



[CYBERSECURITYREADINESS.IT](https://www.cybersecurityreadiness.it)

Nuove Tecnologie Rischi ed Opportunità per le aziende: AI, Wearable, Quantum, Robotics

Roma, 22 Maggio 2024

NUOVE TECNOLOGIE RISCHI ED OPPORTUNITA' PER LE AZIENDE: AI, WEARABLE, QUANTUM, ROBOTICS

22 Maggio 2024 - Ore 15:00 – 17:00

AGENDA

Saluto istituzionale
VITTORIA CARLI

INTERVENTI

Il progetto CSR - Cyber Security Readiness – per le PMI: stato dell'arte e prossimi passi

ROCCO MAMMOLITI
CSR, Poste Italiane

Overview delle tecnologie emergenti e applicazioni in ambito Cyber

MASSIMILIANO ASCHI
CSR

Contesto internazionale, normative europee sulle tecnologie emergenti

LUIGI MARTINO
CSR

PRESENTAZIONI «Showcase»

Advanced Cyber Security and Decision Intelligence

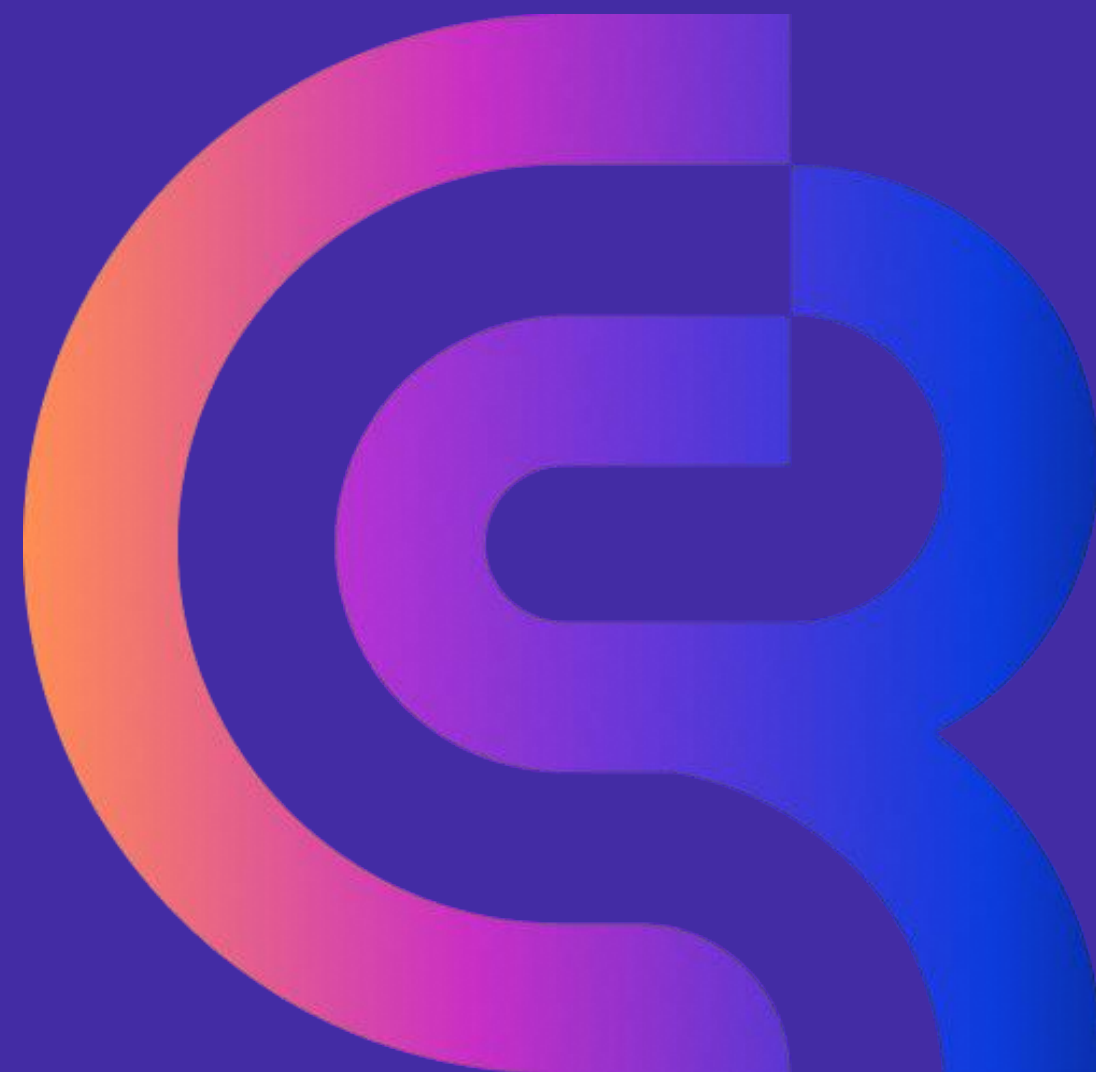
PAOLO CAPODANNO, STEFANIA SICA
ELT Group & Cy4Gate (Roma)

La piattaforma Joshua per la valutazione del Rischio Informatico

GIOVANNI GIOVANNETTI
Almaviva (Roma)

Cyber Minacce Industriali: Come Difendersi dai Rischi dei Dispositivi di Rete e IoT

ALESSANDRO CAPUCCI
Aida46 (Roma)



CYBERSECURITYREADINESS.IT

Cyber Security Readiness

Rocco Mammoliti, GT Cybersecurity Unindustria, Consigliere Sezione IT ,
Poste Italiane



Il Manifesto del Cyber Security Readiness per le PMI

L'obiettivo è Proteggere il
Futuro delle PMI



Supportare e diffondere un adeguato livello di **Cyber Security Readiness** nelle PMI
(Formazione, Awareness, Skills)

Divulgare, formare e sensibilizzare sulle tematiche rilevanti ed a maggior impatto
per il tessuto produttivo nazionale (evoluzione del contesto normativo,
certificazioni, etc.)

