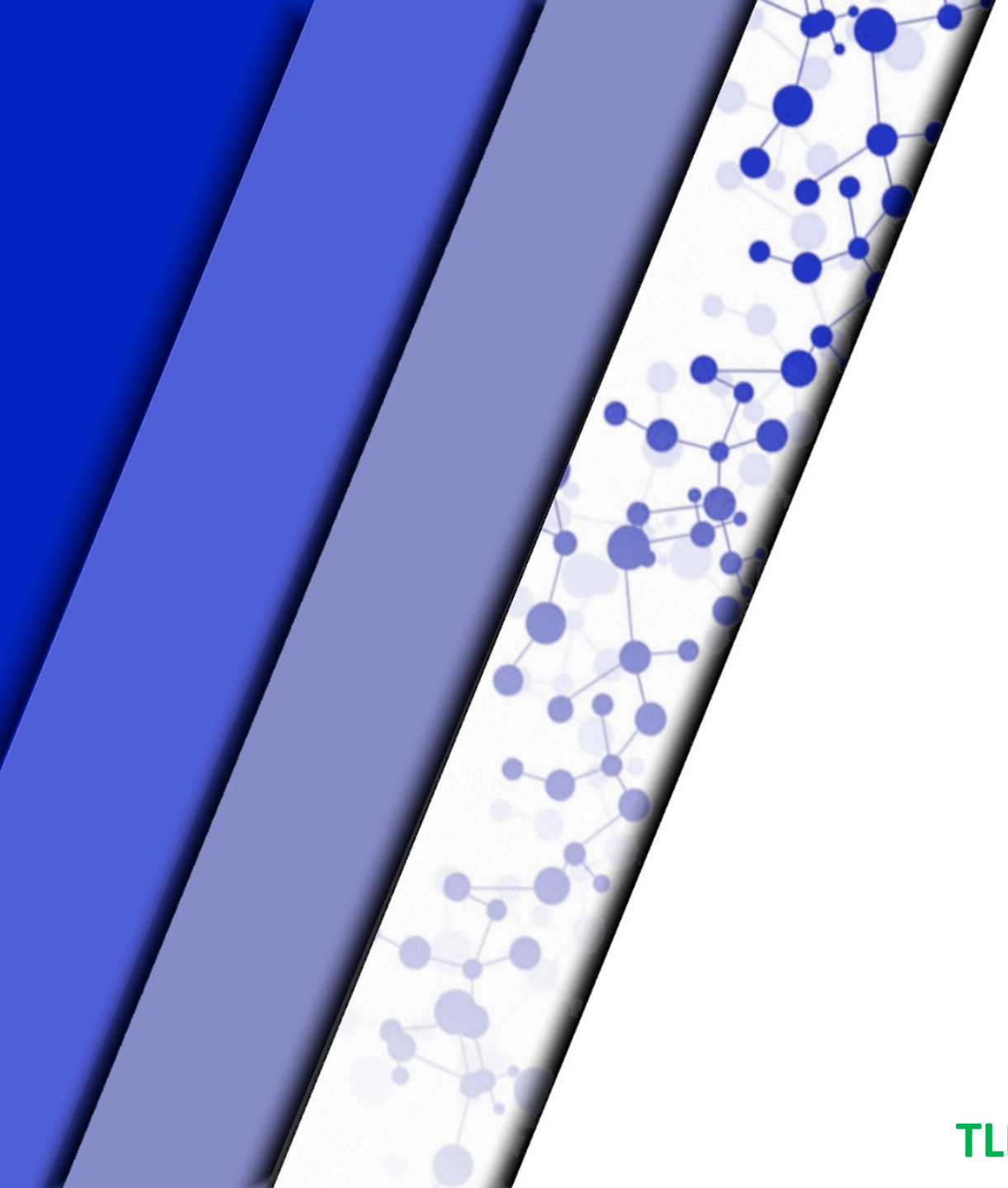


CERTFin

Security Summit 2023

La resilienza operativa del settore finanziario: le nuove sfide presenti e future sulla gestione dei rischi e degli incidenti di sicurezza

