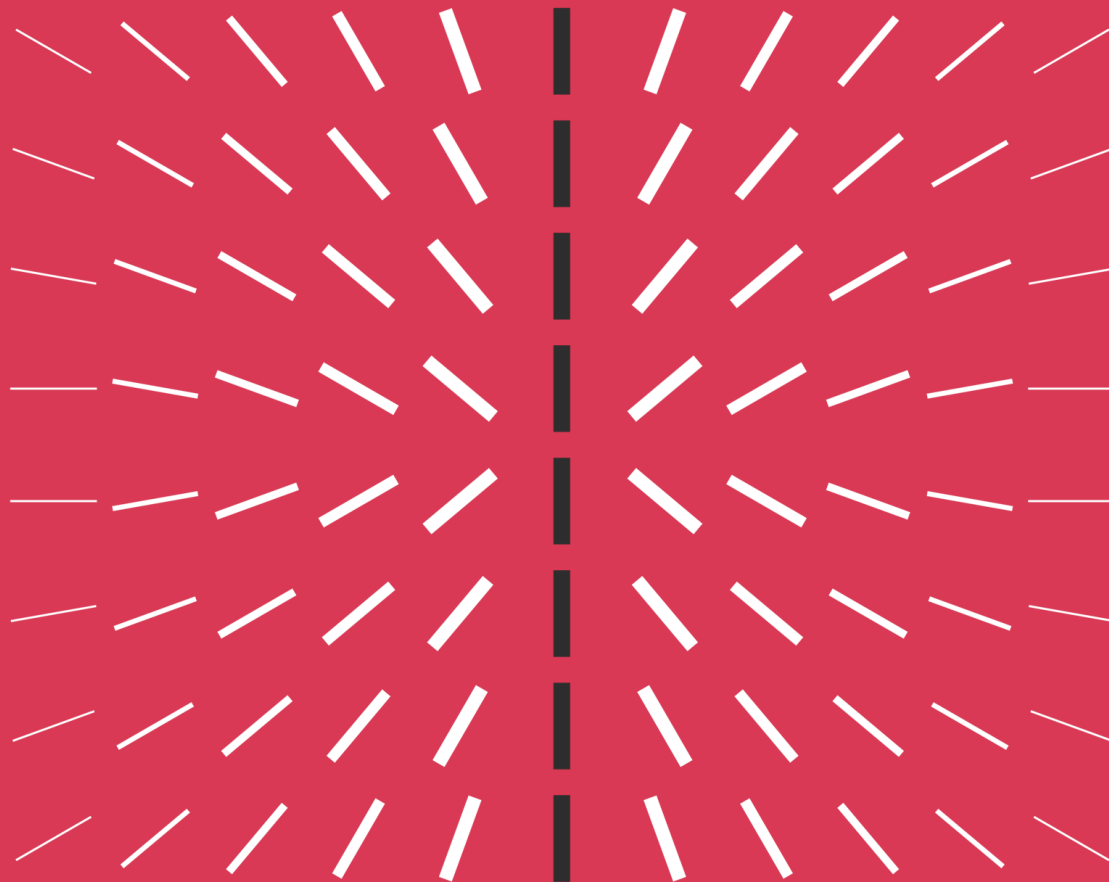


*ABI Banche e Sicurezza 2021
Sessione Plenaria di Apertura –
La Sicurezza dell’Innovazione*

Cybersecurity market overview

25 Maggio 2021



Il contesto attuale (1 of 2)

Fonte: *PwC Global Trust Insights Survey 2021 (Ottobre 2020)*

Abbiamo analizzato i principali cambiamenti di business e la contestuale evoluzione del ruolo della Cybersecurity

Accelerated digitalization for growth



Permanent, full-time remote work for more workers



Larger weight on the quality on IT and telecommunications infrastructure in location decisions



Accelerated automation for cost-cutting



Continuously updated resilience plans and tests



Il modo di fare Businesses è cambiato...