Supportare lo sviluppo di un **Ecosistema Efficace, Innovativo e Resiliente** sulla
Cyber Security, che ha come obiettivo la **Resilienza del Sistema Paese**,
coinvolgimento ed elemento di integrazione tra gli Enti Istituzionali e le PMI

**FORMAZIONE
& AWARENESS**



INNOVAZIONE

RESILIENZA
Ecosistemi, RETI e ISAC

I 3 Pillar del CSR:



**Cyber Security Self
Risk Assessment**



**Censimento soluzioni / servizi
Cyber Made-In-Italy**



**Matching Domanda/Offerta
MarketPlace**



Di cosa hanno bisogno le PMI: serve un approccio strategico alla Cyber

Lo Sviluppo delle PMI passa attraverso un adeguato livello di **consapevolezza** del valore rappresentato della **Digitalizzazione** dei propri processi. **La Cybersecurity è un elemento abilitante** per la **fiducia nel mercato digitale** e la continuità dei servizi e lo **Sviluppo delle PMI**.

BISOGNI GENERALI DELLE PMI

- ❑ **INNOVAZIONE e TECNOLOGIA:** essenziale per essere competitivi.
- ❑ **FORMAZIONE e COMPETENZE:** investire nella formazione e nello sviluppo delle competenze
- ❑ **MERCATI INTERNAZIONALI e NETWORKING:** facilitare l'accesso ai mercati internazionali.
- ❑ **SOSTENIBILITA':** le pratiche sostenibili sono un valore ed una opportunità per le PMI.
- ❑ **AMBIENTE NORMATIVO:** Un ambiente normativo stabile e facilmente comprensibile



BISOGNI CYBER SECURITY DELLE PMI

- ❑ **MODELLI INNOVATIVI** di erogazione dei Servizi di Cybersecurity (SOC as-Services, CISO as-Services, Cyber-Insurance, etc)
- ❑ Utilizzare in modo adeguato le tecnologie **CLOUD ed i Servizi SaaS/IaaS**, avendo la consapevolezza di come gestire i contratti con le Terze Parti
- ❑ Tecnologie Innovative: **IA, Cloud Computing, Blockchain, Servizi Trust**, tutela **IPR/Marchi e Loghi...** : valutare le opportunità e gestire i Rischi
- ❑ **SUPPLY CHAIN SECURITY:** come monitorare le proprie Terze Parti, da cui dipende la resilienza stessa, la continuità dell'organizzazione
- ❑ **Cybersecurity Awareness, Training e FORMAZIONE:** per gestire in sicurezza i propri servizi digitali e le informazioni



Di cosa hanno bisogno le PMI: Serve una guida per gestire la complessità

Cybersecurity		Finance		Trusts & Safety		Data & Privacy	
Regulation for a Cybersecurity Act, (EU) 2019/881 2023/0108(COD)		Common VAT system, (EC) 2006/112, 2022/0407(CNS)		Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)		European Statistics, (EC) 2009/223, 2023/0237(COD)	Regulation on the free flow of non-personal data, (EU) 2018/1807
Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887		Administrative cooperation in the field of taxation, (EU) 2011/16		Toys Regulation, (EC) 2009/48, 2023/0290(COD)		General Data Protection Regulation (GDPR), (EU) 2016/679	Open Data Directive (PSI), (EU) 2019/1024
NIS 2 Directive, (EU) 2022/2555		Payment Service Directive 2 (PSD2), (EU) 2015/2366 2023/0209(COD)		European Standardization Regulation, (EU) 2012/1025		Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Data Governance Act (DGA Regulation), (EU) 2022/868
Information Security Regulation, 2022/0084(COD)		Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554		eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)		ePrivacy Regulation, 2017/0003(COD)	Regulation on data collection for short-term rental, 2022/0358(COD)
Cybersecurity Regulation, 2022/0085(COD)		Crypto-assets Regulation (MiCA), (EU) 2023/1114		Radio Equipment Directive (RED), (EU) 2014/53		European Data Act (Regulation), 2022/0047(COD)	Interoperable Europe Act, 2022/0379(COD)
Cyber Resilience Act, 2022/0272(COD)		Financial Data Access Regulation, 2023/0205 (COD)		Regulation for a Single Digital Gateway, (EU) 2018/1724		European Health Data Space (Regulation), 2022/0140(COD)	Harmonization of GDPR enforcement 2023/0202(COD)
Cyber Solidarity Act (Regulation), 2023/0109(COD)		Payment Services Regulation, 2023/0210(COD)		General Product Safety Regulation, (EU) 2023/988		Access to vehicle data, functions and resources Right to repair Directive, 2023/0083(COD)	GreenData4all
		Digital euro, 2023/0212 (COD)		Machinery Regulation, (EU) 2023/1230			
		Regulation on combating late payment, 2023/0323 (COD)		AI Act (Regulation), 2021/0106(COD)			
				Eco-design Regulation, 2022/0095(COD)			
				AI Liability Directive, 2022/0303(COD)			
				Corporate Sustainability Due Diligence and amending Directive (EU) 2022/0051(COD)			

Legenda

In vigore
In negoziazione
In pianificazione

<https://www.bruegel.org>



Aumenta la difficoltà per le PMI di comprendere ed adattarsi al contesto normativo

