SAVE

Veronafiere, 27-28 ottobre 2021

Fonte Immagine - https://www.publicdomainpictures.net/

"Industria 4.0 - Quali soluzioni per la sicurezza e competitività nel settore industriale in un'ottica di gestione della Continuità Operativa, gestione dei Rischi e della Cyber Security" "

Clusit

Federica Maria Rita Livelli - Carlo Mauceli

Il Clusit

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Il Ruolo Istituzionale

- In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT PA , Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA .

I Rapporti Internazionali

- In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Network and Information Security), ITU (International Telecommunication Union), il Garante Europeo per la protezione dei dati personali, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), European DIGITAL SME Alliance, le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC2, ISSA, SANS) e le associazioni dei consumatori.

I numeri del Clusit

- 500 Organizzazioni rappresentate
- Oltre 10.000 partecipanti alle attività del Clusit nel 2020

EVENTI - FORMAZIONE

- Eventi divulgativi organizzati nel 2020: circa 50
- Webinar e seminari tenuti nel 2020: più di 80
- Speaker e docenti coinvolti: più di 400
- Nel 2019 hanno partecipato agli eventi Clusit oltre 7.000 persone

PUBBLICAZIONI

- Documenti prodotti (rapporti, quaderni, pillole di sicurezza, White Papers): oltre 150
- Contributori/autori delle pubblicazioni Clusit: oltre 130
- Lettori delle pubblicazioni Clusit (rapporti, quaderni, pillole di sicurezza): oltre 80.000

.

- Copertura mediatica nel 2020: più di 500 articoli e servizi su web, cartaceo, Radio e TV.

Le Attività e i Progetti in Corso

- **Formazione specialistica**: i Webinar, 24 nel 2021, di cui 10 dedicati ai DPO.

- **Ricerca e studio**: Premio “Innovare la Sicurezza delle Informazioni” per la migliore tesi universitaria, arrivato alla 16a edizione.

- **Le Conference specialistiche**: i Security Summit Streaming Edition (il prossimo dal 9 al 11 novembre 2021).

- **Security Summit Academy**: Atelier online con cadenza settimanale (https://clusit.it/ateliers/)

- **Gruppi di Lavoro**: portati avanti nell’ambito della Clusit Community for Security

- **Focus per 2020/2021**: Intelligenza Artificiale.

- **Rapporti Clusit**: Rapporti semestrali sugli eventi dannosi (Cybercrime e incidenti informatici) in Italia,

- **Il Mese Europeo della Sicurezza Informatica (ECSM)** , iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit.