Romano Stasi

Chief Operating Officer

TLP GREEN

Digital Operational Resilience Act

- Lo scorso gennaio è stato approvato il nuovo regolamento **DORA**

- Prevede che siano sviluppati dalle ESA oltre **12 RTS** entro gennaio / **giugno 2024** che riguarderanno, fra altro:
  - Articolazione, formati e contenuti dei **Framework di resilienza** operativa ICT
  - Regole e processi per la **classificazione** degli **incidenti** e relative
  - Politiche di gestione e norme di contrattualizzazione e di registro delle **terze parti**,
  - Test armonizzati con **TIBER-EU**

- **L'applicazione** del DORA è prevista per **gennaio 2025** è dunque necessario:
  - avviare subito le attività per implementazione di quanto richiesto da DORA
  - predisporsi per l'integrazione di quanto sarà richiesto negli RTS .

Digital Operational Resilience Act

Tra le principali novità:

- Principi e regole per la gestione del rischio di Terze Parti *
- ….e relativa cornice di sorveglianza coordinate a livello europeo

- Uniformazione su tutte le entità finanziarie dei requisiti di risk management strutturato in 5 fasi: Identification, Protection and prevention, Detection, Response and Recovery

Strategia su rischio terze parti

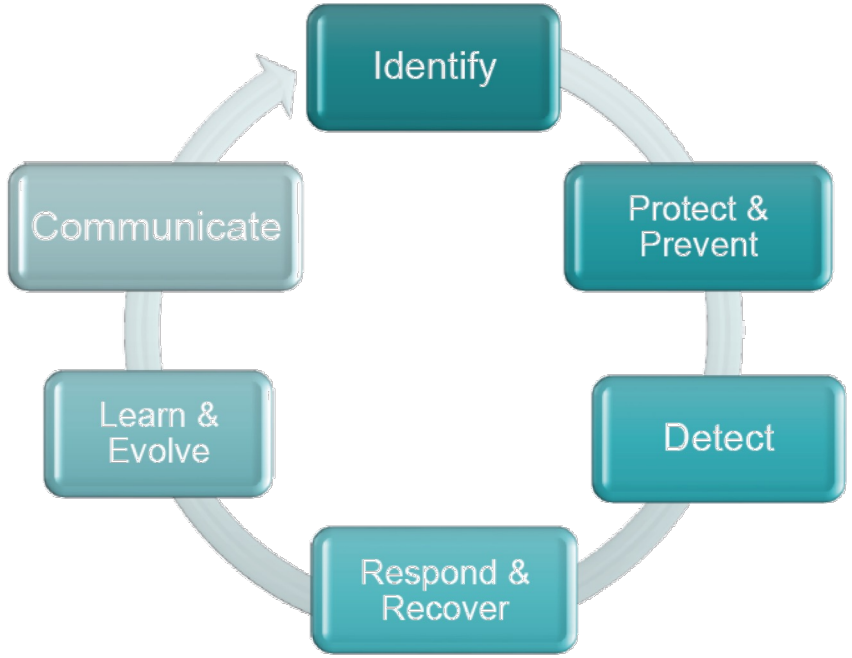
Policy per l'esternalizzazione di **funzioni critiche o importanti**

Rischio di concentrazione con **analisi rischi / costi /benefici** e confronto con soluzioni alternative

Registro di tutti i contratti ICT e relative interdipendenze

Obbligo di **Exit strategies** in caso di esternalizzazione di funzioni critiche o importanti

Attività di **sorveglianza** condotta dalle ESA



Rif. DORA - ICT Risk management (Articoli 5-16).

