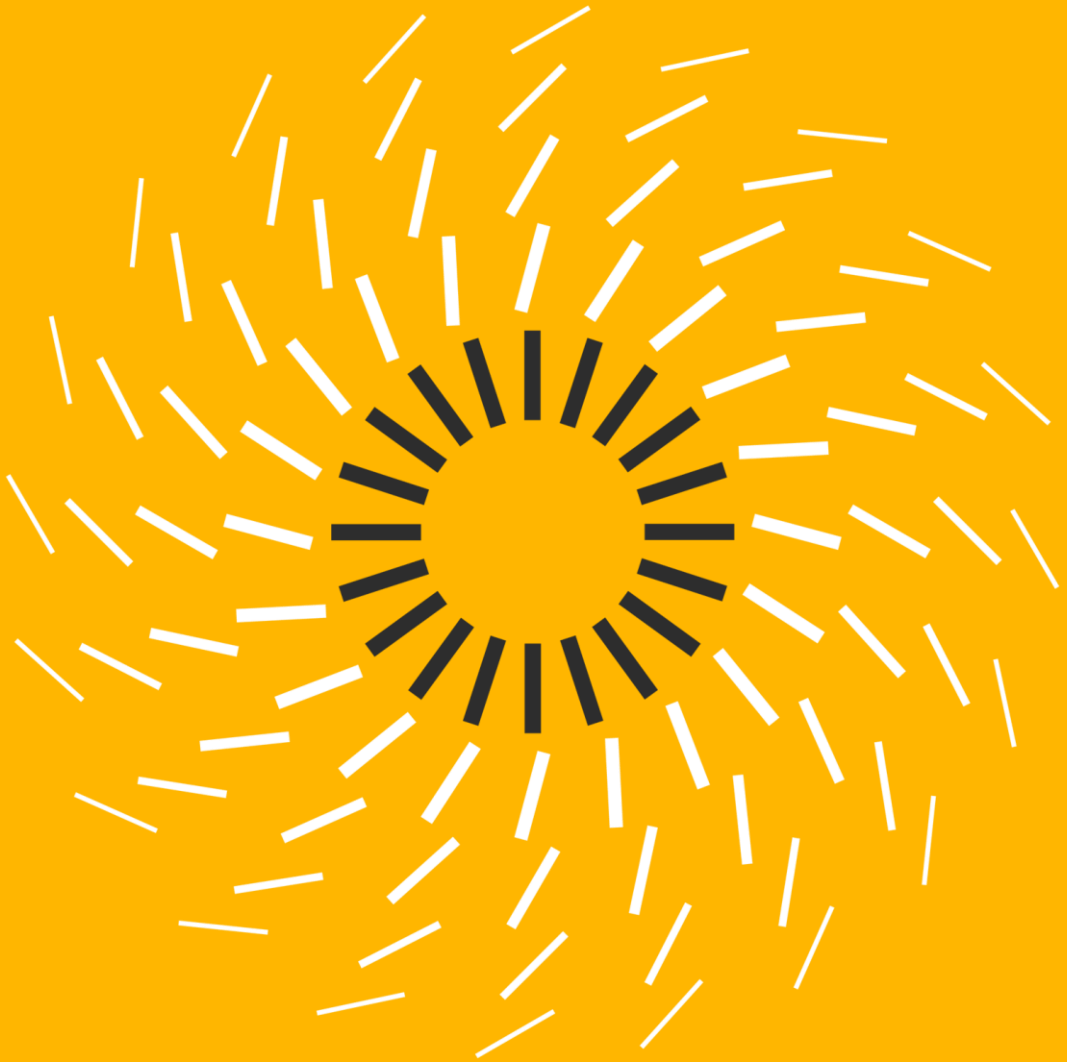
ABI Banche e Sicurezza 2023
Sessione Plenaria

Minacce cyber e paradigmi per la resilienza del sistema finanziario

Milano, Auditorium Bezzi - Banco BPM
16 maggio 2022



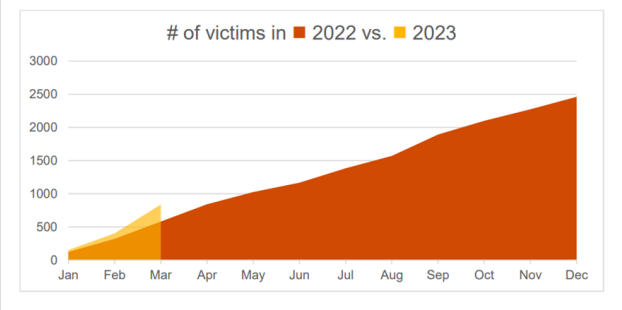
pwc

L’impatto degli attacchi Ransomware può essere catastrofico

Ransomware represents one of the **most persistent and critical risks** to any organisation, particularly in relation to human-operated campaigns which seek to **steal, encrypt, and threaten to leak victim data**.