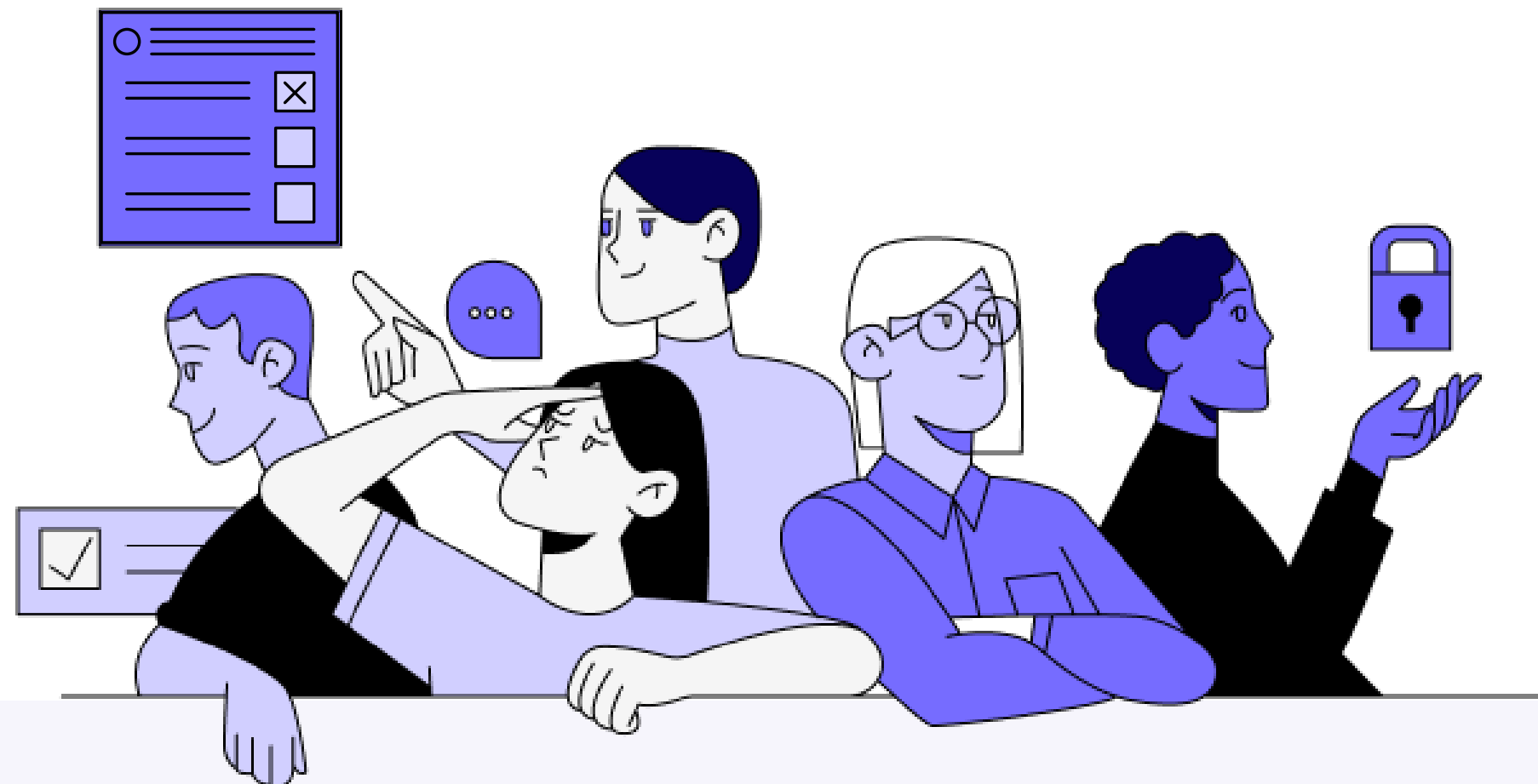


Cosa abbiamo fatto, cosa stiamo facendo



Portale online

[CYBERSECURITYREADINESS.IT](https://www.cybersecurityreadiness.it)



Il portale **Cyber Security Readiness** ospita servizi e prodotti di facile fruizione per valutare, sviluppare e promuovere lo stato di **preparazione cyber** del tessuto economico e produttivo del Paese, con particolare riferimento alle PMI.


**CYBER SECURITY SELF
RISK ASSESSMENT**


**STRUMENTI UTILI PER LA
SICUREZZA AZIENDALE**

**ATTIVITÀ DI AWARENESS
E FORMAZIONE**

Compilazione Questionario

 9 / 20
Complete

 Livello di esposizione dello smart working

 SECURITY INFRASTRUCTURE

B.11 - La tua organizzazione permette accesso alle informazioni ed applicazioni aziendali da dispositivi personali ?

-  NO
 SI

PRECEDENTE

SUCCESSIVA



Visualizzazione rapida domande

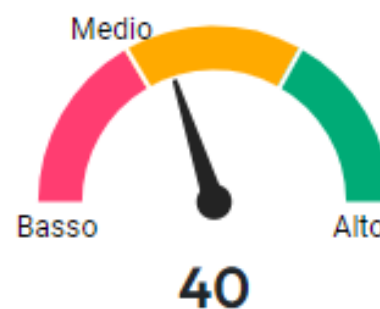
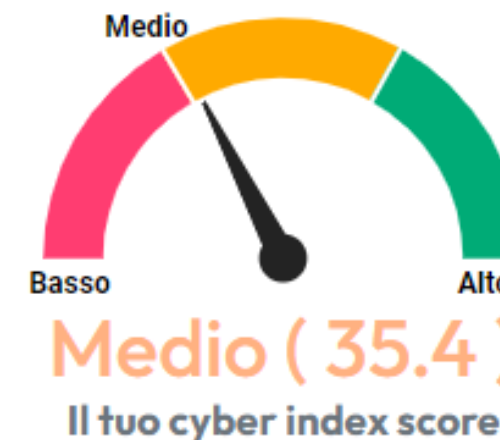
10 - B.11 - La tua organizzazione permette acces 

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	

Ogni questionario fornisce un'analisi dell'esposizione al rischio della società mediante appositi grafici e alcuni suggerimenti per migliorare i propri presidi di sicurezza

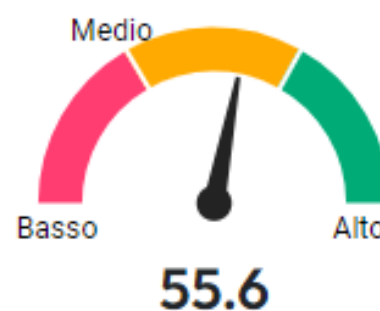
Livello di esposizione al rischio ransomware

Report generato il 30-05-2023 alle ore 11:34



Awareness e Comunicazioni

La formazione e la sensibilizzazione sulla sicurezza delle informazioni è uno dei processi più importanti da implementare per mettere in sicurezza i propri asset, le proprie informazioni. Spesso le Organizzazioni subiscono incidenti che mettono a rischio le informazioni trattate per errori inconsapevoli commessi dai propri dipendenti ed abilmente sfruttati da malintenzionati. Può essere utile ricordare che le Informazioni sono classificate in termini di sicurezza delle informazioni anche per livello di criticità e che a livelli di criticità diversi devono seguire normalmente procedure differenti del dato (permessi di accesso, trattamenti, ecc...). I Dipendenti devono conoscere la differenza di criticità dei dati trattati e l'eventuale rischio che può derivare da un trattamento sbagliato.