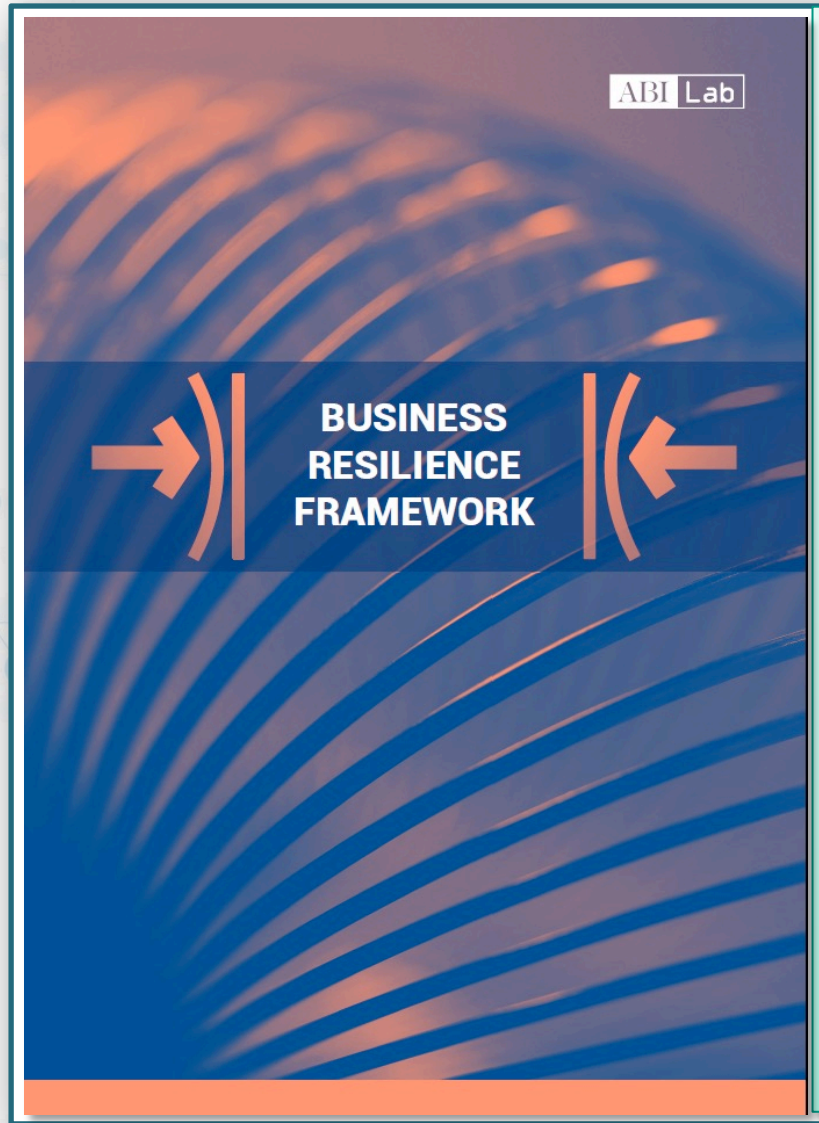
* Necessario lo stabilimento di una sussidiaria su territorio UE per le terze parti qualificate come critiche

Digital Operational Resilience Act

PILLAR	MAJOR INNOVATIONS	Governance	Business functions (Operations)	Compliance	Audit	Business Continuity	Risk Management	Data Protection	Information Technology	Procurement	Communication	Human Resources	Facility and Energy Management	Insurance
ICT RISK MANAGEMENT	Framework of ICT government and risk management uniform for all financial institutions in scope	X	X	X	X	X	X	X	X	X	X	X	X	
ICT MAJOR INCIDENT REPORTING	Harmonise and streamline reporting + extend reporting obligations to all financial entities	X	X	X	X	X	X	X	X		X			
TESTING	Subject financial entities to basic testing or advanced testing (e.g. TLPTs)	X		X	X	X	X		X	X		X		
THIRD-PARTY RISK	Principle based rules for monitoring third party risk, key contractual provisions + oversight framework for critical ICT TPPs	X	X	X	X	X	X	X	X	X			X	X
INFO SHARING	Voluntary exchange of information and intelligence on cyber threats	X					X	X	X					

