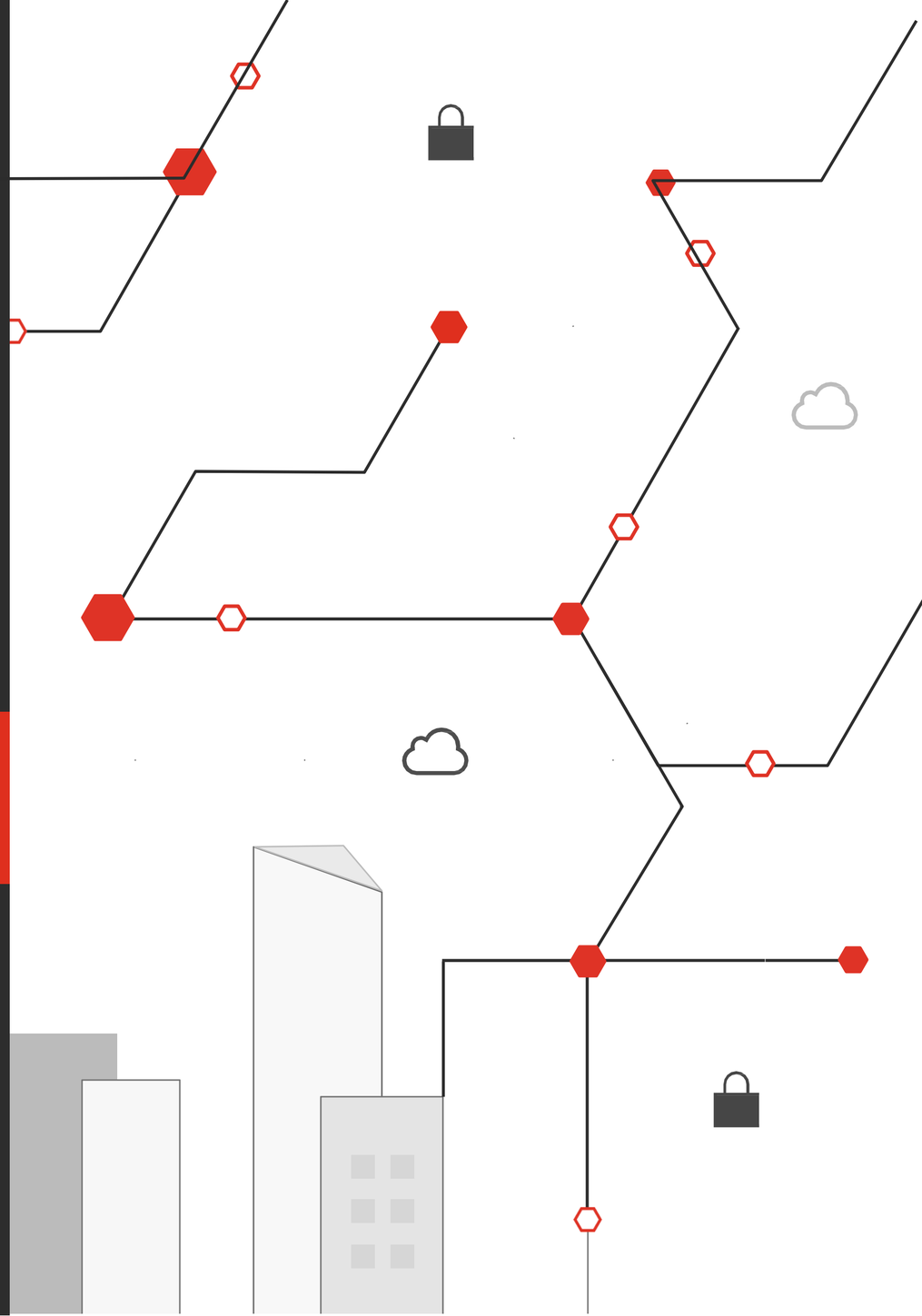
ABI Banche e Sicurezza 2020
Gestione dell'emergenza e impatti organizzativi per la Cybersecurity

Paolo Carcano
Associate Partner
Head of Cybersecurity & Data Protection for Financial Services

pwc



Primi passi nell'emergenza: La gestione della war room

Monitoraggio e reporting

- Predisposizione della reportistica per la Direzione e verso le Autorità
- Gestione del monitoraggio e del reporting periodico

