rendere consapevoli dei rischi tutti gli operatori che possono accedere a dati o ad altre risorse attraverso l'uso dei vari dispositivi;
  - È di fondamentale importanza sviluppare una corretta cultura della sicurezza in tutto il personale, indipendentemente dalle sue responsabilità, per poi considerare con particolare attenzione ruoli critici;
  - La formazione deve essere appropriatamente progettata in base ai ruoli e alle competenze pregresse del personale, su argomenti diversificati e identificati al bisogno.

- Protezione delle reti
  - *Firewall: è un componente (tipicamente, ma non esclusivamente, hardware) che si interpone tra due reti e permette di imporre regole sul transito di informazioni tra queste. Un uso tipico di un firewall prevede la sua installazione tra la rete aziendale e internet per permettere solo ad utenti e flussi di dati autorizzati di transitare, bloccando invece ogni comunicazione potenzialmente illecita;*
  - *Intrusion Detection/Prevention System: è un componente che controlla in modo continuo il traffico e le attività in essere nella rete aziendale per identificare e, laddove possibile, prevenire possibili intrusioni non autorizzate;*
  - *Mail/Web Filter: è un componente che intercetta ogni mail o dati web in transito da internet verso l'azienda, per identificare e bloccare tempestivamente possibili minacce.*

Obiettivo di future azioni sarà il superamento della limitazione ai 15 controlli essenziali e l'apertura verso un mapping completo ed a differenti livelli di specializzazione. Ad esempio, la domanda B1 rappresenta un elemento di estensione del mapping verso il Framework nazionale nella sua interezza, e abilita la necessità di effettuare ulteriori controlli di sicurezza all'interno della filiera produttiva di riferimento. Questi controlli possono essere dettati dalla category ID.SC (Identify – Supply Chain) del Framework che si occupa specificamente di requisiti di sicurezza per la supply chain. Questa attività potrà essere propedeutica alla definizione di un profilo di cybersecurity per le PMI scaturito da una prima attività di survey, che già permette l'individuazione di elementi di criticità, avente come vantaggio una natura più snella ed adatta per le piccole imprese e con la possibilità di valutare il risultato su una griglia comune costituita dal Framework Nazionale di Cybersecurity e Data Protection. Questo profilo potrà essere utilizzato come base di partenza per ulteriori attività di indagine.

7 CONCLUSIONI

In linea con gli obiettivi iniziali, il **Progetto Cyber Risk Self-Assessment** è un contributo utile a valutare lo "stato di preparazione cyber" del tessuto economico e produttivo del Paese, con particolare attenzione alla valutazione quantitativa del rischio cyber e della postura delle PMI italiane. I risultati di tale studio sono un contributo per **i decisori politici e aziendali** che hanno il compito e la responsabilità di emanare apposite *policies* e specifici *piani industriali* che indirizzano i fabbisogni specifici delle PMI italiane rispetto ai rischi cyber, con l'obiettivo ultimo di tutelare il patrimonio nazionale e favorire la diffusione della sicurezza informatica in Italia.

I dati emersi dall'elaborazione delle risposte sopra esposte forniscono una rappresentazione chiara rispetto allo **"stato di salute"** delle PMI nel contesto della cyber security in Italia.

In particolare, nonostante questo studio tratti di una tematica che è per sua natura *in fieri* (motivo per cui è di fondamentale importanza rendere in futuro periodica la rilevazione, estendendone sia il perimetro geografico sia gli ambiti di attività delle PMI e delle Istituzioni interessate), è stato tuttavia possibile estrapolare degli interessanti risultati, che rappresentano degli utili punti di partenza per riuscire ad avere una vista oggettiva dello stato dell'arte sulla sicurezza delle PMI in Italia.