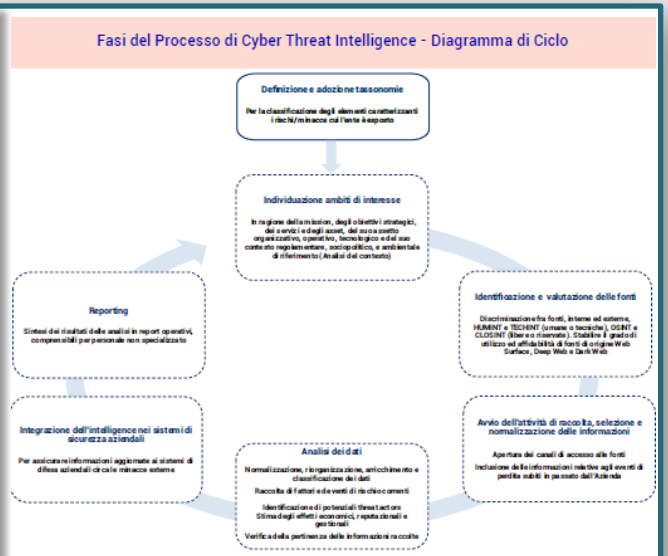
- I requisiti esposti nel DORA riguardano tutta l'organizzazione aziendale a partire dai vertici e coinvolgono esplicitamente, numerose funzioni aziendali
- La resilienza digitale è parte integrante della resilienza operativa dell'intera azienda.

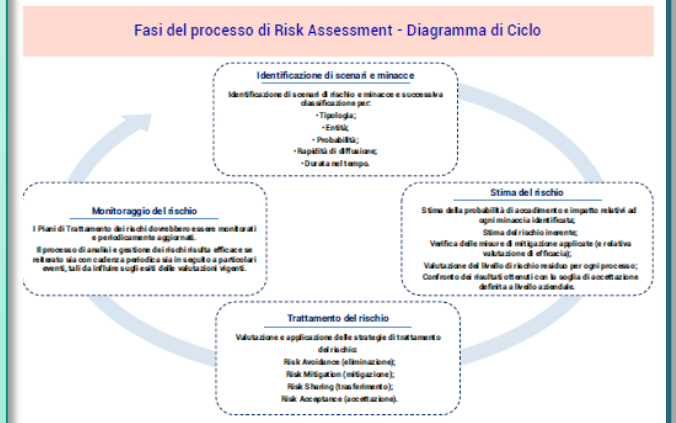
Digital Operational Resilience Act



A supporto del DORA si sta consolidando il **Business Resilience Framework** composto da una collezione di **playbook** di facile consultazione contenenti modelli **operativi** a copertura di tutti i requisiti e tali da:

- suggerire **processi** coerenti con DORA
- descrivere contenuti e metodi di realizzazione per i numerosi **deliverable** richiesti dal DORA
- proporre **misure per valutare** il proprio grado di resilienza
- indurre la adozione **dei principi di resilienza** del DORA oltre il digitale.





Circolare 285/2013 – 40° aggiornamento

Il 2 novembre 2022 la Banca d'Italia ha emanato il **40° aggiornamento delle Disposizioni di vigilanza per le banche (Circolare n. 285/2013)**, modificando il **Capitolo 4** "Il sistema informativo" e il **Capitolo 5** "La continuità operativa" della Parte Prima, Titolo IV, per dare attuazione agli "**Orientamenti sulla gestione dei rischi relativi alle tecnologie dell'informazione (ICT) e di sicurezza**" (EBA/GL/2019/04) emanati dall'EBA.
Le banche dovranno adeguarsi alle nuove disposizioni entro il **30/6/2023**.

BANCA D'ITALIA

Tra le principali novità, si evidenziano, sul fronte IT e Sicurezza:

- Definizioni («**rischio ICT e di sicurezza**» e «**incidente operativo e di sicurezza»**)
- Concetto di «**strategia ICT**»;
- **Piano di formazione e di sensibilizzazione** sulla sicurezza dell'informazione;
- **Funzione di controllo dei rischi ICT e di sicurezza**;
- Paragrafo sulla **Gestione del rapporto con gli utenti dei servizi di pagamento.**

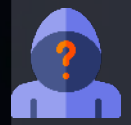
Panorama delle minacce

TLS 2022 – H2

Ripercussioni geopolitiche

Gli eventi geopolitici condizionano l'attuale panorama delle minacce cyber. Le organizzazioni finanziarie devono monitorare lo sviluppo e le vicende legate all'attuale conflitto in corso per anticipar e prevenire tempestivamente attacchi cyber. Organizzazioni italiane di diversi settori sono state oggetto di operazioni cyber rivendicate da gruppi hacktivist.