Governance & Asset


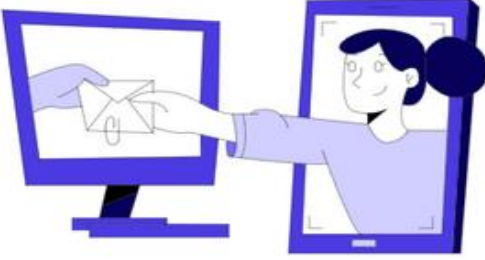


Le risposte fornite indicano la possibilità di migliorare i processi le procedure per la protezione del patrimonio informativo dell'Organizzazione, il vero valore di una Organizzazione. L'adozione di Standard di Sicurezza delle Informazioni rappresentano un valido, e spesso necessario, strumento quando si gestiscono informazioni Critiche. Impostare un Framework processi e controlli consente di avere più facilmente il controllo del proprio Livello di Sicurezza, in particolare l'Analisi del Rischio aiuta a determinare le priorità di intervento. Far rivedere il proprio Sistema di Processi e Controlli da professionisti indipendenti può aiutare a migliorarlo.



Protezione del Dato, Backup e DR



Le Survey: i primi risultati

Cyber Security Self Risk Assessment Autovalutazione del livello di sicurezza della propria azienda  COMPILA QUESTIONARIO	Livello di esposizione al rischio ransomware Ransomware Self Assessment  COMPILA QUESTIONARIO	Livello di esposizione dello smart working Remote Working Risk Assessment  COMPILA QUESTIONARIO	Livello di adeguatezza della sicurezza delle terze parti Third Party Risk Management  COMPILA QUESTIONARIO
---	--	--	---

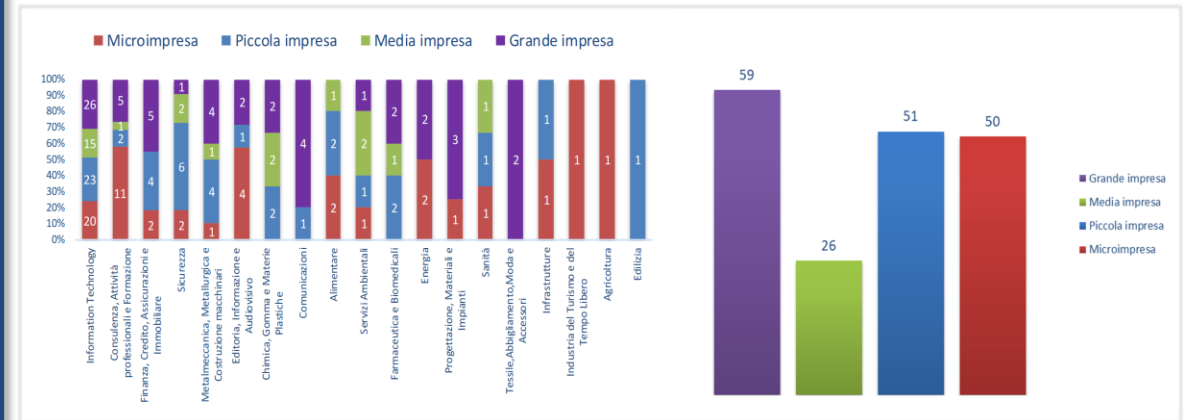
Numero questionari fatti	104	35	32	38
Numero domande per questionario	48	25	20	34
Numero di PMI che hanno risposto al questionario	> 160			
Interesse per la Cybersecurity ? E' fonte di preoccupazione	Si per > 90%			

Il Report 2021



I risultati

186 questionari da aziende appartenenti a diversi settori merceologici e diversificate tra Micro, Piccola, Media e Grande Impresa