I principali risultati emersi dal progetto e dalla survey **Cyber Risk Self-Assessment** riguardano i seguenti aspetti:

- **Cyber Security Score e interdipendenza tra PMI e Grandi Imprese**
- **Commitment Aziendale,Consapevolezza ed Awareness**
- **Livello di Esposizione e livello di Maturità Tecnologica**

Cyber Security Score e interdipendenza tra PMI e Grandi Imprese. Uno dei principali risultati di questo studio che è indispensabile sottolineare è relativo alla imprescindibile correlazione e interdipendenza tra le PMI e le Grandi Imprese nel Sistema industriale italiano. Infatti, se da un lato le Grandi Imprese presentano un Cyber Security Score (CSS) più elevato, questo dato va analizzato nell'ottica della loro forte interdipendenza con le PMI, per le quali al contrario si rileva un CSS molto più basso, in molti casi addirittura sotto i livelli di guardia. In altre parole, il CSS delle Grandi Imprese andrebbe quindi misurato anche rispetto alla loro *Supply Chain* la quale, nel caso specifico del tessuto economico, tecnologico e industriale italiano, è rappresentata per il 90% da PMI. In questo senso, un elevato livello di CSS delle Grandi Imprese può essere fortemente e facilmente compromesso dal più basso CSS delle PMI. Il dato è quanto meno allarmante se si considera il fatto che, da un evento malevolo protratto contro le PMI si possono avere "effetti domino" sull'intera filiera industriale italiana, con effetti deleteri non solo di natura tecnica ma anche economica e sociale, fino ad intaccare potenzialmente la sicurezza e l'erogazione dei servizi essenziali ai cittadini.

Commitment Aziendale, Consapevolezza ed Awareness. Un altro elemento rilevante che emerge dai dati della *survey* è relativo alla questione *Consapevolezza e Awareness* sulle tematiche della cyber security, sia dei vertici aziendali che dei dipendenti. A tal riguardo è stata data particolare attenzione alle domande della survey su questi temi, peraltro indicate anche dagli esperti di sicurezza essere tra quelli di particolare riferimento per avere un adeguato livello di attenzione

aziendale *("Non aver svolto corsi di formazione in cyber security", "Non diffondere la consapevolezza in azienda degli impatti legati ai rischi di sicurezza informatica "*). Inoltre, se al tema della formazione e della consapevolezza si aggregano i dati degli investimenti effettuati *("Non aver investito in Sicurezza Informatica"*) si riesce a rilevare una vista sulla dimensione e sul livello di **Commitment Aziendale** sul tema della Cyber Security. Anche in questo ambito è risultata evidente la correlazione tra CSS e dimensione aziendale, con impatti particolarmente negativi in termini di **risorse, budget e awareness** nel caso delle Medie, Piccole e Micro Imprese. Peraltro, questo ambito è risultato non particolarmente coperto per anche per le Grandi Aziende, che dovrebbero avere su questi temi una attenzione massima e che invece non raggiungono neanche il livello accettabile. E' quindi di particolare rilevanza la carenza rilevata da questo studio in termini di **Commitment Aziendale, Consapevolezza ed Awareness:** se non si raggiungono adeguati livelli di attenzione su questi temi, le **risorse, il budget e le competenze** necessarie per contrastare la minaccia cyber non potranno mai essere commisurate al livello della minaccia cyber esistente. Risulta indispensabile strutturare iniziative specifiche per innalzare la diffusione della cultura della sicurezza informatica, sia a livello orizzontale (verso tutte le componenti aziendali del personale tecnico e non tecnico), sia a livello apicale coinvolgendo il Management in corsi di formazione in cyber security, capaci di fornire adeguati strumenti tecnici e legali, diffondendo la consapevolezza in azienda rispetto agli impatti legati ai rischi cyber e, allo stesso tempo, contribuendo a d effettuare il salto culturale per comprendere che la cyber security rappresenta un investimento ed un vantaggio competitivo e non una semplice spesa o voce di costo. Peraltro, il punto della "consapevolezza" assume rilevanza strategica per un Paese come l'Italia che è continuamente "attenzionato" da migliaia di eventi cyber che colpiscono le PMI italiane al fine di estrapolare il loro *core business* ovvero il *know-how,* con evidenti impatti sul *Made in Italy*.

Livello di Esposizione e livello di Maturità Tecnologica. In merito al Livello di Esposizione, risulta necessario ed urgente sviluppare adeguati modelli di cyber security in grado di aumentare il livello di protezione delle aziende e dei loro asset, sia sotto il profilo tecnologico che organizzativo, in quanto i valori che emergono in generale (e con evidente gravità per le PMI) sono particolarmente bassi. I dati esposti devono preoccupare, per le motivazioni già rappresentate sul legame del CSS tra PMI e Grandi Imprese, anche le grandi realtà industriali oltre che le Istituzioni, le quali devono farsi carico di identificare gli strumenti ed i percorsi più adeguati per ridurre i Gap e minimizzare i rischi cyber esistenti.

