Deloitte.

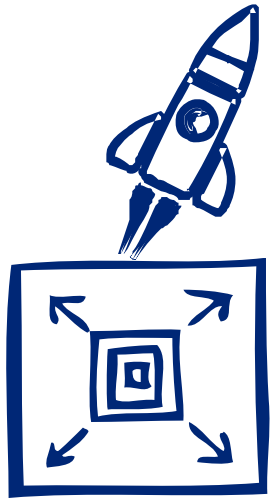
Mefop

Cyber Risk
Introduzione al fenomeno ed alle strategie di intervento

Fabio Battelli, Partner – Deloitte Cyber Risk Services
CISSP, CISA, CISM, ISO 27001, PRINCE2 e ITIL Certified

Seminario on-line | 18 Maggio 2021

L'origine del rischio Cyber…



Extended Enterprise

2013

4.4 ZB

L'universo digitale è enorme e cresce esponenzialmente…

2020

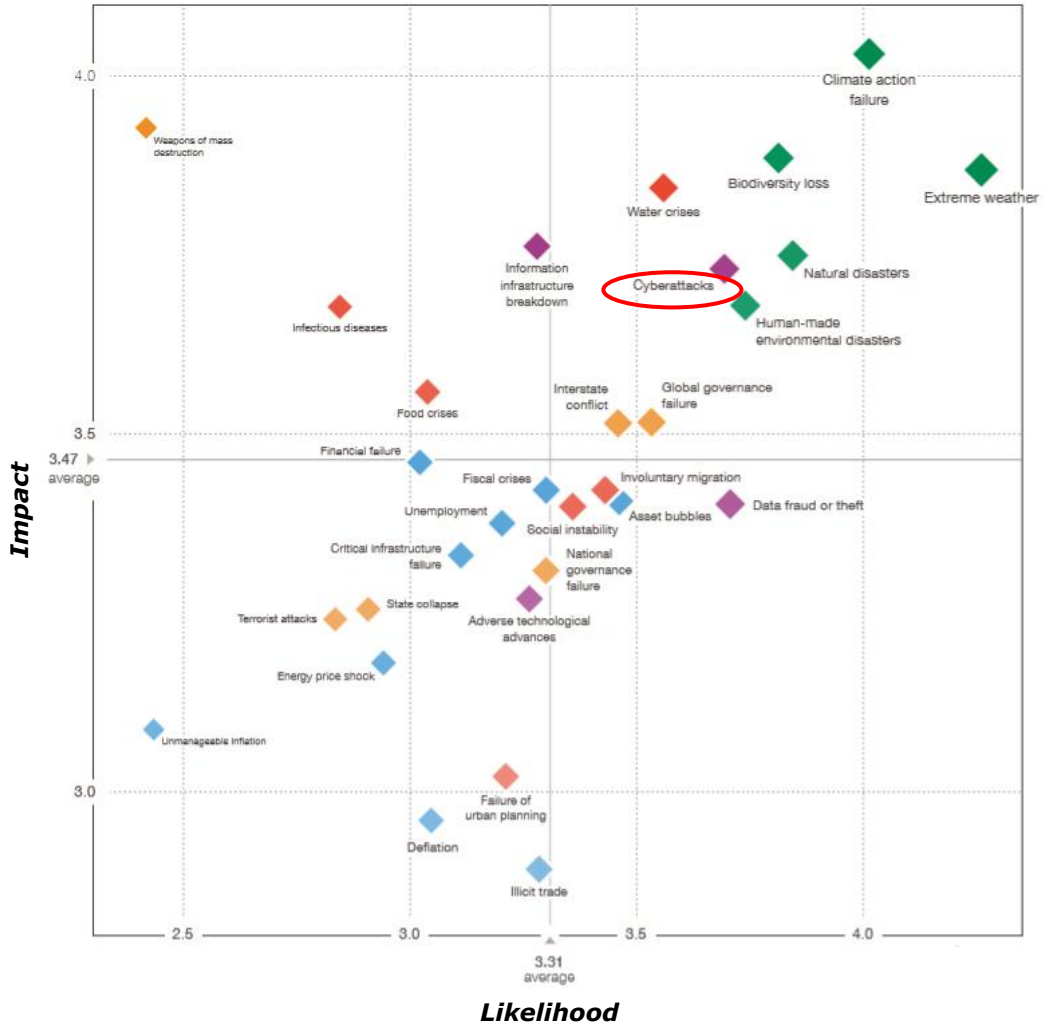
44 ZB

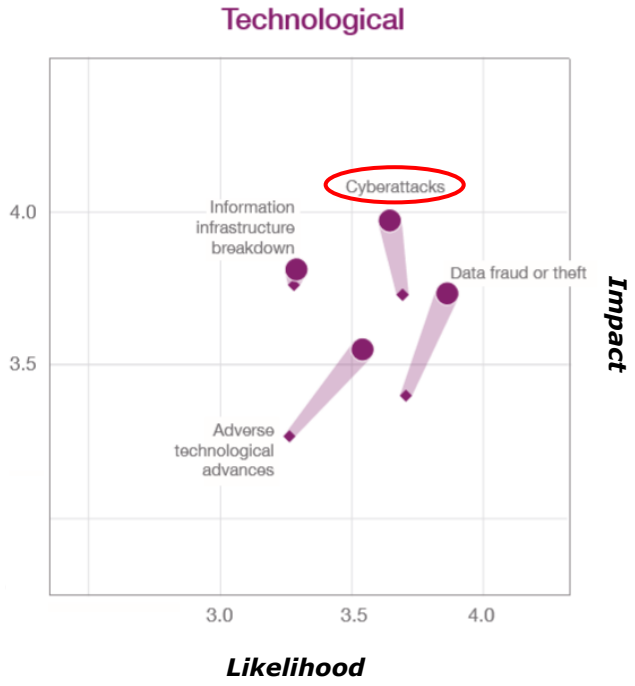
…generando opportunità ed innovazioni incredibili…

…ma anche rischi Cyber che minano la sicurezza delle informazioni e delle infrastrutture informatiche…

…ed è considerato tra i principali rischi per l'umanità…

Il rischio cyber è tra i top 10 rischi a livello globale





Gli attacchi cyber rientrano tra i rischi più significativi per l'umanità in termini di **impatto** e **probabilità**

WORLD ECONOMIC FORUM

Legenda

Rischio Economico | Rischio Societario | Rischio Geopolitico | Rischio Tecnologico | Rischio Ambientale

Fonte: WEF Global Risk Landscape, 2020.

……rendendo le informazioni sempre più appetibili per le organizzazioni dedite al Cyber crime

Cybercrime

Utilizzo di diverse metodologie e tecniche da parte di cybercriminali che hanno come obiettivo principale ricavare **guadagno economico** dall'attacco stesso

Cyber Espionage

Utilizzo di determinate strategie e strumenti di attacco per sottrare intellectual property, finalizzato all'ottenimento di un **guadagno competitivo**

Costo mondiale del **Cybercrime**

600 miliardi $*

800 miliardi $

Volume di affari relativo al traffico di **stupefacenti**

Redditività media del Cybercrime

20:1 *Rapporto medio tra profitto e costi necessari per realizzare i cyberattack***

3.000 $ *Investimento medio per l'acquisto di un malware****

60.000 $ *Stima del profitto medio derivante dall'uso del malware*

*Source: McAfee, Economic impact of cybercrime – 2018, the value takes into account both direct costs (money stolen by means of the crime) and indirect damage (reputational damage, turnover loss, restoration costs, etc.)