Comunicazione

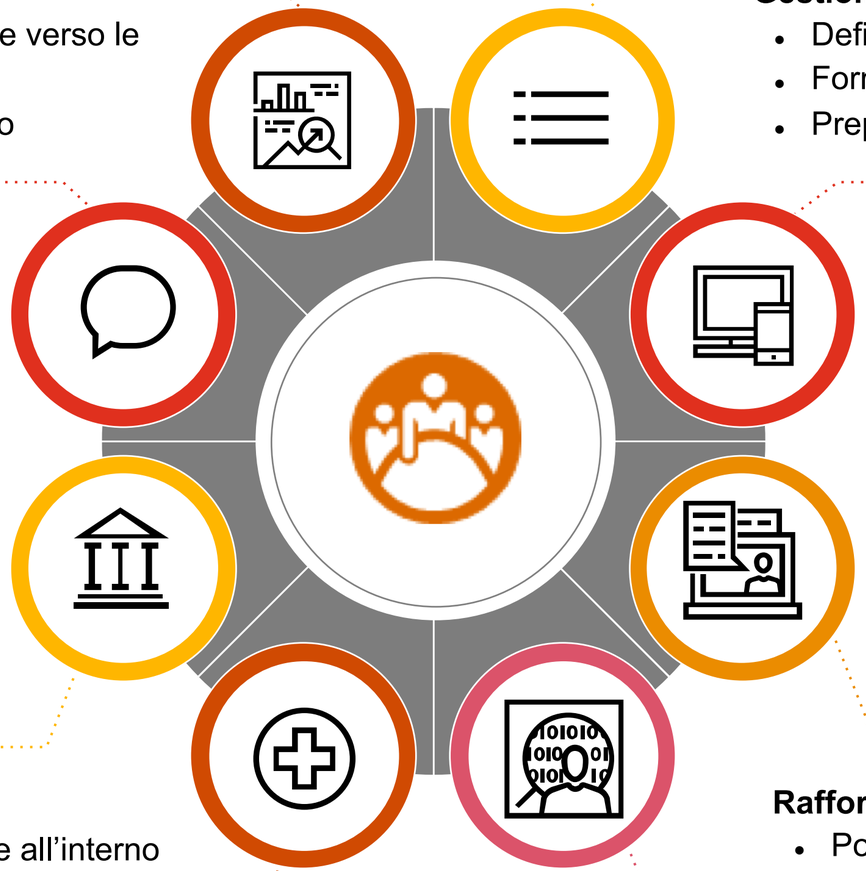
- Predisposizione delle comunicazioni verso l'interno e verso l'esterno
- Attivazione di comunicazioni periodiche verso il personale, la clientela e le Autorità (Protezione civile, Banca d'Italia)

Monitoraggio delle filiali

- Aggiornamento del censimento del personale operante nelle diverse geografie
- Monitoraggio e supporto del personale operante nelle sedi/filiali o da remoto con eventuali problematiche sanitarie

Sicurezza fisica/Safety

- Adozione di presidi per ridurre il rischio di infezione all'interno delle sedi, degli uffici e delle filiali
- Avvio di iniziative specifiche di formazione per dipendenti e clienti



Gestione degli scenari di emergenza

- Definizione del modello DEFCON
- Formalizzazione delle metriche di valutazione
- Preparazione delle misure da realizzare per ogni livello

Attivazione Remote-work

- Fornitura PC e strumenti di comunicazione
- Configurazione connessioni sicure (VPN)
- Gestione dotazioni speciali per aree di business specifiche (Finanza, …)

Digitalizzazione dei servizi di business

- Rafforzamento dell'offerta dei servizi erogati mediante canali digitali
- Gestione di un processo di sottoscrizione ed attivazione dei servizi digitali in emergenza (e.g. online banking)

Rafforzamento infrastruttura IT

- Potenzialmento dell'assistenza di I e II livello
- Prioritizzazione degli interventi di manutenzione
- Rafforzamento presidio Anti-frode e Cybersecurity

Priorità dei CISO nell'emergenza

01

Sicurezza e smart-working

Garantire la sicurezza delle nuove modalità di organizzazione del lavoro da remoto

02

Continuità delle funzioni di sicurezza

Assicurare la continuità delle funzioni critiche Cybersecurity e di Business

03

Gestione strategica delle minacce

Contrastare minacce opportunistiche rispetto al nuovo scenario di smartworking e digitalizzazione dei servizi