Particolare attenzione merita anche il livello di Maturità Tecnologica/Organizzativa rilevata, che risulta essere anche in questi ultimi anni oggetto di una rivoluzione continua dovuta alla Digital Transformation ed alla necessità di utilizzare, anche nell'ambito delle PMI, nuove tecnologie (**Cloud, AI, 5G, IoT,** etc.) per innovare i processi di produzione e le modalità di erogazione dei servizi. Per il governo di questa trasformazione è dirimente sviluppare capacità diffuse di **cyber risk management (CRM)** in grado di coinvolgere non soltanto le Grandi Aziende (già in possesso di tali strumenti implementati *in-house*) quanto le PMI che, come emerso dalla *survey* scontano un basso livello di Maturità. Al fine di sviluppare tali capacità di CRM è indispensabile implementare e diffondere metodologie basate sui controlli essenziali forniti dal **Framework Nazionale di Cyber Security e Data Protection (FNCSDP)** adattandolo non solo alla realtà aziendale specifica, ma soprattutto alla dinamicità dell'evoluzione tecnologica e dei rischi cyber.

8 APPENDICE A: METODOLOGIA PER ASSEGNARE I PUNTI ALLE DOMANDE

Nell'ambito del presente studio è stato realizzato un indicatore olistico di rischio legato alla cyber-security che tenga conto di tali fattori. A tal fine si osserva come i vari fattori possano, in generale avere un peso diverso nella costruzione dell'indicatore complessivo; nello specifico, l'indicatore olistico Cyber Security Score (CSS) può essere rappresentato dalla seguente formula

$$CSS = \sum_{u=1}^{15} p_u x_u,$$

dove $p_u = 1$ se l'azienda presenta il fattore u (ad esempio, se l'azienda non aggiorna regolarmente il software) $p_u = 0$ se non presenta il fattore u (ad esempio, se l'azienda aggiorna regolarmente il software), mentre $x_u > 0$ è il valore numerico che rappresenta il peso dell' u-esimo fattore nella costruzione dell'indicatore olistico CSS. Tali valori numerici soddisfano:

$$\sum_{u=1}^{15} x_u = 1.$$

tale esperienza è stata opportunamente codificata in un problema formale di decisione multi-criterio. Nello specifico, il presente studio sfrutta la metodologia Sparse Analytic Hierarchy Process (SAHP) [1,2,3], che consente di combinare informazione di natura relativa fornita dai vari esperti per estrarre un valore numerico di importanza per ogni criterio.

Al fine di realizzare l'indicatore olistico, si è chiesto agli esperti di confrontare coppie di fattori e di fornire per ogni coppia considerata una indicazione di preferenza relativa, compilando opportunamente un questionario grafico (un esempio di questionario compilato è riportato in Figura 1). Tale questionario presenta 15 riquadri disposti a cerchio, ciascuno relativo ad uno dei fattori considerati[3]. Per compilare il questionario, all'esperto è stato chiesto di considerare coppie di fattori e di tracciare una freccia dal fattore A al fattore B qualora ritenesse il fattore A maggiormente importante. Inoltre, si è chiesto all'esperto di fornire una misura qualitativa di preferenza per ogni coppia considerata, apponendo dei simboli a fianco della freccia; in particolare, i simboli utilizzati sono: = (il fattore A è equivalente al fattore B), > (il fattore A è leggermente preferito al fattore B), >> (il fattore A è preferito al fattore B), >>> (il fattore A è preferito di gran lunga al fattore B).

Una caratteristica fondamentale della metodologia SAHP, che la differenzia da metodi quali il metodo Analytic Hierarchy Process (AHP) [4], è che gli esperti non erano tenuti a confrontare ogni coppia di alternative, ma solo quelle per le quali ritenevano di poter esprimere la loro opinione con confidenza: si è visto sperimentalmente [3] come questa caratteristica del metodo consenta da un lato di ridurre le distorsioni ed inconsistenze e dall'altro di minimizzare lo sforzo di compilazione per gli esperti.