Industria 4.0 e Industrial Cyber Security

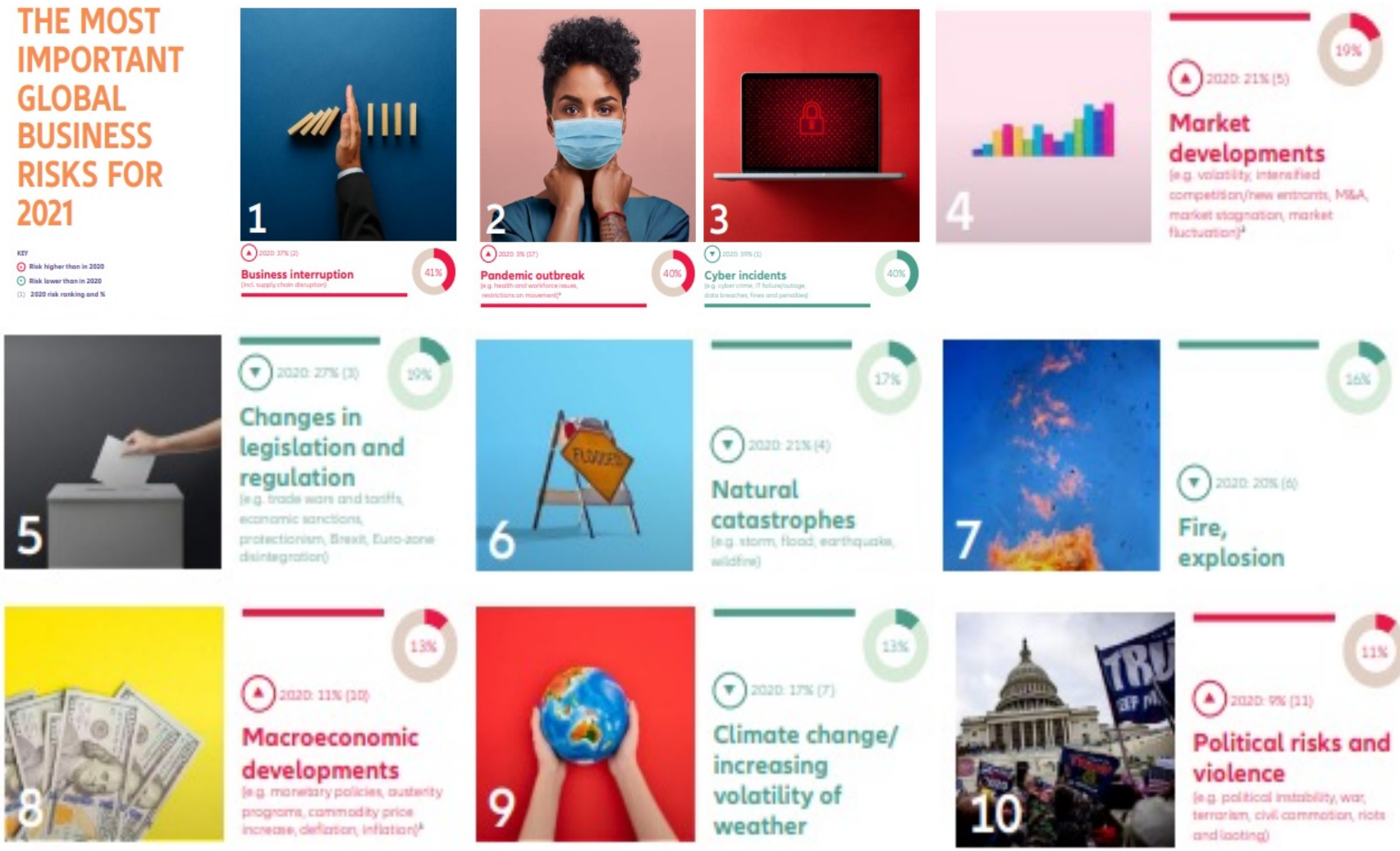
Fonte Immagine: www.analisidifesa.it

La minaccia cyber è un grave problema per l'Industria 4.0:

- Blocco immediato della produzione,
- Ripercussioni sui volumi finanziari e sulla sicurezza delle macchine
- Danno di immagine
- Impatto sociale

Rischi & Scenari

ALLIANZ RISKS REPORT 2021



Rischi & Scenari

AXA - THE FUTURE RISKS REPORT 2021

Rischi & Scenari

- La sicurezza informatica non è *una* sfida, né certamente è *la* sfida del XXI secolo;
- La sicurezza informatica costituisce un **tragitto**;
- Quello che per la società 4.0 costituisce, invece, una **minaccia concreta e problematica sono gli attacchi cibernetici**.

L'esigenza di creare nuovi modelli di business, per aumentare la produttività
delle industrie, ha portato a una generale tendenza verso l'automazione, l'informatizzazione, la virtualizzazione, il cloud e verso tutte
le funzionalità presenti su mobile.
L'insieme di queste caratteristiche definisce **l'industria 4.0** a cui le varie componenti sociali sono chiamate a rapportarsi e su cui agisce il **rischio dei cyber attacchi**.

Identità Digitale

Con l'avvento delle nuove tecnologie, l'uso sempre più massivo della rete internet e l'evoluzione di tutti gli strumenti che consentono la diffusione e la condivisione dei propri dati sensibili online, si è assistito ad un aumento del fenomeno che oggi viene definito **Identity theft**, ovvero il furto dell'identità digitale.

