La complessità dello scenario esistente

Necessità di **compliance** alle **normative** con impatti sulla sicurezza

Sviluppo di **servizi** attraverso i **canali digitali** e l'uso di **sistemi informativi** in maniera massiva per la **gestione e il governo dei dati**, che hanno **semplificato** e **innovato** fortemente la relazione tra e con cittadini e imprese

PRESIDIO CYBERSECURITY

Nuovi **possibili rischi** sotto il profilo della **sicurezza** legati al **mondo digitale** ed **evoluzione** dei **meccanismi di attacco esistenti**, con potenziali impatti elevati e dunque da monitorare con finalità di contrasto e prevenzione

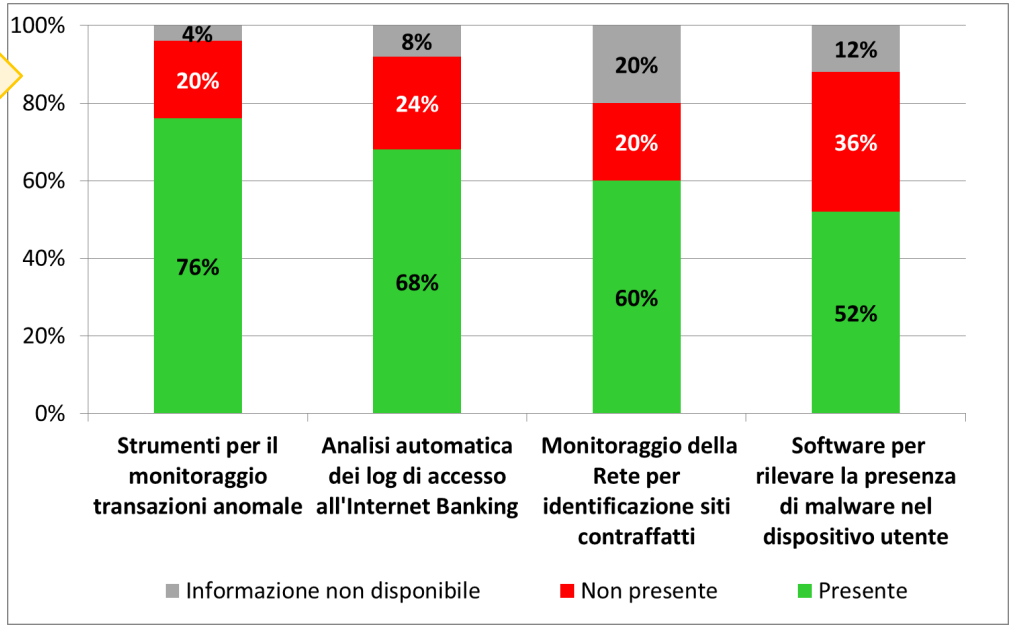
- **Cosa fanno le singole banche?**
- **Quali sviluppi per il settore?**
- **Quali azioni per rafforzare i presidi di cybersecurity?**

Cosa fa la banca per proteggersi

AZIONI INTERNE

- Adozione di una **strumentazione** adeguata per la **rilevazione** di transazioni **anomale** e per il **monitoraggio** accessi
- Definizione policy e procedure
- Attività di **risk assessment**
- Analisi **minacce/vulnerabilità** e definizioni contromisure
- **Formazione** personale interno

Attività di monitoraggio e dotazione tecnologica



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2015, 25 rispondenti

AZIONI VERSO IL CLIENTE

- **Attività informativa e di awareness** verso la clientela svolta da tutte le banche su almeno un canale
- Soluzioni di **II fattore** offerte della clientela da tutte le **banche** per garantire maggiore sicurezza in fase di accesso e di autorizzazione delle disposizioni

Forte attenzione a:

- **Gestione sicura identità e accessi**
- **Education dell'utente** rispetto a un **uso consapevole della rete e dei servizi bancari**

