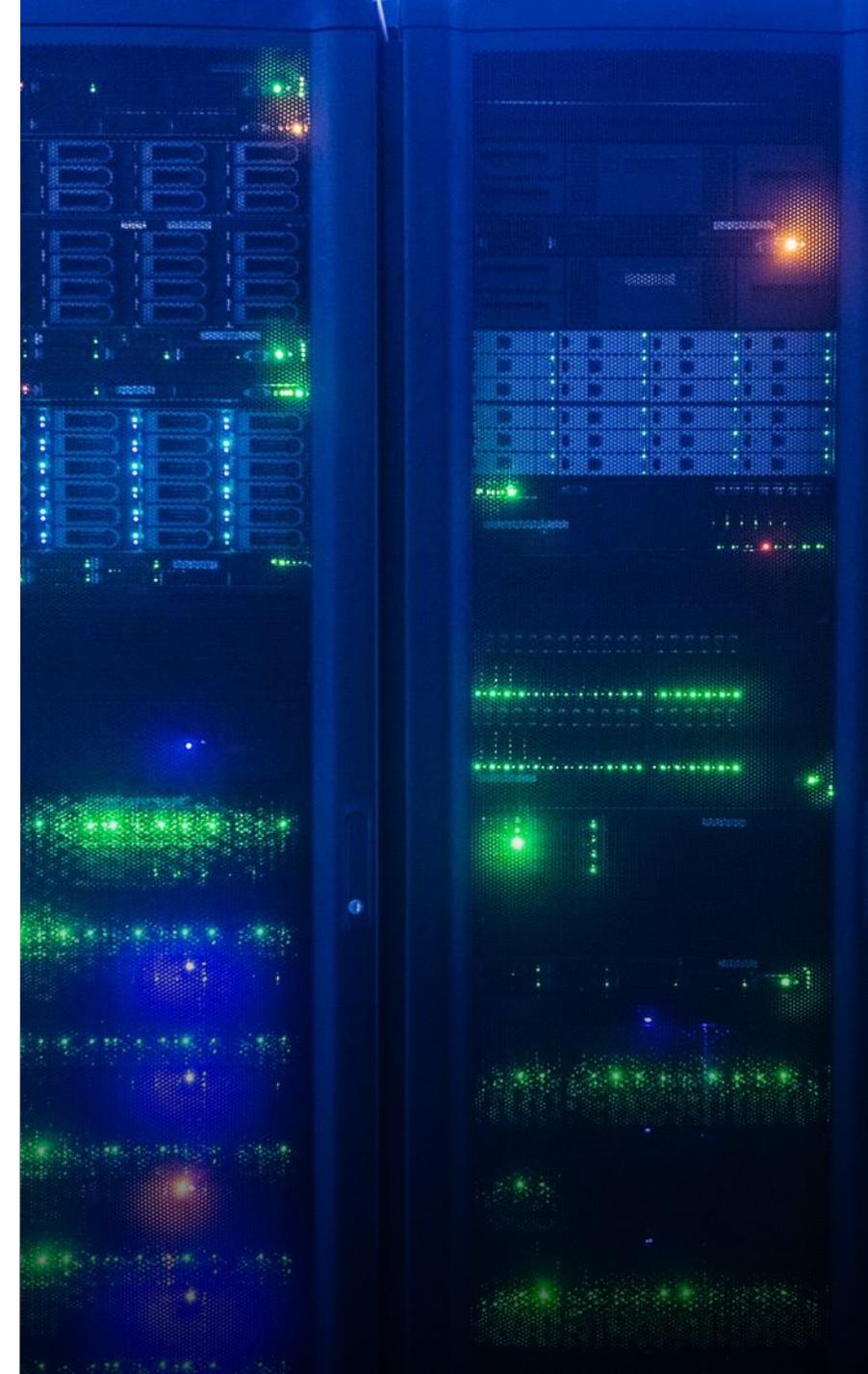


# ABI Banche e Sicurezza 2022

## Panel I - Ecosistema della sicurezza: un virtuoso rapporto tra pubblico e privato

---

Paolo Carcano, Partner – Head of Cybersecurity & Privacy FS  
19 maggio 2022



# The New Equation

Community of solvers

Building  
trust



Delivering  
sustained  
outcomes

Human-led and tech-powered

Delivering quality

Community of solvers



La nostra nuova strategia globale pone al centro persone, processi, tecnologia e promuove il dialogo tra tutti gli stakeholder allo scopo di affrontare temi importanti