Metodi di autenticazione

Bad: Password

123456

qwerty

password

iloveyou

Password1

Good: Password +

SMS

Voice

Conditional Access

Best: Passwordless

Windows Hello

Microsoft Authenticator

FIDO2 security key

Rischi & Scenari

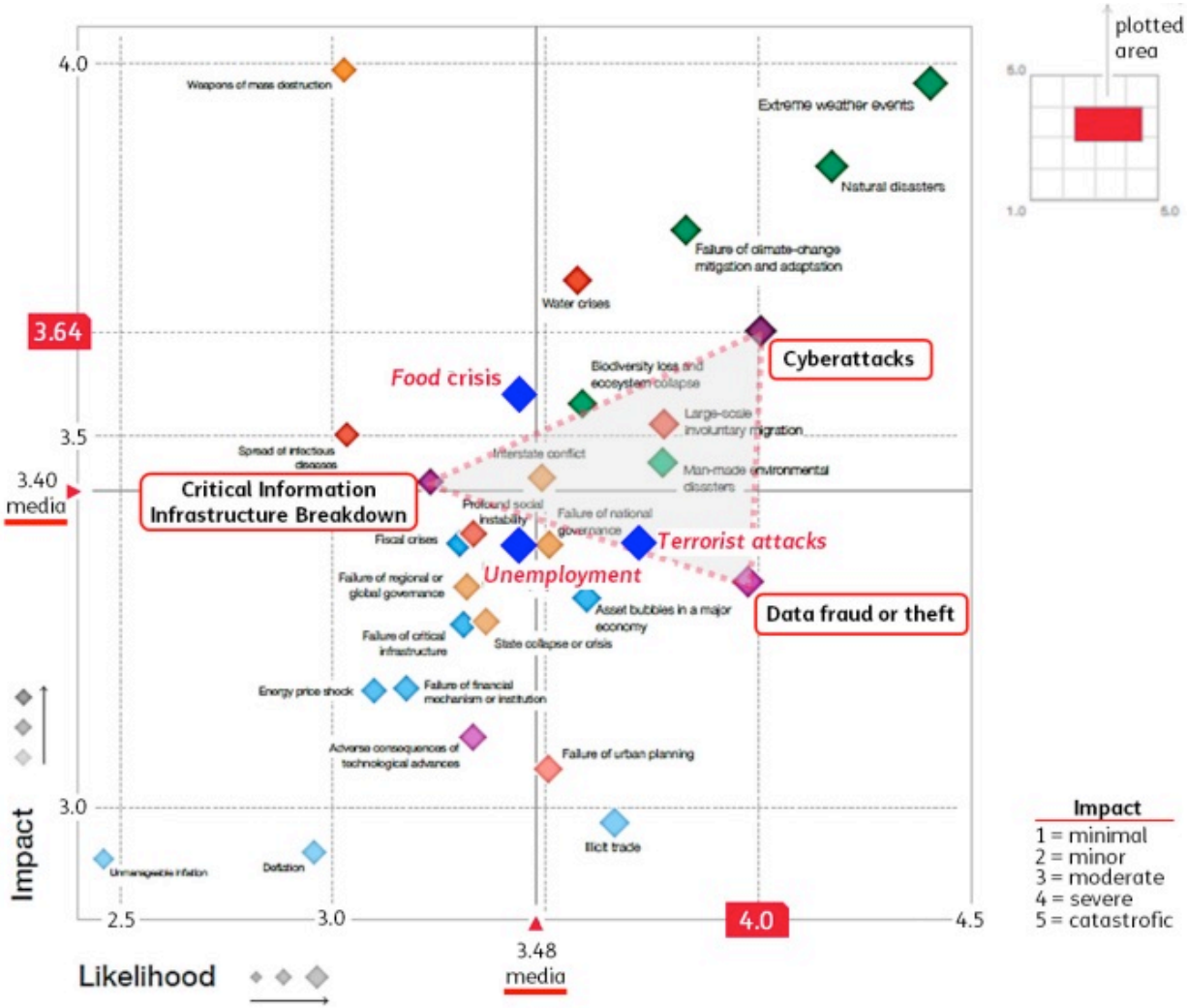
E' NECESSARIO METTERE IN SICUREZZA L'ORGANIZZAZIONE

- Il problema non è **SE** un evento avverso ci impedirà di continuare la nostra operatività…ma **QUANDO AVVERRA'.**
- Il problema non è **SE** saremo bersaglio di una crisi, pandemia, attacco Cyber…ma **QUANDO AVVERRA**'.
- E' **UTILE**, anzi **NECESSARIO**, prepararsi con continuità alle emergenze , in modo tale che, quando si verificano, si abbiano in essere **LE RISORSE COMPORTAMENTALI E OPERATIVE** necessarie per affrontarle con efficacia.

IN CASO CONTRARIO… L'IMPRESA CHIUDE…

Fonte Immagine: www.businessplanvincente.com

Global Risk Landscape



I cyberattacchi comportano un **rischio (probabilità x impatto) più elevato** rispetto ai più tradizionali rischi legati ad attacchi terroristici, crisi alimentari e disoccupazione.

Le Sfide Chiave della Cybersecurity

L'approccio tradizionale alla sicurezza fallisce, senza se e senza ma – Gli Insegnamenti:

- Gli Hacker non rompono muri: fanno log-in
- Mancanza di visibilità e correlazione di eventi- Visione a silos
- Il raggio d'azione di un attacco è limitato all'identità
- Gli attacchi sfruttano la mancanza di igiene e di gap tecnico
- Dispersione ed esplosione dei dati
- Mancanza di skill professionali
- Obsolescenza Tecnologica
- Lock-in applicativo