PwC’s Global Threat Intelligence team

RANSOMWARE



2462 victims leaked in 2022

Top 10 sectors	# victims	% victims
1. Manufacturing	365	15%
2. Construction	248	10%
3. Professional Services	225	9%
4. Retail	203	8%
5. Technology	191	8%
6. Hospitality & Leisure	127	5%
7. Education	125	5%
8. Healthcare	122	5%
9. Government	112	5%
10. Logistics	85	3%

- Data recovery: spesso è possibile **ripristinare solo in parte** i dati cifrati.
- Il ripristino dei dati da file di backup e di recovery: **può richiedere settimane.**
- Tecniche di attacco: I threat actors **evolvono le tecniche** in funzione delle soluzioni di sicurezza.

Tempo medio di interruzione: **3 settimane**

- Perdita di business,
- Costo delle remediation,
- Danno reputazionale,
- Costi legali e sanzioni in caso di violazione dei dati personali

Catastrophic Cyber Attack - la percezione delle aziende e le iniziative delle Autorità

World Economic Forum: The Global Cyber Outlook 2023

Un **evento Cyber catastrofico** è almeno in qualche modo **probabile nei prossimi due anni**.

PwC 2023 Global Digital Trust Insights

Un **evento Cyber catastrofico** è lo **scenario maggiormente temuto** nel 2023 secondo 3,522 chief in ambito business, technology e security.

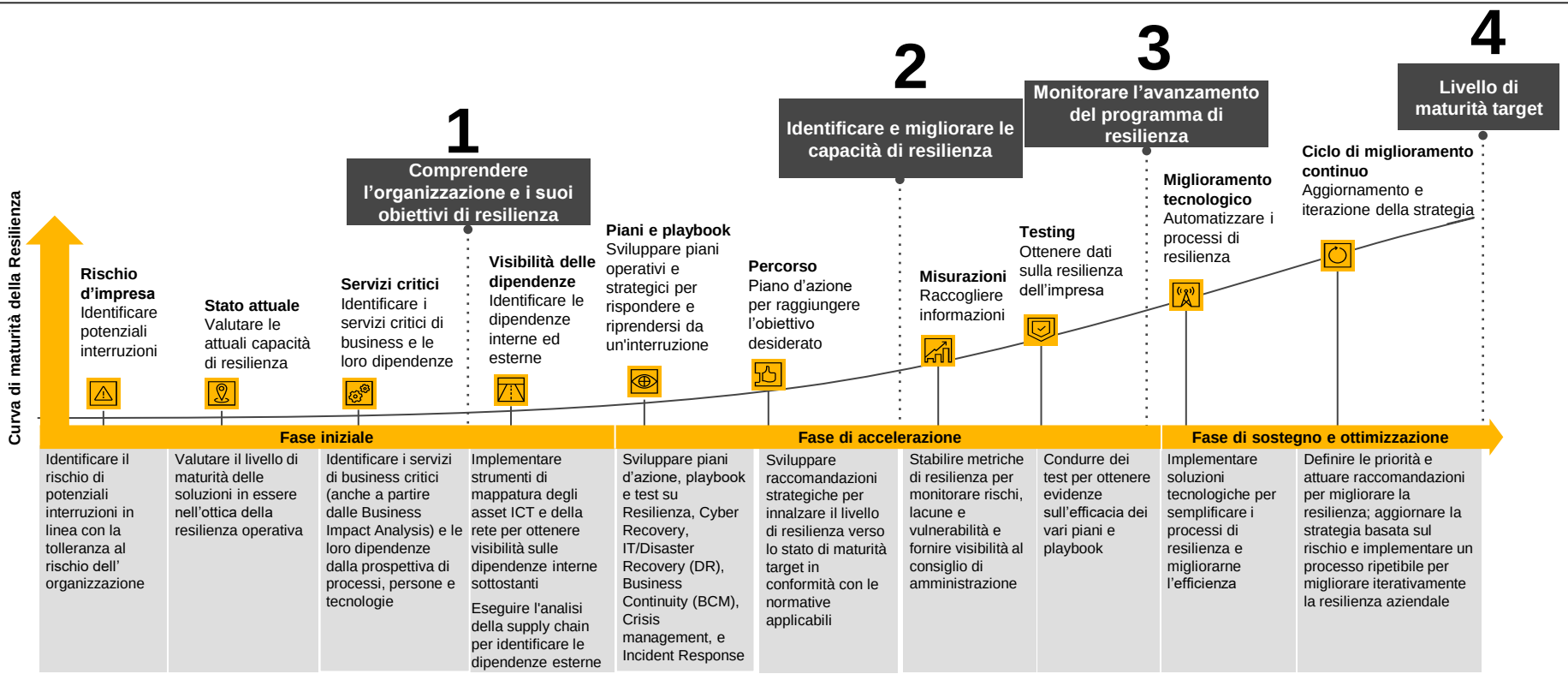
Financial Times - 10 marzo 2023

La ECB lancerà "uno **stress test tematico** sulla resilienza informatica" su tutte le 111 banche che vigila.

