Un progetto di

fondirigenti

CYBER

CREAZIONE DI UN MODELLO DI VALUTAZIONE DEL RISCHIO CYBER CON FOCUS SULLE PMI

Realizzato da

FONDAZIONE PIEMONTE INNOVA

In collaborazione con

UNIONE INDUSTRIALI Torino

FEDERMANAGER TORINO APDAI

SOMMARIO

INTRODUZIONE

La frequenza e la sofisticatezza degli attacchi informatici stanno aumentando rapidamente, di pari passo con l'utilizzo di infrastrutture e tecnologie dell'informazione e della comunicazione da parte di persone, enti, aziende, istituzioni. Il fabbisogno di conoscenze e competenze in materia di sicurezza informatica supera l'offerta, bisogna perciò investire nello sviluppo di competenze e talenti in questo ambito a tutti i livelli, dai non esperti ai professionisti altamente qualificati. Tali investimenti devono puntare non solo ad ampliare il bagaglio delle competenze di cybersecurity nelle aziende, ma anche a garantire che le stesse possiedano capacità adeguate ad affrontare il panorama delle minacce informatiche e che i dirigenti che le governano abbiano contezza del tema e competenza sufficiente per identificarne le caratteristiche e l'applicazione nelle rispettive aziende.

A fronte del contesto generale, il progetto CYBER ha permesso a manager e dirigenti di 28 imprese di confrontarsi nel corso di sette mesi (maggio-novembre 2022) e di individuare le migliori strategie per accrescere la consapevolezza e la conoscenza di sicurezza informatica (cybersecurity), al fine di rendere le aziende significativamente più sicure e resilienti, e quindi in grado di intraprendere azioni e buone pratiche per proteggere adeguatamente i sistemi informativi, i dati aziendali e i processi aziendali garantendo livelli di continuità del business, anche in caso di attacchi cyber. Inoltre, attraverso questa azione il territorio ha acquisito know-how ed elementi distintivi che gli consentono di posizionarsi come territorio di riferimento su questi temi.

Il progetto, quindi, ha investigato in una prima fase il livello di consapevolezza sul tema della cybersecurity di manager e dirigenti, per poi approfondire, attraverso due focus group, un world cafè e un simulation game, le strategie adottate nell'acquisire competenze, strumenti e policy che consentono di prevenire e di gestire i rischi cyber attraverso l'uso di tecnologie e l'implementazione di processi e modelli organizzativi per resistere a possibili attacchi informatici. Dal lavoro congiunto è nata una proposta di linee guida da seguire, descritte nel paragrafo *Metodi, strumenti e persone*, per aumentare la cybersecurity aziendale. Ora a disposizione del management, il Cyber Readiness Level, è lo strumento creato durante il progetto per valutare il livello di cybersecurity di un'impresa.

In particolare, il progetto CYBER ha previsto le seguenti fasi di lavoro:

- **Fase 1** - **Indagine**: finalizzata a comprendere lo stato dell'arte in materia di awareness delle imprese sul tema della cyber security;
- **Fase 2** - **Esplorazione**: confronto attivo tra i dirigenti partecipanti al progetto in merito alle azioni messe in atto prima, durante e dopo un attacco cyber in termini organizzativi, di adeguamento tecnologico, di revisione dei processi e policy aziendale;
- **Fase 3** - **Misurazione:** progettazione di uno strumento di analisi / self-assesment che può essere utilizzato dal management e dalle imprese come strumento in grado di misurare lo stato di consapevolezza e comprensione, le prassi adottate, gli ostacoli e barriere legate alla sicurezza dei dati e dei processi;
- **Fase 4** - **Costruzione collaborativa del Modello**: elaborazione di un modello ripetibile per sostenere la capacità di gestione del rischio cyber e la resilienza del management delle imprese – in particolare PMI - prima, durante e dopo un potenziale attacco;
- **Fase 5** – **Simulazione di processo**: un'analisi sugli scenari possono scaturire dal punto di vista tecnologico, di processo e legale, durante un attacco cyber. Il risultato è l'implementazione di linee guida e raccomandazioni per prevenire possibili attacchi;
- **Fase 6** - **Modellazione:** il progetto, gli strumenti e i modelli atti a supportare una diffusione rapida delle competenze cyber e degli strumenti atti a sostenere la resilienza e capacità di ripresa delle imprese;
- **Fase 7** - **Diffusione dei risultati:** gli output dell'iniziativa sono stati presentati durante un evento finale alla presenza di rappresentanti del Fondo e dei principali stakeholder.

CYBERSECURITY AWARENESS

La consapevolezza in tema cybersecurity è un costrutto complesso che risulta dalla interazione tra informazioni, conoscenze e comportamenti. Non è solo una caratteristica individuale, ma si riflette e si articola a livello organizzativo e di sistema. Inoltre, è importante considerarne la natura dinamica, sulla quale si possono basare strategie di engagement, formazione e promozione.

Per andare a comprendere meglio il contesto della cybersecurity, il progetto Cyber ha preso le mosse da un'azione di indagine del livello di consapevolezza delle imprese sul tema, condotta da fine maggio a inizio luglio 2022.

Il campione dell'indagine è stato di 100 aziende, per il 40% di manufatturiere, rappresentative di diversi comparti produttivi, seguite da imprese ICT e TLC (20%). Le imprese del campione sono prevalentemente piemontesi e il 22% ha sedi distribuite in diversi Paesi (di queste, il 12% ha sedi sia in Paesi europei sia extra EU). I rispondenti sono prevalentemente uomini (69%), over 45 (73%) e il 58% ricopre ruoli apicali, seguiti dai tecnici 17%; solo il 3% del totale è un profilo specialistico della cybersecurity.

Lo strumento quantitativo ha cercato di cogliere e descrivere su una scala ampia alcune dimensioni di consapevolezza:

- cultura della cybersecurity;
- processi;
- tecnologie e soluzione;
- competenze e formazione.

In particolare, dall'indagine è emerso il seguente quadro della situazione e di seguito vengono riportati i risultati suddivisi sulle dimensioni individuate.

Cultura della cybersecurity

Le imprese hanno confermato la **rilevanza** e la **sensibilità** verso la promozione della cybersecurity, a cui in particolare le **piccole imprese** (81%) guardano con attenzione.

I driver decisionali che muovono le imprese a investire in cybersecurity sono tuttavia ancora di natura esterna. **Il rispetto delle normative** (46%) e l'evidenza - per chi li ha affrontati - di **attacchi** (32%) o **eventi avversi** (42%) sono il motore principale.

La **cultura della cybersecurity** è presente in diversi aspetti, tuttavia non sembra trovare realizzazione in traiettorie di implementazione che bilancino l'adeguamento tecnologico (58%), l'organizzazione dei processi (35%), il fattore umano (25%).

Tra le misure di promozione e sviluppo della cybersecurity è emersa come rilevante anche la **formazione**, azione da svolgere a tappeto, che dovrebbe interessare tutto il personale, incluso top management ed enti tecnici.

Processi a supporto della cybersecurity

L'indagine ha messo in evidenza la **centralità dei profili tecnologici** nella gestione della cybersecurity. Tuttavia, sono poche le realtà in cui la gestione avviene in modo strutturato. Il tipo di informazioni e sistemi di monitoraggio della sicurezza sono tradizionali.

Come conseguenza, ad esempio, si è rilevata una bassa o assente consapevolezza di alcuni tipi di rischi (attacchi ai siti web, nessun attacco: 48%).

Il **CISO** è una figura istituzionale **solo per il 10%** delle imprese, mentre la responsabilità della cybersecurity è nella maggior parte dei casi in capo all'**IT manager** che è ad interim la persona **responsabile anche per la cybersecurity** (**36% del totale**).

Vi sono spazi per la promozione di un **approccio multidisciplinare alla cybersecurity**, con il coinvolgimento di funzioni organizzative a supporto (quali amministrazione, HR, marketing e legal).

Tecnologie e soluzioni in uso

La dotazione di soluzioni e sistemi per la cybersecurity rispecchia lo stato dell'arte delle misure richieste dalle normative in vigore.

