CERTFin

Report Sicurezza e Frodi nel settore finanziario

Romano Stasi
Chief Operating Officer

CYBER in FINANCE 2021
10 novembre

Report Sicurezza e Frodi nel settore finanziario ...in Sintesi

20% di maggiori investimenti nelle banche dedicati alla sicurezza dei servizi
il 73% delle imprese assicurative prevede un aumento delle spese sulla «security posture»

del budget banche

La clientela retail si conferma la più colpita

del totale

Enorme aumento del numero di transazioni anomale

Rispetto allo scorso anno

Le tecniche di attacco miste sono diventate dominanti

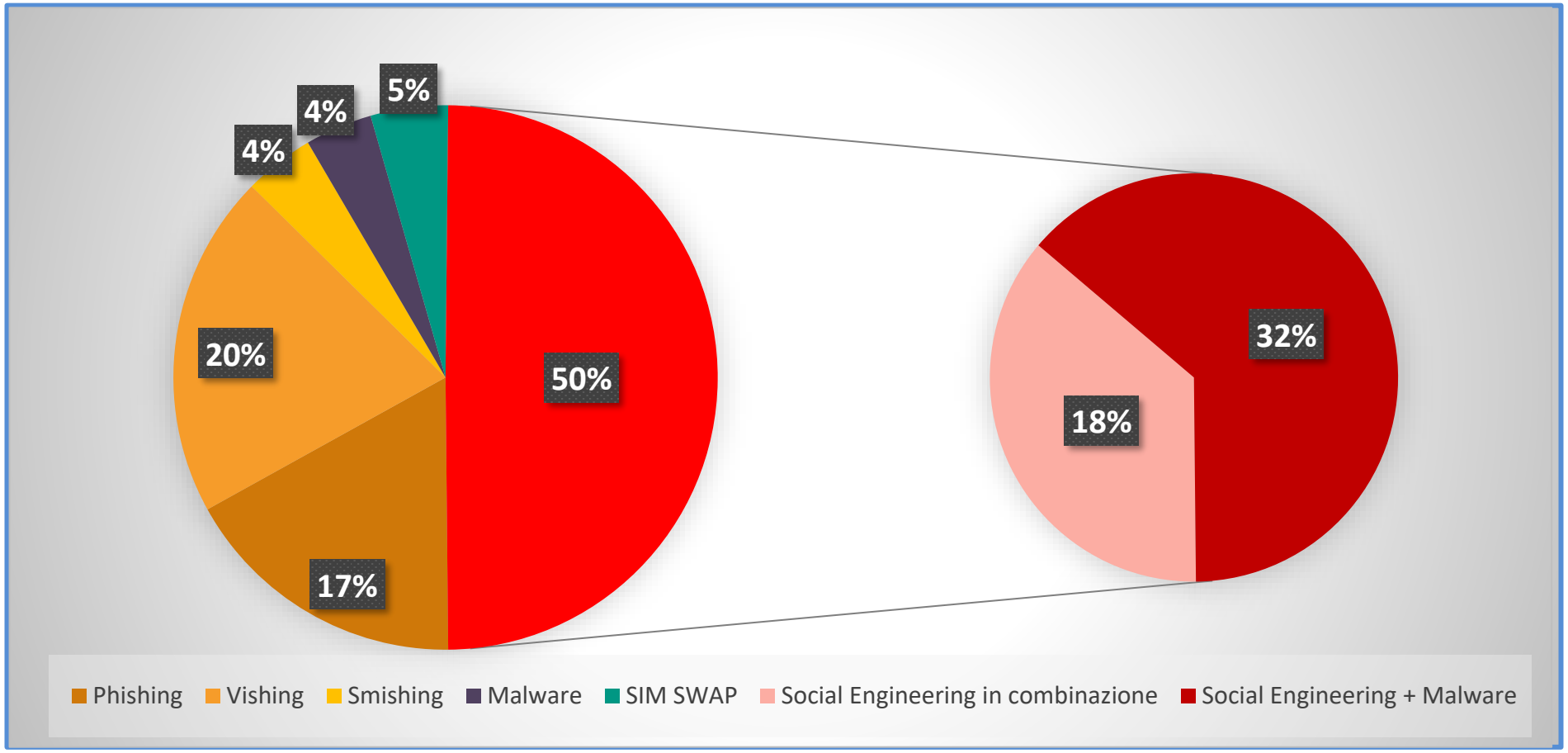
del totale

La gestione delle transazioni fraudolente resta efficace

Transazioni bloccate o recuperate sul totale delle anomale

Tipologie di Frode

Clientela Retail - Tipologie di frode rilevate sul canale Internet Banking



Clonazione siti web bancari

La clonazione a scopo fraudolento dei siti web delle imprese è un fenomeno di specifico interesse per il settore bancario. La maggior parte delle banche italiane si è dotata di strumenti utili per la «*detection*» di questo tipo di minaccia.

+930

Più di 930 siti di Phishing segnalati dal CERTFin nel 2021*

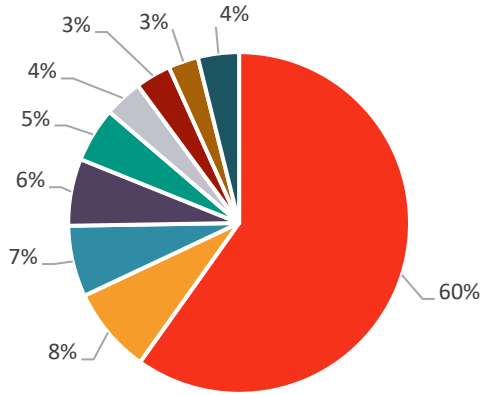
47%

Il 47% dei siti fraudolenti segnalati utilizzano il protocollo HTTPS*

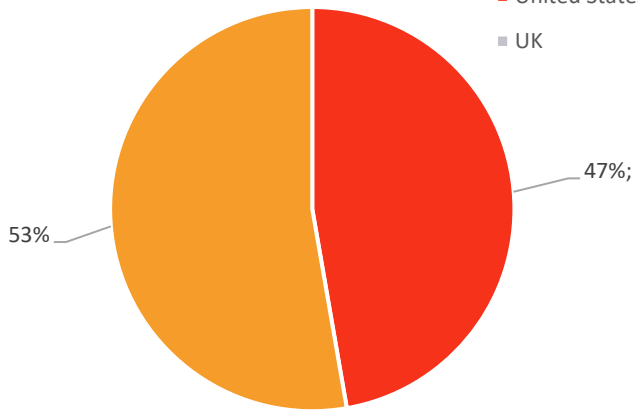
60%

Il 60% dei siti fraudolenti sono ospitati da fornitori si servizi di Hosting negli Stati Uniti