# Italia 2022: Persone, Lavoro, Impresa

#TheNewEquation



Abbiamo sviluppato negli ultimi anni una piattaforma di dialogo, in collaborazione con il gruppo editoriale GEDI, per condividere **idee, sviluppare proposte e progettare azioni coinvolgendo i massimi esponenti del mondo delle istituzioni, della finanza e dell'impresa**, ascoltando e facendo tesoro, di volta in volta, delle testimonianze di imprenditori che hanno saputo, creando valore, scrivere la storia economica ed industriale del nostro Paese

## Italia 2021

### Competenze per riavviare il futuro

Temi trattati: L'energia, l'industria, il turismo, la mobilità, il rilancio dei costumi, la finanza, le infrastrutture, I media, NGEU, Smartworking, ASEAN, il settore immobiliare

## Italia 2021

### È tempo di ricostruire

Temi trattati: come ricominciare, persone il vero motore della ripartenza, un paese sostenibile, il piano, missione PNRR, PNRR e riforme verso il futuro

## Italia 2022

### Persone, Lavoro, Impresa

Temi trattati (primi 3 incontri): crisi Ucraina e riflessi sull'economia, quale paese per l'impresa, Mercato e regole

# Cyber resilience: le iniziative svolte nell'ambito degli Other Trusted Services (OTS) di PwC a vantaggio del mercato FS

## Gestione del rischio E2E nel contesto evolutivo della normativa EU

**Dialogo tra le funzioni di controllo Cyber, Risk, Compliance e Audit** per la valutazione dell'evoluzione dei modelli organizzativi per il presidio del Cyber Risk con un confronto tra top management e istituzioni così da guidare l'evoluzione dei modelli nel contesto FS

## Servizi di Threat Intelligence & Incident response per le FSI

**Proposizione proattiva** dei nostri **report di TI&IR** al mercato FS in occasione di **importanti discontinuità** tra cui

- Log4J
- Spring4Shell
- Crisi Ucraina

## CyberAwareness (Evento CTF promosso dal CERTFin)

Organizzazione del primo **Capture the Flag** promosso da **CERTFin** per il **mercato FS** con alcuni tra i principali operatori di settore

## DORA Integrated Solution (Pillole e Survey)

**Monitoraggio dell'evoluzione normativa**, organizzazione di un **team composto da competenze trasversali** tra cui Legal, Risk & IT Gov e guidato dalla Cyber. **Pubblicazione di 6 Pillole tematiche** per aumentare la consapevolezza del mercato e **avvio di una survey** verso alcuni tra i principali operatori FS per ABI Banche e Sicurezza

# DORA: le nostre Pillole e la Survey per ABI Banche e Sicurezza

## Pillole di DORA

### Digital Operational Resilience Act

La Digital Operational Resilience Act (DORA) come nuovo paradigma europeo per un'efficace ed omnicomprensiva gestione dei temi Cybersecurity ed ICT nel Financial Services, secondo una visione olistica End-to-End basata sull'integrazione dei rischi e che comprende il presidio delle terze parti.

**#6** Governo e Gestione delle Terze Parti  
DORA si ispira ai principi TPRM nel presidio delle Terze Parti, introducendo inoltre nuovi poteri per le Autorità di Vigilanza.

**#5** Digital Operational Resilience Testing  
DORA definisce un programma onnicomprensivo di test di resilienza operativa digitale comprendendo gli aspetti Cyber ed inclusivo delle logiche Tiber EU.

**#4** I presidi delle prime linee di difesa ICT e Cybersecurity  
Le Responsabilità delle 1e Linee di Difesa Cybersecurity ed ICT nel presidio End-to-End dei Rischi introdotto dal Regolamento EU DORA.

**#3** La Gestione degli Incidenti ICT e Cybersecurity  
DORA evolve la gestione degli incidenti IT e Cyber, richiamando le best practice, ed introducendo novità per la comunicazione e segnalazione alle Autorità.

**#2** Operational Resilience e le interconnessioni con il framework di Risk Management  
Visione End-to-End del modello di Gestione dei Rischi Operativi, ICT e Cyber come game changer del Regolamento EU DORA.

**#1** Contesto di mercato ed implementazione del Regolamento  
La view PwC sul contesto del Regolamento EU DORA, una priorità per i Financial Services date le novità in ambito Rischi Operativi, ICT e Cybersecurity.

## DORA Survey

✓ Banking

✓ Asset & Wealth Management

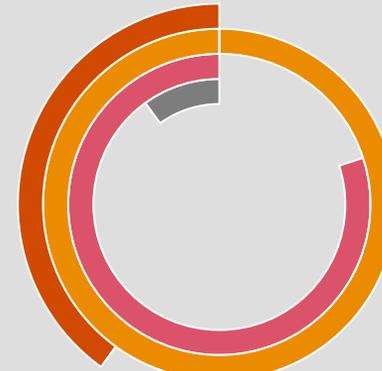
✓ Insurance

**12** Domande

**30** Entità coinvolte

### La vostra percezione del Regolamento DORA

Q12 - Come viene percepita l'imminente emanazione del Regolamento DORA?



