ABI

L'Open Banking alla prova della sicurezza
"Salone dei Pagamenti"

Milano, 24 novembre 2017

Marco Iaconis
Coordinatore OSSIF
Centro Ricerca ABI
Sicurezza Anticrimine

Le declinazioni della sicurezza

SICUREZZA LOGICA
- Furto d'identità elettronica
- Identificazione e controllo degli accessi
- Phishing

PRIVACY
- Protezione dei dati personali e aziendali
- Protezione dei dati dei clienti
- Amministratori di sistema

Approccio Integrato alla sicurezza

- **Individuazione e sfruttamento delle sinergie tra processi correlati**
- **Bilanciamento degli investimenti e allocazione delle risorse**

SICUREZZA FISICA
- Contanti e valori
- Furti e Rapine
- Frodi «fisiche»

SAFETY
- Dipendenti
- Edifici

SISTEMI DI PAGAMENTO
- Clonazione carte
- Mobile Payment

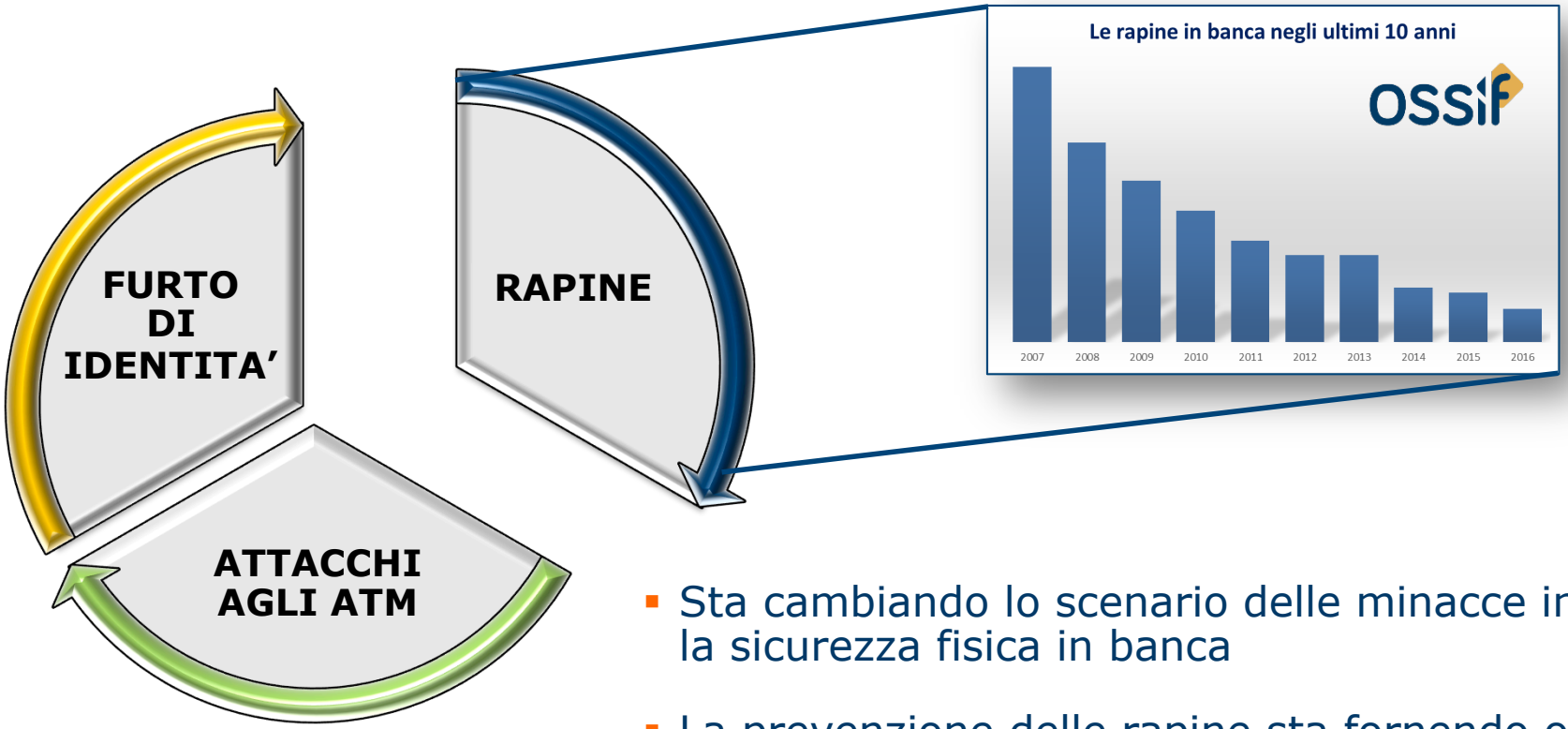
BUSINESS CONTINUITY
- Crisis Management
- Processi critici
- Testing