Industria 4.0

SCENARIO FUTURO

PRODOTTI SMART CONNESSI

PROCESSI DECISIONALI VIRTUALIZZATI

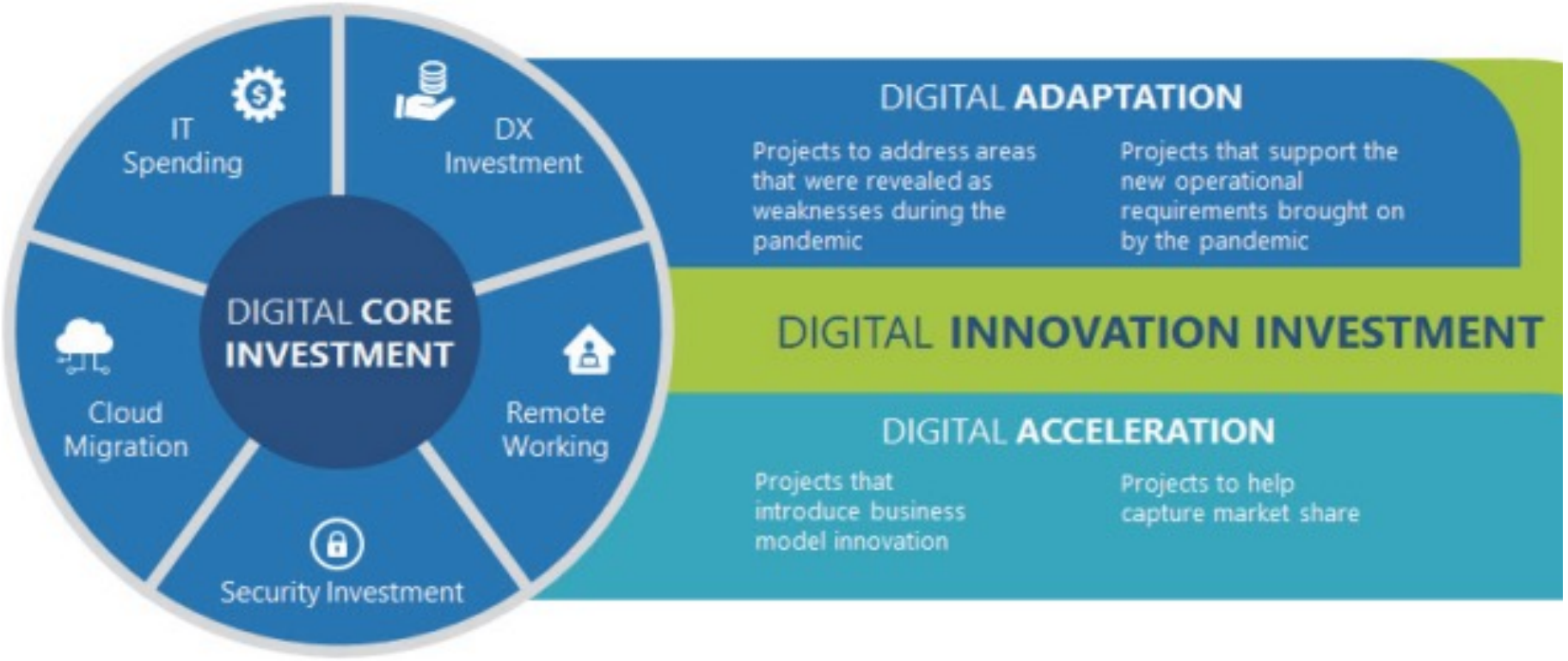
Fonte Immagine: www. it.vecteezy.com

PROCESSI DIGITALI

NUOVI PARADIGMI & NUOVI MODELLI ORGANIZZATIVI

Scenario – Digitalizzazione & Innovazione

SCENARIO FUTURO: DIGITAL RESILIENCE



Molte imprese per garantire la **resilienza organizzativa ed operativa** investiranno in **Digital Innovation**.

Scenario – Digitalizzazione & Innovazione

PRIORITA' DI INVESTIMENTO RIF. INNOVAZIONE DIGITALE GRANDI IMPRESE

2020	2021
BIG DATA E ANALYTICS	INFORMATION SECURITY
INFORMATION SECURITY	BIG DATA E ANALYTICS
ERP	ECOMMERCE
CRM	SMART WORKING
DATA CENTER	CRM
MOBILE BUSINESS	COMPLIANCE & RISK MANAGEMENT

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation *Survey Osservatorio Digital Transformation Academy che ha visto il coinvolgimento di 116 grandi imprese*

14

ISO 22301 – 31000 – 27001 – Harmonized Systems

LEVE PER LA RESILIENZA

Trattasi di sistemi di gestione che seguono una struttura armonizzata ed un approccio olistico.