Compromissione delle terze parti e supply chain

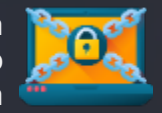


La compromissione delle terze parti è un fenomeno in crescita e che può avere ripercussioni per organizzazioni di ogni settore. Tali compromissioni spesso causano violazioni di dati e possono anche provocare effetti devastanti in caso di attacchi di tipo *supply-chain.* Tale minaccia solleva grandi preoccupazioni a causa della difficoltà nel garantire che tali organizzazioni adottino elevati standard di sicurezza.

Attacchi DDoS

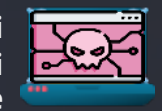
Nel corso del 2022, gruppi filorussi (e.g., Killnet e NoName057(16)) hanno rivendicato diversi attacchi DDoS aventi come obiettivo diversi siti istituzionali italiani, nonché diversi PSP italiani. Entrambi i gruppi sono guidati da motivazioni geopolitiche.

Ransomware



Il ransomware ha consolidato nuovamente la sua onnipresenza nel panorama delle minacce cyber, con LockBit 3.0 in cima alla classifica dei ransomware più attivi del periodo. I ransomware stanno evolvendo in termini di evasione, rafforzando al contempo le tecniche volte a trasmettere una maggiore pressione alla vittima, al fine di costringerla al pagamento.

Wiper Malware



Threat actor russi hanno utilizzato massivamente malware distruttivi (*wipers*) per danneggiare infrastrutture critiche. A differenza dei tipici attacchi ransomware, gli attacchi wiper sono di natura distruttiva e non comportano un riscatto.

Sfruttamento di vulnerabilità 0-day

Nel corso del 2022, i threat actor hanno continuato a sfruttare le vulnerabilità note e 0-day nei loro attacchi cyber per ottenere l'accesso alle reti target. Le vulnerabilità sfruttate sono critiche e interessano prodotti ampiamente utilizzati.