Il livello di innovazione delle soluzioni potrebbe crescere, soprattutto tra le piccole e medie imprese, grazie al traino di alcune grandi imprese e di innovazioni tecnologiche provenienti da startup.

Competenze e formazione

Le competenze e la formazione sulla cybersecurity sono riconosciute come un **asset centrale** dalle imprese, tuttavia la **formazione** nella maggior parte dei casi è risultata un'**attività occasionale**, utile sicuramente a rispondere a obblighi di legge, ma **non sufficiente a coprire e rinforzare altri aspetti della cybersecurity**, inclusi il versante tecnologico e il fattore umano. Tale dato si riscontra in modo distribuito nelle imprese di tutte le dimensioni.

La maggior parte delle imprese ha dichiarato che gestisce la cybersecurity con **competenze interne**: sono soprattutto le micro e le piccole imprese a esternalizzare, coadiuvando o vicariando la funzione IT.

Il fabbisogno formativo rilevato include i temi tecnici proposti, ma è alta la percentuale di imprese (50%) che non "sa indicare" tematiche di formazione auspicabili. Questa informazione suggerisce spazi di miglioramento, soprattutto per lavorare sull'**aggiornamento del personale**, su temi che vanno oltre la formazione obbligatoria.

La **periodicità** della formazione è un fattore importante per mantenere alto il livello di consapevolezza e attenzione di tutto il personale sui possibili rischi.

Non sorprende rilevare una buona adozione di strumenti di **formazione a distanza**, anche come conseguenza alla massiccia remotizzazione di molte attività e task professionali.

Viene confermato l'**approccio non strutturato** alla formazione sulla cybersecurity, per una parte importante del campione affidata a modalità informali di passaggio delle informazioni.

In conclusione, i dati raccolti attraverso il questionario disegnano un perimetro di interesse e conoscenza che ha messo in evidenza importanti aspetti e chiavi di lettura del tema della cybersecurity.

Gli aspetti di consapevolezza sono emersi nella rilevanza che le imprese riconoscono ai processi e alle componenti della cybersecurity.

I dati raccolti hanno offerto uno spaccato, che seppur parziale e meritevole di analisi più approfondite, è stato particolarmente utile per sollevare ulteriori domande di approfondimento, che sono state occasione di lavoro per le fasi successive del progetto.

METODI, STRUMENTI E PERSONE

In questa sezione si forniscono indicazioni e raccomandazioni per massimizzare la cybersecurity in azienda attraverso l'adozione di **metodi e procedure**, l'implementazione di **strumenti** a livello organizzativo, tecnologico e normativo e la pianificazione di azioni di **formazione** e di sviluppo delle competenze del personale.

Alcune raccomandazioni generali sul **modello operativo** costruito durante il progetto Cyber comprendono l'aggiornamento del personale, il livello di commitment del top management, l'attenzione alle policy e alla normazione dei processi, l'individuazione di esperti esterni in ambito cyber, il coinvolgimento dell'HR in termini di cultura aziendale e l'istituzione di figure dedicate alla cybersecurity.

A livello di **strumenti organizzativi**, oltre a implementare la sicurezza fisica, è fondamentale avere un Asset Inventory, costruire la mappa della rete e dei dati, realizzare una valutazione del rischio (Risk Assesment), avere un piano di Data Loss Prevention, strutturare un Disaster Recovery Plan, effettuare un Business Impact Assesment, e istituire piani di continuità operativa (Business Continuity Plan) sfruttando checklist di self-assesment. A livello **normativo**, è consigliabile raggiungere le certificazioni ISO e conoscere le principali normative italiane ed europee. A livello di **strumenti tecnologici** sono imprescindibili l'autenticazione multi-fattore, l'anti-malware, l'aggiornamento automatico dei sistemi, il monitoraggio continuo, la Data Protection con la gestione degli accessi alle informazioni.

Il tema della **formazione** è cruciale per una gestione corretta della cybersecurity in azienda. In particolare, è importante formare il personale di base sugli obblighi di legge (privacy, GDPR) e sui temi tecnici (in modo sincrono e asincrono). Un piano di formazione e aggiornamento, come meglio descritto in seguito, deve quindi prevedere, in maniera continua e ciclica: eduzione di base, formazione a tappeto e aggiornamento su temi specifici. La formazione può poi avvenire analizzando casi specifici (adoption by example), simulando attacchi cyber (training by doing) e fornendo resoconti dettagliati di tali simulazioni (feedback). Il mix formativo deve comunque essere multicanale, esperienziale, continuativo e trasversale durante tutte le attività.

Metodi

In ogni impresa è fondamentale individuare le corrette procedure per un'efficace gestione della cybersecurity. In particolare, si evidenzia la necessità di implementare procedure di:

- Asset Inventory (con mappa della rete, mappa dei DATI);
- Risk Assesment;
- Piani di continuità operativa con BIA (Business Impact Assesment) e Disaster Recovery plan;
- Audit di 2° livello ai fornitori: approccio collaborativo per accompagnare i fornitori a raggiungere e garantire i livelli di sicurezza attesi.

Da momento che la cybersecurity non è (solo) una questione di tecnologie, è fondamentale comprendere che si tratta di un processo trasversale, che coinvolge qualsiasi livello aziendale. È però importante sottolineare che è necessario che organizzazione e processi siano aspetti interdipendenti tra loro ed entrambi legati al **commitment del top management**. Spetta quindi ai manager e ai dirigenti istituire **tavoli stabili multifunzione** e incentivare la formazione in ambito cybersecurity, continua e

mirata. Un metodo efficace può essere **simulare un attacco informatico**, descritto nel seguito, dove le persone in azienda si trovano, in un contesto sicuro e protetto, a gestire una situazione avversa.

Tavoli stabili multifunzione

Al momento attuale, nella maggior parte delle imprese incontrate, la governance della cybersecurity non è un processo strutturato e sistematico. In particolare:

- nelle **Grandi Imprese:** la governance è frammentata tra diverse figure specialistiche, le quali curano aspetti specifici, ciascuno per la sua competenza (tecnica/legale);
- nelle **PMI**: quando presente, la governance è accentrata nella figura dell'IT manager.

Entrambe queste situazioni possono esporre le imprese a rischi di varia natura.

Si raccomanda quindi un **TAVOLO STABILE MULTIFUNZIONE**, che includa le funzioni:

- IT (gestione sistemistica, gestione della rete, progettazione, sviluppo e conduzione dei software applicativi, considerando anche gli attori esterni);
- CISO, DPO;
- Legale;
- Amministrazione (acquisti).

Simulazione di un attacco informatico

Il role-play è una delle **tecniche di formazione** più conosciute, da svolgersi con esperti[1] che guidano il confronto e la discussione tra i partecipanti. In particolare, si tratta di una **tecnica di simulazione** e cerca di riprodurre, in una situazione protetta (aula, laboratorio), eventi e problemi della vita reale. Nel role-play si mettono in atto ruoli organizzativi o sociali in genere (non personali).

Il risultato dell'attività è la **rappresentazione scenica di un'interazione** interpersonale che risulta dall'assunzione di comportamenti in una situazione immaginaria. Nel gruppo dei partecipanti, alcuni svolgono per un tempo limitato il ruolo di "**attori**", impersonando il ruolo scelto o assegnato, e gli altri sono gli "**osservatori**".

La tecnica implica la **successiva analisi delle dinamiche giocate**, delle modalità di esercizio di specifici ruoli, e più in generale dei processi di comunicazione agiti nel contesto rappresentato.

Si affronta uno scenario immaginario per **svolgere un esercizio di problem solving**, con una particolarità: tutti saranno chiamati a **giocare un ruolo diverso da quello che svolgono quotidianamente**. Questo è il meccanismo scelto per guardare alla stessa situazione da prospettive diverse da quelle a cui si è abituati.