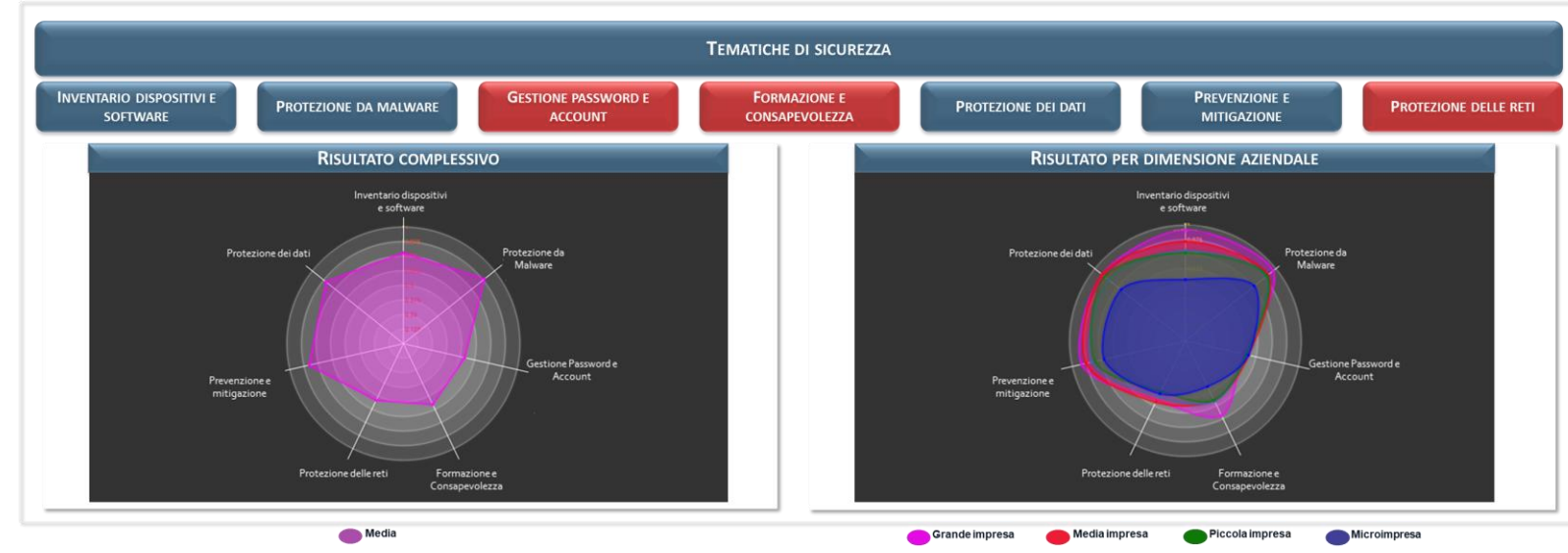


La Survey

La Survey si compone di 32 domande suddivise tra domande di carattere generale sull'organizzazione della società e domande di carattere tecnico/organizzativo. Le domande di carattere tecnico/specifico si suddividono nelle seguenti macro categorie

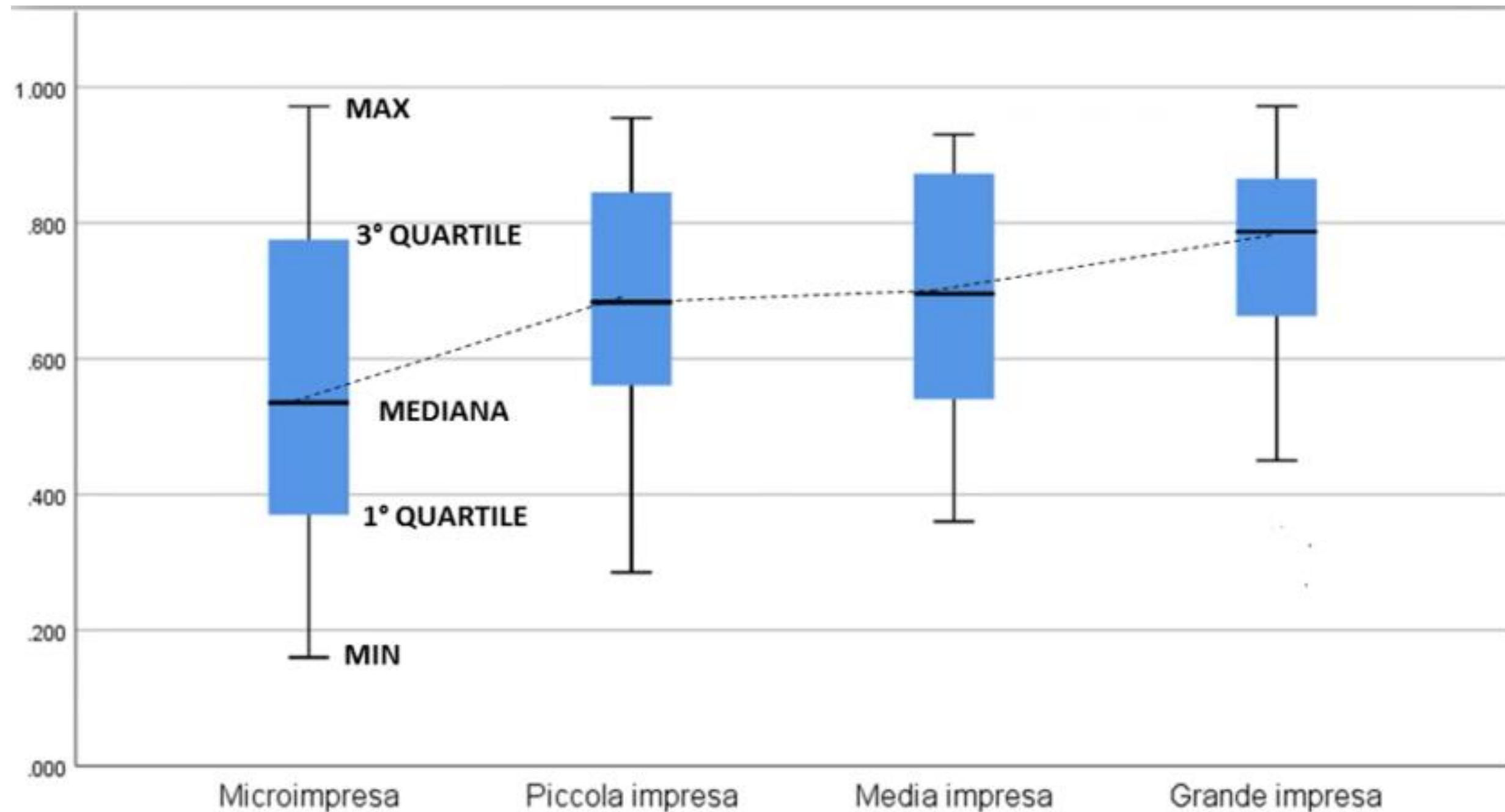
- COMMITMENT AZIENDALE**
misurare l'attenzione del management in termini di risorse, budget e awareness sulle tematiche di cyber security.
- LIVELLO DI ESPOSIZIONE**
misurare l'esposizione dell'azienda a minacce/attacchi cyber in funzione della rilevanza servizi/prodotti erogati dall'Azienda
- MATURITA' TECNOLOGICA/ORGANIZZATIVA**
misurare il grado di maturità tecnologica/organizzativa dell'azienda nel prevenire, contrastare, mitigare le minacce del cyber spazio.

Il legame tra Cyber Risk Self Assessment e Controlli Essenziali di Cybersecurity è stato riscontrato in 7 tematiche di sicurezza



- Inventario Dispositivi e Sw
- Protezione Malware
- Gestione Pwd ed Account
- Formazione
- Protezione Dati
- Prevenzione e Mitigazione
- Protezioni Reti

Cyber Security Score (CSS) e Dimensione Societaria



- il «CSS» cresce sensibilmente al crescere della dimensione societaria.
- All'aumentare della dimensione dell'azienda diminuisce la variabilità ovvero diminuisce la distanza tra i valori massimo e minimo.