[3] Per ogni questionario i blocchi sono stati disposti in maniera casuale per minimizzare fenomeni di bias di presentazione.

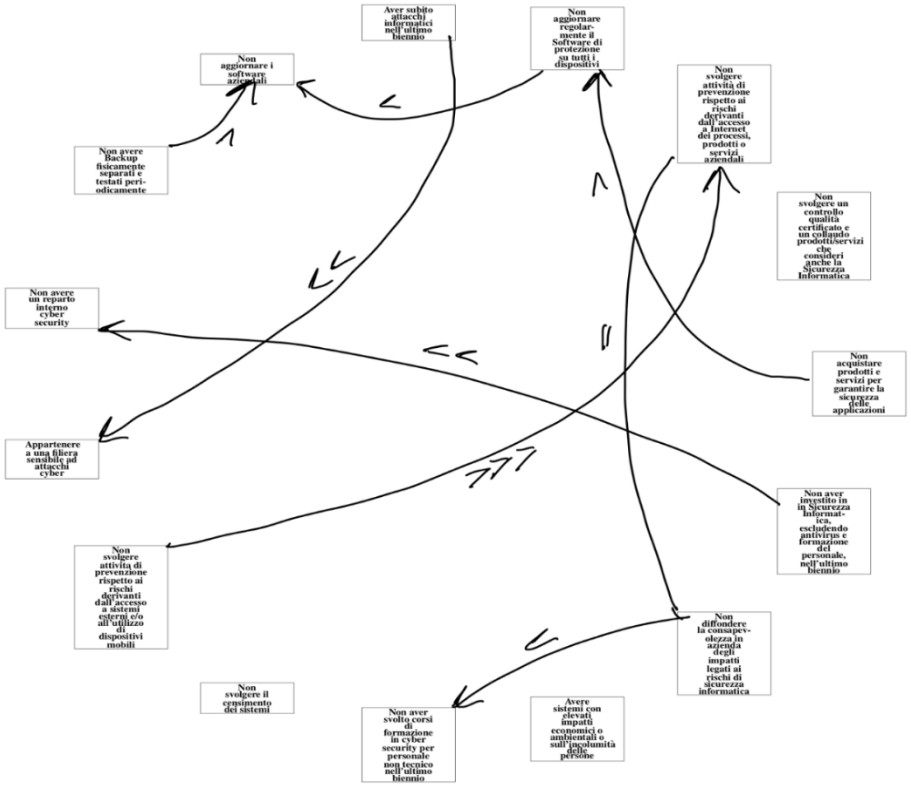


Figure 1 Esempio di questionario compilato da un esperto.

Nell'ambito della metodologia SAHP, i dati raccolti dall' i-esimo esperto sono stati collezionati in una matrice $W^{(i)}$, detta matrice dei rapporti, di dimensione 15x15; gli elementi $W_{uv}^{(i)}$ della matrice contengono una valutazione della preferenza relativa del fattore u rispetto al fattore v. Nello specifico, si è scelto di porre $W_{uv}^{(i)} = 1$ in corrispondenza di una preferenza descritta dal simbolo =, mentre valori $W_{uv}^{(i)} = 3$, $W_{uv}^{(i)} = 5$ e $W_{uv}^{(i)} = 7$ corrispondono, rispettivamente, ai simboli >, >> e >>>. Si è inoltre proceduto a settare $W_{vu}^{(i)} = \frac{1}{W_{uv}^{(i)}}$.

A seguito della procedura di raccolta dati da parte degli esperti, si dispone dunque di sei matrici di rapporti, una per ciascun esperto; sulla base di tali matrici, il metodo SAHP mira ad identificare il vettore $x \in \mathbb{R}_+^n$ (a componenti positive) che risolvere il seguente problema di ottimizzazione log-quadratico:

$$\arg min_{x \in \mathbb{R}_+^n} \frac{1}{2} \sum_{i=1}^{k} \sum_{u=1}^{n} \sum_{v=1}^{n} \left(\ln\left(W_{uv}^{(i)}\right) - \ln\left(\frac{x_u}{x_v}\right) \right)^2.$$

Il problema mira ad identificare i valori numerici di utilità x_u per ciascun fattore u tali per cui il rapporto $\frac{x_u}{x_v}$ minimizza simultaneamente il disaccordo con gli elementi $W_{uv}^{(i)}$ forniti da ogni esperto.