Applicare **questo approccio in azienda**, potendo costruire scenari realistici, con dati reali, che permettano di sviluppare prima una consapevolezza allargata in diversi profili e funzioni aziendali, è un modo efficace per studiare strategie e tattiche per rafforzare la cyber security in azienda e le competenze nelle persone. In particolare, il simulation game è particolarmente utile come strumento per il top management per testare la catena decisionale in occasione di un attacco cyber e fare una stima dei costi da sostenere per difendere i sistemi attaccati.

[1] In occasione del progetto CYBER, Fondazione Piemonte Innova è stata affiancata dagli esperti di metodi partecipativi di Links Foundation, dagli esperti di cybersecurity di Actarvs dagli esperti di normative e compliance di Profice.

Il gioco "giocato"

Di seguito si riporta la struttura del simulation game realizzato nell'ambito del progetto Cyber. Le imprese che partecipati al "gioco" hanno provato a costruire una possibile risposta per gestire l'attacco informatico seguendo le differenti fasi del gioco e stimolate dalle questioni poste dagli esperti.

LE FASI DEL GIOCO

FASE 0: IL GIORNO PRIMA: la sfida è iniziata il giorno prima del simulation game, con l'e-mail di promemoria dell'incontro che conteneva inneschi potenzialmente pericolosi

FASE 1: IL SET-UP

- Scenario aziendale: ProtoMec[2] è un'impresa manufatturiera che produce bulloni e componenti metallici per autoveicoli;
- Contesto:
    - Sede principale: Settimo Torinese
    - Organico: 30 persone
    - Fatturato annuo: 3,5 ml di euro
    - Sistemi IT e Cybersecurity: Antivirus, Firewall, back-up automatico giornaliero online (stesso supporto e stessa sede).
    - Budget per gestire l'emergenza: 35mila €
- Assegnazione dei ruoli (6 partecipanti per tavolo): amministrazione, IT Manager, Tecnico IT, AD, HR, DPO;
- Schede personaggi: descrizione del proprio "nuovo" ruolo per focus sul gioco;
- Gli strumenti di gioco: carte azione per ciascuna fase di gioco, carte consulenza.

FASE 2: L'ATTACCO E IL SUO VETTORE: primo confronto tra i partecipanti.

FASE 3: LA PRIMA GESTIONE: dal problem setting… al problem solving.

In conseguenza dell'attacco, i computer iniziano a dare problemi:

- Non si aprono più i file
- Si aprono finestre di dialogo che chiedono autorizzazioni
- Il malware prende possesso della rete

Quali sono le azioni da svolgere? Quali sono gli assets dell'azienda che potrebbero essere sottoposti ad attacco? Quale valore hanno? Qual è la priorità tra questi? Quali sono gli strumenti di monitoraggio più opportuni? Qual è la strumentazione hardware e software per il ripristino?

FASE 4: IL CONTENIMENTO: dopo la prima reazione, come ripristinare l'operatività?

FASE 5: L'IMPREVISTO: ai due gruppi viene notificata una richiesta di riscatto da parte di chi ha lanciato il ransomware. Che cosa fare?

FASE 6: L'ANALISI POST-INCIDENTE

L'azienda ha ripreso la sua attività. A valle dell'incidente subito, è il momento di fare un'analisi del decorso per capire come rendere più sicura l'azienda. Quali i punti deboli? Che cosa non va ripetuto in futuro? Che cosa va potenziato?

[2] Azienda immaginaria. Eventuali riferimenti a imprese reali sono puramente casuali.

FASE 7: L'ESITO E I FEEDBACK AI GRUPPI

- **Gestione pienamente riuscita**: corretta escalation interna, analisi eseguita, riscatto non pagato, comunicazione ai clienti, pulizia macchine prima della ripresa operatività, misure avanzate in post incidente.
- **Gestione parzialmente riuscita**: escalation incompleta, analisi dell'incidente parziale, pagamento riscatto, nessuna comunicazione ai clienti, riavvio backup ma senza pulizia, solo misure tecnologiche per il post incidente.
- **Gestione non riuscita**: gestione interna, nessuna analisi, pagamento riscatto, nessuna comunicazione ai clienti, riavvio backup senza pulizia macchine, solo controllo stato attuale in post incidente.

Rispetto agli eventi avversi si rileva che:

- le aziende tendono a **non denunciare**. Questa reticenza si spiega con una generale sfiducia nell'atto della denuncia e negli enti preposti. Denunciare un tentativo o un attacco non garantisce di poterne arginare gli impatti. Vi è inoltre il timore di mettere l'azienda in cattiva luce, con un portato negativo sulla reputazione, soprattutto per le imprese più grandi.
- le **assicurazioni** non sono considerate misure protettive, anzi sono spesso giudicate dannose, perché a fronte della spesa non garantiscono né risarcimenti, né soprattutto il recupero dei dati. Si aggiunge a questi aspetti il **disorientamento**: è difficile per le imprese trovare un'assicurazione unica, che riesca a proteggere da diversi fattori di rischio. Infine, emerge una generale sfiducia.

Strumenti

Tecnologici

- **Autenticazione multi-fattore**: le password sono un elemento fondamentale per la sicurezza informatica, la gestione delle stesse andrebbe regolamentata da policy formalizzate. Per un'autenticazione più sicura, alle password devono essere affiancati diversi fattori, come, per esempio, l'autenticazione biometrica tramite impronte digitali o i sistemi di OTP (One Time Password) per un accesso con doppia verifica;
- **Anti-malware**: è un software di cybersecurity specifico per l'identificazione e l'eliminazione dei malware, programmi che sono ideati per il danneggiamento o il furto dei dati e dei sistemi informatici. Gli anti-malware moderni sono in grado di identificare le minacce verificando il cosiddetto "comportamento", eliminando anche malware nuovi o software malevoli sviluppati ad hoc;
- **Aggiornamento automatico sistemi**: l'aggiornamento dei programmi e dei sistemi operativi è fondamentale per garantirne il corretto funzionamento e protezione. Quando una vulnerabilità viene rilevata in un sistema è dovere del produttore rilasciare le cosiddette patch di sicurezza per chiudere eventuali falle, abilitare dei sistemi per l'aggiornamento automatico evita che eventuali attaccanti possano sfruttare le vulnerabilità zero-day;
- **Monitoraggio continuo**: un servizio di monitoraggio continuo, fornito da un SOC, permette alle aziende che non hanno un reparto di cybersecurity interno di monitorare costantemente i dispositivi e la rete. In caso di attacchi, rilevamento di vulnerabilità o malfunzionamenti sulla rete si è quindi in grado di agire tempestivamente e isolare i dispositivi per evitare la propagazione dell'attacco;
- **Data protection e gestione accessi alle informazioni**: la data protection è un processo/insieme di comportamenti, regole e soluzioni tecnologiche cui obiettivo è la salvaguardia dei dati, evitando quindi di perderli, che vengano modificati o esfiltrati; la gestione degli accessi alle informazioni è importante all'interno dei processi di compliance e sicurezza. Dal punto di vista compliance è necessario verificare e tracciare quali dati vengono trattati attraverso l'apposito registro, quali operatori ci accedono e con quali mezzi e la finalità del trattamento. Dal punto di vista della sicurezza informatica limitare l'accesso a diverse aree o dati è un modo per limitare eventuali danni, accidentali o meno.