Il grafico a Boxplot indica la distribuzione del CSS nelle quattro tipologie di dimensioni aziendali.



Le Survey: i primi risultati 2024

Impiego di SOC (security
Operation Center) ?

NO 46%

SI 54%

Accesso 2FA ?

SI - 42%

NO - 58%

certificazioni di Sicurezza
– ISO 27001 ?

SI - 42%

NO - 58%

Data Masking e Data
Encryption?

SI - 55%

NO - 45%

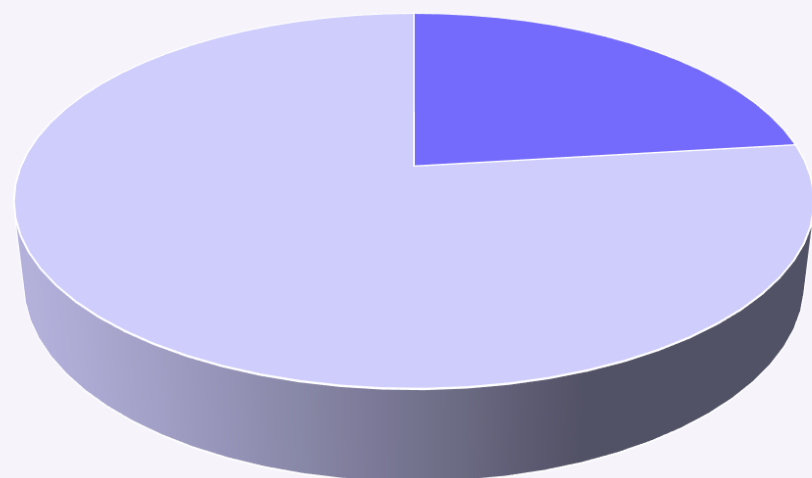
E' necessario far comprendere l'importanza di gestire la CyberSecurity con strumenti adeguati



Le Survey: i primi risultati

attacchi informatici?

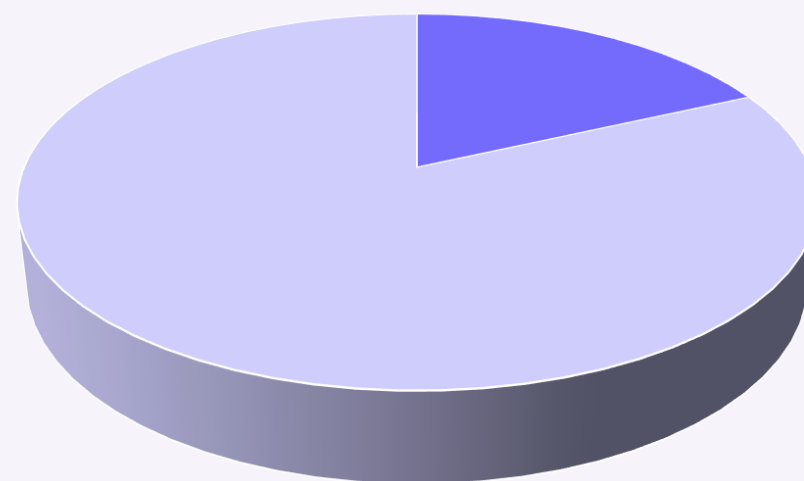
SI - 23%



NO - 77%

piano protezione Ransomware?

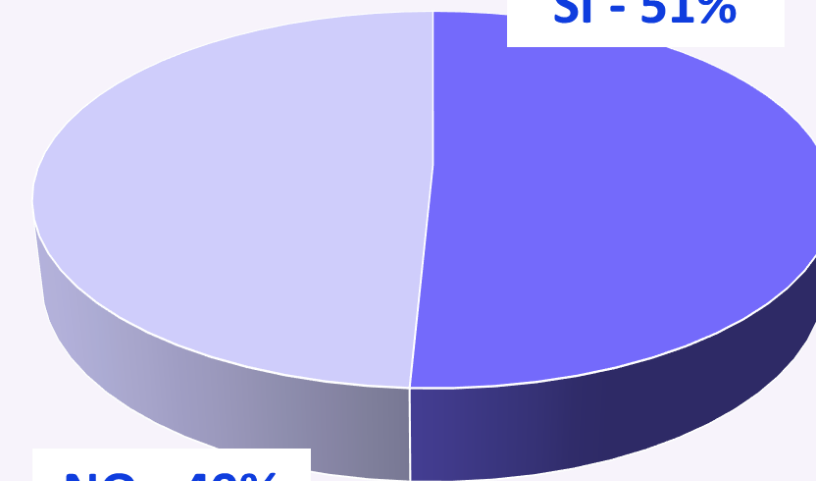
SI - 18%



NO - 82%

Risk Management ?

SI - 51%



NO - 49%

Una fotografia che può far pensare che eventuali rischi-eventi possano non essere individuati dalle PMI



RISCHIO CYBER

PERCHÉ AUTOVALUTARSI



Scopri gli ambiti specifici in cui è maggiormente esposta la tua organizzazione e le relative pratiche di sicurezza migliori

Domini di sicurezza del QUESTIONARIO

Il raggruppamento delle domande nei principali domini della *cyber security*, ci consente di fornire indicazioni chiare nell'esito finale riguardo gli interventi più urgenti da effettuare per diminuire il proprio livello di esposizione al rischio informatico.

Governance e Asset

Gestione della sicurezza dell'organizzazione con politiche, procedure, standard e certificazioni; controllo delle risorse aziendali attraverso l'inventario degli elementi della catena di valore.

Protezione del dato, Backup e Disaster Recovery

Impiego di soluzioni per la protezione del dato che ne garantiscano riservatezza, integrità e disponibilità in casi di possibili situazioni catastrofiche e di attacchi informatici distruttivi.

Security infrastructure

Adozione di misure di sicurezza per proteggere il patrimonio informativo dell'organizzazione (informazioni classificate o riservate, proprietà industriale, ecc.)