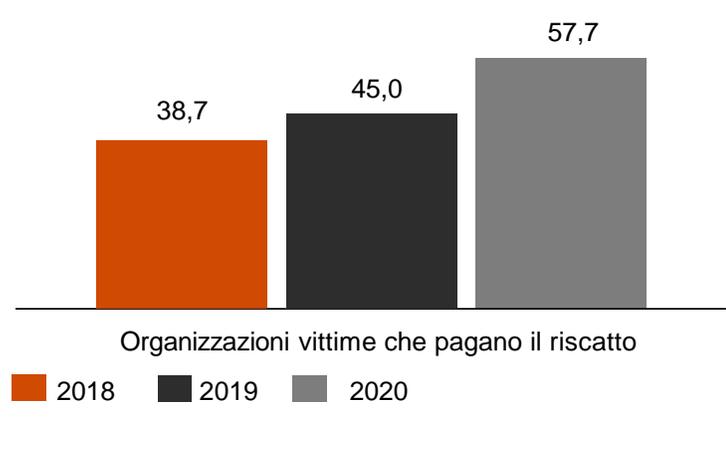
- Over regulation (40%)
- Opportunità per attivare temi legati alla Cyber Hygiene (100%)
- Opportunità per evidenziare l'importanza delle competenze e dello staffing cyber (50%)
- Opportunità per visibilità verso il BoD/Top Management (6%)

**Sessione Parallela F**

Evolvere in sicurezza: nuovi strumenti per la resilienza operativa con **Samantha Trama**, Senior Manager di PwC

# Ransomware: the "Pay or not to Pay" dilemma

L'ingente numero di attacchi Ransomware realizzati nel 2020 ha comportato un incremento significativo del numero di aziende che hanno pagato per riottenere l'accesso ai propri sistemi<sup>1</sup>. Secondo un'indagine condotta da Chainalysis anche l'importo totale pagato dalle vittime di Ransomware è aumentato, a livello globale, del 311% nel 2020, raggiungendo quasi 350 milioni di dollari di criptovaluta.



1 | Sophos - The State of Ransomware 2021

2 | Nel mese di Maggio 2021, il Gruppo assicurativo AXA ha interrotto i risarcimenti inerenti i «ransomware payment»

 Razionale Positivo

 Razionale Negativo



## The Pay or Not to Pay Dilemma

La decisione di pagare il riscatto può essere condizionata dai seguenti razionali:



Il pagamento di solito funziona e consente di recuperare i dati (65% dei casi<sup>2</sup>);



Volontà degli hacker di onorare le promesse di ripristino per costruire un'idea di trust nel poter pagare;



Pagare, incoraggia l'invio di altri ransomware;



Non esistono garanzie che i dati verranno restituiti dopo il pagamento;



Sempre meno assicurazioni sono disposte a risarcire i costi generati dalle «cyber extortion»<sup>2</sup>;



In forte ascesa il nuovo trend della «doppia estorsione»;



Il pagamento potrebbe inoltre comportare il sovvenzionamento di gruppi terroristici e pertanto configurarsi come fattispecie di reato.

Pagare il riscatto può sembrare il modo più semplice e veloce per porre fine all'attacco e recuperare i dati aziendali. **PwC non consiglia** di percorrere questa strada per diverse **ragioni** di ordine **morale, etico e legale**, ma raccomanda piuttosto che le problematiche poste da un attacco ransomware vengano analizzate e affrontate da un apposito **tavolo di sicurezza** opportunamente predisposto all'interno di ciascuna organizzazione, meglio ancora se con il **supporto delle Istituzioni**.

# #TheNewEquation La Cybersecurity per l'innovazione sostenibile

Coerentemente con quanto formalizzato nella nostra #TheNewEquation, sono numerosi i temi Cyber sui quali come PwC ci presentiamo al mercato FS con soluzioni e paradigmi pensati per affrontare in modo concreto ed efficace temi di grande interesse e che richiedono il coinvolgimento delle istituzioni:



Integrazione del process mining nei processi antifrode

**Sessione Parallela A**  
Frodi e furto d'identità nel settore finanziario:  
il fattore umano e tecnologico nella vita privata e in azienda con **Dante Niro**, Senior Manager di PwC

# Grazie

**Paolo Carcano**

Partner – Head of Cybersecurity & Privacy FS

+39 334 6896335

paolo.carcano@pwc.com

[pwc.com/it](https://pwc.com/it)

© 2022 PricewaterhouseCoopers Business Services Srl. All rights reserved. PwC refers to PricewaterhouseCoopers Business Services Srl and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](https://www.pwc.com/structure) for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.