Organizzativi

- **Tavoli stabili multifunzione**, come precedentemente citato;
- **Governance**: catena decisionale lunga nelle GI, accentrata nelle PMI in una figura sola;
- **Budget dedicato**: la cybersecurity non è generalmente un'attività considerata core;
- **Controlli organizzativi**:
    - **Asset Inventory**: l'inventario degli asset serve a conoscere e controllare gli elementi di un sistema di gestione per la sicurezza delle informazioni. Tra questi elementi ci sono i server, i pc, i dispositivi di uso personale, i dispositivi di rete, le sedi, gli impianti di sicurezza, gli archivi fisici, le informazioni stesse e il personale;
    - **Risk Assessment**: la valutazione del rischio (Risk Assessment) è il processo complessivo di identificazione, analisi e ponderazione del rischio. Questo permette di identificare i rischi da mitigare e quelli da accettare;
    - **Business Impact Assessment (BIA)**: analisi dei processi tale da individuare i loro massimi tempi di indisponibilità (MTPD), le infrastrutture (informatiche e non

informatiche) minimali da assicurare in caso di emergenza e quindi il massimo tempo di indisponibilità dei sistemi informatici e la frequenza massima dei backup e delle repliche dei dati. La Business Impact Assessment (BIA) permette di identificare le soluzioni di continuità tali che assicurino un determinato tempo di indisponibilità dei sistemi informatici (RTO) e la frequenza dei backup (RPO);

- **Piani di continuità operativa** (Business Continuity Plan - BCP): si tratta di procedure, tra loro correlate, che specificano i passi da seguire in caso di indisponibilità di processi o di risorse. Parte del BCP è il DRP. Solitamente si tratta di documenti con indicati, come minimo, le persone responsabili delle diverse attività (coordinamento, attivazione delle soluzioni tecniche, relazioni con il pubblico, relazioni con i clienti) e le soluzioni scelte e i relativi RTO e, per i sistemi IT, RPO. In realtà molto grandi, sono usati anche strumenti software per mantenere queste informazioni aggiornate e allineate con il personale effettivamente disponibile. Il BCP deve considerare le procedure da attuare in caso di eventi pertinenti (mancanza di sede, di fornitori, di sistemi IT, di connettività, di risorse non IT, di personale, ecc.);
- **Self-assessment, audit e certificazioni**: verifiche periodiche delle misure di sicurezza. Le misure dovrebbero essere originate da una valutazione del rischio e verificate per completezza con i riferimenti più noti (per esempio, ISO/IEC 27001, NIST CSF);
- altri: **mappa della rete, mappa dei dati, Data Loss prevention, Disaster Recovery Plan** (parte del BCP).

Normativi

- Informarsi sugli enti esistenti (diritti e doveri);
- Dotarsi di figure aziendali preposte (CISO e DPO);
- Valutare l'applicazione delle normative ISO (per poi arrivare anche in un secondo momento alla certificazione).

In questo ambito, i riferimenti più significativi sono:

- **ISO/IEC 27001**
- **ISO/IEC 27002** con i suoi controlli relativi alla sicurezza fisica, relativi soprattutto al controllo accessi, alla prevenzione di intrusioni fisiche e alla sicurezza e manutenzione degli impianti),
- **EN 50600**: riferimento principale per la sicurezza fisica dei data center (divisa in più parti e recepita a livello internazionale nel 2018 con la ISO/IEC 22237, divisa in 7 parti). La **ISO/IEC 22237**, a differenza della ISO/IEC 27001, non è uno standard per sistemi di gestione, ma permette comunque di ottenere una certificazione del data center.
- la **normativa privacy**, regolata primariamente dal **Regolamento europeo 679/2016** noto come **GDPR** e dal **D. Lgs. 196/2003** (ovviamente modificato negli anni) che stabilisce alcune specificità italiane; attenzione va posta anche ai Provvedimenti del Garante per la privacy, ossia l'autorità di controllo italiana;
- la **normativa relativa alla responsabilità civile delle imprese**, che regola le modalità con cui un ente può essere ritenuto responsabile in caso di reati del personale che portano vantaggi all'ente stesso; la materia è regolata dal **D. Lgs. 231/2001**;
- la **normativa sul Diritto d'autore** (in particolare la **L. 633/1941**, modificata negli anni) e il **D. Lgs. 30 del 2005**, **Codice della proprietà industriale**; la normativa è stata di recente oggetto di interventi a livello europeo;
- **normativa specifica per le infrastrutture critiche** e gli enti che costituiscono il «perimetro nazionale di sicurezza cibernetica».

Persone

È fondamentale lavorare su tre differenti livelli:

1. **Educazione di base**: oltre all'utilizzo dei sistemi aziendali, è necessario creare una conoscenza di base sui rischi informatici e le conseguenze. Utile a questo proposito proporre un percorso di alfabetizzazione alla sicurezza informatica, che parta da e includa anche la sfera personale, per creare buone abitudini e competenze sulla sicurezza che portino a tenere comportamenti sicuri sempre, anche in azienda e in modo indipendente dal contesto;
2. **Formazione** a tappeto, nessuno escluso, per rispondere a esigenze e obiettivi specifici:
    a. il top management e il personale per acquisire consapevolezza e capacità di riconoscere possibili rischi e attuare procedure safe nel day-by-day, senza eccezioni;
    b. i tecnici per ricevere aggiornamento continuo su rischi e strumenti, che sono in continuo sviluppo;
3. **Aggiornamento**: la formazione va mantenuta e aggiornata in modo continuativo per mantenere alta l'attenzione ai rischi e la conoscenza delle misure preventive e protettive.

Percorso formativo

Con riferimento alla norma **ISO/IEC 27002**, in Italia recepita come **UNI CEI EN ISO IEC 27002 Tecnologie Informatiche - Tecniche di sicurezza - Codice di pratica per la gestione della sicurezza delle informazioni**, stabilisce che la sicurezza dell'informazione è caratterizzata da integrità, riservatezza e disponibilità. Il documento è organizzato in dieci aree di controllo e ogni sezione è dedicata a una parte specifica. In particolare, facendo riferimento a un percorso formativo, le raccomandazioni includono in seguenti temi:

- **politiche di sicurezza** (intesi come messaggi della Direzione);
- le **motivazioni** per cui è necessario seguire le regole di sicurezza (ricordando anche la necessità di rispettare le normative vigente, i contratti con i clienti);
- le **regole di base** da seguire (per es., non aprire allegati a e-mail sospette, lasciare la scrivania pulita, mantenere segrete le password);
- le **sanzioni disciplinari** previste;
- le **procedure di base** (per es., chi contattare in caso di incidente);
- modalità per **approfondire** (procedure e politiche interne, siti web, ecc.).

APPROFONDIMENTO 1 | Controlli base e avanzati: checklist[3] ready-made

Tale approfondimento si propone di fornire al top management di un'azienda controlli di cybersecurity, minimi e avanzati, da implementare seguendo la checklist. L'elenco di azioni e buone pratiche da introdurre vuole favorire una gestione più rapida, ma al contempo completa, della cybersecurity.

CONTROLLI MINIMI	CONTROLLI AVANZATI
Politiche: ☐ **ORG** - valutazione del rischio e piano di trattamento del rischio; ☐ **ORG** - politiche e regole al personale (dipendente e collaboratori, inclusi gli stagisti) – uso dell'e-mail, dei dispositivi aziendali e personali quando usati per trattare i dati aziendali;	**Politiche**: ☐ **ORG** - istituzione di una bacheca (anche digitale, p.e. con wiki); ☐ **ORG** - piano della sicurezza, anche economico, con riesame annuale;
Responsabilità: ☐ **NORM** - identificazione di un responsabile per la sicurezza (CISO); ☐ **ORG** – censimento degli amministratori di sistema; ☐ **ORG** - monitoraggio delle fonti di informazione in merito alla sicurezza;	**Responsabilità**: ☐ **ORG** - attribuzione del ruolo di responsabile per la sicurezza (CISO) a una persona indipendente dall'IT; ☐ **ORG** - tavolo periodico con IT (gestione sistemistica, gestione della rete, progettazione, sviluppo e conduzione dei software applicativi, considerando anche gli attori esterni), CISO, DPO, Legale, amministrazione (acquisti); ☐ **ORG** - assegnare un budget alla cybersecurity da far gestire ai responsabili tecnici; ☐ **ORG** - stabilire un SOC e uno "sportello informatico" (per domande, dubbi); ☐ **ORG** - esplicitare e monitorare i livelli dei servizi interni (come IT e assistenza tecnica); ☐ **ORG** - sottoscrizione di assicurazioni (considerandone i limiti); ☐ **ORG** - identificazione dei processi critici e a rischio di frode (p.e. quelli di pagamento) e delle opportune misure da attuare;
Personale: ☐ **ORG** - formazione (o alfabetizzazione) al personale (non solo dipendenti), anche con corsi online (es. con strumento Moodle); ☐ **ORG** - formazione ai dirigenti; ☐ **ORG** – prevedere formazione tecnica ai tecnici sugli strumenti usati (p.e. sistemi operativi Windows o Linux); ☐ **ORG** - partecipazione ad associazioni e gruppi che si occupano di sicurezza;	**Personale**: ☐ **ORG** - formazione continua al personale (non solo dipendenti), anche con finte tecniche di attacco (simulazione di campagne di phishing); ☐ **ORG** - formazione de visu, se possibile **esperienziale**; ☐ ORG - sensibilizzazione continua, con un programma specifico, con anche messaggi dalla Direzione in diverse occasioni (e osservando che le abitudini nel privato vengono poi applicate anche in ambito lavorativo); ☐ **ORG** - affiancamento, oltre alla formazione e alle attività di sensibilizzazione; ☐ **ORG** – test sulla formazione; ☐ **ORG** - condivisione dei risultati di valutazione del rischio;

[3] ORG: misure organizzative, TECH: misure tecnologiche, NORM: misure normative. Checklist realizzata in collaborazione con Cesare Gallotti.