DISTRIBUZIONE GEOGRAFICA DEI FORNITORI DI SERVIZI DI HOSTING CHE OSPITANO SITI DI PHISHING*



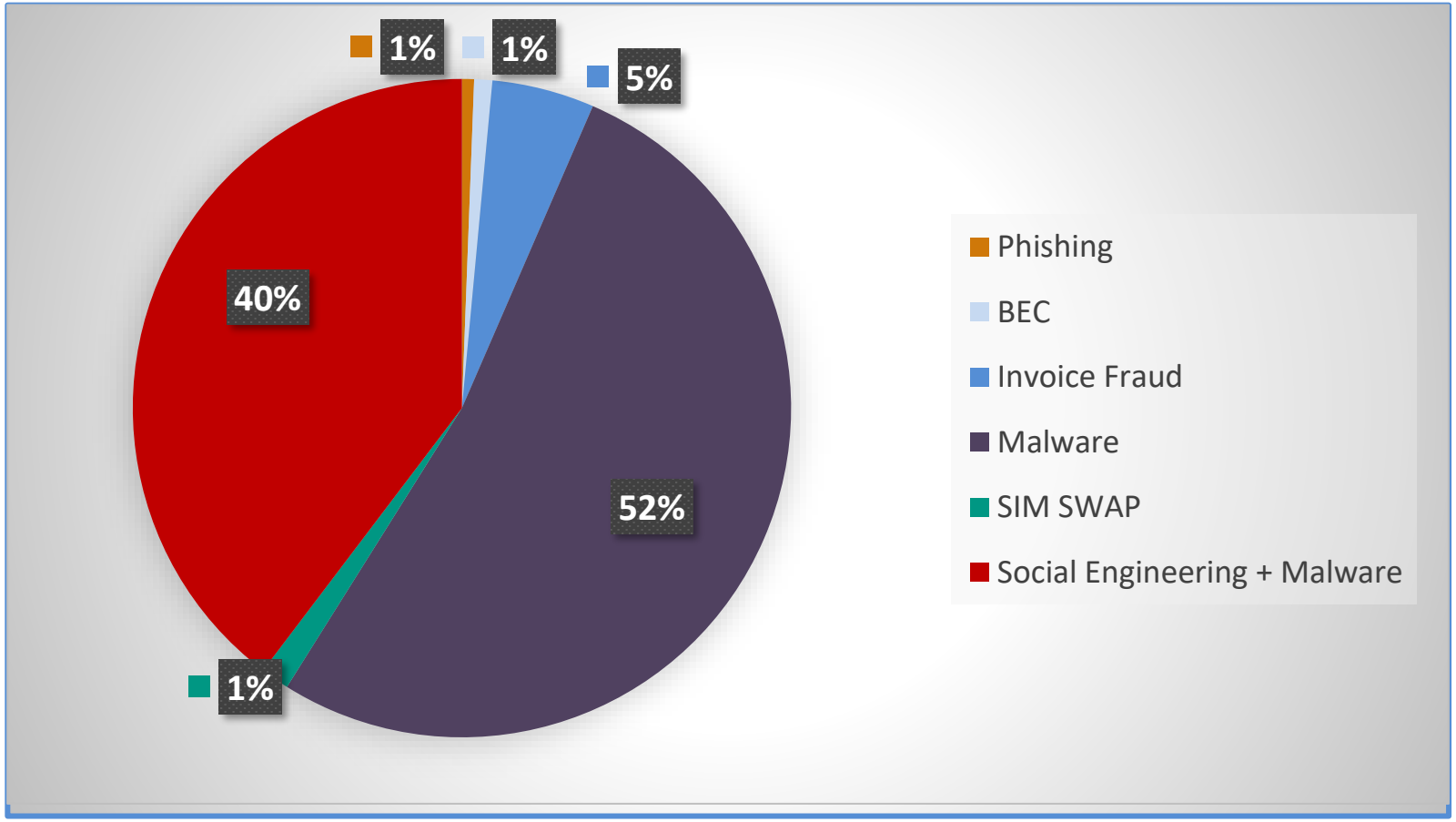
UTILIZZO DI CERTIFICATI SSL NEI SITI CLONE*



* Dati raccolti ed analizzati dalla Direzione Operativa del CERTFin

Tipologie di Frode

Clientela Corporate - Tipologie di frode rilevate sul canale Internet Banking



I Principali Steps della frode bancaria

Furto di credenziali e/o dati riservati della vittima

Accesso non autorizzato all'home banking e/o Account Takeover

Realizzazione operazioni non autorizzate

Transaction Monitoring

Blocco Operazione

Spostamento del denaro verso uno o più conti di appoggio e successivo riciclaggio

Procedure di collaborazione

Blocco C/C

Debolezze del canale di comunicazione

Negli ultimi anni gli attaccanti hanno imparato a sfruttare abilmente alcuni *vulnus* propri delle comunicazioni elettroniche, contattando i clienti con finalità malevole fingendo di essere la banca.

Social Engineering: nell'ambito bancario, un attacco di ingegneria sociale, condotto ai danni della clientela, prevede l'interazione del cybercriminale con l'utente al fine di indurlo a cedere i suoi dati riservati (es. dati bancari, codici OTP, etc.).

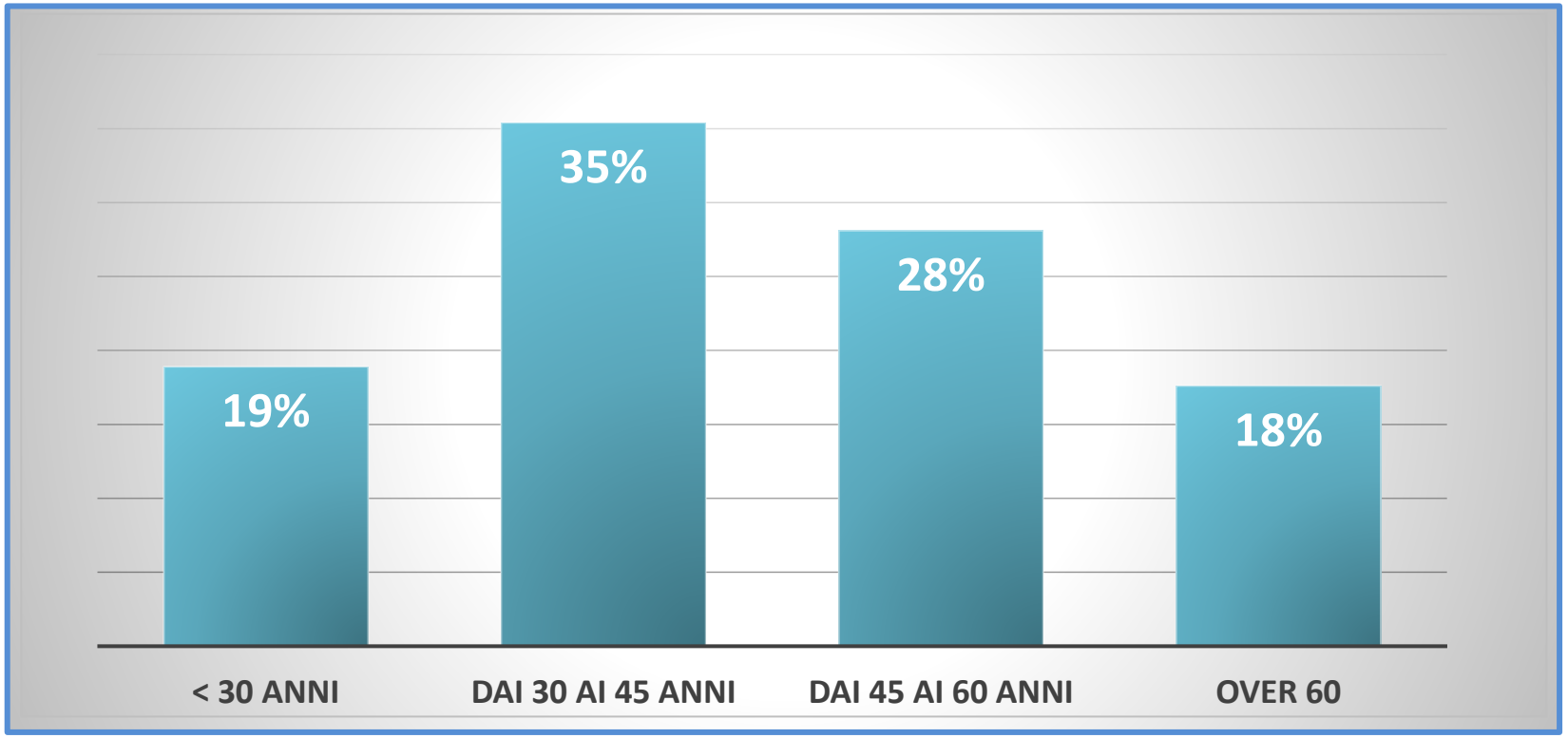
Tali attacchi sono stati resi sempre più sofisticati e spesso l'attaccante perfeziona il suo mascheramento utilizzando diverse tecniche, a volte anche in combinazione tra loro:

Smishing: descrive i tentativi dei truffatori di ottenere informazioni personali, finanziarie o di sicurezza tramite SMS. Spesso la vittima viene invitata a cliccare su un link malevolo.

Vishing: la vittima riceve una telefonata in cui i truffatori, sempre mascherandosi da qualcun altro, cercano di indurre la vittima a rivelare informazioni personali, finanziarie o di sicurezza o anche a trasferire denaro.

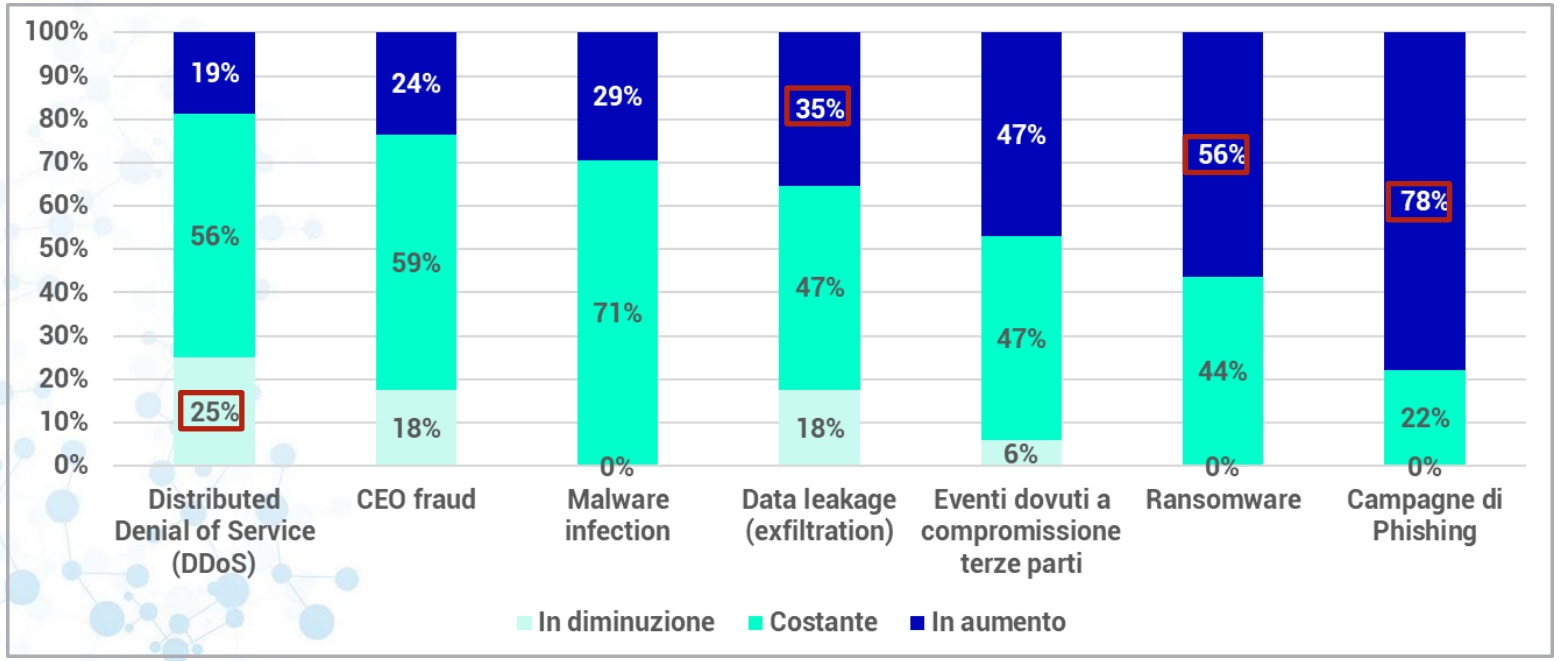
Età delle vittime

Età delle vittime di frodi effettive (solo clientela Retail)



Trend degli eventi cyber - settore assicurativo

TENDENZA EVOLUTIVA DEGLI EVENTI CYBER



La cybersecurity nel settore assicurativo 2021 – Tendenza evolutiva degli attacchi cyber rilevati (16 rispondenti)

Il fenomeno del «furto di credenziali» ai danni della clientela resta molto circoscritto ma comunque segnalato da diverse organizzazioni.

