Strategia e direttrici di sviluppo

Le linee di azione su cui stanno lavorando le banche

ORIENTARSI SU UNA DIMENSIONE EUROPEA

Tendenza all'**uniformità** a livello comunitario delle norme e dei servizi offerti al cliente

DIGITAL TRANSFORMATION IN BANCA

Evoluzione dei servizi bancari in ottica sempre più **digitale** e usufruibili da remoto e in mobilità

STRATEGIA DI CYBERSECURITY

Gestione degli aspetti di sicurezza legati a **incidenti** e al rafforzamento dei **presidi di sicurezza**

Dimensione europea

- Realizzare il **Digital Single Market**
  È necessario **sviluppare un mercato dei servizi digitali** in grado di uniformare processi e servizi erogati al proprio interno.

- Prestare **attenzione all'evoluzione normativa**
  - ✓ Meccanismo di Vigilanza Unico
  - ✓ Mondo pagamenti (PSD2)
  - ✓ Aspetti Privacy (Regolamento Europeo)
  - ✓ …

- Creare una **rete di reti di infosharing** e di **collaborazioni operative** sulla cybersecurity
  - ✓ Accordo EBF-Europol
  - ✓ Iniziative del CERT Nazionale
  - ✓ Attività della Polizia Postale e delle Comunicazioni

Necessità di armonizzare la normativa e di **promuovere la collaborazione** e la cooperazione tra pubblico e privato e tra i diversi Stati Membri

UN ESEMPIO ITALIANO È IL PROGETTO EU OF2CEN

Verso la digital transformation

Le banche stanno adeguando la propria offerta all'**evoluzione digitale**..

Il **56%** delle banche ha indicato di voler **potenziare l'Internet Banking***

Gli **accessi** al canale di **Internet Banking in aumento del 37%** rispetto al 2014 (**1,8 miliardi nel 2015**)*

Mediamente **ogni banca** gestisce **8 App***

..anche attraverso lo **sviluppo di nuove competenze bancarie**

Per il **74%** delle banche i **digital skills** sono una **leva** per la trasformazione digitale*

Le **iniziative di formazione** sulla cybersecurity sono erogate da oltre il **70%** delle banche*

Il **63%** delle banche sta formando la figura del **Data Scientist** **

Importante **mantenere elevato il livello di fiducia** della clientela rispetto all'uso dell'Internet Banking: le **maggiori preoccupazioni** riguardano un uso improprio dei **dati personali** (43%) e il livello di sicurezza non adeguato nei **pagamenti on line** (42%) ***

*Fonte : ABI Lab – Report 2016
**Fonte: CIPA-ABI,, 2015
***Fonte: Commissione Europea - Cyber Security Report 2014

Strategie di cybersecurity

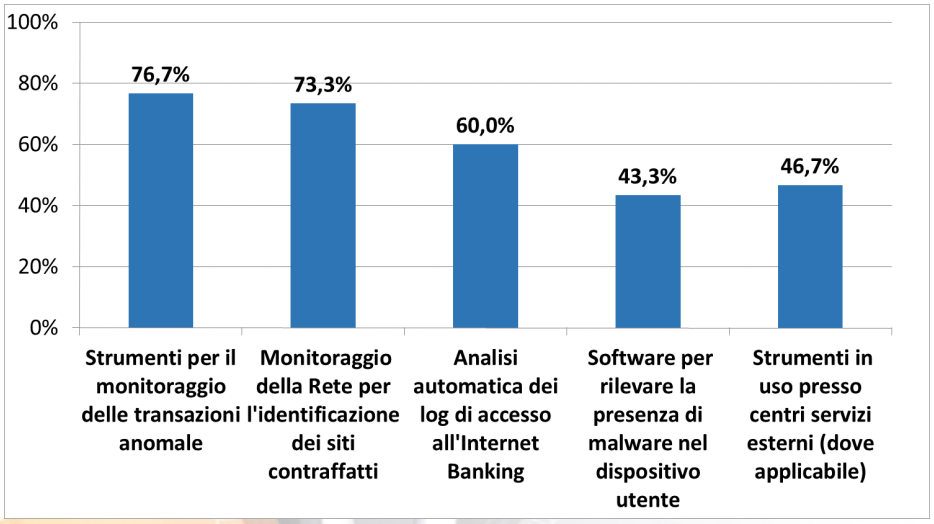
Con lo sviluppo del Digital Banking, è necessaria la **valutazione di nuovi scenari di rischio** e l'**adeguamento delle relative metodologie di analisi**