CONTROLLI MINIMI	CONTROLLI AVANZATI
Inventario: ☐ **TECH** - inventario dei server e delle applicazioni; ☐ **ORG** - inventario dei dispositivi assegnati agli utenti;	**Inventario**: ☐ **TECH** - inventario dei server, delle applicazioni, dei dispositivi, della rete con strumenti di discovery; ☐ **ORG** - inventario dei dati (Quali vengono utilizzati? Quando? Da chi? Dove sono archiviati? Chi accede?); ☐ **ORG** - identificazione dei dati che dovrebbero essere solo su cartaceo;
Controllo accessi: ☐ **ORG** - limitazione degli accessi (con però attenzione alla produzione in ambito industriale), considerando il ruolo di ciascuno; ☐ **ORG** - segregazione dei dati; ☐ **ORG** - modalità di archiviazione dei dati (su server e non su dispositivo; cartelle e faldoni specifici anche per poterli segregare correttamente e impostare il controllo degli accessi); ☐ **ORG** - processo di gestione delle credenziali (assegnazione, cambio, cancellazione), con canali di comunicazione ben definiti; ☐ **ORG** - processo di gestione delle autorizzazioni, con canali di comunicazione ben definiti (con particolare attenzione all'eterogeneità dei sistemi usati, anche cloud); ☐ **ORG** - riesame periodico delle autorizzazioni assegnate; ☐ **TECH** - controllo degli accessi degli amministratori di sistema;	**Controllo accessi**: ☐ **TECH** - uso di strumenti di conservazione dei documenti; ☐ **TECH** - controllo degli accessi centralizzato; ☐ **TECH** - uso di tecniche di autenticazione a più fattori (evitando SMS, usando generatori di OTP come p.e. quelli di Google o Microsoft); ☐ **TECH** - uso di tecniche basate su riconoscimento biometrico; ☐ **TECH** - uso di strumenti di single-sign-on (SSO); ☐ **TECH** - uso di strumenti di password vault per gli amministratori; ☐ **TECH** - identità digitale anche per le macchine;
Sicurezza fisica: ☐ **TECH** - manutenzione degli impianti, inclusi quelli collegati all'informatica (UPS, generatori, trasformatori);	**Sicurezza fisica**: ☐ **TECH** - programma di manutenzione, che includa: UPS, Aria condizionata Uffici, Aria condizionata CED, verifica impianto elettrico (trasformatori MT-BT e cablaggio), Impianto Rilevazione incendio, Estintori, Derattizzazione, Antintrusione, ascensori. ☐ **NORM** – stabilire, concordare con i fornitori (dove applicabile) e monitorate le scadenze delle manutenzioni;
Gestione dei sistemi IT e dei dispositivi: ☐ **ORG** - processo di gestione dei cambiamenti dei sistemi informatici; ☐ **TECH** - processo di ritiro dei dispositivi e cancellazione delle memorie; ☐ **TECH** - cifratura dei dispositivi; ☐ **TECH** – anti-malware; ☐ **TECH** - backup (con piano anche di conservazione); ☐ **TECH** - logging con raccolta su sistema dedicato (in particolare per gli amministratori di sistema); ☐ **TECH** - aggiornamento automatico o semi-automatico di dispositivi e server;	**Gestione dei sistemi IT e dei dispositivi**: ☐ **ORG** - processo di gestione dei cambiamenti dei sistemi informatici stabilito con diversi livelli di autorizzazione; ☐ **ORG** - PoC prima dell'introduzione di nuovi strumenti e per dimostrare il funzionamento e l'efficacia di soluzioni e servizi e analisi dei fabbisogni di competenze e di persone necessarie per la manutenzione degli strumenti; ☐ **TECH** - controllo dei dispositivi anche di P.IVA, fornitori, clienti; ☐ **TECH** - uso di strumenti di controllo dei dispositivi (AD per i pc e MDM per smartphone e tablet), anche per la cancellazione da remoto;

CONTROLLI MINIMI	CONTROLLI AVANZATI
	☐ **TECH** - vietare l'uso di dispositivi personali o non aziendali; ☐ **TECH** - configurazione degli apparati aziendali per evitare l'uso promiscuo di account aziendali; ☐ **TECH** - blocco dei dispositivi usati per accedere ai dati aziendali; ☐ **TECH** - collegare gli strumenti informatici al SOC (o ad altre entità) affinché sia verificato lo stato degli aggiornamenti dei sistemi; ☐ **TECH** - strumenti di DLP e di end-point protection; ☐ **TECH** - blocco delle porte USB; ☐ **TECH** – anti-malware centralizzato; ☐ **TECH** - log anche delle attività sul cloud, in particolare degli amministratori di sistema; ☐ **TECH** - logging con strumenti SIEM (p.e. Sumologic) e monitoraggio comportamenti (non per profilazione, ma per evidenziare attività "fuori dal comune"); ☐ **TECH** - uso di IDS (intrusion detection system) e NIDS (network IDS); ☐ **TECH** - conduzione periodica di Vulnerability Assessment e Penentration Test (nei casi più importanti, necessario usare fornitori esterni);
Sicurezza di rete: ☐ **TECH** - firewall; ☐ **TECH** - canali di trasmissione cifrati (e loro censimento);	**Sicurezza di rete**: ☐ **TECH** - firewall e VLAN per separare le reti di amministrazione, dei server e degli utenti; ☐ **TECH** - per il controllo degli accessi alla rete, usare un NAC (network access control); ☐ **TECH** - uso di proxy web per il controllo della navigazione (p.e. limitando l'uso dei social network); ☐ **TECH** - segregazione delle reti OT (dove applicabile); ☐ **TECH** - uso di strumenti di file sharing privati (es. Data space easy di TIM); ☐ **TECH** - uso di strumenti di file sharing privati con limitazione del download dei file; ☐ **TECH** - per l'accesso da remoto, uso di VPN con connessione non statica (p.e. uso di Authenticator);
Sicurezza applicativa: ☐ **TECH** - regole per lo sviluppo sicuro delle applicazioni (almeno funzionali);	**Sicurezza applicativa**: ☐ **TECH** - regole per lo sviluppo sicuro delle applicazioni, conduzione di test funzionali di sicurezza e della sicurezza del codice (OWASP); ☐ **TECH** - uso di strumenti di verifica del codice (SAST e DAST);
Gestione dei fornitori: ☐ **NORM** - contratti con i fornitori con clausole di sicurezza e privacy (soprattutto se responsabili del trattamento);	**Gestione dei fornitori**: ☐ **ORG** - identificazione e monitoraggio SLA; ☐ **NORM** - richiesta di certificazioni ai fornitori; ☐ **NORM** - audit e verifiche ai fornitori più critici; ☐ **ORG** - gestione dei fornitori con collaborazioni anche tecniche;