Priorità dei CISO nel medio/lungo periodo

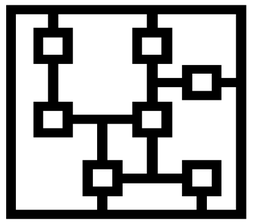
Protezione degli Endpoint

E-Collaboration e Automazione (Threat Intel, SOC, Fraud)

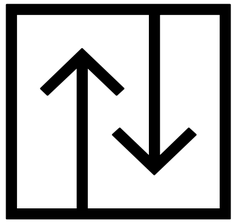
Sicurezza delle III e IV parti

Gestione fisico-logica della sicurezza

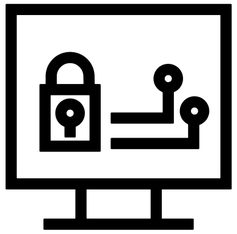
La gestione delle terze parti: quali sono le sfide da affrontare



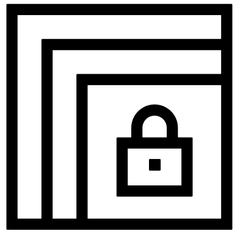
Ridotta visibilità sugli asset IT e sul livello di cyber resilience delle terze parti, includendo sempre più anche le quarte e quinte parti.



Ridotta capacità computazionale o connettività per eventuali partner critici operanti in modalità offshore.



Aumento dei rischi di sicurezza e privacy per la gestione di dati e documenti critici a causa del remote working



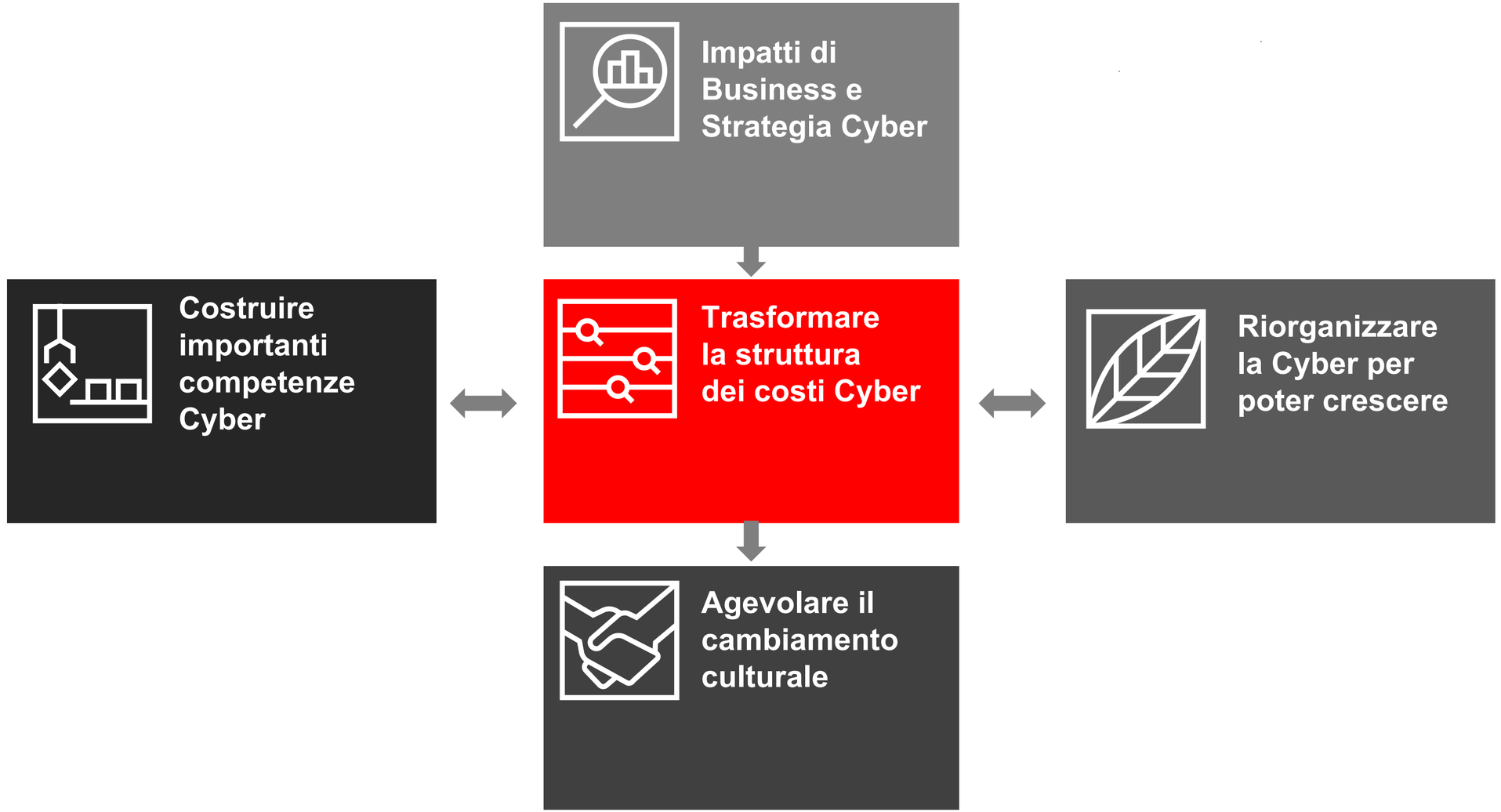
Gestione della sicurezza delle connessioni con le terze parti assicurando adeguati controlli