Security update e monitoring

Aggiornamento frequente dei sistemi di sicurezza e monitoraggio costante degli eventi per migliorare la consapevolezza sul proprio livello di esposizione alle minacce informatiche e per consentire interventi di contrasto tempestivi

Awareness e comunicazioni

Sensibilizzazione e formazione del personale per migliorare i presidi di sicurezza aumentando la consapevolezza sugli attacchi informatici e le loro possibili conseguenze

Risorse utili:
• Standard ISO/IEC 27001 per la gestione della sicurezza informatica
• Guida alla cybersicurezza per le piccole e medie imprese - ENISA
• Vademecum Sicurezza Piccole e Medie Imprese - CYBER 4.0



Sicurezza delle terze parti



Collaborare con partner e fornitori per ridurre le vulnerabilità informatiche in modo sistemico

1763

Attacchi informatici rilevati e contrastati dall'Agenzia per l'Italia Digitale nel 2022

93%

Segnalazioni di campagne malware basate sul tentativo di furto dei dati (personali, professionali e bancari)

50%

Casi in cui si invitano le vittime a prendere visione di falsi ordini e pagamenti

Proteggere i propri sistemi e le informazioni trattate per conto di altre aziende costituisce un elemento fondamentale per la reputazione e il valore di un'impresa.

Allo stesso tempo, assicurarsi che partner e fornitori soddisfino i livelli di sicurezza concordati, estende la protezione aziendale alla catena di approvvigionamento (supply chain) realizzando un modello di difesa collettiva.



Identificare i rischi cibernetici e i vincoli normativi applicabili sulla base dei prodotti commerciali o servizi erogati



Valutare e monitorare nel tempo l'esposizione dei partner ad attacchi informatici tramite questionari o audit



Mappare le relazioni commerciali e tracciare gli accessi ai dati e alle informazioni dell'organizzazione

Risorse utili:
• Report ENISA sulle tecniche di attacco rivolte contro la filiera di fornitura
• D.L. 21/09/2019, n. 105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
• D.P.C.M. 14/04/2021, n. 81 - Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici
• Norma ISO 28000:2007 per la gestione della sicurezza della catena di fornitura
• NIST SP 800-161 Rev. 1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations



PERICOLO RANSOMWARE

Osserva i dettagli prima di agire online

COS'È

È un programma malevolo che:

- **infetta** i dispositivi elettronici (PC, telefoni, ecc.)
- **blocca** l'accesso a ciò che contengono
- **chiede un riscatto** (ransom) per tornare alla normalità.



Si diffonde principalmente attraverso **email, sms e messaggi** provenienti da soggetti apparentemente conosciuti e affidabili oppure navigando su **siti creati o compromessi** dagli hacker.

“ Ogni dispositivo infettato ne può contagiare altri, sfruttando la sincronizzazione o accedendo alla rubrica per spedire automaticamente messaggi contenenti il malware. ”

COME DIFENDERSI

Anche se i messaggi provengono da persone conosciute, controlla sempre la destinazione dei link passandoci sopra il cursore del mouse senza cliccare. Usa market ufficiali per scaricare le applicazioni e installa software antivirus su tutti i dispositivi.

Aggiornamenti regolari

Copia frequente dei dati

Rivolgersi a tecnici specializzati

Denunciare attacchi alla Polizia Postale

Segnalare furto dati al Garante Privacy

STOP

Diffida di inviti allettanti: quasi sempre si tratta di trappole ben congegnate

Per segnalare un attacco, visita il sito [NO MORE RANSOM](https://www.no-more-ransomware.eu/) gestito da Europol, polizia olandese, Kaspersky e McAfee



SMART WORKING

Adotta le giuste misure di sicurezza

Il lavoro da remoto espone le aziende a rischi specifici legati all'accesso indesiderato a informazioni di rilievo, anche in modo inconsapevole.

Queste vulnerabilità possono essere mitigate da alcuni interventi basati sulla protezione degli strumenti e sulla formazione del personale coinvolto.

1 Proteggere le comunicazioni su internet, i dispositivi aziendali e quelli personali usati per lavorare da remoto



Indicazioni generali:

- Installa un software antivirus
- Esegui aggiornamenti regolari
- Evita di collegare supporti elettronici senza effettuare una scansione antivirus

Imposta:

- Username e password personalizzati su tutti i dispositivi (no default)
- Codice di accesso per smartphone e tablet
- Salva schermo con codice di sblocco per PC
- Nome della rete Wi-Fi personalizzato
- Firewall sul router
- Crittografia sulla rete
- Log di accesso alla rete

Usa:

- Connessioni sicure (Wi-Fi privato, connessione dati sim aziendale, ecc.)
- Rete privata virtuale (VPN)
- Doppio fattore di autenticazione (strong-authentication)
- Autenticazione biometrica
- Applicazioni autorizzate e verificate



2 Conoscere i comportamenti corretti da assumere per un uso adeguato degli strumenti professionali

Posta elettronica:

- Comunicazioni professionali
- Mittente conosciuto e affidabile
- Scansione antivirus degli allegati
- Filtro antispam
- Log-out al termine dell'attività

Password:

- Diverse per ogni strumento e servizio
- Non condivise
- Lunghe e complesse
- Aggiornate regolarmente
- Sequenze di caratteri imprevedibili
- Generatore e Gestore verificati e attendibili

Navigazione internet:

- Visitare solo siti utili all'attività lavorativa
- Indirizzi web con protocollo https://
- Assicurarsi che l'indirizzo (url) visualizzato nella barra del browser corrisponda al sito che si intende visitare

Risorse utili:
• Strumento SecureHello per generare password robuste
• Servizi di protezione dei sistemi informatici - Cyber 4.0
• Standard ISO/IEC 27033 - Sicurezza della rete



Il Manifesto Cybersecurity PMI 12 Azioni per rendere sicura la propria Azienda



Piano di Formazione ed Awareness 2023-2024

Workshop di Formazione

2023- 2024

- ✔ Supply Chain Security
- ✔ Certificazione ISO 27001
- ✔ Certificazioni Cyber Prodotti EU/ITA
- ✔ Attacchi Informatici: difendersi
- ✔ Nuove Tecnologie ed opportunità
- Strumenti per la Cybersecurity