CONTROLLI MINIMI	CONTROLLI AVANZATI
Gestione degli incidenti: ☐ **NORM** - procedura di gestione degli incidenti relativi alla sicurezza delle informazioni e alla privacy (data breach); ☐ **ORG** - piano di comunicazione ai clienti in caso di incidenti con impatto sui loro dati o sulle loro attività;	**Gestione degli incidenti**: ☐ **ORG** - gruppo di persone dedicato alla gestione degli incidenti informatici;
Continuità operativa: ☐ **TECH** - piano e sito di disaster recovery o DR (ossia backup presso una sede distinta da quella primaria, anche sul cloud; dove possono anche trovarsi sistemi di backup); ☐ **TECH** - fare test del DR;	**Continuità operativa**: ☐ **TECH** - ridondanze dei sistemi critici (load balancing, cluster, ecc.); ☐ **ORG** - piano di continuità operativa basato su un'analisi di impatto (BIA); ☐ **ORG** - uso di strumenti di contatto multipli (per la messaggistica istantanea, meglio Signal o MS Teams);
Conformità: ☐ **ORG** - audit interni periodici; ☐ **ORG** - verifica dell'operato degli amministratori di sistema	**Conformità**: ☐ **NORM** - mantenimento di un elenco della normativa applicabile alla sicurezza delle informazioni (diritto d'autore, 231); ☐ **NORM** - audit interni a sorpresa su alcuni temi specifici (p.e. verifica della scrivania pulita, dei biglietti con password) e richiami; ☐ **NORM** - funzione di audit interno dedicata.

APPROFONDIMENTO 2 | Nomenclatura cyber: legenda dei più comuni acronimi di riferimento

Acronimo	Significato
2FA	Autenticazione a 2 fattori
BCP	Business Continuity Plan o piano di continuità operativa
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CISO	Chief Information Security Officer
CSF	CyberSecurity Framework
DAC/RDAC	Discretionary Access Control
DLP	Data Loss Prevention
DPIA	Privacy Impact Assessment
DPO	Data Protection Officer
DR/DRP	Disaster Recovery Plan
EDR	End-point Detection and Response
GDPR	General Data Protection Regulation
IDS	Intrusion detection system
IACS	Industrial Automation and Control Systems
IoT	Internet of Things (Internet delle cose)
ISO	International Organization for Standardization
IT	Information Technology
MDM	Mobile device management
MFA	Multi-Factor Authentication
MAC	Mandatory Access Control (Controllo accesso obbligatorio)
NAC	Network Access Control
NIS	Network and Information systems
NIST	National Institute of Standard and Technology (USA)
PDCA	Plan-Do-Check-Act (ciclo di Deming)
PT	Penetration test
RID	Riservatezza, Integrità e Disponibilità
SGSI	Sistema di Gestione per la Sicurezza delle Informazioni
SIEM	Security Information and Event Management
SOC	Security Operation Center
SoD	Separation of Duty
VA	Vulnerability Assessment
XDR	Extended Detection and Response

APPROFONDIMENTO 3 | Riferimenti e Agenzie nazionali ed europee

Si forniscono di seguito i siti di maggiore utilità e di riferimento in tema di cybersecurity:

- acn.gov.it, l'ACN è Autorità nazionale per la cybersecurity. Assicura il coordinamento tra i soggetti pubblici coinvolti nella materia e promuove la realizzazione di azioni comuni volte a garantire la sicurezza e la resilienza cibernetica necessarie allo sviluppo digitale del Paese;

- clusit.it, una delle associazioni italiane più importanti con l'obiettivo di promuovere e diffondere la cultura e la consapevolezza della sicurezza informatica in tutti i suoi aspetti;

- csrc.nist.gov, uno dei siti più importanti per quanto riguarda la sicurezza informatica, legato al governo USA;

- enisa.europa.eu, European Network and Information Security Agency. L'Agenzia collabora con le organizzazioni e le imprese per rafforzare la fiducia nell'economia digitale, promuovere la resilienza delle infrastrutture dell'UE e, in ultima analisi, garantire la sicurezza digitale dei cittadini dell'UE. Ciò avviene attraverso la condivisione delle conoscenze, lo sviluppo di personale e strutture e la sensibilizzazione;

- garanteprivacy.it, Garante per la protezione dei dati personali;

- Gallotti C. (2022). *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione. La ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*;

- Hadlington, L. *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*. Heliyon 3 (2017) e00346.

CYBER READINESS LEVEL

Introduzione al tool

Il Cyber Readiness Level (CRL) nasce da un confronto durato otto mesi tra esperti di cybersecurity e imprese, prevalentemente PMI, del territorio piemontese, che hanno lavorato insieme, coordinati da Torino Wireless, con l'obiettivo di costruire un modello concreto di analisi del livello della cybersecurity aziendale. Strumento reale a disposizione dei manager sarà il Cyber Readiness Level, un questionario di self-assesment per valutare il livello di resilienza della propria azienda verso attacchi cyber e, allo stesso tempo, permettere ai dirigenti di capire quali possano essere gli step successivi per migliorare la propria cyber-resilienza. In altri termini, uno strumento di formazione e sensibilizzazione del management sul tema della cybersecurity.

Il CRL è la congiunzione tra un aspetto pratico, dato dal confronto strutturato con le aziende a guida Torino Wireless, e uno teorico, fornito da una integrazione con le normative esistenti grazie al lavoro congiunto degli esperti con Torino Wireless. L'attuale proposta dello strumento è stata raggiunta seguendo il flusso di attività individuato per il progetto: indagine preliminare sul tema della cyber awareness (oltre 100 rispondenti), esplorazione delle buone pratiche e delle criticità tra le aziende (20 imprese) con due Focus Group e un World Cafè e, infine, la modellizzazione dello stesso. L'ultimo step è stato la validazione sul campo, chiedendo ai manager delle imprese di compilare lo strumento costruito al fine di testarne la bontà e settare al meglio gli output per i dirigenti che in futuro compileranno il questionario di self-assesment.

Il tool è stato messo a punto e sperimentato nel progetto e, al momento, sono allo studio (d'intesa con Fondirigenti) le modalità per la diffusione dello strumento.

La struttura

Strumento in grado di raccogliere e misurare lo stato di consapevolezza e comprensione, le prassi adottate, gli ostacoli e barriere legate alla sicurezza dei dati e dei processi, individuando possibili aree di miglioramento e crescita di competenze sul quale investire per una migliore gestione della sicurezza.

Il CRL è strutturato su 5 dimensioni, ognuna articolata in 5 criteri; per ogni criterio sono poi descritti 5 differenti scenari. A ogni persona che compila il questionario è richiesto di collocarsi sullo scenario che corrisponde maggiormente al posizionamento della sua azienda.

Protezione

Il tema della protezione relativo alla cybersecurity è ampio e tocca differenti aspetti. In particolare, i cinque criteri individuati per la dimensione PROTEZIONE rappresentano i temi principali a cui un'impresa, in particolare una PMI, deve prestare particolare attenzione per far crescere il proprio livello di cyber-resilienza. Si parla quindi di **aggiornamento dei sistemi operativi**, degli applicativi e delle librerie utilizzate all'ultima patch rilasciata, di una corretta **gestione dei sistemi IT** da parte dei dipendenti, di **crittografia** delle informazioni per evitare possibili data breach, di **politiche di backup** (e delle modalità possibili) per ripristinare dati persi o alterati, e di **sicurezza della rete** con sistemi quali firewall, IDS, NIDS, Antivirus, EDR e SIEM.

Criteri

- Aggiornamento software;
- Policy di sicurezza;
- Crittografia;
- Backup;
- Sicurezza della rete.

Gestione e tecnologie

Oggi sono sempre più diffusi **strumenti cloud** e ogni azienda deve domandarsi quanto e quali di questi siano affidabili e se rispettino la normativa GDPR; è importante poi per ogni impresa dotarsi di un **inventario dei prodotti hardware e software**, creato e aggiornato grazie all'ausilio di appositi strumenti, che effettuino anche la scansione della rete e dei software installati nei pc e di regole corrette per la **gestione degli applicativi**. È fondamentale capire quale livello si vuole dare ai dipendenti nella gestione hardware e software, individuando con precisione chi rendere **amministratore di sistema**.