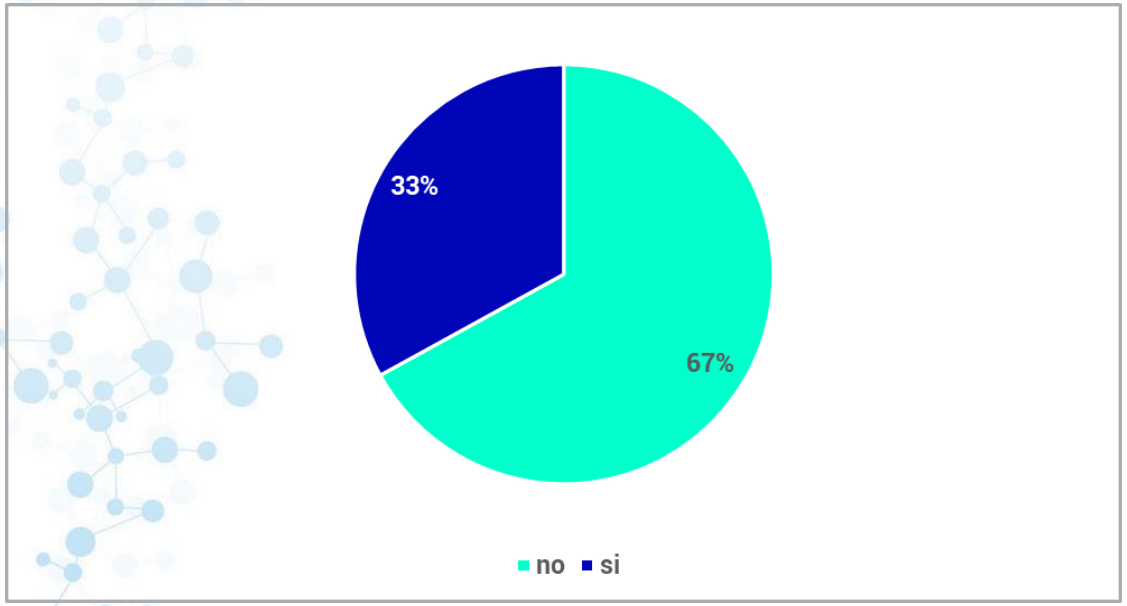
Alcune evidenze.....

- Il 25% dei rispondenti dichiara una diminuzione degli attacchi DDoS;
- Aumento delle campagne di Phishing;
- Aumento degli attacchi Ransomware;
- Aumento dei casi di Data Leakage.

Ghost Broking

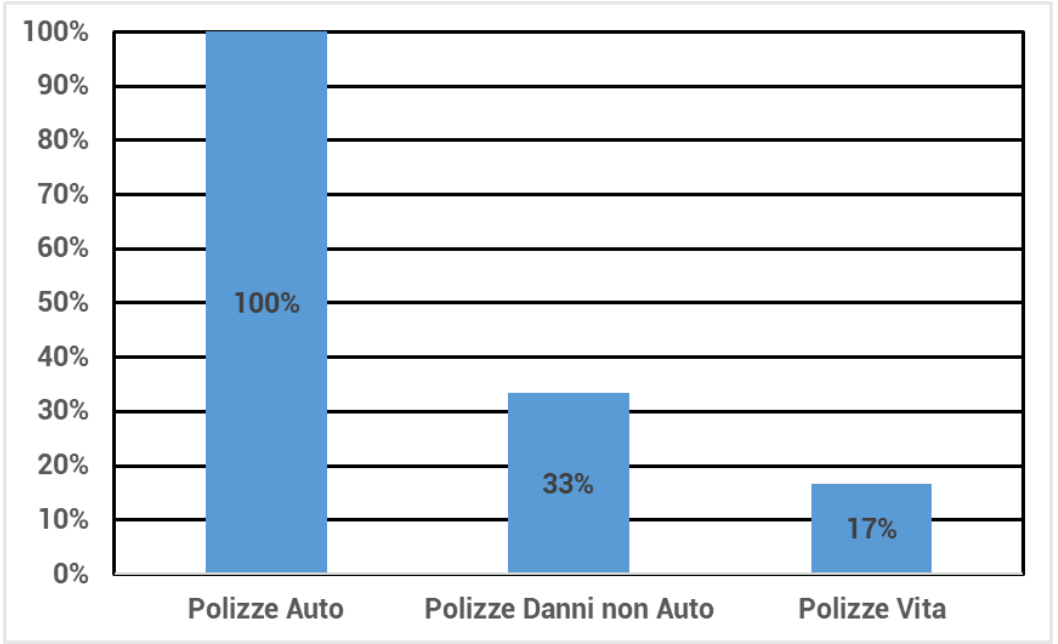
Con il termine ***«Ghost Broking»*** si intende quel fenomeno nel quale il frodatore, spacciandosi per agente di una impresa assicurativa, a seguito del pagamento di una somma di denaro rilascia una «polizza» assicurativa falsa.

IMPRESE CHE HANNO GHOST BROKING ATTRAVERSO IL CANALE INTERNET



La cybersecurity nel settore assicurativo 2021 – Percentuale di imprese che hanno rilevato casi di clonazione di siti web ufficiali di proprietà dell'azienda. (17 rispondenti)

IMPRESE CHE HANNO RISCONTRATO FENOMENI DI CLONAZIONE DI SITI UFFICIALI DELL'AZIENDA

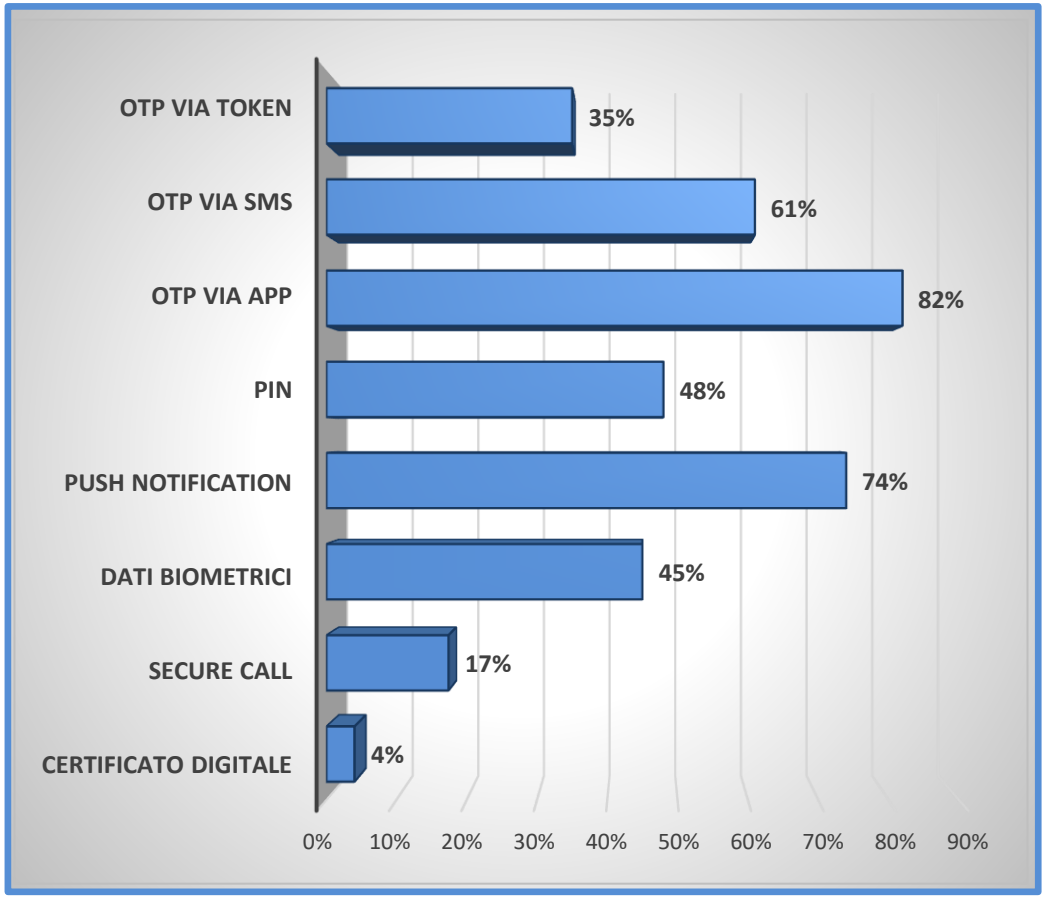


La cybersecurity nel settore assicurativo 2021 – Ambiti all'interno dei quali si sono verificati casi di «ghost broking» nell'anno 2020 (6 rispondenti)