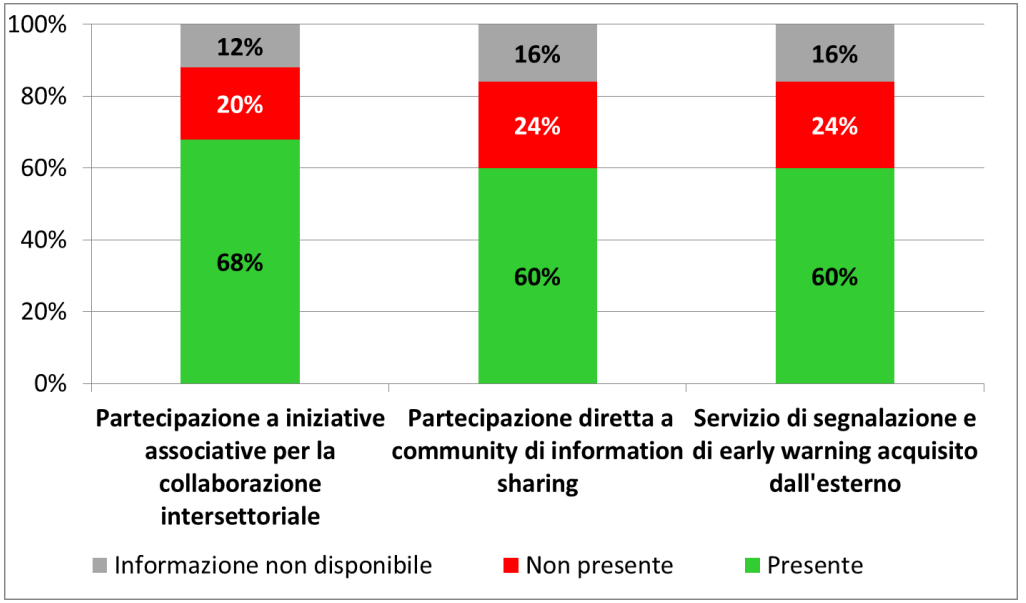
Verso un ecosistema bancario sicuro

Per combattere efficacemente il cybercrime non si può non fare sistema: il raggiungimento di adeguati livelli di sicurezza deve essere un obiettivo comune

Disponibilità ad abilitare un **ecosistema operativo e cooperativo**

Uscire dal singolo contesto bancario per definire i **processi integrati e coordinati**

Partecipazione a community e network per aggiornamenti e segnalazioni sul cybercrime



Fonte: ABI Lab, Osservatorio Sicurezza e Frodi Informatiche, Rilevazione sulle Frodi Identitarie 2015, 25 rispondenti

Priorità

- Costituire un **fronte unico di risposta**, in un **dialogo continuo** tra banche
- Abilitare **partnership tra pubblico - privato** con Forze dell'Ordine e Istituzioni competenti
  - → ***Rinnovo convenzione ABI – Polizia di Stato***
  - → ***Convenzione ABI – ISCOM @MISE su attività del CERT nazionale***
- Definire **modelli di cooperazione** su scala internazionale

Potenziamento collaborazioni istituzionali
Rinnovo convenzione ABI – Polizia di Stato

Dicembre 2010
Sottoscrizione della ***Convenzione ABI – Polizia di Stato per la prevenzione dei crimini informatici nel settore bancario italiano***

Aprile 2011
Lettera Circolare ABI "Azioni di sistema in materia di frodi informatiche": **modalità di partecipazione** delle banche al processo di scambio informativo

Novembre 2013
Avvio **piattaforma OF2CEN** per lo **scambio di informazioni** tra banche e Polizia Postale su frodi tentate ed effettive

Sottoscrizione **accordi operativi** tra **singole banche** e **Polizia Postale e delle Comunicazioni**

In continuità con le azioni già in essere, è stata **rinnovata in data 3 giugno 2015 la convenzione ABI – Ministero dell'Interno** sui temi legati al cybercrime

ABI Lab e **Polizia Postale e delle Comunicazioni** continuano a collaborare **operativamente** e reciprocamente per:

- **Scambiarsi informazioni** su eventi o allarmi legati a minacce specifiche per il settore bancario
- **Informare** in merito a **studi, analisi aggregate e ricerche** in materia di frodi e attacchi informatici, con finalità di condivisione e arricchimento competenza
- **Partecipazione** a rispettivi **tavoli tecnici** di approfondimento
- **Collaborare** a iniziative di **comunicazione**
- **Partecipare** congiuntamente a **progetti di ricerca** in materia di sicurezza informatica e prevenzione frodi

Potenziamento collaborazioni istituzionali
Collaborazione con il CERT nazionale

Sottoscrizione dell'accordo di **collaborazione** tra **ABI** e **Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione** sui temi di **cybersecurity**

L'accordo si formalizza attraverso la collaborazione operativa tra il **Consorzio ABI Lab** e il **CERT Nazionale**, che si impegnano a

- **scambiarsi** reciprocamente e tempestivamente **segnalazioni** di allarme, notizie, avvisi relativi a minacce, attacchi, vulnerabilità, meccanismi di frode e incidenti informatici
- condividere **informazioni** su "**botnet**" di interesse per le banche;
- **cooperare** in caso di **incidenti** informatici
- **divulgare** informazioni finalizzate alla **sensibilizzazione** di cittadini e imprese nella materia della sicurezza informatica
- realizzare iniziative di **formazione** e organizzare **eventi** in tema di sicurezza informatica
- **partecipare** ai rispettivi **tavoli di lavoro tecnici** e scambiarsi informazioni sulle attività afferenti a tavoli di discussione in ambito nazionale ed internazionale
- **partecipare** a **progetti di ricerca** europea focalizzati sui temi di interesse comune