Cybersecurity and privacy baked into every business decision or plan



New process of budgeting for cyber spend or investments



Better and more granular quantification of cyber risk



More frequent interactions between CISO and the CEO or boards



Greater resilience testing for more low-likelihood, high-impact events

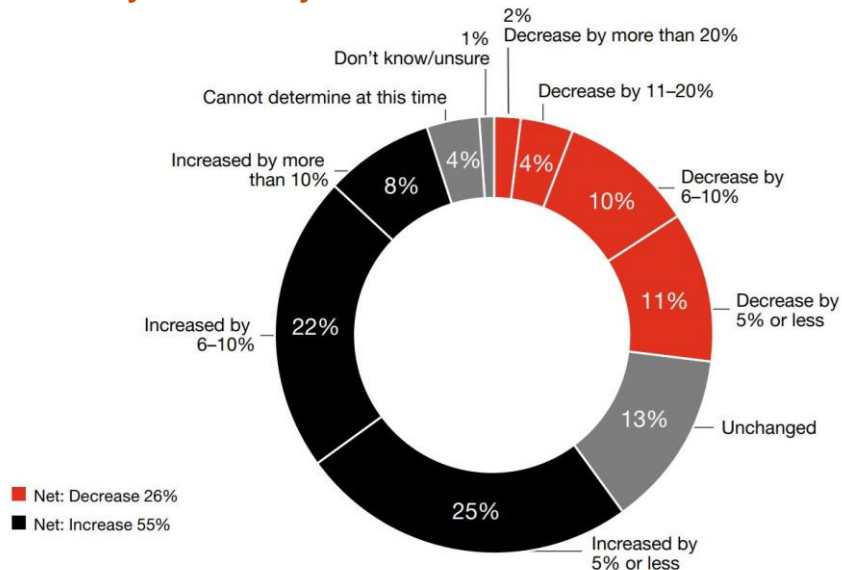


...come anche le Strategie Cyber

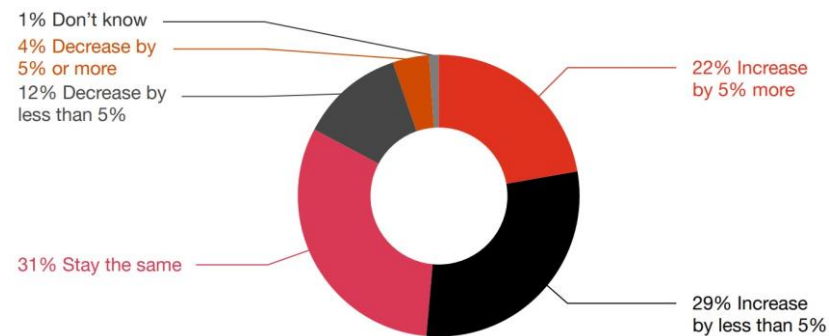
Il contesto attuale (2 of 2)

Fonte: PwC Global Trust Insights Survey 2021 (Ottobre 2020)

Come è cambiato il budget per la Cybersecurity nel 2021?



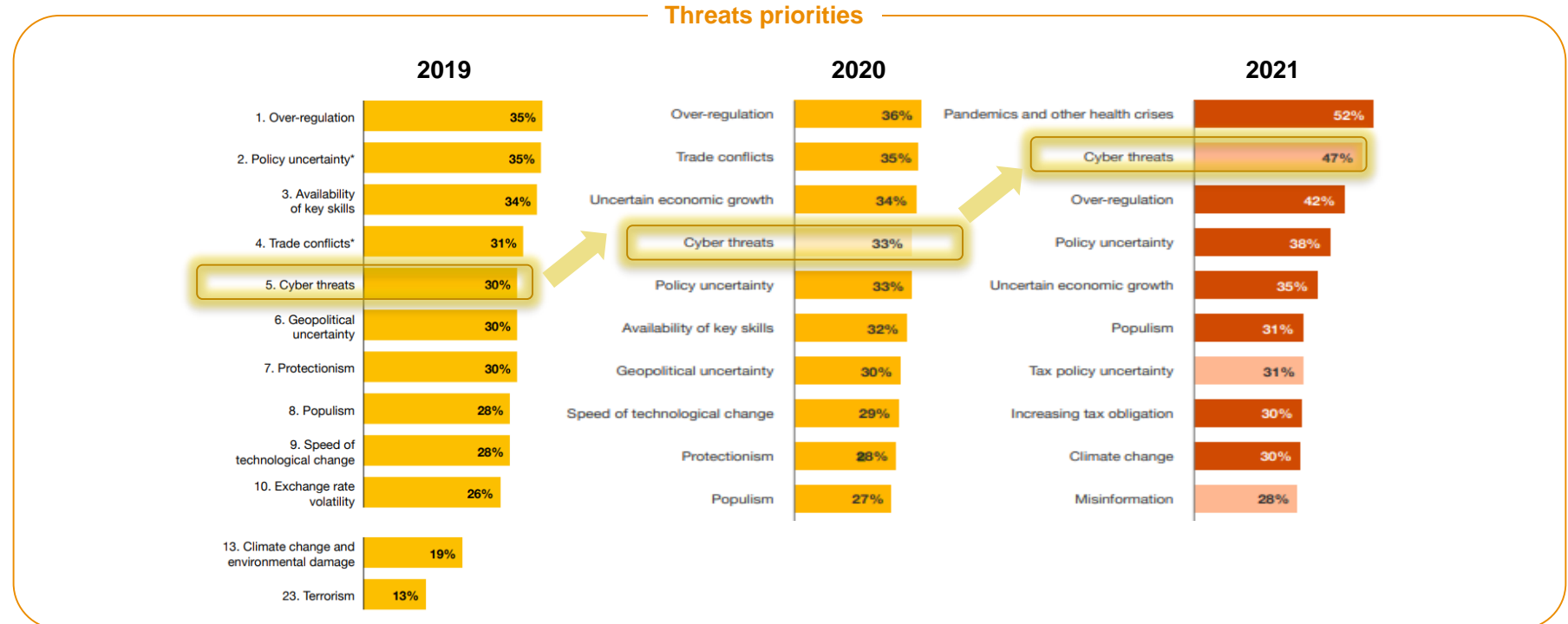
Come cambierà il dimensionamento dei team dedicati alla cybersecurity nei prossimi 12 mesi?