Gestione degli incidenti informatici e **rafforzamento dei SOC/CERT** interni come iniziative prioritarie per una nuova gestione del rischio informatico

Interazione sempre più forte con le altre funzioni: la **business continuity** è coinvolta in **oltre il 60%** delle banche per la **gestione degli incidenti cyber***

- Il **76%** delle banche si avvale di **strumenti avanzati di monitoraggio** delle transazioni anomale**
- **Meno del 6% del volume economico** dei tentativi di frode si è trasformato in **una perdita****

Attività di monitoraggio e dotazione tecnologica



Non c'è Digital Single Market senza un'adeguata strategia di cybersecurity

*Fonte: ABI Lab – Osservatorio Business Continuity - 2016
Fonte: ABI Lab – Osservatorio Sicurezza e Frodi Informatiche – 2016

Evoluzione normativa in materia di sicurezza e gestione degli incidenti informatici

✓ Normativa di Vigilanza di Banca d'Italia – Circolare 285

- *Analisi del rischio informatico*
- *Gestione sicurezza informatica e dati*
- ***Gestione e notifica incidenti***

✓ Quadro strategico nazionale cybersecurity

- *Rafforzamento partnership pubblico privato e cooperazione internazionale*
- *Potenziamento capacità di difesa infrastrutture critiche*

Crescente attenzione verso i temi di sicurezza informatica e incremento della richiesta di notifica incidenti di sicurezza IT verso Authority

Nuova PSD ✓

- *Strong customer (e transaction) authentication*
- *Sicurezza delle operazioni di pagamento gestite da TPP*
- ***Gestione e notifica degli incidenti legati alla sicurezza dei pagamenti***

Direttiva Europea NIS

- *Adozione di piani nazionali di cybersecurity*
- ***Gestione e notifica degli incidenti***

✓ Raccomandazioni BCE e Orientamenti EBA per la sicurezza dei pagamenti Internet

- *Risk Assessment, strumentazione e monitoraggio*
- *Strong customer authentication*
- *Education e awareness della clientela*

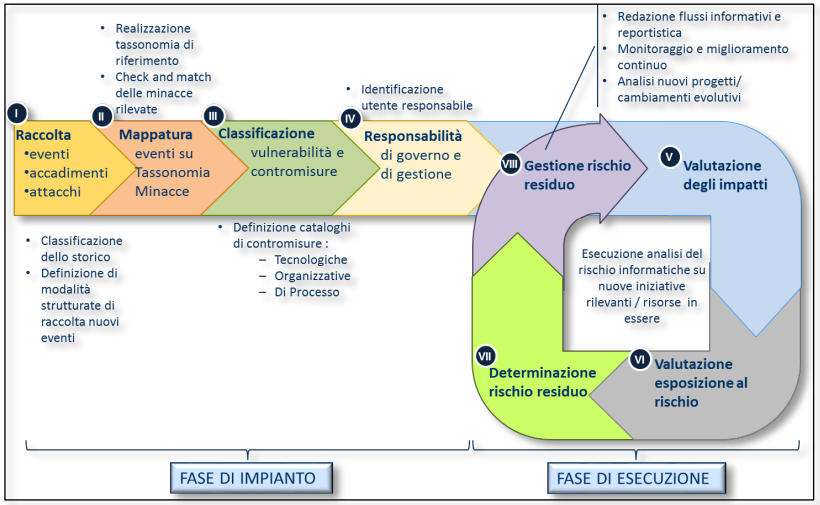
✓ emanato in corso di emanazione

Metodologie di analisi e gestione dei rischi

COSA CHIEDE LA NORMATIVA

- Individuare e **definire le metodologie** di analisi dei rischi, anche in linea con quanto previsto a livello normativo
- **Informare i vertici** rispetto all'evoluzione delle risultanze delle analisi, per un indirizzo sempre più efficiente

Metodologia ABI Lab di analisi del rischio informatico



- Nella fase di definizione della metodologia di analisi del rischio informatico oltre il **60%** delle banche prevede un **coinvolgimento attivo della funzione business continuity**
- **Oltre 1 banca su due** integra la **BIA con altre modalità** di risk assessment