Cose emerge dalla nostra Global Digital Trust Insights 2021 per il mercato dei Financial Services

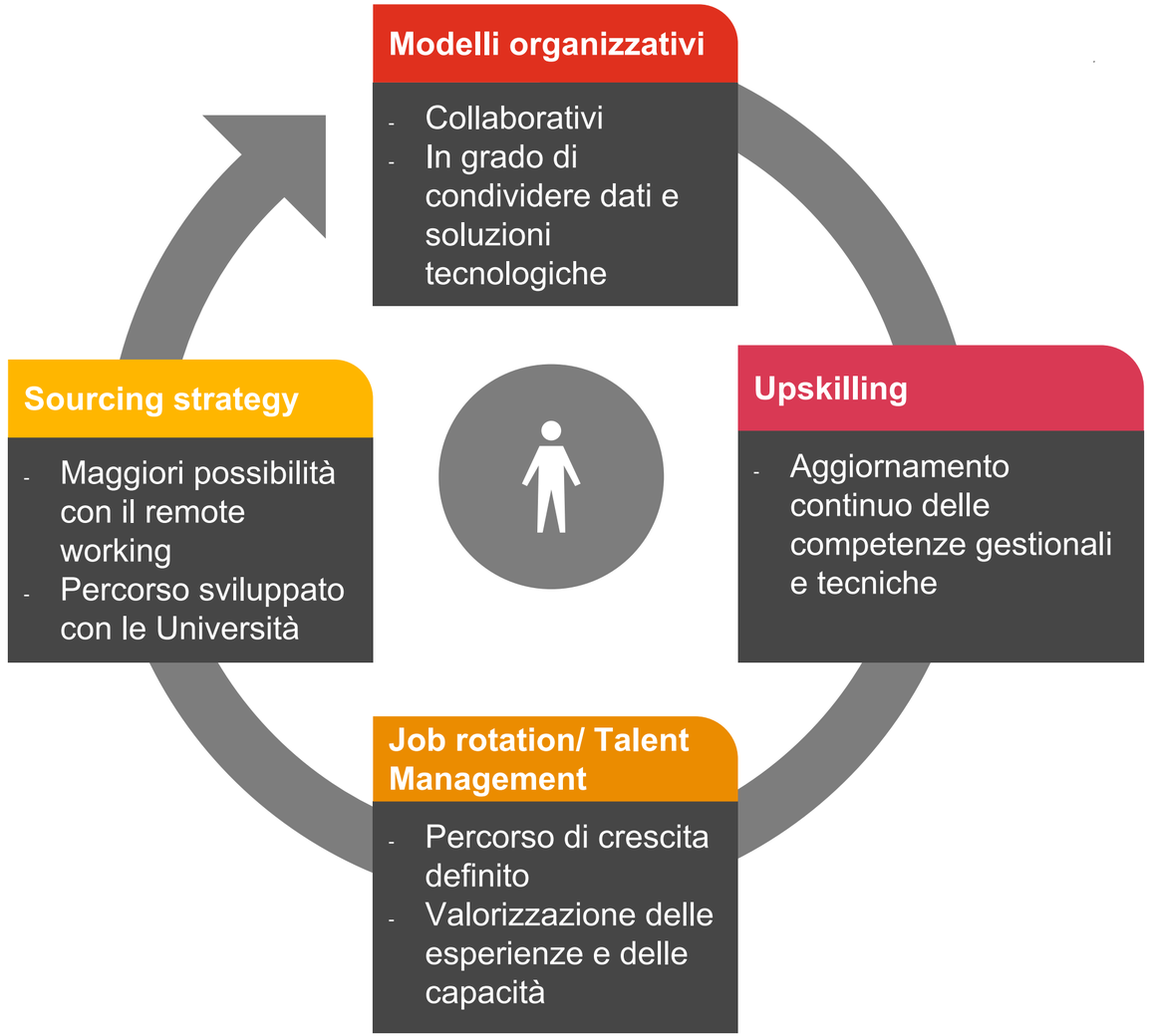
Intervistati: 3,249 dirigenti in ambito business/technology a livello globale