ECB Banking Supervision: SSM supervisory priorities for 2023-2025

Rafforzare la Resilience del sistema finanziario è tra le priorità ispettive di ECB.

Il percorso Risk-Based verso la Resilience



Tali sfide sono indirizzate da un programma di compliance DORA

Priorità 1
Iniziative di impostazione del Programma DORA o senza dipendenze dagli RTS

- Strategia Resilienza
- Metodologia Funzioni critiche e importanti
- Threat e scenario modelling
- Mappatura dei Servizi ICT
- Definizione soglie di tolleranza
- Mappatura servizi di business

Priorità 2
Iniziative di impostazione e messa a terra delle evoluzioni dei modelli di gestione e delle tecnologie

- Evoluzione Framework Gestione dei Rischio Operativi, ICT/Cyber
- Sicurezza logica, fisica, infrastrutture, security by design *(incl. Network segregation)*
- Evoluzione Framework Continuità Operativa
- Incident and Event Management
- Evoluzione processi IT Delivery, CMDB e mappatura interdipendenze
- Mappatura fornitori Servizi ICT
- Rafforzamento presidi di Infrastructure & op. resilience
- Backup strategy e nuove tecnologie *(incl. Backup vaulting)*

Priorità 3
Iniziative da attivare a complemento della messa a terra dei modelli di gestione e tecnologie

- Implementazione Framework TPRM
- Implementazione Framework Gestione del Rischio ICT/Cyber
- Aggiornamento contratti Servizi ICT
- Test di resilienza Operativa digitale
- Exit Strategies
- Evoluzione presidi di Change Management

Priorità 4
Iniziative di reporting e consolidamento della strategia di resilienza digitale

- KPI e Dashboarding Framework Resilienza integrato
- Comunicazione interna ed esterna
- Reporting alle Autorità

Legenda
- CISO / Sicurezza Informatica
- CRO / Operational Risk
- CIO / Funzione ICT
- Procurement / Uff. Outs./Terze Parti
- Organizzazione
- Legal
- Business Continuity
- Funzioni di Business

I fornitori possono giocare un ruolo fondamentale per la Resilience e devono essere coinvolti nell'indirizzo dei requisiti DORA

Comportare impatti operativi in caso diventino vittime di attacchi cyber

Richiedere la definizione di specifiche clausole contrattuali nel contesto di un processo di TPRM

Essere vigilati direttamente dall'Autorità nel contesto dei requisiti DORA

Fornire servizi a valore aggiunto per la resilience e la compliance DORA

DORA introduce la sorveglianza regolamentare individuale per ICT TPP

Requisiti

Impatto sistemico su **larga scala** in caso di disservizio del fornitore	**Grado** di **sostituibilità** del **fornitore**
Numero di istituzioni di importanza **sistemica** a livello **globale /interdipendenza** tra esse ed altre entità cui il fornitore presta servizi ICT	**N. di Stati membri** in cui il **TPP fornisce servizi**
Rischio di **concentrazione**	**N. di Stati membri** in cui operano **imprese** che sono **supportate dal fornitore**

Autorità di **Sorveglianza Capofila**

Nominata tra EBA, ESMA o EIOPA sulla base del valore delle attività delle Entità finanziarie che utilizzano i servizi ICT del fornitore critico.

Sorveglianza Individuale →

Fornitore ICT designato **critico**

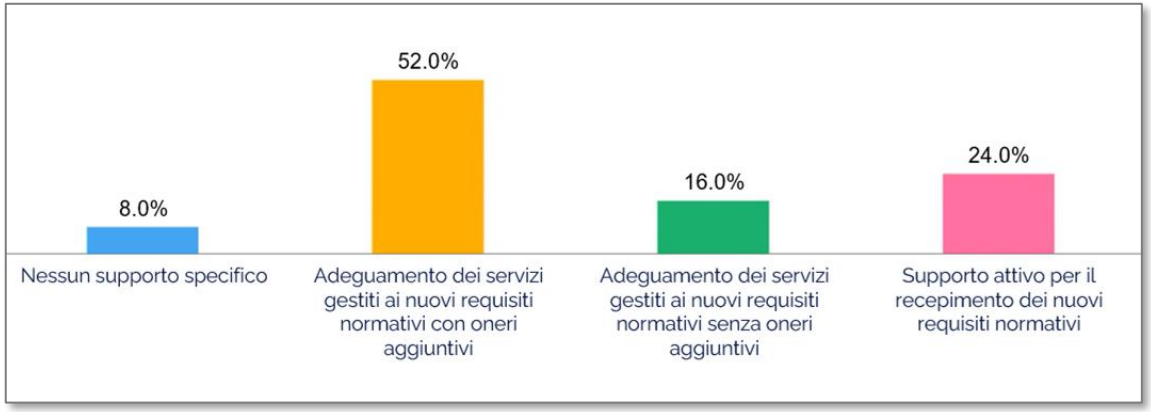
- **Richiesta** di **informazioni** e **documentazione** rilevanti;
- Conduzione di **indagini ed ispezioni**;
- **Richiesta** di **relazioni** successive alle attività di vigilanza ove il fornitore critico relazioni in merito alle **azioni di rimedio** intraprese;
- **Formulazione di raccomandazioni** verso il **fornitore critico** per ridurre al minimo il possibile impatto sistemico;
- **Applicazione di** una **penalità di mora*** per imporre al **fornitore** critico il **rispetto** del quadro di sorveglianza;
- **Richiesta di Risoluzione** degli **accordi contrattuali con le imprese** interessate in caso il fornitore critico si opponga ad un'ispezione.