Il problema di cui sopra ha il vincolo che i valori numerici di utilità x_u siano positivi; al fine di semplificarne il calcolo, la metodologia SAHP risolve equivalentemente il problema di identificare il vettore $y \in \mathbb{R}^n$ che risolve il seguente problema

$$\arg min_{y \in \mathbb{R}^n} \frac{1}{2} \sum_{i=1}^{k} \sum_{u=1}^{n} \sum_{v=1}^{n} \left(\ln\left(W_{uv}^{(i)}\right) - y_u + y_v \right)^2,$$

per poi imporre $x_u = e^{y_u}$; in questo modo il problema può essere espresso come un problema di ottimizzazione non vincolata (non si richiede che le y_u siano positive) e convesso, la cui soluzione ottima y^* è facilmente ottenibile imponendo che la derivata della funzione obiettivo sia uguale a zero.

Utilizzando tale procedura, è possibile dimostrare che la soluzione ottima y_u soddisfa l'equazione

$$\sum_{i=1}^{k} L^{(i)} y^* = \sum_{i=1}^{k} r^{(i)}$$

Dove $r^{(i)}$è un vettore ad n componenti tale che

$$r_u^{(i)} = \sum_{v\ t.c. W_{uv}^{(i)} > 0} ln\left(W_{uv}^{(i)}\right)$$

ed $L^{(i)}$è la matrice Laplaciana che corrisponde alle informazioni fornite dall' i-esimo decisore, ovvero una matrice n x n tale che

$$L_{uv}^{(i)} = \begin{cases} \sum_{j=1}^{n} L_{uj}^{(i)}, se\ u = j \\ -1, se\ u \neq j\ e\ W_{uv}^{(i)} > 0 \\ 0, \quad altrimenti. \end{cases}$$

Pertanto, la soluzione del problema SAHP è ottenuta ponendo

$$y^* = pinv\left(\sum_{i=1}^{k} L^{(i)}\right) \sum_{i=1}^{k} r^{(i)},$$

dove $pinv\left(\sum_{i=1}^{k} L^{(i)}\right)$ è la pseudoinversa di Moore-Penrose della matrice $\sum_{i=1}^{k} L^{(i)}$ (si può dimostrare che tale matrice è sempre singolare per costruzione e dunque non invertibile) e calcolando $x_u = e^{y_u}$. Si noti che i valori x_u sono successivamente normalizzati per garantire che la somma dei valori sia unitaria.

9 APPENDICE B: DOMANDE E RISPOSTE

DOMANDA	RISPOSTE	% RISPOSTE
Tipologia di azienda	Società di persone	7,0%
	Società a responsabilità limitata (S.r.l.)	48,4%
	Società per azioni (S.p.a.)	38,2%
	Startup/Spinoff	3,2%
	Altro	3,2%
Anni di attività dell'azienda	Minore di 5 anni	21,0%
	Tra 5 e 10 anni	10,8%
	Tra 10 e 20 anni	17,7%
	Maggiore di 20 anni	50,5%
N° sedi dell'azienda	Unica sede aziendale	48,9%
	Due o più sedi aziendali	51,1%
Provincia della sede operativa principale	Roma (RM)	58,6%
	Latina (LT)	1,6%
	Frosinone (FR)	2,2%
	Savona (SV)	0,5%
	Cagliari (CA)	1,6%
	Milano (MI)	8,6%
	Cosenza (CS)	0,5%
	Potenza (PZ)	1,1%
	Brescia (BS)	0,5%
	Ancona (AN)	1,1%
	Ravenna (RA)	2,2%
	Pordenone (PN)	2,2%
	Bergamo (BG)	0,5%
	Varese (VA)	0,5%
	Treviso (TV)	0,5%
	Firenze (FI)	3,2%
	Salerno (SA)	0,5%
	Catania (CT)	0,5%
	Belluno (BL)	0,5%
	Viterbo (VT)	0,0%
	Novara (NO)	1,1%
	Perugia (PG)	0,5%
	Monza (MB)	0,5%
	Padova (PD)	1,6%
	Aosta (AO)	1,1%
	Bari (BA)	0,5%
	Bologna (BO)	1,1%
	Rieti (RI)	1,1%
	Udine (UD)	0,5%
	Lecce (LE)	0,5%