Gli obiettivi e le conseguenze derivanti dagli attacchi cyber sono tangibili…

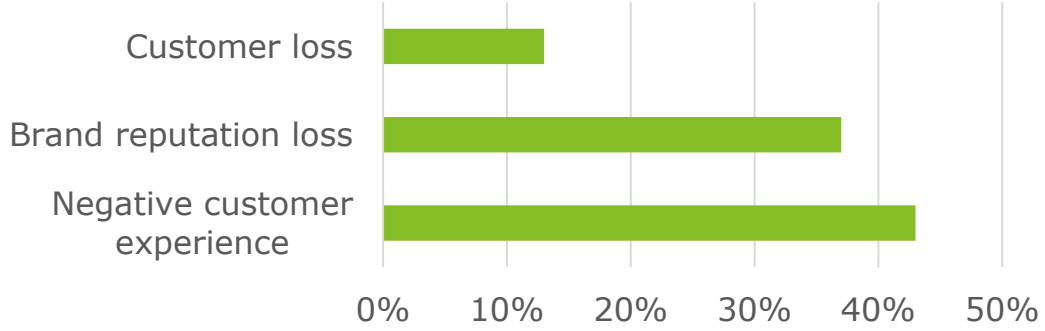
La maggior parte degli attacchi cyber mira ai seguenti **obiettivi**:

Interruzioni di **servizio:**45%

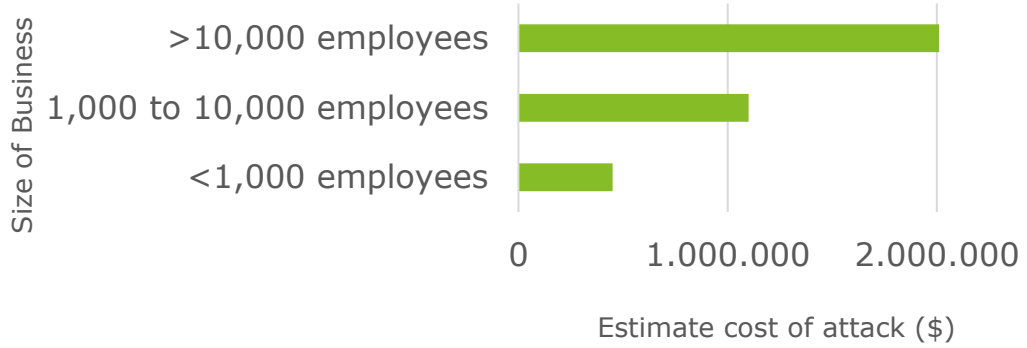
Furto di **dati**:35%

Conseguenze

Il **93%** delle organizzazioni dichiara di aver subito un **impatto negativo** nei **rapporti** con i **clienti** a seguito di un attacco cyber.