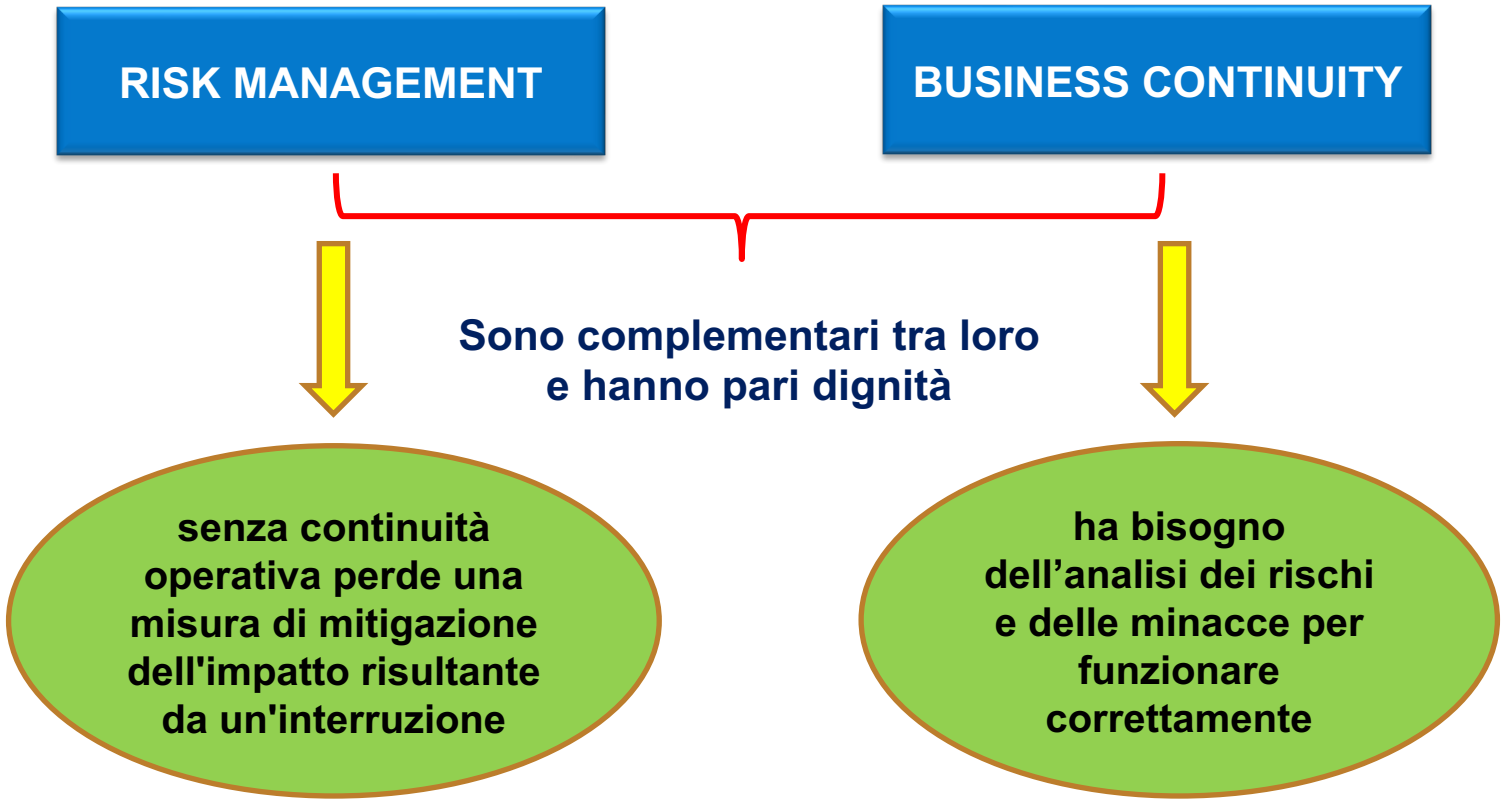
Permettono alle organizzazioni di:

- **Perseguire una strategia di cybersecurity & gestione del rischio tecnologico integrata** con le operazioni aziendali, **senza silos**.
- **Prevenire i cyber attack** per salvaguardare **l'integrità, la disponibilità e la riservatezza dei dati e garantire la continuità dei processi critici**.
- **Affrontare i cyber attack** sempre più frequenti.

Fonte immagine Darwin Laganzon da www.Pixabay.com

ISO 22301 – 31000

COME INTERAGISCONO



Iso 22301-31000-27001

DREAM TEAM PER LA RESILIENZA

Punti in comune

- Definizione degli obiettivi e misurazione
- Gestione delle Risorse Umane
- Audit interno
- Revisione della gestione
- Azioni correttive
- Gestione documenti & record