A disposizione delle aziende, ci sono poi controlli specifici e periodici chiamati **Vulnerability Assessment (VA) e Penetration Test (PT)**, generalmente svolti da aziende terze specializzate per testare il livello di sicurezza dell'azienda.

Criteri

- Strumenti cloud;
- VA e PT;
- Inventario;
- Gestione applicativi;
- Amministratori di sistema.

Organizzazione e processi

Strutturare in maniera chiara e precisa l'organizzazione della cybersecurity è il primo passo per rendere l'azienda più cyber-resiliente. Tra i principali criteri da prendere in considerazione la **manutenzione dei sistemi IT** individuando del personale dedicato, prevedere un **piano di rientro** degli incidenti (Disaster Recovery Plan per garantire la Business Continuity), gestire il processo di **autenticazione** (password e altri sistemi più evoluti) ai dispositivi e alla rete aziendale (**segregazione della rete**) per evitare contaminazione in caso di attacco e avviare un processo di acquisto strutturato di **strumenti di sicurezza** adeguati (come antivirus di nuova generazione, next-gen firewall, logger, SIEM).

Criteri

- Manutenzione IT;
- Piano di rientro;
- Autenticazione;
- Segregazione della rete;
- Acquisizione strumenti di sicurezza.

Compliance e normative

L'adeguamento alla **normativa privacy (GDPR)** attualmente in vigore è uno dei requisiti fondamentali richiesto ad aziende di ogni dimensione per una corretta gestione delle informazioni; è consigliato, seppur non sempre obbligatorio, dotarsi di un Data Protection Officer (DPO). Prezioso è poi il **monitoraggio della normativa** esistente, generale e specifica del settore aziendale, e la valutazione se perseguire o meno la **conformità ISO/IEC 27001**. Esistono poi strumenti a disposizione delle aziende di **valutazione del rischio**, fisico e digitale, ed è buona norma procedere con **audit interni/esterni** periodici.

Criteri

- Adeguamento privacy (GDPR);
- Monitoraggio normativa;
- Conformità ISO/IEC 27001;
- Valutazione del rischio;
- Esecuzione audit interni/esterni.

Fattore umano

È molto importante che il management dell'azienda provveda a trasmettere una cultura in tema di cybersecurity ai propri dipendenti, con particolare attenzione alla **sensibilizzazione** delle persone sui possibili rischi derivanti da una mala gestione o da una scarsa cura da parte del personale; fondamentale è il tema della **formazione**, a ogni livello, periodica e ripetuta per tenere aggiornati tutti i dipendenti e mantenere alta l'attenzione sul tema. A livello dirigenziale è poi fondamentale l'efficace **gestione di regole** chiare e precise per la sicurezza delle informazioni e per la gestione degli incidenti, anche con l'**identificazione di responsabili**, e l'**individuare autorizzazioni** di accesso a livello di dati e sistemi aziendali per delimitare i possibili effetti negativi di un attacco a una specifica area / business unit aziendale. Non per ultimo, l'aggiornamento manageriale è un fattore chiave e la **partecipazione ad associazioni** di settore (eventi, convegni, tavoli di lavoro) è suggerita alle aziende di tutte le dimensioni.

Criteri

- Formazione e sensibilizzazione;
- Ruoli e responsabilità;
- Gestione regole;
- Partecipazione ad associazioni;
- Gestione autorizzazioni.

La restituzione alle aziende

L'azienda che compila il questionario di self-assesment riceve una doppia restituzione:

- una vista grafica che riporta il punteggio generale raggiunto (overall score) e mostra il posizionamento su ciascuna delle cinque dimensioni del Cyber Readiness Level, con un valore target da raggiungere;
- un report sintetico che indica azioni migliorative da mettere in campo su ciascuna dimensione.

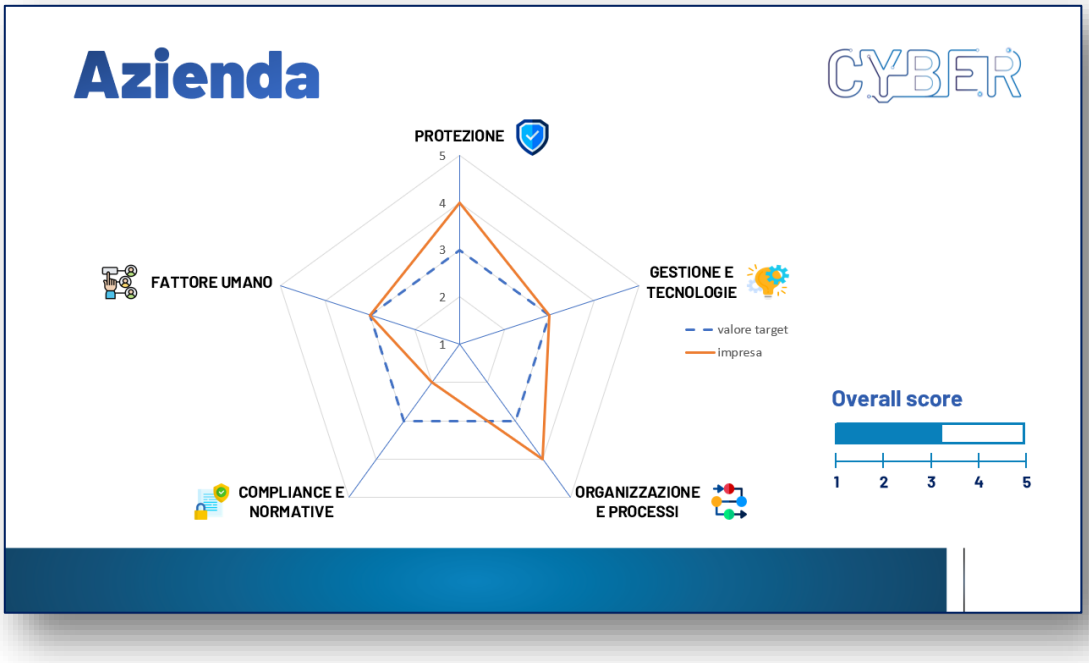


*Figura 1 - Quadro generale di restituzione, con **spider diagram**, che riporta il posizionamento dell'azienda su ciascuna dimensione, e **Overall score**, il punteggio globale ottenuto*

Analisi del posizionamento di un'azienda

Si riporta di seguito un esempio di restituzione a un'azienda che ha compilato il questionario di self-assesment. Il caso selezionato è di particolare interesse in quanto presenta un posizionamento differente sulle cinque dimensioni.

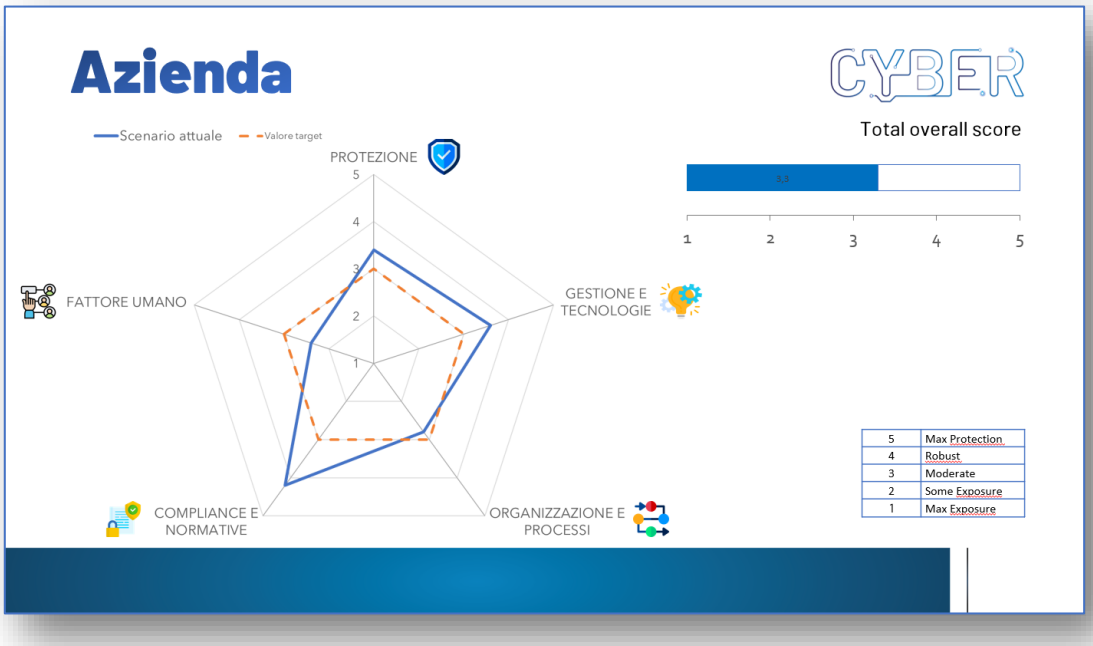


Figura 2 - Il posizionamento di una generica azienda che ha compilato il CRL

L'azienda si presenta robusta per quanto concerne la dimensione "Compliance e normative", e supera la media in ambito "Gestione e tecnologie" e "Protezione". Maggiore attenzione dovrebbe essere invece posta all'"Organizzazione e processi"; un cambio di rotta è invece fondamentale per una corretta gestione del "Fattore umano".