Il ruolo della sicurezza

Il settore bancario dedica forte attenzione a mantenere elevati livelli di **fiducia nell'utilizzo dei propri servizi** attraverso **investimenti** in sicurezza informatica, sicurezza fisica, antifrode e per la continuità operativa:

- Le **Autorità di Vigilanza** sono attive nel far evolvere il contesto normativo adeguandolo alle nuove **necessità di utilizzo sicuro dei servizi bancari** anche da remoto
- La **cybersecurity** monitora costantemente l'**evoluzione degli attacchi** con l'obiettivo di **intercettare e contrastare** i tentativi di frode informatica
- Le **soluzioni di sicurezza** devono poter garantire un **presidio dinamico** al fine di conoscere e contrastare l'evoluzione dei fenomeni criminali e predisporre adeguate contromisure e attività di prevenzione
- La **sicurezza fisica** focalizza l'attenzione nella **riduzione delle attività predatorie** delle rapine e nell'identificazione di **nuove modalità di protezione** di filiali e ATM
- La **crescita dei pagamenti internet** richiede **nuove azioni di rafforzamento** nella gestione delle carte di pagamento

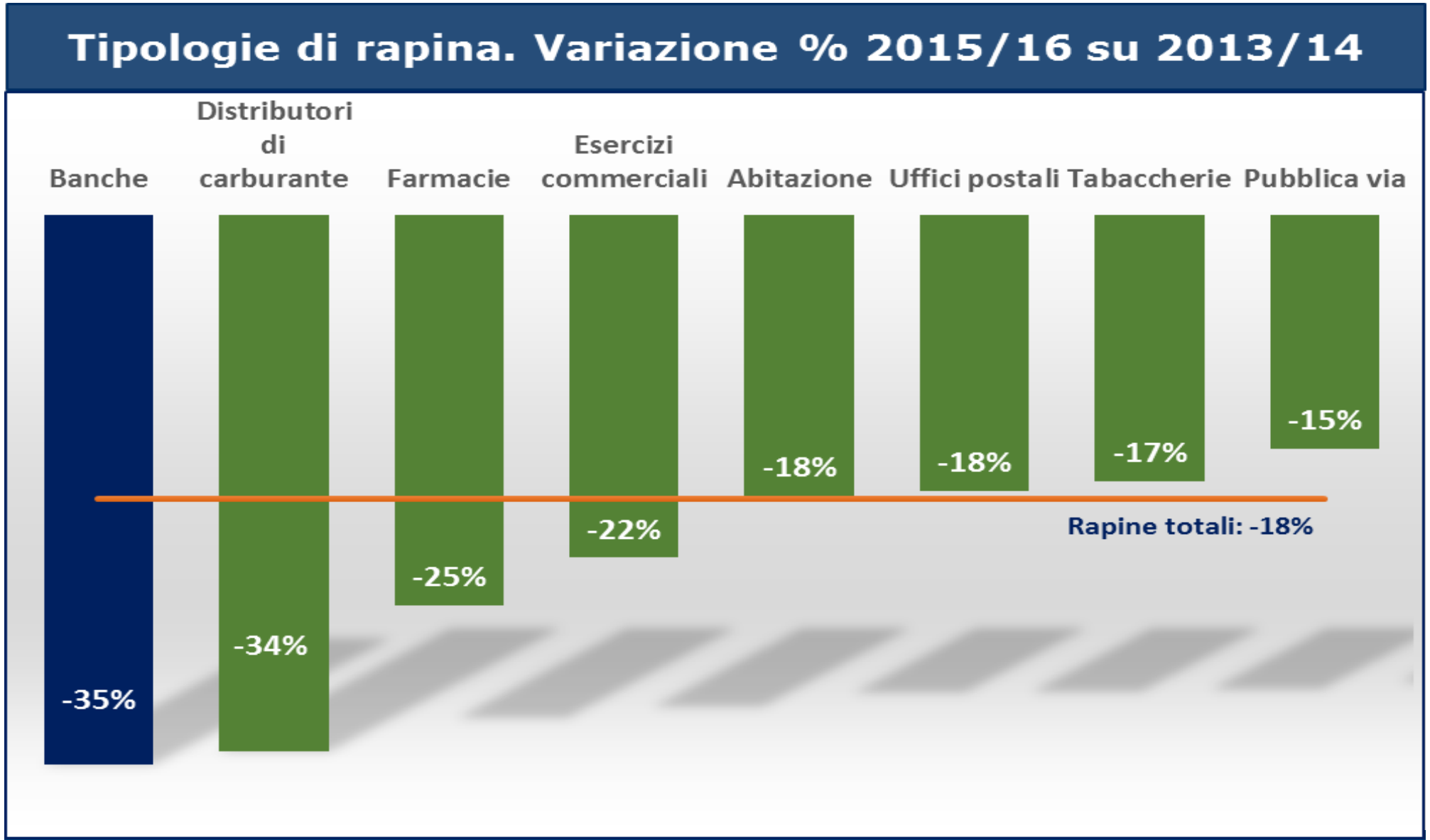
L'evoluzione della Sicurezza fisica in Banca