Sviluppo e potenziamento collaborazioni internazionali

***European Agenda on Security* pubblicata nel 2015 dalla Commissione Europea*:**

*Il **cybercrime** è una tra le **priorità** verso cui è necessaria un'**azione coordinata** e **condivisa** a livello **europeo**, data la **dimensione internazionale** del fenomeno e il coinvolgimento di **strutture criminali** sempre più **organizzate** e attive a livello **cross-border***

Principali collaborazioni in materia di sicurezza in cui è attivo ABI Lab in rappresentanza di ABI e delle banche italiane	Soggetti coinvolti nel network
Cybersecurity Working Group (Federazione Bancaria Europea)	Associazioni bancarie, banche e EC3
FI-ISAC – Financial Institutions Information Sharing and Analysis Centre (ENISA)	Banche, Forze dell'Ordine, associazioni bancarie, CERT, ENISA e EC3
PSSG – Payment Security Support Group (European Payments Council)	Associazioni bancarie, banche e EC3
European Cybercrime Center (Europol)	Forze di polizia in collaborazione con le banche per i temi di interesse comune

È importante potenziare le community e i network esistenti per rafforzare ulteriormente le azioni di contrasto e prevenzione e la cooperazione operativa a livello cross-border

*http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

Quali azioni per rafforzare i presidi di cybersecurity nel settore bancario

OPPORTUNITÀ DI CONDIVISIONE DI CONOSCENZA

Le nuove **necessità di segnalazione** degli incidenti di sicurezza che provengono dal regolatore nazionale ed europeo e la definizione del **quadro strategico nazionale per la protezione dello spazio cibernetico** possono costituire un'**opportunità** per promuovere ulteriormente la cultura della **cybersecurity** nel settore **bancario**, in termini di:

- **Maggior consapevolezza** dei fenomeni cyber
- Sviluppo e costruzione di **competenze specialistiche**
- Passaggio **dall'obbligo** di segnalazione in ottica di notifica **alla volontà di segnalazione** a fini di *early warning*
- Creazione di una **conoscenza condivisa** sui fenomeni di cybersecurity

ACCRESCERE LE CAPACITÀ DI SEGNALARE AL SETTORE

Quali azioni per rafforzare i presidi di cybersecurity nel settore bancario

ABI Lab
Tecnologia utile

COME AGIRE SUI PRESIDI DI SICUREZZA

Settore bancario

Banche di rilevanza sistemica

Tutte le banche

SOC

SOC

SOC

Opportunità di coordinamento centralizzato per la gestione degli incidenti di sicurezza secondo la logica CSIRT

Interlocutori Nazionali e Governativi

- DIS
- CERT nazionale
- CNAIPIC/ Polizia Postale
- …

Interlocutori Internazionali

- BCE
- Banche centrali
- Associazioni Bancarie
- ENISA
- EBF/ EPC
- FI-ISAC
- Europol
- …

Sono in corso approfondimenti da parte di Banca d'Italia e ABI, tramite il consorzio ABI Lab, su un possibile piano di azione

Quali azioni per rafforzare i presidi di cybersecurity nel settore bancario

BENEFICI PRINCIPALI DALLA REALIZZAZIONE DI UN MODELLO DI COOPERAZIONE STRUTTURATO

- **Prevenire e mitigare incidenti IT**, proteggendo **asset** e **risorse**
- Mettere a **fattor comune** le **competenze** e **stimolare** la **cooperazione** all'interno della comunità di riferimento in merito alla sicurezza IT
- **Tenersi al corrente** degli **sviluppi** nel campo della **sicurezza** e incrementare i **livelli di awareness**
- Avere un **coordinamento centralizzato** a livello di settore per le **questioni di sicurezza IT**
- Gestire e **rispondere** in maniera **centralizzata e specializzata** agli **incidenti IT**
- Approfondire gli ambiti **al di fuori del perimetro** di interesse di ogni singolo soggetto

È strategico definire quali sono le attività di risposta e prevenzione di incidenti e attacchi a maggior valore per le banche che potrebbero essere gestite attraverso un coordinamento centralizzato

Fonte: Elaborazione ABI Lab da documento ENISA WP2006/5.1 «Un approccio graduale alla creazione di un CSIRT»

Quali azioni per rafforzare i presidi di cybersecurity nel settore bancario

FOCUS SU ASPETTI OPERATIVI

Cybersecurity e Intelligence → protegge da:

- **cybercrime**
- **cyberterrorismo**
- **cyberwarfare**
- **cyberespionage**
- **…**

Le attività in ambito cybersecurity a supporto dell'analisi e la gestione di specifici incidenti e attacchi di sicurezza, includono inevitabilmente aspetti che rientrano nel **crimine informatico** (intrusioni, furto informazioni, furto credenziali, etc.)

È importante **definire processi strutturati** anche con i **soggetti competenti a svolgere attività forense** e a seguire i fenomeni e gli incidenti rilevati sotto il **profilo giudiziario → Polizia Postale e delle Comunicazioni**