Protezione (3,4 su 5)

È positivo che l'azienda effettui aggiornamenti software centralizzati e automatici e che siano presenti policy di sicurezza formalizzate, ma dovrebbe far accedere i guest alla rete aziendale con password e regolare meglio i diversi aspetti della gestione dei dispositivi aziendali, dedicando dei momenti di formazione/informazione ai dipendenti in merito alle policy in essere. L'azienda effettua backup in modo efficace e ha effettuato una valutazione dei rischi e formalizzato un piano per la cybersecurity. Manca invece la crittografia dei dispositivi e dei dati, a qualsiasi livello, fattore su cui bisogna intervenire quanto prima.

Gestione e tecnologie (3,6 su 5)

In azienda vengono effettuati Penetration Test periodici e frequenti (almeno ogni mese, anche con scansioni automatizzate) su tutte le applicazioni web e servizi cloud aziendali. L'impresa ha adottato specifiche procedure che definiscono la gestione degli applicativi, inclusi quelli per la sicurezza

informatica; è ottimo anche che gli utenti non abbiano i privilegi di amministratore sulle macchine e che la configurazione degli applicativi sia compito del reparto IT interno o di una azienda esterna con contratto continuativo di manutenzione (non a chiamata).
Va però segnalato che l'azienda non gestisce correttamente l'inventario per i prodotti hardware e software, avendo strutturato solo quello relativo a quelli hardware. Non è positivo che l'azienda non faccia uso di servizi cloud, certificati e garantiti.

Organizzazione e processi (2,8 su 5)

In azienda c'è un programma di manutenzione specifico ed è incaricata una realtà esterna che se ne occupa in modo continuativo, monitora e interviene anche collegandosi da remoto (con sue password di accesso). La collaborazione con il reparto IT e BU è stretta. L'azienda prevede policy precise e formalizzate per la gestione delle password, che sono controllate con sistemi automatizzati che impongono di seguire determinate regole di lunghezza e complessità.
Il piano è presente ma è strutturato solo internamente: possibili miglioramenti potrebbero essere l'esecuzione di test periodici dello stesso, effettuare una BIA (Business Impact Analysis) e arrivare quindi a strutturare un Business Continuity Plan, di cui fa parte il piano di rientro, basato su BIA.
È stata applicata la segregazione delle reti base, tra quella operativa e quella per gli ospiti. Implementazione successiva consigliata: collegare ogni area operativa a una apposita VLAN, non collegare i dispositivi IoT alla stessa rete degli endpoint ed effettuare una valutazione del rischio riguardante la sicurezza dei dispositivi.

Compliance e normative (4,6 su 5)

L'impresa è molto attenta al tema dell'adeguamento privacy e GDPR, monitora la normativa ed è certificata ISO/IEC 27001; esegue audit periodici ma dovrebbe investire su una migliore valutazione del rischio, non spinta solamente da obblighi di legge.

Fattore umano (2,4 su 5)

L'azienda dovrebbe prevedere un'attività generale di presentazione delle procedure di sicurezza al momento dell'assunzione e sviluppare un piano di formazione personalizzato per mansioni aziendali, attività che al momento mancano. Tale piano, all'inizio può essere aggiornato periodicamente ma poi deve essere affiancato da attività di sensibilizzazione ripetute e continue; in particolare, per il personale va strutturato un piano di formazione che tenga conto delle tecnologie usate e della necessità di apprenderne anche le caratteristiche di sicurezza degli applicativi.

Ruoli e responsabilità non sono stabiliti: la sicurezza deve essere allocata a diverse persone, e deve essere individuata una persona indipendente dall'IT con la responsabilità di monitorare l'applicazione delle misure di sicurezza.

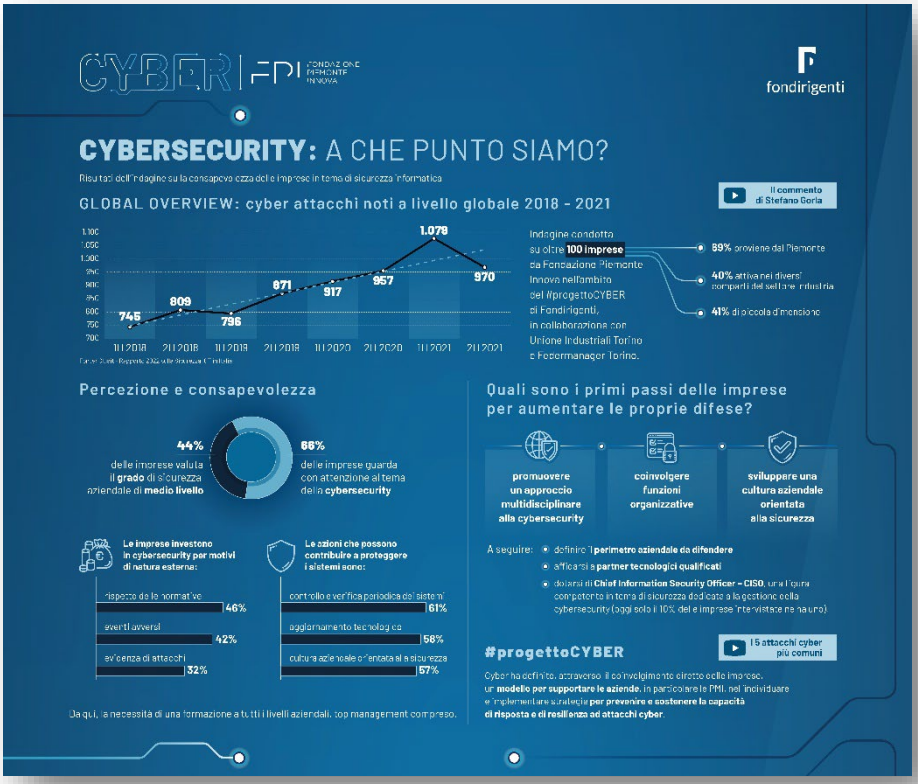
In azienda sono presenti regole comportamentali per il personale e sono descritti alcuni processi di sicurezza, ma non coordinati tra loro. Non è presente una distribuzione controllata dei documenti a tutto il personale e verifiche periodiche.

La partecipazione a eventi di settore è su spinta individuale, l'azienda dovrebbe invece iniziare ad allocare un budget per queste iniziative e valutare l'iscrizione ad associazioni di settore.

RISULTATI: LONGFORM DI PROGETTO

La longform qui di seguito, suddivisa in tre infografiche, riporta in maniera sintetica ed efficace i risultati principali del progetto: i risultati dell'indagine sulla cybersecurity awareness, la proposta di metodi, strumenti organizzativi, tecnologici e normativi, l'attenzione alla formazione e il Cyber Readiness Level.

Infografica 1: CYBERSECURITY AWARENESS



Infografica 2: METODI, STRUMENTI E PERSONE

Infografica 3: CYBER READINESS LEVEL