- Sta cambiando lo scenario delle minacce inerenti la sicurezza fisica in banca
- La prevenzione delle rapine sta fornendo ottimi risultati: -88% in 10 anni

- «*Displacement*» del rischio verso altri obiettivi e/o altri canali

La Sicurezza fisica negli altri settori



ABI

I sistemi cyber fisici e le banche

… ci accorgiamo che le banche sono piene di sistemi cyber fisici

- Allarmi
- Caveaux
- ATM
- Controlli accessi
- Sistemi di videosorveglianza
- Conteggio del denaro
- …

Fonte: ABI Lab, Scenario e trend del mercato ICT per il settore bancario, 2017

ABI

Minacce emergenti

- La comprensione delle minacce di natura cyber e physical rappresenta il punto di partenza per lo studio e la progettazione di un qualsiasi sistema e strategia di protezione.

- La valutazione di una Vulnerabilità (vulnerability assessment – VA) è un'attività complessa che può rilevarsi critica quando si palesano inadeguatezza o inosservanza delle semplici policy di sicurezza esistenti ovvero da un progettazione dell'architettura di security errata.

In ottica di Cyber Physical Security vanno considerate le seguenti vulnerabilità:

- ✓ HARDWARE (es. assenza di ridondanza di componenti strategiche)
- ✓ SOFTWARE (es. avvio di servizi non necessari)
- ✓ CONFIGURAZIONI (es. configurazioni applicative non aggiornate)
- ✓ VIRUS INFORMATICI (es. assenza di firewall o aggiornamenti)
- ✓ COMUNICAZIONI (es. assenza di criptazioni)

Attacchi con "BLACK-BOX" su ATM

physical

- violazione dell'hardware in prossimità del card reader e della tastiera tramite due fori
- attraverso i fori viene staccato il cavo che connette tutte le periferiche al pc dell'ATM riconnettendolo ad un device di tipo fake (black box) esterno

cyber

- tramite black box vengono inviati i comandi al dispensatore per l'erogazione delle banconote
- il cavo non è più connesso al pc e quindi l'attività non viene rilevata nel giornale di fondo

erogazione

- L'erogazione viene può essere effettuata con singole operazioni i cui importi variano dai 1.200€ ai 1.500€ a seconda delle banconote presenti nei cassetti ed al limite fisico dell'ampiezza della bocchetta di erogazione.
- Frodatori hanno la possibilità di configurare un loop che dispensa 40 banconote ogni 20 secondi (6000€ al minuto cominciando a svuotare il cassetto dei 50 e 2400€ al minuto proseguendo con quello dei 20).

Art. 6 – Prevenzione dei rischi multivettoriali *(cyber physical security)*

NOVITA'

- Le banche si impegnano a prevenire gli attacchi multivettoriali realizzati con tecniche di cyber physical security a danno delle dipendenze bancarie, che integrano le tecniche di violazione di tipo fisico con quelle di tipo informatico e di ingegneria sociale.

- In particolare le banche si impegnano a censire gli attacchi realizzati ai danni delle dipendenze bancarie con le nuove tecniche di cyber physical security. OSSIF provvederà ad acquisire i dati presso le diverse fonti di raccolta per effettuare analisi che verranno messe a disposizione delle Forze dell'Ordine.

Il valore della cooperazione operativa attraverso il CERTFin

ESIGENZE CRESCENTI SUL FRONTE CYBER

- Rafforzare la **cooperazione pubblico-privato** anche a livello di settore
- Integrarsi e **dialogare** con le **istituzioni** nel **quadro strategico nazionale** di protezione cibernetica
- **Potenziare** il **confronto** e lo **scambio informativo** tra **banche** e con altri settori per **anticipare i trend ed essere proattivi**

Dal **1°gennaio 2017** è operativo il **CERTFin CERT Finanziario Italiano, governato** da **ABI** e **Banca d'Italia** e **operato** dal **Consorzio ABI Lab**

CERTFin

CERT Finanziario Italiano

Iniziativa cooperativa pubblico-privata finalizzata a **innalzare** la **capacità** di **gestione dei rischi cyber** e la **cyber resilience** degli **operatori bancari e finanziari**