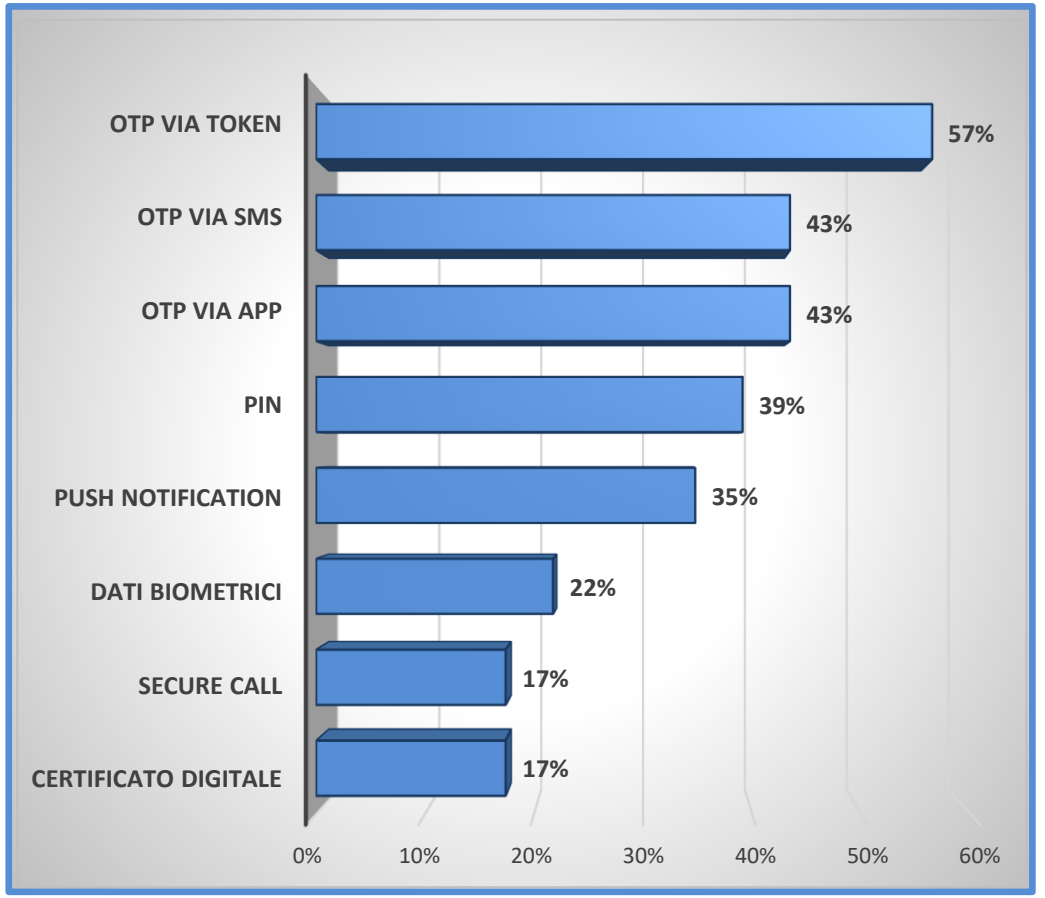
Per questo particolare fenomeno di frode si prevede, per il futuro, un trend in crescita