	Venezia (VE)	1,1%
	Prato (PO)	0,5%
	Genova (GE)	0,5%
	Napoli (NA)	1,1%
	Ascoli Piceno (AP)	0,5%
	Andria (BT)	0,5%
Numero di dipendenti dell'azienda	Inferiore a 10 dipendenti	26,9%
	Da 10 a 49 dipendenti	28,5%
	Da 50 a 249 dipendenti	14,5%
	Superiore a 250 dipendenti	30,1%
Fatturato medio annuo nell'ultimo triennio	Minore di 500 K€	21,5%
	Da 500K a 2 M€	21,0%
	Da 2 M € a 10 M€	16,1%
	Da 10 M€ a 50 M€	15,1%
	Da 50 M€ a 100 M€	4,8%
	Maggiore di 100 M€	21,5%
Sezione di appartenenza a UNINDUSTRIA / attività prevalente	Alimentare	2,7%
	Attività estrattive	0,0%
	Carta, Stampa e Cartotecnica	0,0%
	Chimica, Gomma e Materie Plastiche	3,2%
	Comunicazioni	2,7%
	Consulenza, Attività professionali e Formazione	10,2%
	Distribuzione	0,0%
	Edilizia	0,5%
	Editoria, Informazione e Audiovisivo	3,8%
	Elettronica ed Elettrotecnica	0,0%
	Energia	2,2%
	Farmaceutica e Biomedicali	2,7%
	Finanza, Credito, Assicurazioni e Immobiliare	5,9%
	Industria Ceramica	0,0%
	Industria del Turismo e del Tempo Libero	0,5%
	Information Technology	45,2%
	Infrastrutture	1,1%
	Legno, Arredo e Nautica	0,0%
	Metalmeccanica, Metallurgica e Costruzione macchinari	5,4%
	Progettazione, Materiali e Impianti	2,2%
	Sanità	1,6%
	Servizi Ambientali	2,7%
	Sicurezza	5,9%
	Tessile, Abbigliamento, Moda e Accessori	0,5%
	Agricoltura	0,5%
La tua azienda ha un reparto interno che cura gli aspetti di Cyber Security?	Si	62,9%
	No	37,1%
	Si	86,6%

Nella tua azienda vengono censiti i sistemi e gli apparati fisici in uso (dispositivi mobili, computer, server, etc)?	No	13,4%
I server della tua azienda dove sono collocati?	Presso l'azienda	42,5%
	Presso un centro servizi esterno	22,0%
	Entrambe le risposte precedenti	35,5%
Le applicazioni della tua azienda (acquistate e/o sviluppate internamente) sono utilizzate da:	Dipendenti	41,9%
	Clienti (utenti)/Fornitori	6,5%
	Entrambi	51,6%
Per la sicurezza delle applicazioni della tua azienda vengono acquistati prodotti/servizi?	Si	81,7%
	No	18,3%
Nella tua azienda è previsto l'accesso alle applicazioni aziendali da parte di personale in mobilità (tramite App su smartphone/tablet)? Se si, sono previste azioni finalizzate a prevenire possibili rischi?	No	25,3%
	Si, ma non sono svolte attività di prevenzione	21,5%
	Si e sono svolte attività di prevenzione	45,2%
	Non so	8,1%
Nella tua azienda il personale accede a sistemi esterni (di clienti per manutenzione, di committenti per condivisione dati, etc.)? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?	No	24,7%
	Si, ma non sono svolte attività di prevenzione	19,4%
	Si e sono svolte attività di prevenzione	39,8%
	Non so	16,1%
Puoi indicarci il principale strumento di approvvigionamento di servizi/prodotti di sicurezza della tua azienda?	Trattativa diretta con società specializzate	54,8%
	Acquisto diretto web/digital stores	21,0%
	Gare e accordi quadro	13,4%
	Altro	7,0%
	Non so	3,8%
Ritieni che nella tua azienda ci sia una adeguata consapevolezza rispetto agli impatti connessi alle problematiche legate ai rischi di sicurezza informatica?	Si	60,8%
	No	23,7%
	Non so	15,6%
Quale ritieni sia per la tua azienda il budget annuo adeguato da destinare alla protezione contro le minacce informatiche?	Fino a 10k/anno	54,3%
	Fino a 100k/anno	25,8%
	Più di 100k/anno	19,9%
Sei interessato ad approfondire il tema della sicurezza informatica?	Si	73,7%
	No	26,3%
L'azienda è inserita in una filiera "sensibile" per le minacce cyber (energia, sanità, finance, etc)?	Si	38,7%
	No	61,3%
I processi aziendali necessitano di accesso a internet per poter funzionare? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?	No	13,4%
	Si, ma non sono svolte attività di prevenzione	21,0%
	Si e sono svolte attività di prevenzione	59,7%
	Non so	5,9%
I prodotti dell'azienda possono essere (o saranno) connessi a internet? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?	No	17,2%
	Si, ma non sono svolte attività di prevenzione	23,1%
	Si e sono svolte attività di prevenzione	53,8%