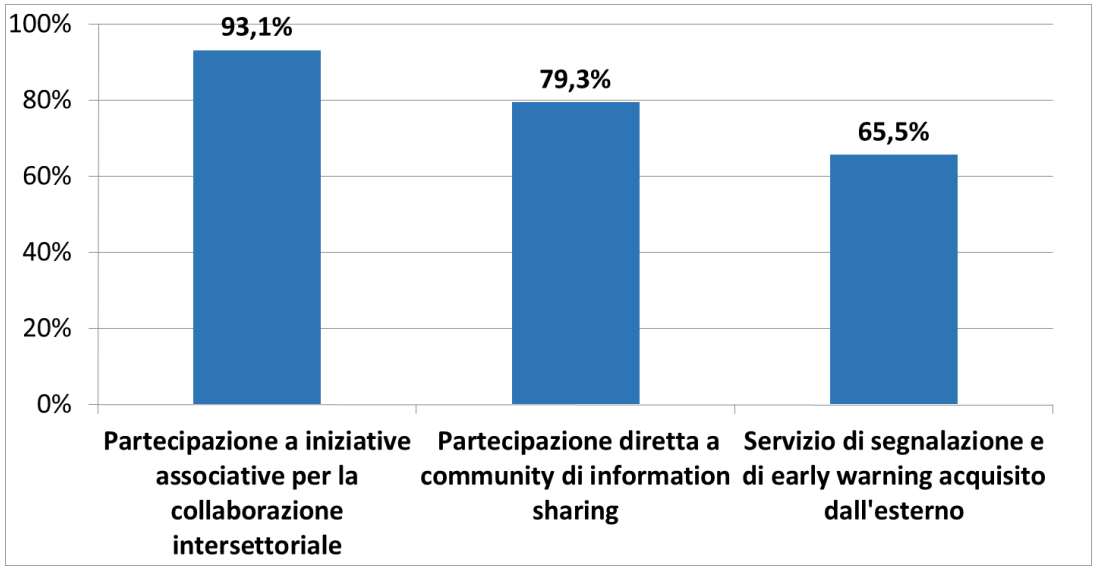
Il coinvolgimento di diverse funzioni aziendali e l'integrazione delle metodologie utilizzate può rappresentare un valore aggiunto

Fonte: ABI Lab – Osservatorio Business Continuity - 2016

Il valore della cooperazione

Rafforzare i presidi di cybersecurity a livello nazionale ed europeo e **contrastare in modo condiviso** e strutturato i crimini informatici

Partecipazione a community e network per aggiornamenti e segnalazioni sul cybercrime



- Cogliere l'importanza derivante dalla **partecipazione a iniziative di scambio di informazioni** per anticipare i trend ed essere proattivi rispetto ai fenomeni
- Ripensare a **logiche maggiormente strutturate di cooperazione** tra pubblico e privato ma anche a livello di singolo settore

Fonte: ABI Lab – Osservatorio Sicurezza e Frodi Informatiche – 2016

Quale direzione per la cybersecurity in banca

Opportunità di **coordinamento centrale** delle attività di contrasto e prevenzione per una strategia di cybersecurity sempre più efficace

DIFFONDERE LE COMPETENZE E FARE AWARENESS

- **Approfondire** temi di **sicurezza informatica** e **normative di riferimento**
- Sviluppare **campagne di sensibilizzazione** sulla cybersecurity
- Svolgere **esercitazioni** e **simulazioni su scenari cyber**

SVILUPPARE ULTERIORMENTE UNA LOGICA DI FI-ISAC ITALIANO

- **Incrementare l'infosharing** su minacce/ vulnerabilità/ incidenti
- **Svolgere analisi evolutive delle minacce cyber**
- **Studiare il dimensionamento** e l'evoluzione dei fenomeni

COORDINARE GLI INCIDENTI INFORMATICI

- **Svolgere attività di coordinamento** centrale in caso di **incidente**
- **Supportare operativament**e le strutture di presidio delle **singole realtà**
- **Definire e aggiornare** a livello di settore lessons learned e strategie di risposta

ABI Lab, insieme alle Istituzioni di riferimento, sta progettando un possibile rafforzamento dei presidi di settore sulla cybersecurity