1	**Ripensare la strategia cyber ed evolvere il ruolo del CISO**	• il **46% ha attivato in modo permanente il remote work** per la maggior parte della forza lavoro; il **40% ha accelerato la digitalizzazione** dei propri processi • il **51% ha integrato valutazioni relative a cybersecurity e privacy** in tutte le decisioni di business • il **21% ha svolto il ruolo di guida operativa e di supporto** per l'identificazione delle soluzioni tattiche da adottare
2	**Rivedere il budget cyber per massimizzare il valore di ogni investimento**	• **Il 29% ha aumentato del 5% il proprio budget di sicurezza** mentre **il 22% sino al 10%** • **Oltre il 53% dichiara che il budget Cyber non è direttamente connesso all'evoluzione del budget aziendale** • **Il 45% ha avviato iniziative per arrivare ad una migliore quantificazione del cyber risk**
3	**Investire per avvantaggiarsi rispetto agli attaccanti**	• **Investire in tecnologie avanzate per migliorare la cyber defense** (detection & response) • **Unificare il reporting tra le diverse aree organizzative che trattano il Cyber Risk** • Il 21% ha integrato soluzioni per la cloud security e la network security • Il 22% ha integrato la security e privacy nei propri processi di business critici
4	**Essere preparati a gestire ogni scenario di attacco**	• **Oltre il 60% si prepara a gestire minacce che possano provenire dai Cloud service provider** • **Il 27% si prepara a gestire possibili attacchi ransomware** • **Oltre il 50% si prepara a gestire in generale il Cybercrime**
5	**Evolvere il team Cyber per gestire le prossime minacce**	• **Circa il 30% prevede di aumentare il team sino al 5% mentre il 24% anche oltre il 5%** • **In termini di competenze, il 44% investirà in Analytics, il 42% investirà in soluzioni cloud mentre il 41% in progetti innvativi e nel miglioramento dell'ambiente di lavoro**

Anche ai CISO è richiesto di rivedere gli investimenti



Le persone e le competenze devono essere al centro dei piani evolutivi



Cosa possiamo dire di aver imparato sino ad ora

01 Le aziende erano mediamente impreparate a gestire il rischio pandemico. I processi di Crisis Management non erano pensati per gestire impatti su molteplici aspetti e per un periodo prolungato

02 Le terze parti sono state spesso problematiche nella gestione della Crisi in quanto ancora più impreparate nella gestione del rischio pandemico

03 Nonostante tutto le persone hanno fatto la differenza attivando misure straordinarie per fronteggiare, primi fra tutti, la crisi pandemica

04 Il CISO ha svolto un ruolo importante nella definizione delle misure per la gestione della Crisi

05 Il ruolo del CISO è cambiato, diventando sempre più centrale nelle decisioni di Business

06 Tale evoluzione deve portare a rivalutare competenze e capacità che i security manager devono avere, mediante upskilling e talent management

07 I budget della Cyber sono comunque destinati a crescere ma devono essere rivisti per ottimizzare l'efficacia della spesa e monitorare il contributo verso il business

08 Investire in automazione (con riferimento a Threat Detection & Response) consente di migliorare l'efficacia del lavoro da remoto

09 Terze Parti (inclusa la Cloud Security) e gestione della sicurezza degli Endpoint sono le tematiche non nuove ma la cui importanza è cresciuta con l'emergenza

Grazie!