Valutazione dell'esistenza di **policy, procedure** e **presidi** solidi ed efficaci per la **gestione End-to-End dei rischi ICT e Cyber:**

- Capacità di garantire **sicurezza**, **disponibilità**, **continuità**, **scalabilità** e **qualità** dei **servizi**;
- Capacità di mantenere **standard di sicurezza**, nonché **riservatezza** e **integrità** dei dati;
- Processi efficaci di **gestione del rischio**;
- Strutture **organizzative**, **modelli operativi** e presidi di **governance**;
- **Meccanismi** per garantire l'effettivo **esercizio dei diritti di risoluzione/ recesso (**es. portabilità di dati/applicazioni);
- **Test** di sistemi, infrastrutture **ICT** e modelli di **controllo** e **monitoraggio**.

** In caso di mancata compliance, le penalità di mora verranno calcolate nella misura dell' 1% del fatturato medio quotidiano realizzato a livello mondiale dal fornitore terzo di servizi di TIC critico nel precedente esercizio.*
Le Autorità di Vigilanza possono comunicare pubblicamente la penalità di mora applicata.

Il mercato si attende che le terze parti contribuiscano a raggiungere la compliance al DORA



Fonte: Giornata formativa in ambito ICT RISK E SICUREZZA - GLI ADEMPIMENTI IN VISTA DELLE PROSSIME SCADENZE, LA MESSA A TERRA DELLE NOVITÀ DEL 40° AGGIORNAMENTO DELLA CIRCOLARE 285/2013 BANCA D'ITALIA del 3.05.2023

- Financial Entities,
- European Supervisory Authorities (ESAs),
- European Commission,
- National Competent Authorities (NCAs),
- Cloud Service Providers (CSPs)

L’approccio alla Digital Resilience in ambito financial services deve includere il punto di vista del business e coinvolgere le III parti

Digital Operational Resilience Act - DORA

I — Superare le logiche tradizionali del BC/DR

- Forte **coinvolgimento del top management e del business**
- Revisione di ruoli e responsabilità con l’eventuale istituzione di un **Chief resilience Officer**
- Definizione di un **Remediation Program cross funzionale**

II — Mappare i Business service e definire le soglie di tolleranza

- Analisi ex-novo della **criticità dei business services** considerando il punto di vista del cliente ed **abbandonando la vista per processi**
- **Analisi approfondita delle dipendenze tra** servizi, processi, asset tecnologici e alter controparti interne ed esterne
- Introduzione dei concetti di “**impact tolerance” e di “restoration target”** nell’ambito della definizione dei **processi operativi di ripristino**

III — Analizzare i rischi e valutare l’efficacia del programma

- **Impact assessments e test** realizzati con un focus sul ripristino dei servizi di business
- **Revisione/definizione di indicatori per il monitoraggio** dell’efficacia delle soluzioni di resilience e la rispondenza alla normativa vigente (DORA)
- Evoluzione verso un processo completo e rigoroso per il **third-party risk management**

IV — Gestire l’impatto dell’evoluzione dei trend di mercato e del contesto dei rischi

- Aggiornamento delle **librerie degli scenari** per **considerare nuovi rischi** tra cui la Perdita di dati dovuta ad attacchi cyber o l’interruzione prolungata dei servizi
- Definizione di **modelli operativi di resilienza più complessi che includano terze parti**, fornitori di servizi cloud, fornitori di risorse, vendor tecnologici, …
- **Introduzione di logiche di failover automatizzate** per ridurre I tempi di ripristino legati ad operazioni manuali

Grazie

Paolo Carcano
Partner | Cyber Security & Privacy FS

+39 334 6896335
paolo.carcano@pwc.com

pwc.com/it