Tecnologie 2FA utilizzate in fase dispositiva

Retail

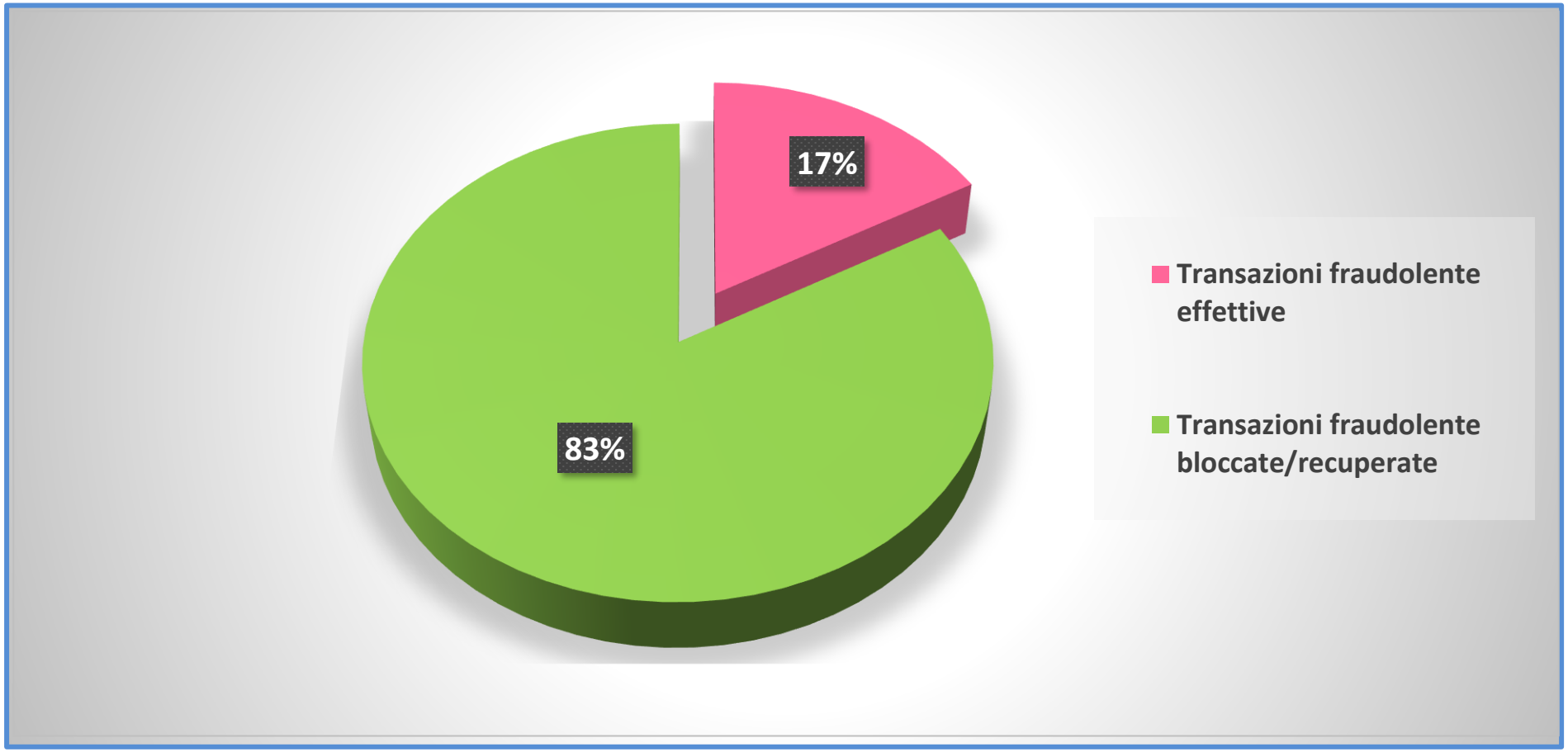


Corporate



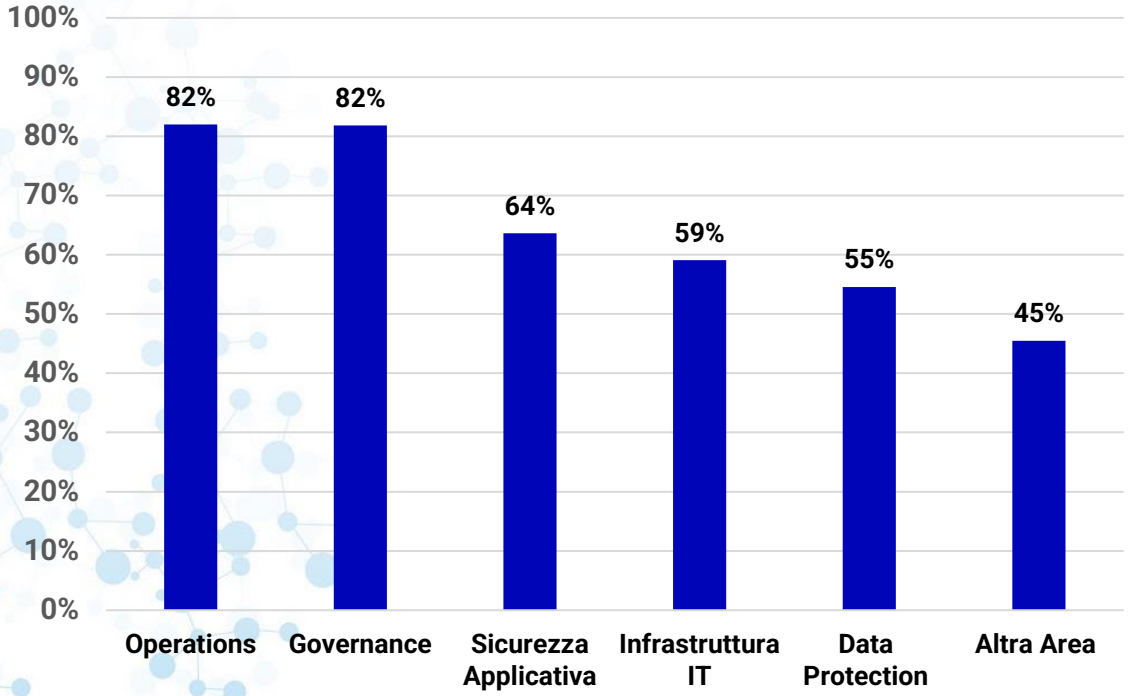
Transazioni Anomale

Ripartizione percentuale sul numero di accadimenti (complessivo Retail e Corporate)



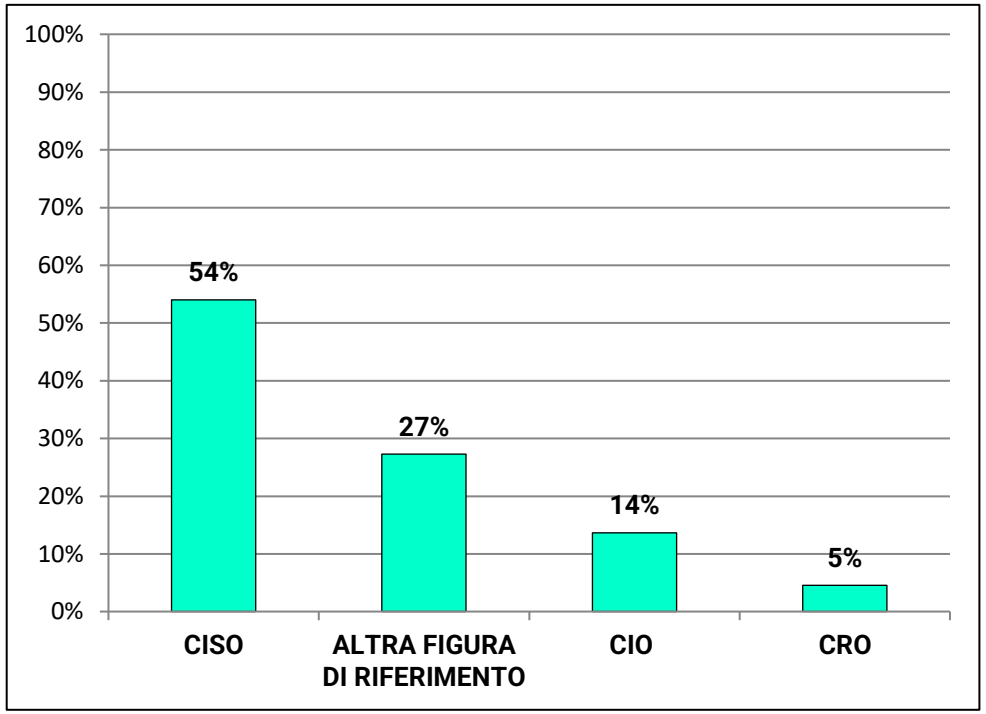
Le Strutture di Cybersecurity nelle banche