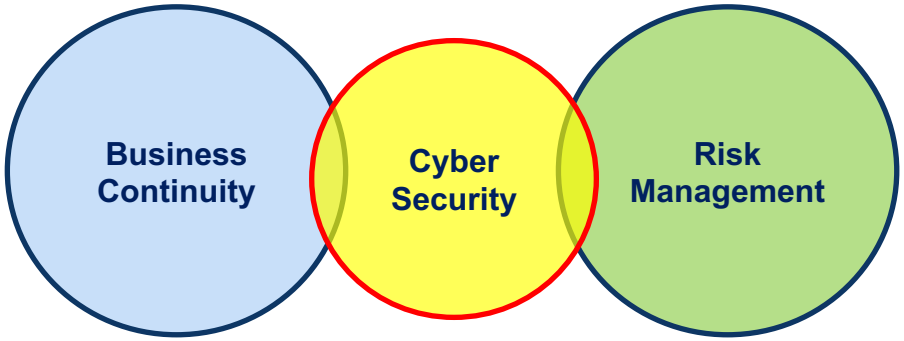
Iso 22301-31000-27001

DREAM TEAM PER LA RESILIENZA

Fiducia tra Forza Lavoro & Leadership

Vantaggio Competitivo

Efficacia Decisionale



Mitigazione Rischio aziendale & Finanziario

Equità & Reputazione del Marchio

Requisiti Legali & Vantaggi di Conformità

Leve strategiche

GOVERNANCE

COMPLIANCE

Creazione di Organizzazioni Agili, Flessibili & Anti-fragili vs. processo di Digitalizzazione & Innovazione

Iso 22301-31000-27001

IL FATTORE HUMANO: CENTRALE – Dati Proofpoint

63% CISO italiani >> organizzazione impreparata vs. Cyber Attack

97%minacce informatiche >> richiede un intervento umano per l'attivazione

50%CISO italiani >> errore umano la più grande vulnerabilità

LE 3 ISO leva per diffondere
Formazione, Cultura e Consapevolezza alla Sicurezza

INDUSTRIA 4.0/INNOVAZIONE ARMONICA

HUMAN CENTRIC

Iso 22301-31000-27001

CONVERGENZA VS. IL FATTORE UMANO

- **Team collaborativi >>** migliore comprensione delle attività più importanti di un'organizzazione, delle risorse che le supportano e delle sfide sul campo che devono affrontare.
- **Integrazione Team >>** metodologia, approccio e una nomenclatura comuni per supportare dialoghi significativi sul rischio reale.
- **Terminologia comune ai vari Team >>** per garantire che l'organizzazione continui a funzionare e a raggiungere gli obiettivi.
- **No silos >>** ecosistema tra funzioni e persone = calibrata sintesi tra la missione e gli obiettivi di BC, sicurezza delle informazioni e gestione del rischio operativo.
- **Training & Formazione >>** acquisizione delle competenze necessarie come *conditio sine qua non* per garantire resilienza.

360-Degree Risk Management

Iso 22301-31000-27001

CAMBIO DI PARADIGMI

Imprevedibile Certezza del Rischio

Una volta si diceva:
"Aspettati l'inaspettato"…

Oggi occorre dire:
"ANTICIPA L'INASPETTATO"