Come è cambiata la percezione della Cybersecurity per i CEO

Fonte: PwC CEO Survey 2019 - 2021

Negli **ultimi 3 anni**, secondo la nostra Global CEO Survey, la **Cybersecurity** ha continuato a crescere quale **priorità per i CEO a livello globale**, arrivando **nel 2021 ad essere seconda solo alla gestione della crisi pandemica**.



Perchè le organizzazioni sono così vulnerabili agli attacchi Ransomware?



Ransomware

I Ransomware continuano a crescere come meccanismo di attacco.

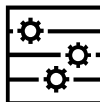
Organizzazioni criminali sempre più sofisticate hanno costituito veri e propri “programmi di affiliazione” per la distribuzione di malware.



Abbiamo identificato **5 criticità comunemente presenti** nelle aziende e che portano tipicamente ad essere rmente vulnerabili agli attacchi ransomware.



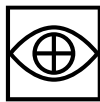
Sistemi Legacy che possono introdurre vulnerabilità di sicurezza sfruttabili dagli attaccanti.



Soluzioni tecnologiche che **non vengono configurate in modo sicuro** così da prevenire comuni attacchi cyber



Prassi insecure per la gestione amministrativa dei sistemi che consentono agli attaccanti di compromettere credenziali privilegiate



Ridotta efficacia delle soluzioni di detection & response che lasciano libertà di operare agli attaccanti.



Infrastrutture on-premise gestite autonomamente e non disegnate per prevenire attacchi Cyber

Quanto costa un Cyber Breach?

Costo per cliente



22.7%

Aumento dal
2017

Frequenza



27.4%

Aumento dal
2017

Costo per cliente nelle diverse Industry

Health

€376

Financial

€190

Services

€167

Pharma

€160

€3.56m

Costo medio
a livello
globale



6.4%

Aumento del
costo medio a
livello globale
dal 2017



**€37m –
€323m**

Ipotesi di costo di
un 'mega breach'



Come proteggere i clienti da attacchi e frodi rafforzando la relazione di fiducia con la Banca?



Prepare

Attivare soluzioni evolute per il controllo degli accessi

Evolgere le tecnologie di controllo accessi integrando soluzioni passwordless e di strong authentication orchestrate in base al rischio di ogni transazione

Informare attivamente fornitori e clienti

Informare in modo semplice e diretto fornitori e clienti in merito alle minacce e alle modalità più efficaci per identificare le frodi più comuni. Adeguare la comunicazione alle esigenze e alle caratteristiche della clientela



Respond

Rafforzare processi e soluzioni di detection & response

Utilizzare soluzioni basate su Big Data Analytics per il monitoraggio in real time delle frodi, includendo funzionalità di Behavioural Analytics, nel rispetto delle normative vigenti.



Emerge Stronger

Verificare i modelli organizzativi ed operativi

Verificare se le cause di una frode possano essere riconducibili all'eccessiva compartimentazione delle responsabilità e dei processi decisivi per il fraud management e rivedere l'organizzazione verso un approccio più collaborativo e orientato all'info-sharing

Cogliere le opportunità di miglioramento

Utilizzare le frodi subite come un'opportunità per migliorare i processi esistenti e costruire un ecosistema fraud-resilient in grado di affrontare le future sfide della digitalizzazione

Condividere le lesson learnt

Analizzare le frodi subite ed identificare le informazioni da condividere quali lesson learnt con Clienti, Dipendenti e terze parti

www.pwc.com/it

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2021 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

190624-142613-AS-OS