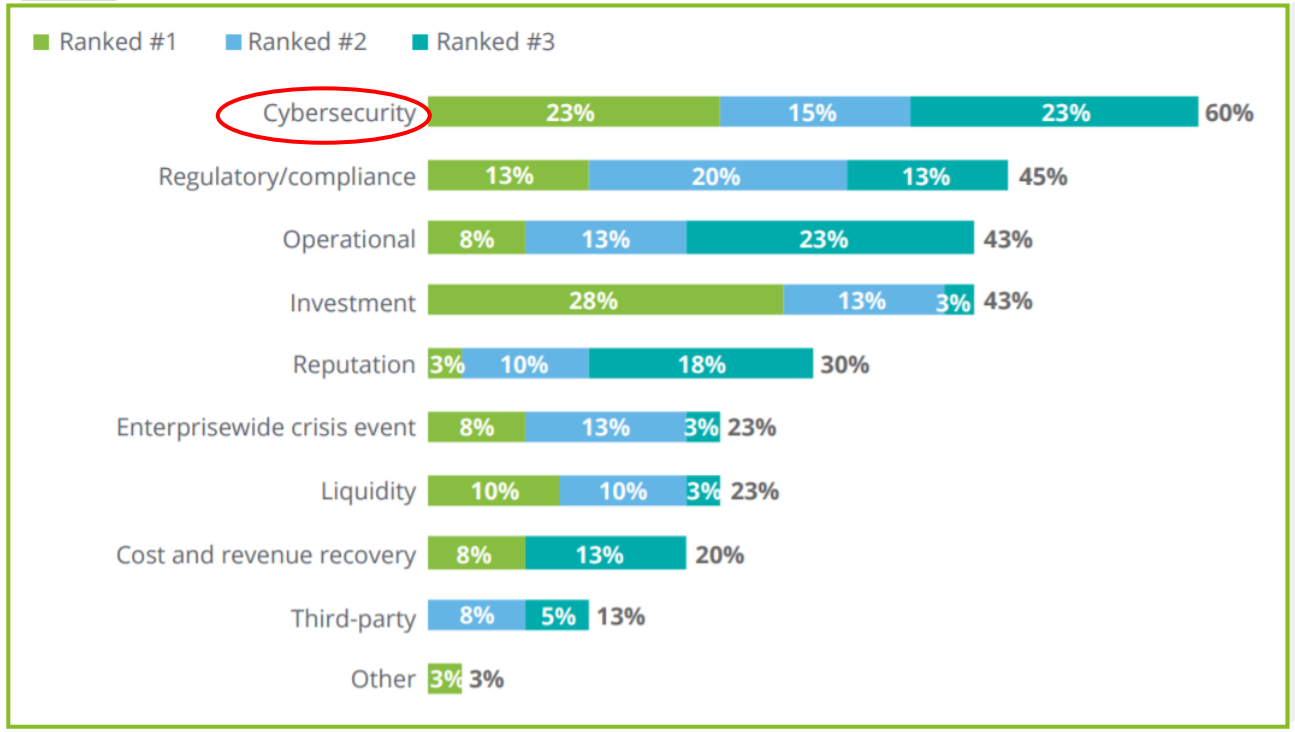
La **perdite economiche medie** causate da un singolo attacco subito ammontano a circa **1,1 milioni di dollari**.

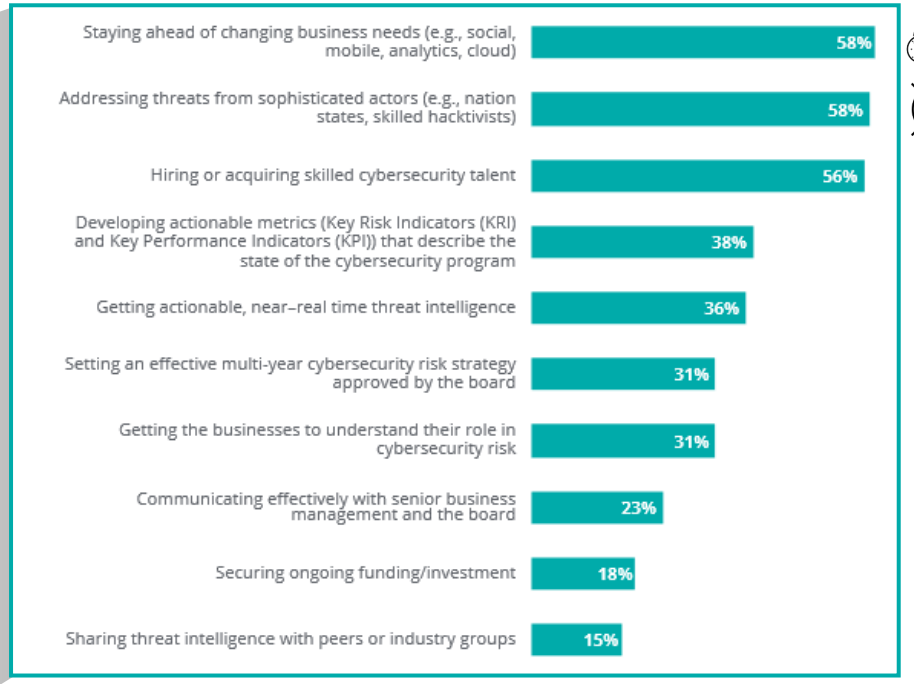


Fonte: Radware - Global Application & Network Security Report, 2018-2019.