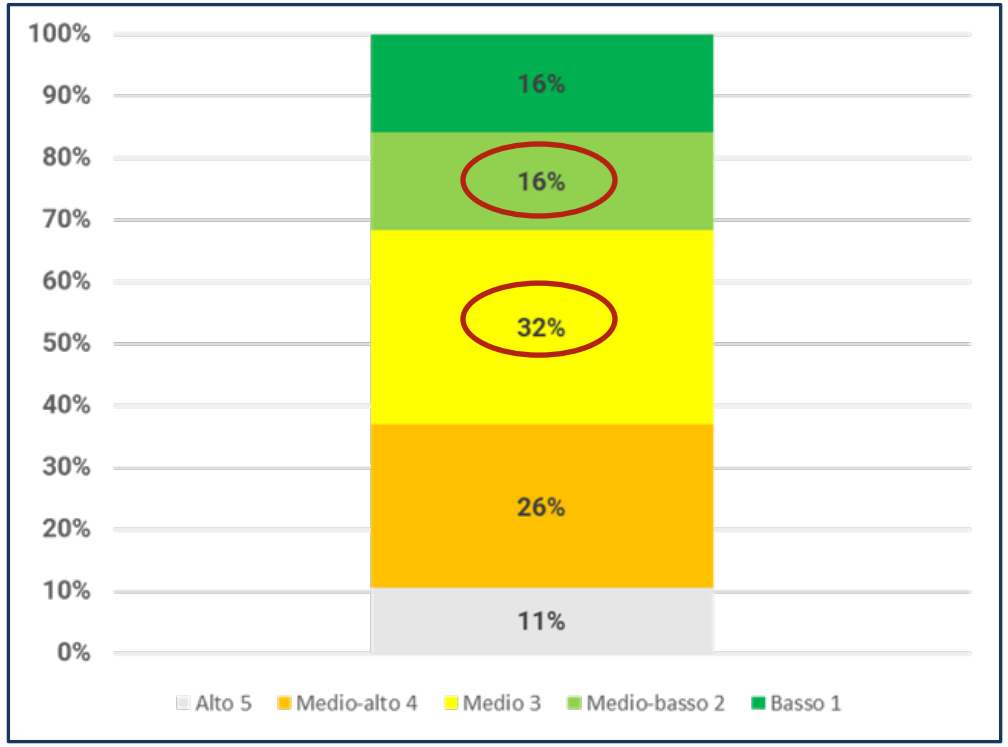
Minacce rivolte agli utenti finali

Durante la seconda metà del 2022 è stato osservato un aumento significativo di applicazioni malevole (*droppers*) sugli store ufficiali (e.g., Google Play Store) volte a veicolare malware per dispositivi mobili. Tra le app malevole individuate figurano Vultur, Sharkbot e Teabot. È stato inoltre osservato l'impiego del trojan bancario, Ramnit, per la compromissione di perimetri corporate.

Rischi cyber: azioni e contromisure 1/2

Il conflitto in corso tra Russia e Ucraina ha avuto **ripercussioni sul panorama delle minacce cyber.**

In questo contesto le banche italiane, **nell'ambito della valutazione dei rischi cyber**, hanno iniziato a considerare come elemento di rilevanza anche **l'evoluzione degli eventi geopolitici.**