Workshop di Formazione

2023- 2024

Approfondimenti tecnologici

- Log Management
- Security Container
- Ciclo di vita del Software
- IA: Rischi ed Opportunità
- Esperienze di CISO e CTO



Progetto Le Terze Parti

Standardizzare i processi
per aiutare le PMI

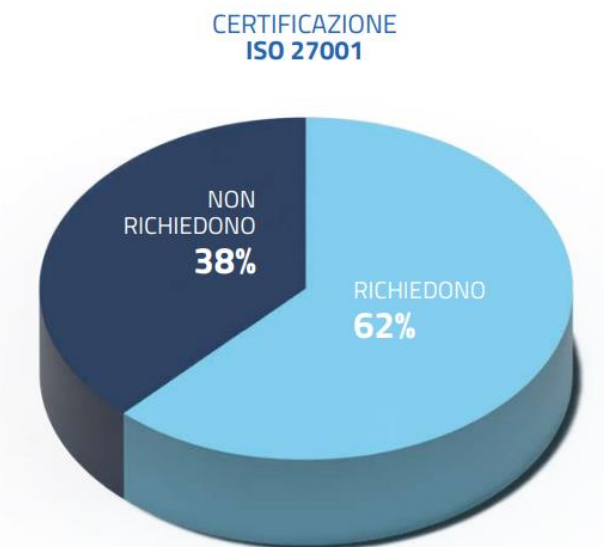
1 IL RISCHIO CYBERSECURITY DOVUTO ALLE TERZE PARTI

Le rilevazioni del World Economic Forum (WEF) e del rapporto Anchore indicano che tra il 39% e il 62% delle organizzazioni è stato colpito da un incidente informatico di Terze Parti. ...le compromissioni della catena di fornitura sono state il secondo vettore di infezione iniziale più diffuso identificato nel 2021.

3 REQUISITI DI SICUREZZA NELLE GARE

ANALISI DEI REQUISITI PRESENTI NEI CAPITOLATI DI GARA IN TEMA DI CYBER SECURITY

...non tutte le aziende richiedono espressamente alle PMI di essere in possesso di detti certificati, ma richiedono che vengano rispettati degli standard minimi che tutelino le informazioni condivise e consentano continuità nell'erogazione del servizio



2 FRAMEWORK E LINEE GUIDA DI GESTIONE



NISTIR 8276
Key Practices in Cyber Supply Chain Risk Management

4 IL PROCESSO

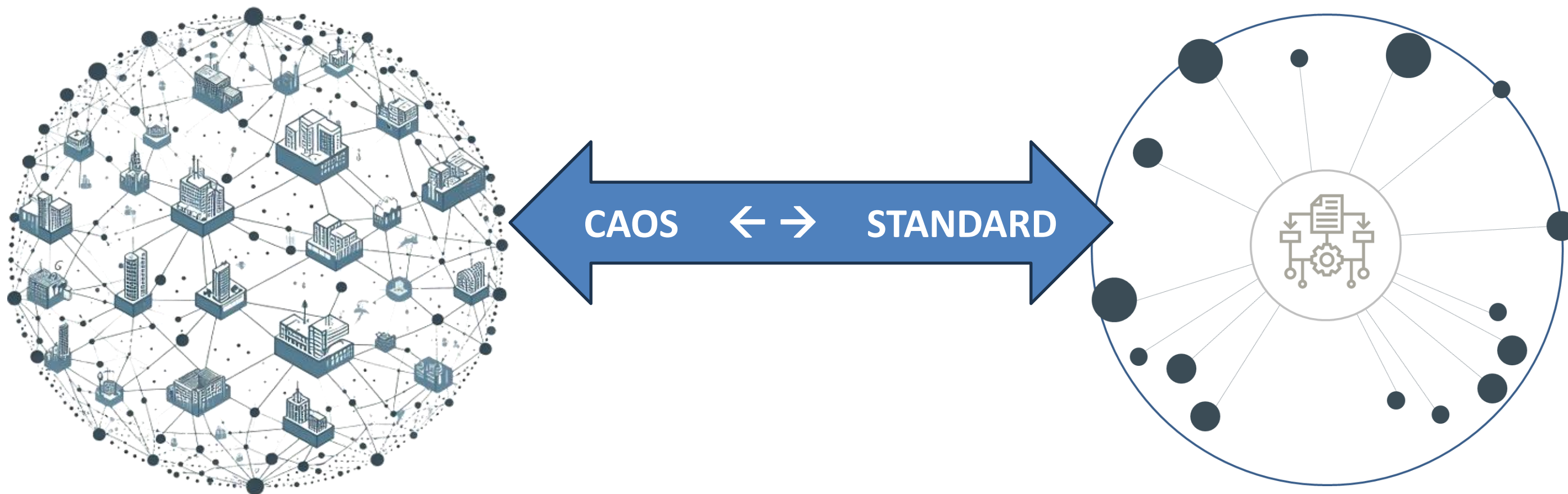


Loghi:
EBA/EIOPA
Banca d'Italia
IVASS
ACN



Le Terze Parti: stato dell'arte ed opportunità di migliorare l'ecosistema

Le PMI/SME, oltre 22 Milioni in EU, rappresentano la struttura portante dell'economia comunitaria ed in questo momento sono fortemente coinvolte dalle misure messe in atto dall'EU, in termini di **Monitoraggio di Cybersecurity** e sostenibilità. L'Obiettivo è di ottenere una **Supply Chain più Resiliente**. Oggi la **Supply Chain** sta fronteggiando un enorme sforzo per adeguarsi.



Le PMI sono raggiunte da numerose e continue richieste di attività di **Due-Diligence** da parte dei loro Clienti rispetto a:

- *Survey Cybersecurity / Privacy*
- *Survey ESG*
- *Analisi della loro postura internet (cybersecurity)*
- *Audit di seconda parte*

Standardizzare il processo di Analisi delle Terze Parti consente di:

- Ridurre il carico di lavoro per le PMI
- Migliorare l'efficacia dei processi di controllo
- Poter avere aggiornata una fotografia a Livello Paese sullo stato di salute delle PMI e della Supply Chain

CYBERSECURITYREADINESS.IT



Grazie per l'attenzione.