FUNZIONI E NUMERO DI RISORSE COINVOLTE NEI PROCESSI DI GESTIONE DELLE FRODI ALL'INTERNO



7	6	5	4	5	NUMERO DI RISORSE IMPIEGATE IN MEDIA

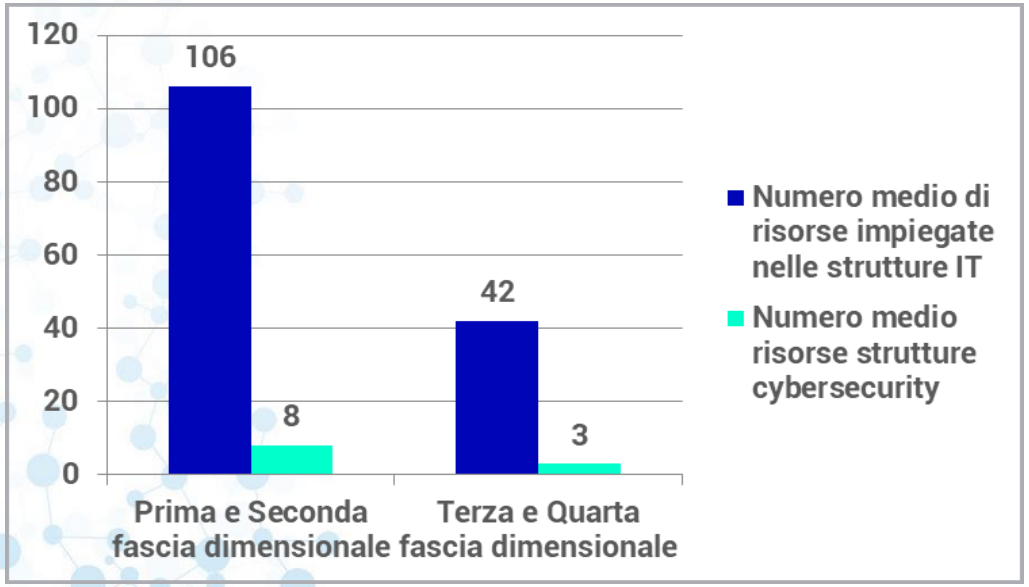
Figure interne responsabili dei processi di Cybersecurity



Le **funzioni di governance e operations**, sono coinvolte nell'82% dei casi nei **processi di gestione delle frodi**. Nella maggior parte delle banche (il 54%), le **attività di cybersecurity** interne risultano essere in capo ad un **CISO**.

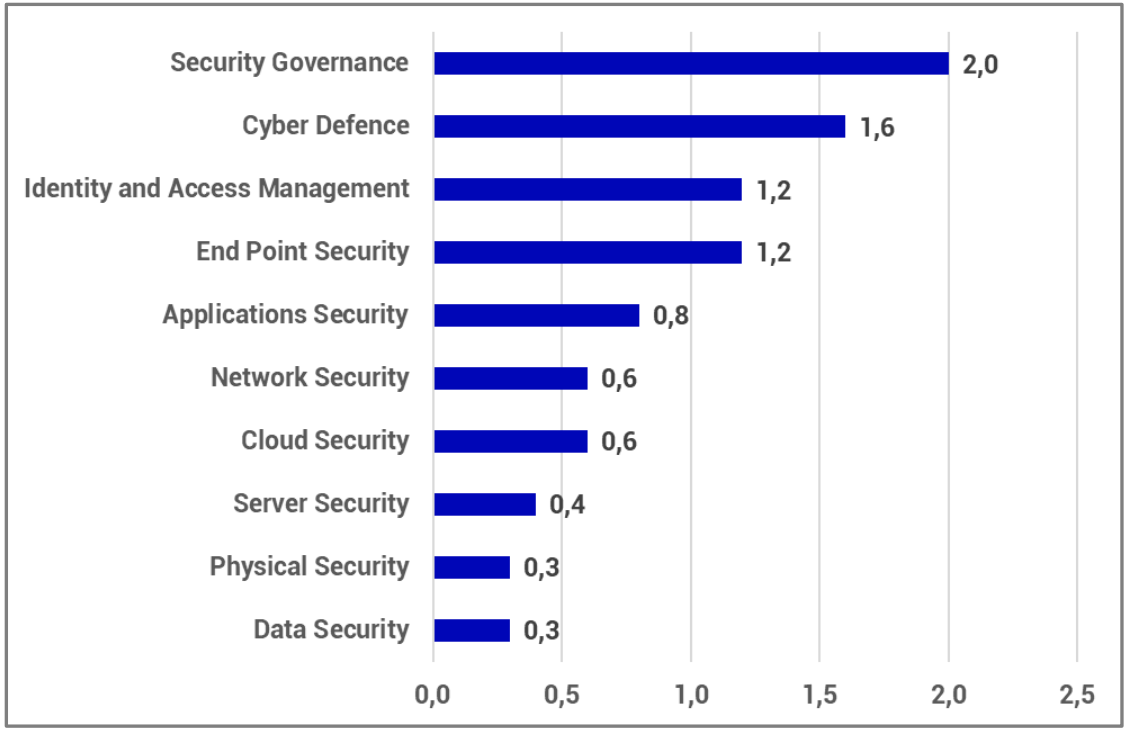
Le Strutture di Cybersecurity
Le Risorse umane dedicate dalle compagnie assicurative

NUMERO DI RISORSE IMPIEGATE NELL'IT E NELLA CYBESECURITY



La cybersecurity nel settore assicurativo 2021 – Numero medio di risorse impiegate nelle strutture IT e numero medio di risorse impiegate per le attività di cybersecurity (15 rispondenti)