…e anche la percezione futura del rischio cyber sembra rimanere costante

*Il rischio cyber risulta la maggiore **sfida** per la **gestione** degli **investimenti** nei prossimi anni*





*Nella **gestione** del rischio cyber risulta estremamente impegnativo e sfidante:*

Stare al passo con le esigenze di **business** in continua **evoluzione**

Affrontare minacce sofisticate

Fonte: Deloitte Global Risk Management Survey, 11° edition.

Secondo diverse statistiche il Cyber Risk è anche quello che desta maggiori preoccupazioni dal punto di vista del Risk Manager

Cyber risks da parte dei Risk Manager*

2018
16%

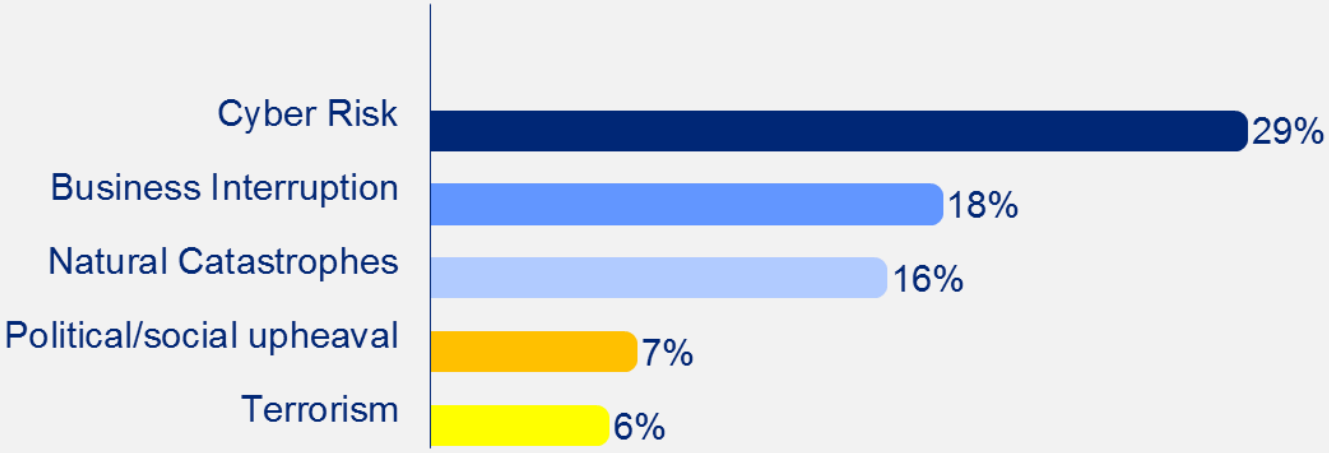
Ranked 7th

2019
20%

Ranked 5th

2020
25%

Ranked 3th



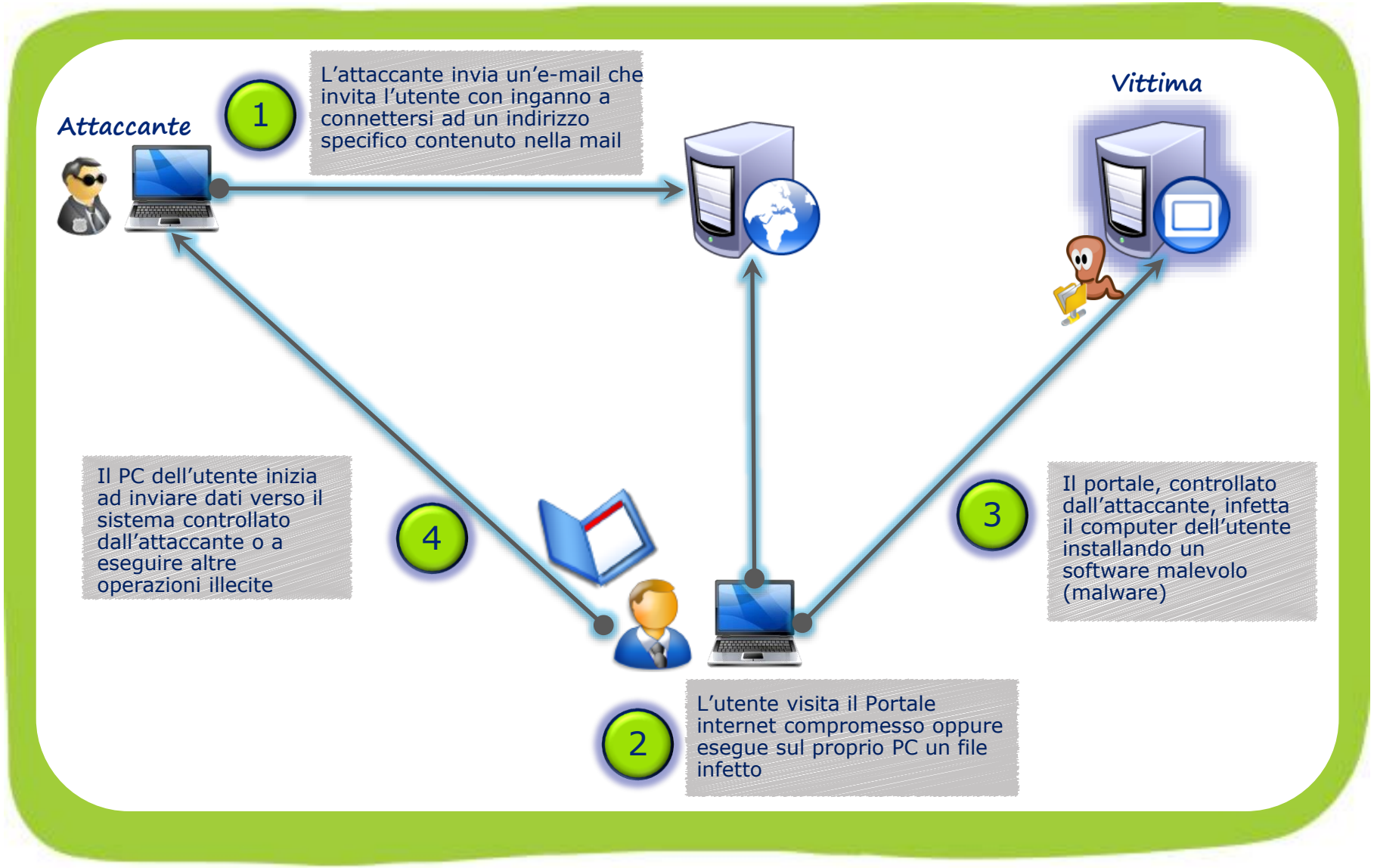
*"Il Cyber Risk è considerato il principale rischio per il quale il Business non si sente adeguatamente preparato a gestirlo"**