Fonte Immagine: FMRLivelli
Fonte Immagine: FMRLivelli

Fattori d'Impatto

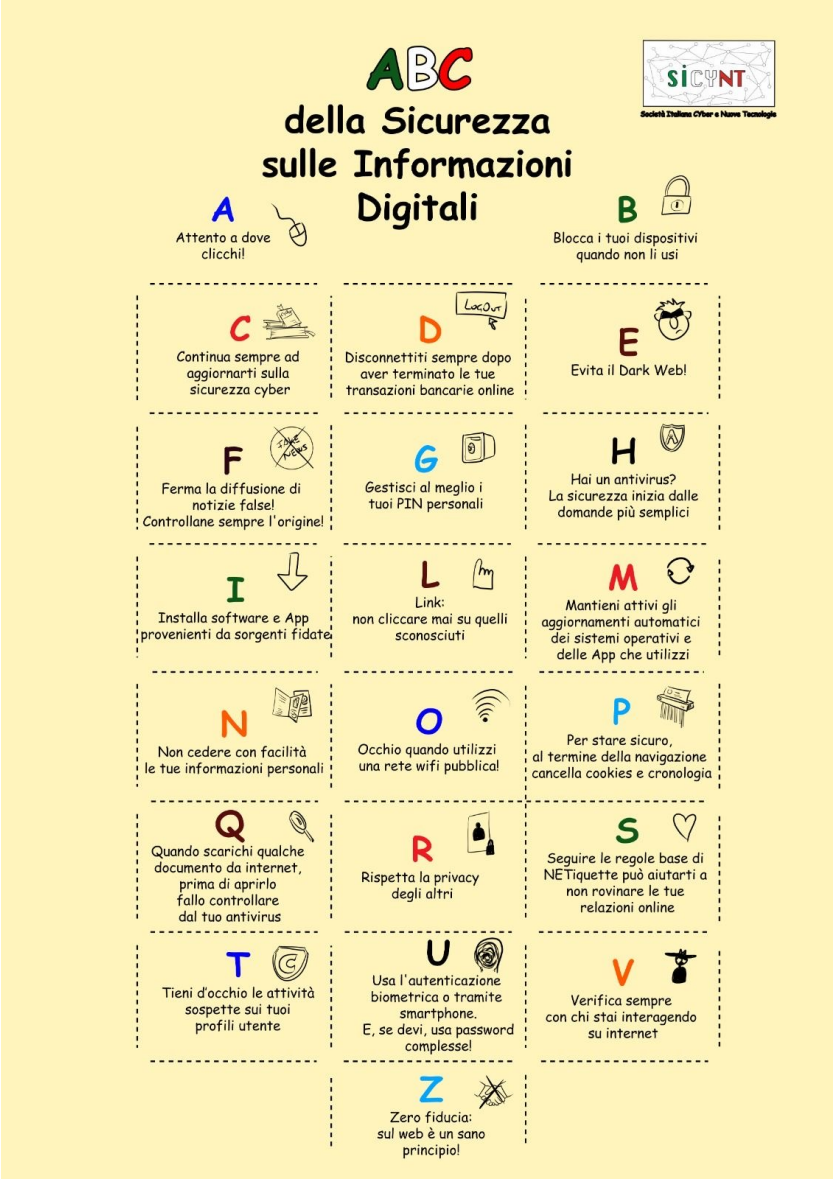
Fonte Immagine: www.puntosicuro.it

- ❑ Fattore Umano
- ❑ Supply Chain
- ❑ Utilizzo non governato del Software Open Source
- ❑ Complessità, Obsolescenza, Patching
- ❑ Transizione al Cloud Pubblico Non Governata

Fattori d'Impatto

+	La rivoluzione digitale ha in molti modi potenziato le nostre capacità - attraverso i social ci ha offerto la possibilità di intrattenere tantissime relazioni contemporaneamente.
-	La polarizzazione delle opinioni, gli haters, i troll, le fake news, un contesto ottimo per "distruggere" consenso ma per niente in grado di "costruirlo".
=	Tutti si scoprono estremamente vulnerabili al social engineering/phishing che si conferma essere il canali più di frequente utilizzato in fase di innesco di attacchi anche complessi.

Bisogna partire dalla Formazione

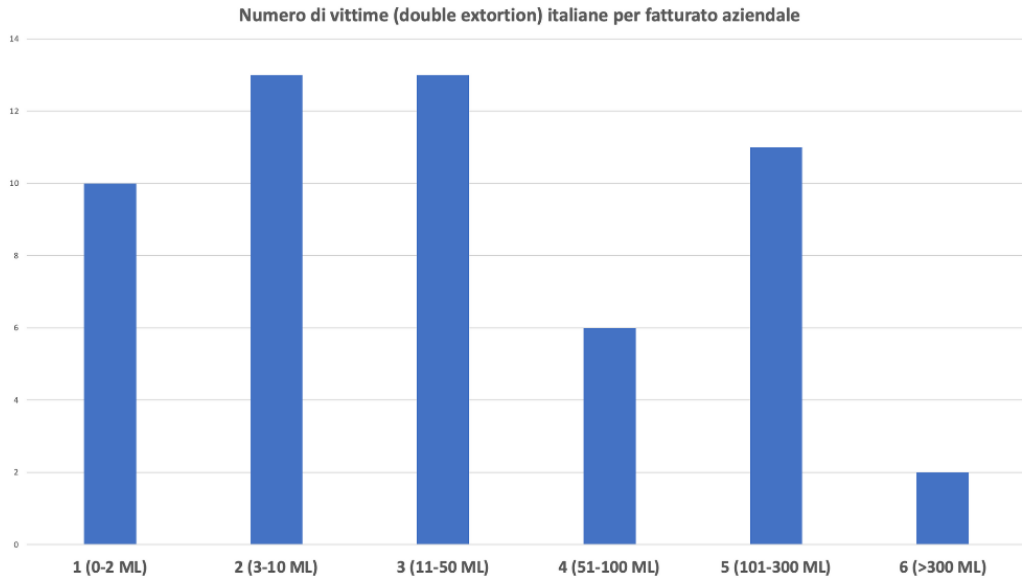


Attacchi alle aziende italiane – Anno 2020

I media raccontano soltanto le violazioni informatiche ai danni di grandi aziende o multinazionali.

Tutto ciò ha alimentato, nel corso del tempo, la percezione che le PMI siano poco interessanti per i cyber criminali.