NUMERO DI RISORSE IMPIEGATE NEI DIVERSI AMBITI DI CYBERSECURITY

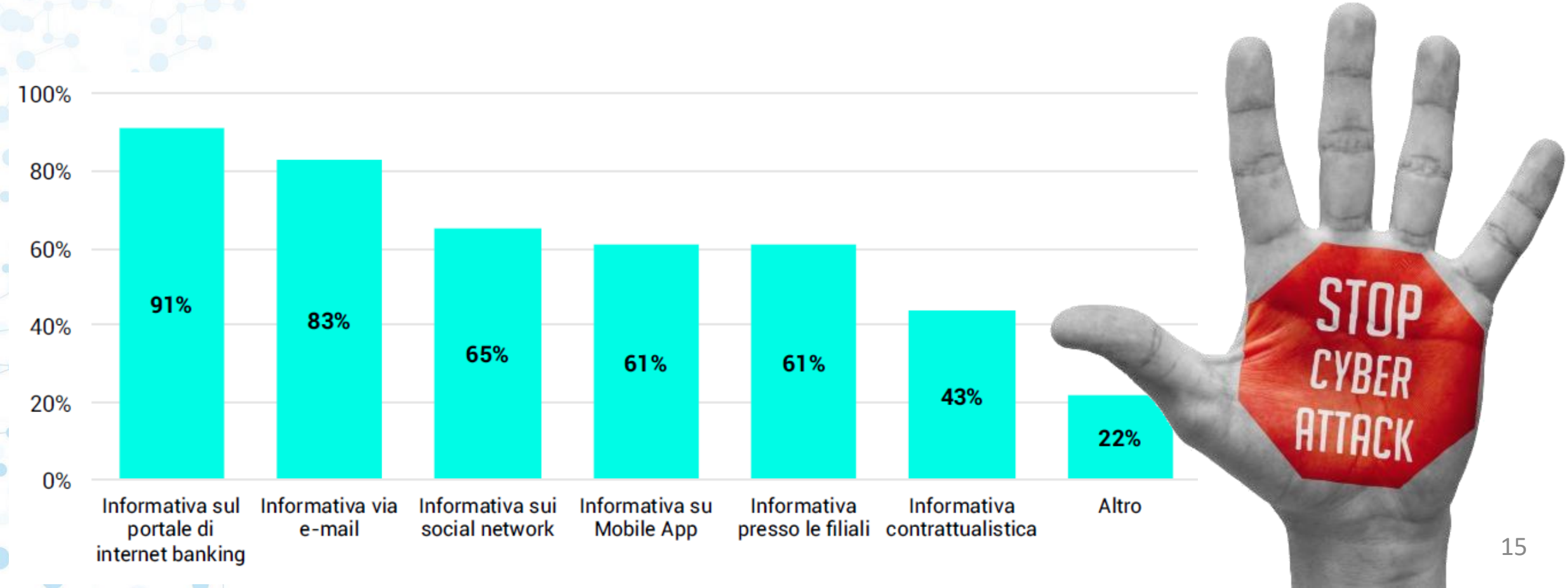


La cybersecurity nel settore assicurativo 2021 – Numero di risorse dedicate ai diversi ambiti della cybersecurity in FTE (15 rispondenti)

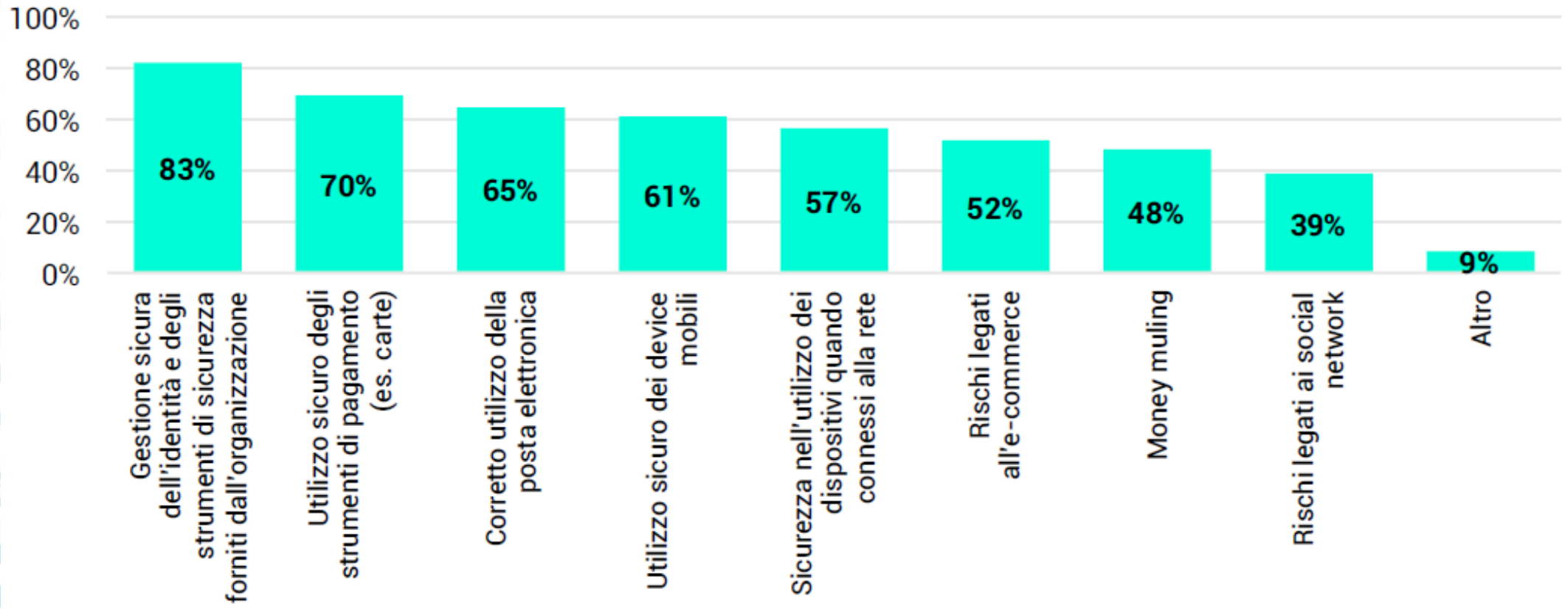
In entrambi i cluster di analisi, **il rapporto tra il numero medio di risorse impiegato all'interno delle strutture IT e il numero medio di risorse dedicato alle attività di cybersecurity si aggira intorno al 7%.**

Cybersecurity awareness per la clientela: i canali

Le banche sfruttano tutti i diversi canali disponibili per comunicare con i propri clienti e condividere aggiornamenti e raccomandazioni su un corretto uso dei device e su buone pratiche di comportamento nella gestione di credenziali e strumenti di pagamento.



Cybersecurity awareness per la clientela: i canali



I clienti sono periodicamente informati in merito a diverse tematiche che vanno da un uso corretto dei dispositivi per realizzare operazioni bancarie a distanza a buone pratiche nella gestione di credenziali e password.

Iniziative di settore per la clientela
Campagna di awareness

Il CERTFin, insieme a ABI, Banca d'Italia e Ivass, sta per lanciare una **campagna di comunicazione integrata** volta ad evidenziare l'attenzione e l'impegno del settore finanziario sui temi legati alla cybersecurity, con lo scopo di informare e proteggere la propria clientela.

OBIETTIVI:

- innalzare il livello di attenzione sulla cybersecurity
- motivare l'utenza finale ad un uso sicuro dei canali e strumenti digitali
- aumentare la consapevolezza dei clienti e sensibilizzarli sui comportamenti virtuosi da adottare per ridurre i rischi di attacchi informatici e frodi online e sull'uso sicuro degli strumenti digitali, mantenendo alta la fiducia verso i canali remoti
- valorizzare l'azione congiunta di settore e rendere consapevole la clientela del ruolo di presidio/protezione svolto dal sistema finanziario e dalla propria banca
- moltiplicare il messaggio attraverso azioni di partnership con le realtà aderenti al progetto

Alcune considerazioni....

Le istituzioni finanziarie aumentano il budget dedicato alla sicurezza, **affinano costantemente i propri sistemi di monitoraggio** e provvedono ad una identificazione continua di nuovi pattern di frode attraverso acquisizione di Indicators of Compromise.

L'evoluzione delle soluzioni di sicurezza (es. SCA) ormai è continua e adattiva per la necessità di cambiare appena si rilevano nuove modalità /vulnerabilità utilizzate dai frodatori.

La sofisticazione delle frodi ormai passa da tecniche miste, ma ogni tecnica non prescinde dalla **manipolazione, diretta o indiretta, dell'utente**

Tuttavia, l'attaccante non compromette i sistemi informativi ma agisce prevalentemente con azioni di social engineering, che la banca può prevenire **solo con campagne di awareness**

Thank You!

CERTFin

Defend.Inform.Evolve.

For more info visit www.certfin.it or write to ricerca@certfin.it