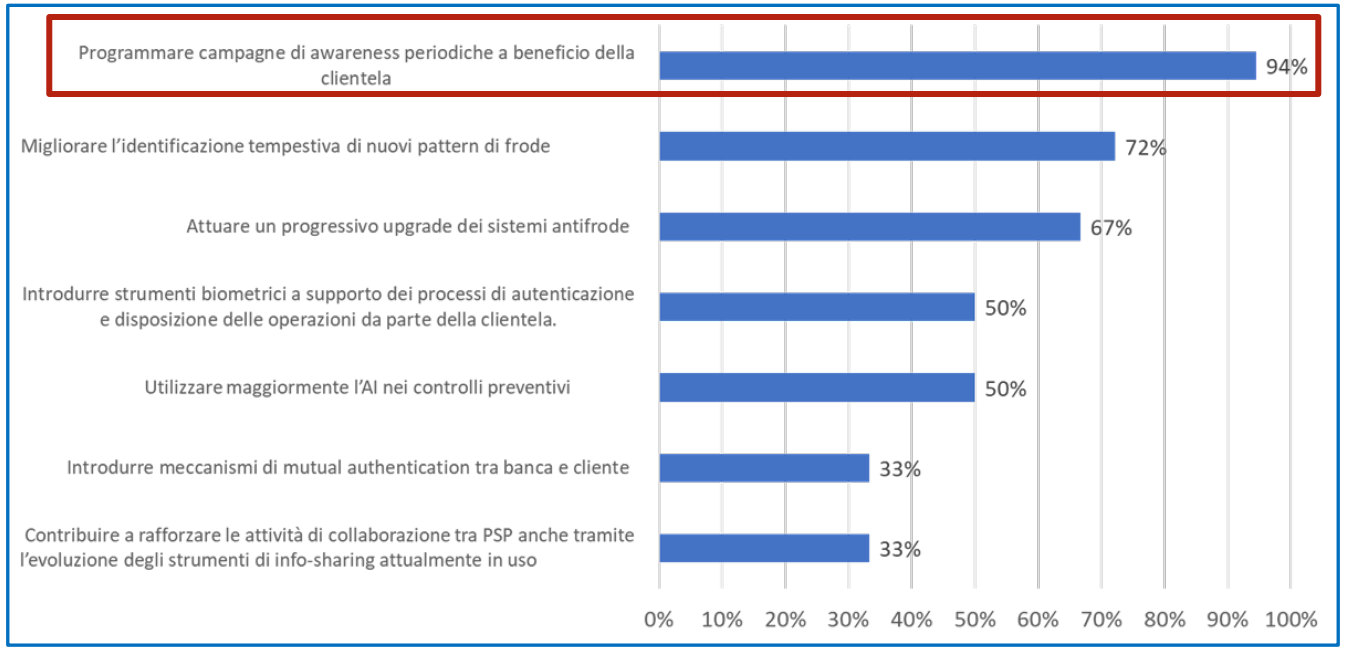


Fonte: ABI Lab, Rilevazione sulle priorità ICT delle banche italiane, marzo 2023, 19 rispondenti.

Nell'ambito della valutazione dei rischi cyber, il 48% dei rispondenti assegna all'evoluzione degli eventi geopolitici, un livello di rilevanza medio o medio-alto.

Rischi cyber: azioni e contromisure 2/2

In prospettiva, gli operatori finanziari sembrano volersi **concentrarsi maggiormente sulle vulnerabilità non del tutto controllabili** come, ad esempio, il **«fattore umano»** sia in relazione ai dipendenti che alla clientela.



Fonte: ABI Lab, Rilevazione sulle priorità ICT delle banche italiane, marzo 2023, 20 rispondenti.

Nell'arco del 2023, in ambito anti-frode, il 94% dei rispondenti intende programmare campagne periodiche di awareness verso la clientela, mentre in ambito prevenzione degli attacchi ransomware, il 90% dei rispondenti intende attivare iniziative di awareness verso il personale dipendente.

Ransomware Playbook

In linea con i risultati delle ultime analisi che caratterizzano l'attuale scenario di minaccia, la Direzione Operativa del CERTFin ha ritenuto opportuno redigere un *playbook* dedicato alla gestione degli attacchi ransomware con l'obiettivo di:

- Supportare i team di sicurezza informatica nel pianificare adeguati processi per gestire un possibile attacco ransomware;
- Analizzare le tre fasi principali che caratterizzano la gestione di un attacco: **preparazione**, **risposta** e **ripristino**;
- Facilitare la definizione delle politiche interne da attuare in caso di attacco;
- Fornire una panoramica degli strumenti di mitigazione esistenti (tecnologie, chiavi di decrittazione, strumenti di cyber insurance, ecc.).

Hanno partecipato alla redazione del playbook 8 istituti bancari e 2 imprese assicuratrici operanti sul mercato italiano

I Navigati
2a vague

Alla fine del 2021 si è svolta la prima campagna di cybersecurity awareness del CERTFin che ha coinvolto, oltre a Banca d'Italia, IVASS e ABI, 12 banche e compagnie assicurative: **I NAVIGATI - Informati e sicuri**.

Nel 2022 con Banca d'Italia, IVASS, ABI e un numero ancora maggiore di aderenti, avrà luogo una ripresa della campagna.

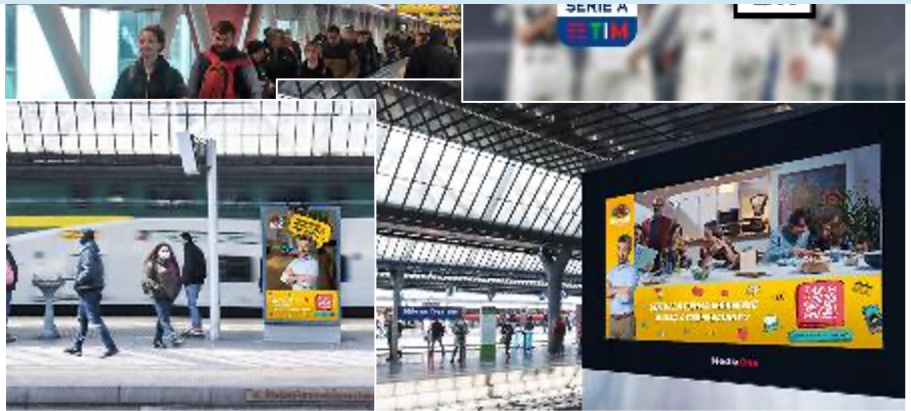
Nel 2021 gli spot e la web serie de' i Navigati sono stati promossi su tv, radio, stampa, web e social, anche grazie al supporto dell'ACN e del DIE (Dipartimento per l'Editoria della PCM).