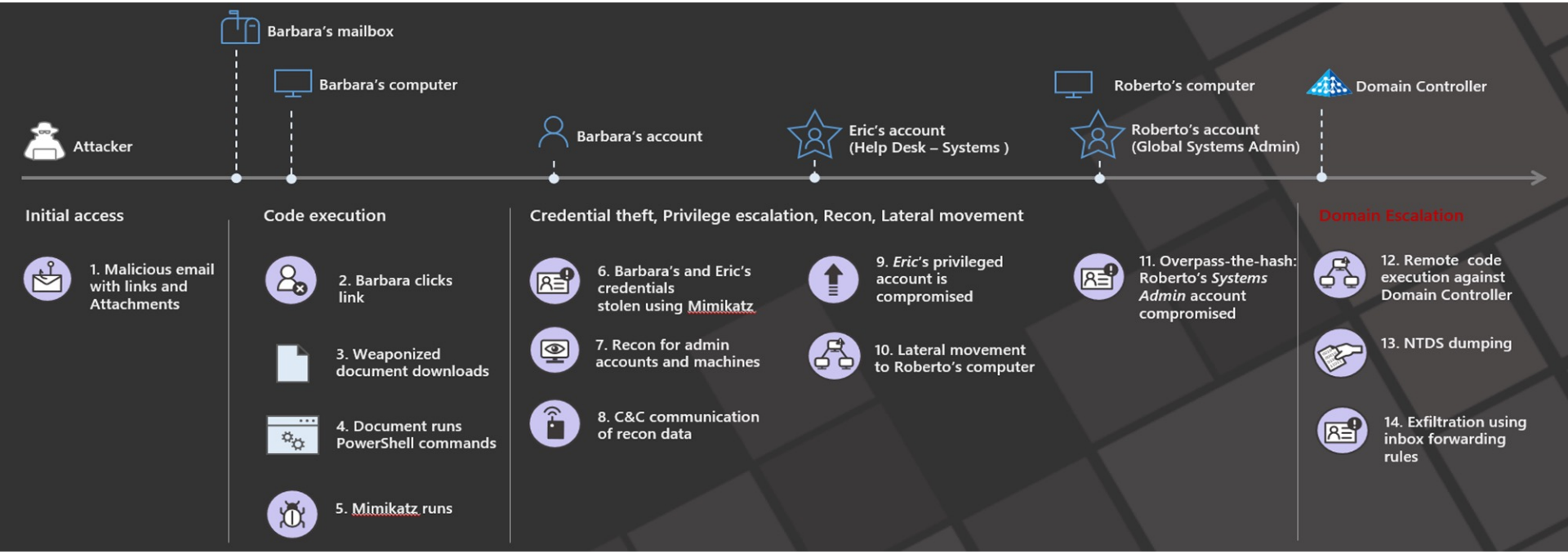
Attacchi alle aziende italiane – Anno 2020



Double Extortion | Ransomware and Breach Tracker

- **81 le aziende italiane coinvolte** (e pubblicate) da gang criminali che utilizzano la tecnica della doppia estorsione.
- **10 sono Pubbliche Amministrazioni** (comuni, associazioni, etc)
- **15** non hanno dati disponibili relativi a fatturato e dipendenti.
- La media del fatturato delle aziende colpite è di **76,4 ML di Euro**.
- La media del numero di dipendenti delle aziende colpite è di **332 dipendenti.**

La Kill Chain Attack evolve



Raccomandazioni

- Abbracciare la **strategia Zero Trust**
- Evolvere verso l'**identità come nuovo perimetro** abbandonando il concetto di perimetro di rete
- Abbracciare "**password-less**"
- Rimuovere la complessità attraverso il **consolidamento dei servizi e dei tool di sicurezza**
- Sfruttare le **funzionalità di sicurezza native** dei sistemi
- **Prevenire e rispondere velocemente** sono le chiavi per minimizzare l'impatto – **Artificial Intelligence & Automation**
- Sfruttare la **transizione al cloud** per portare ordine e struttura alla sicurezza
- **Secure Score for Hygiene**

Conclusione

Come per la maggior parte delle cose che costituiscono una minaccia nella vita il primo passo per la **costruzione di una difesa** è:

Comprensione delle metodologie utilizzate dagli attaccanti

Conoscenza = consapevolezza

In un mondo sempre più automatizzato e digitalizzato implicherà:

- Attuazione dell'**Innovazione armonica che pone l'uomo al centro**
- Diffusione **cultura del rischio, della continuità e della cybersecurity**
- Un approccio **risk-based & resilience-based** quale ***conditio sine qua non*** per un'organizzazione **anti-fragile!**

Fonte Immagine: FMRLivelli

Fonte Immagine - https://www.publicdomainpictures.net/

GRAZIE!

Clusit
Federica Maria Rita Livelli - Carlo Mauceli