	Non so	5,9%
I servizi dell'azienda richiedono connessione a internet? Se si, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?	No	11,8%
	Si, ma non sono svolte attività di prevenzione	20,4%
	Si e sono svolte attività di prevenzione	63,4%
	Non so	4,3%
È prevista una politica di aggiornamento del software/firmware dei dispositivi utilizzati nell'azienda?	Si	88,2%
	No	11,8%
È prevista una politica di aggiornamento del software/firmware dei dispositivi utilizzati nell'azienda da remoto ?	Si	75,3%
	No	24,7%
I prodotti dell'azienda possono essere impiegati in sistemi/applicazioni critiche (sistemi che in caso di malfunzionamento possono provocare morte o gravi rischi alle persone, perdita o grave danneggiamento di mezzi e materiali, gravi danni ambientali, danno economico)?	Si	39,8%
	No	60,2%
È previsto un controllo di qualità certificato ed una fase di collaudo per tutti i prodotti/servizi dell'azienda?	Si	53,2%
	No	46,8%
L'azienda utilizza software di protezione (antivirus, antimalware, ecc) regolarmente aggiornato su tutti i dispositivi?	Si	93,0%
	No	7,0%
Nell'ultimo biennio è stato effettuato un corso di formazione sulla cyber security al personale non tecnico? (es riconoscere allegati e-mail maligni, utilizzare solo software autorizzato, ecc)?	Si	54,3%
	No	45,7%
Escludendo software antivirus ed eventuale formazione del personale, l'azienda ha investito parte del budget dello scorso anno in attività relative alla sicurezza informatica?	Si	64,5%
	No	35,5%
Utilizzate soluzioni di backup delle informazioni mantenuti fisicamente separati e periodicamente testati?	Si	85,5%
	No	14,5%
L'azienda ha subito nel corso dell'ultimo biennio attacchi informatici?	Si	36,6%
	No	63,4%
Il controllo di qualità considera anche la sicurezza informatica?	Si	59,1%
	No	40,9%

10 RIFERIMENTI BIBLIOGRAFICI

[1] G. Oliva, R. Setola and A. Scala, “Sparse and Distributed Analytic Hierarchy Process", Automatica, vol. 85, pp. 211–220 (doi: 10.1016/j.automatica.2017.07.051).

[2] G. Oliva, R. Setola, A. Scala and P. Dell’Olmo, “Opinion-Based Optimal Group Formation”, Omega, vol. 89, pp. 164–176, 2019 (doi: 10.1016/j.omega.2018.10.008).

[3] G. Oliva, R. Setola, A. Scala and P. dell’Olmo, “Sparse Analytic Hierarchy Process. An Experimental Analysis”, Soft Computing, vol. 23, no. 9, pp. 2887–2898, 2019. (doi: 10.1007/s00500-018-3401-9).

[4] T. L. Saaty, “A scaling method for priorities in hierarchical structures”, Journal of Mathematical Psychology, vol. 15, n. 3, pp. 234–81, 1977.

[5] Decreto Ministeriale del 18 Aprile 2005.

[6] Framework Nazionale per la Cybersecurity e la Data Protection, 2019,
https://www.cybersecurityframework.it/

[7] Italian Cybersecurity Report: Controlli Essenziali di Cybersecurity, 2016