Nel 2022 I Navigati torneranno sui canali più performanti della campagna 2021 e su nuovi canali, per farsi conoscere da sempre più persone.

MATERIALI 2022

- **Review sito web**
- **Review materiali social**
- **Review Video**
- **Review banner Display**
- **Review materiali rete fisica**
- **Nuovi contenuti per out of home**
- **Nuovi contenuti vishing & spoofing**
- **Nuove video interviste**
- **Nuovo Trailer**
- **Nuovo Leaflet**

A PARTIRE DA METÀ OTTOBRE LA FAMIGLIA NAVIGATI TORNERÀ ON AIR



PIANO MEDIA 2022

- **SOCIAL**
(facebook, instagram, linkedin)

- **DIGITAL**
(youtube, display banner/video)

- **DOOH**
(out of home e digital out of home su circuiti GO TV e MUPI)

- **TV DAZN**
(2 turni / 7 giornate serie A calcio)

I Navigati
primi risultati

Campagna di cybersecurity awareness a cura del CERTFin in coll. con Banca d'Italia, ABI, Ivass e 16 soggetti bancari.

NUOVI MATERIALI:

- trailer di lancio della webserie;
- leaflet per web e stampa sulle maggiori frodi;
- infografiche e video infografiche su vishing e spoofing (via sms e tel.);
- otto video con i suggerimenti per proteggersi dalle diverse tecniche di frode;
- nove video realizzati in collaborazione con l'influencer Marco Camisani Calzolari;
- sette nuove videointerviste agli esperti di cybersecurity delle realtà aderenti alla campagna.

DAZN: 20 passaggi, spot 15"
audience (totale dei telespettatori) : 12,6 MLN

DOOH: circuiti Go TV, DigiMupi, Mupi - N. impianti: 1360 - Pianificazione: 3 settimane - Reach: flusso 30 MLN

DIGITAL DISPLAY: 59 MLN visualizzazioni - CTR medio: 0,40%

YOUTUBE: 6,5 MLN visualizzazioni
Completion rate (visualizzazioni del video per tutta la sua durata): 55% - CTR: 0,12%

SOCIAL:

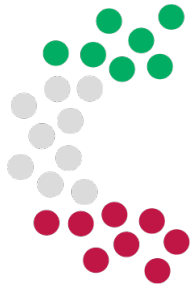
- Copertura Pagina (numero di utenti unici che hanno visualizzato la pagina): FB 1,078 MLN - IG 702.000 - Sponsorizzate 1,5 MLN
- Copertura Post Facebook: 60.382 - Interazioni: 2.778
- Copertura Post Instagram: 701.773 - Interazioni: 754

LANDING PAGE: 280.000 visite (70,3% da campagne digital, 26,6% ingressi diretti, 1,5% da altri siti web, 1,3% da social, 0,4% motori ricerca)

Key Messages

- **Risorse:** Continuare a garantire che i *response team* siano adeguati, attraverso investimenti utili a rafforzare le strutture difensive in modo da mantenerle sempre adeguate ad affrontare uno scenario delle minacce in costante evoluzione.
- **Consapevolezza**: Prevedere continue azioni di awareness per sensibilizzare sia la clientela, sia il personale dipendente della banca, sul corretto uso degli strumenti digitali e sul rispetto delle buone pratiche necessarie ad evitare fenomeni di frode e a preservare dati personali e finanziari
- **Resilienza:** In un panorama in continua evoluzione, un approccio pragmatico e flessibile alla resilienza operativa è necessario per di rispondere, adattarsi e indirizzare differenti scenari di rischio - non sempre prevedibili a priori - e quindi mitigare eventuali impatti negativi, potenzialmente anche gravi.

Thank You!



CERTFin

Defend. Inform. Evolve.

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