**Fonte: Allianz Risk Barometer*

Scenario di attacco comune: "spear phishing" e data breach

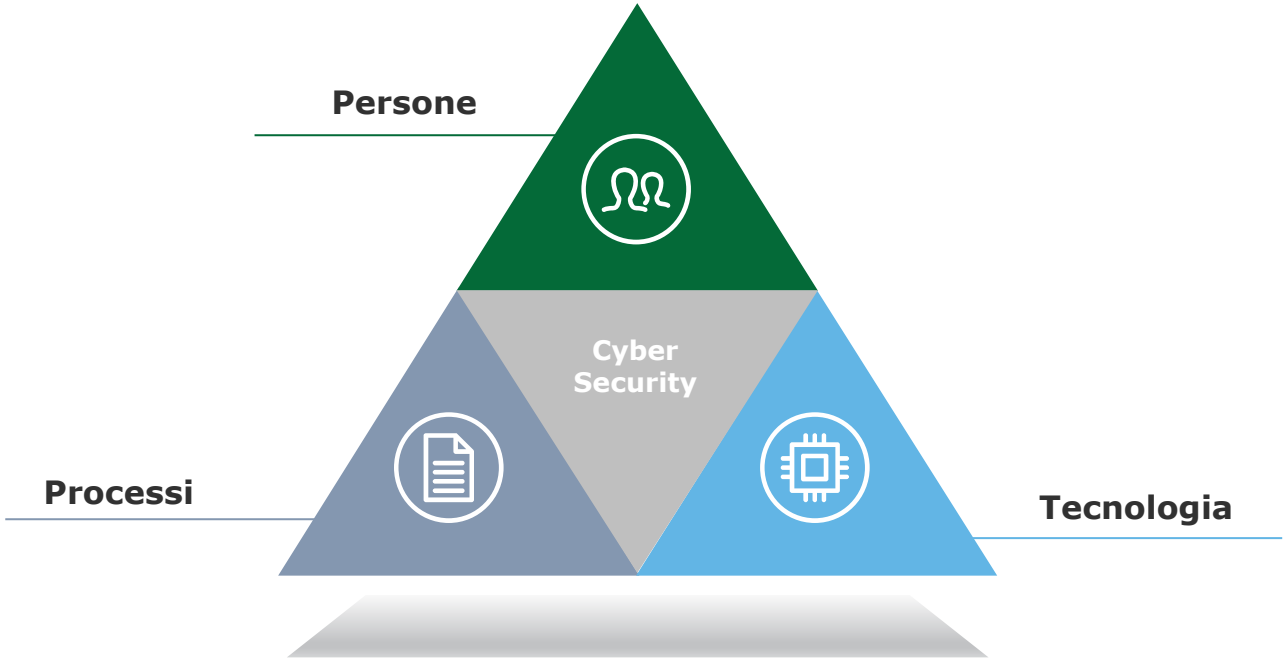
*Le tecniche di "**spear phishing**" sono propedeutiche a diverse tipologie di compromissioni, finalizzati a:*

- Acquisire informazioni riservate
- Creare disservizi per favorire estorsioni (e.g. ransonware)
- Realizzare frodi (e.g. esecuzioni di bonifici a destinatari illegittimi)
- Ottenere il controllo delle vittime per realizzare altri attacchi (e.g. Distributed Denial of Services)



Cyber Risk – Strategia di intervento

Come per altri rischi operativi, anche la gestione della cyber security deve prevedere un equilibrio tra rischio residuo/accettabile e misure di sicurezza adottate



Un strategia integrata per la gestione del rischio Cyber deve includere tecnologie, persone e processi

Cyber Risk – Strategia di intervento

Riduzione del rischio Cyber

Cyber Risk – Ambiti esemplificativi di intervento

Esemplificativo

	Descrizione	Tipologia primaria di intervento
Prevenire	**Campagne** di **Awareness** rivolte ai dipendenti al fine di **sensibilizzarli** su **tematiche** di **Cyber Security**, per la **prevenzione** di attacchi di **Phishing**, **Social Engineering** e **data breach**	Persone
	Misure tecnologiche (e.g. **firewall, antivirus, antispam, sistemi di intrusion prevention, crittografia**) per la **protezione attiva** della principali minacce Cyber (e.g. malware, spam, phishing, denial of service)	Tecnologie
	Attività di **Vulnerability Assessment** e **Penetration Testing** effettuate sui **sistemi** e **applicativi aziendali**, al fine di identificare tempestivamente le vulnerabilità esistenti ed il livello di "resistenza" ed attacchi esterni	Persone
Individuare	**Monitoraggio continuo (Security Operations Center)** delle infrastrutture IT applicative per individuare **tempestivamente** eventuali **tentativi di compromissione**	Processi
	Identificare eventuali **minacce cyber esterne** al perimetro aziendale che potrebbero interessare l'organizzazione mediante attività di **Cyber Threat Intelligence** e/o **Digital Risk Protection**	Tecnologie
Rispondere	**Processi, procedure, strumenti** e competenze per gestione degli **incidenti cyber,** al fine di ridurre le conseguenze in caso di compromissione	Processi
	Capacità di garantire la **continuità operativa** (e.g. Disaster Recovery e Business Continuity) in caso di disastro o attacchi finalizzati a creare disservizi	Persone

Legenda

Persone Processi Tecnologie