MPS: Prevenzione delle frodi Internet Banking

Roma, 05 Giugno 2015

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

ABI Lab

MPS è una delle principali realtà bancarie italiane con oltre 5 Milioni di Clienti

MPS in pillole

- 3^ Banca Italiana
- Oltre 5 milioni di Clienti
- Oltre 2.100 filiali
- Oltre 25.000 impiegati
- 1 mln + di Clienti Internet

Trasformazione IT come Key Driver del Piano Industriale 2012-2017

Ambiti di trasformazione IT

Infrastruttura:

"Liquefazione" del Layer infrastrutturale, allocabile a supporto dei servizi applicativi e di business in modalità automatica e on-demand - **Migliorare Affidabilità, Performance e Scalabilità, riducendo TCO**

Applicazioni:

Standardizzazione e razionalizzazione delle soluzioni architetturali risolvendo dualità, massimizzando modularità e riusabilità – **Innovare il Servizio, riducendo TCO**

Processi:

Standardizzazione e industrializzazione dei principali processi IT in linea con le Best Practice di Settore – **Migliorare Livelli e Qualità del Servizio**

Sicurezza:

Evoluzione delle soluzioni di Sicurezza Logica. Contrasto al Cyber Crime e alle Frodi Informatiche Internet e Mobile Banking – **Mitigare eventuali vulnerabilità in ambito IT**

Velocità di esecuzione e ritorno immediato dell'investimento

La sfida della trasformazione IT per MPS

La sfida…

- Necessità di una **trasformazione radicale**, su più dimensioni complesse, veloce e con **benefici rilevanti** su qualità del servizio e riduzione costi
- **Investimenti frugali** con **ritorni immediati**
- **Nessun 'silver bullet'** di prodotto

…e l'approccio

A. **Pensare** (un po') **prima di fare**, per non disperdere investimenti (Non sparare nel mucchio!)
B. Elaborare un **modello** di attacco dei problemi **semplice, ma solido**, per orientare le azioni, misurarne l'efficacia e correggere il tiro in corsa

Un caso di successo di questo approccio? Il contrasto alle frodi informatiche!

La frode non si elimina ma si contrasta

Il fenomeno delle frodi informatiche

La frode informatica…

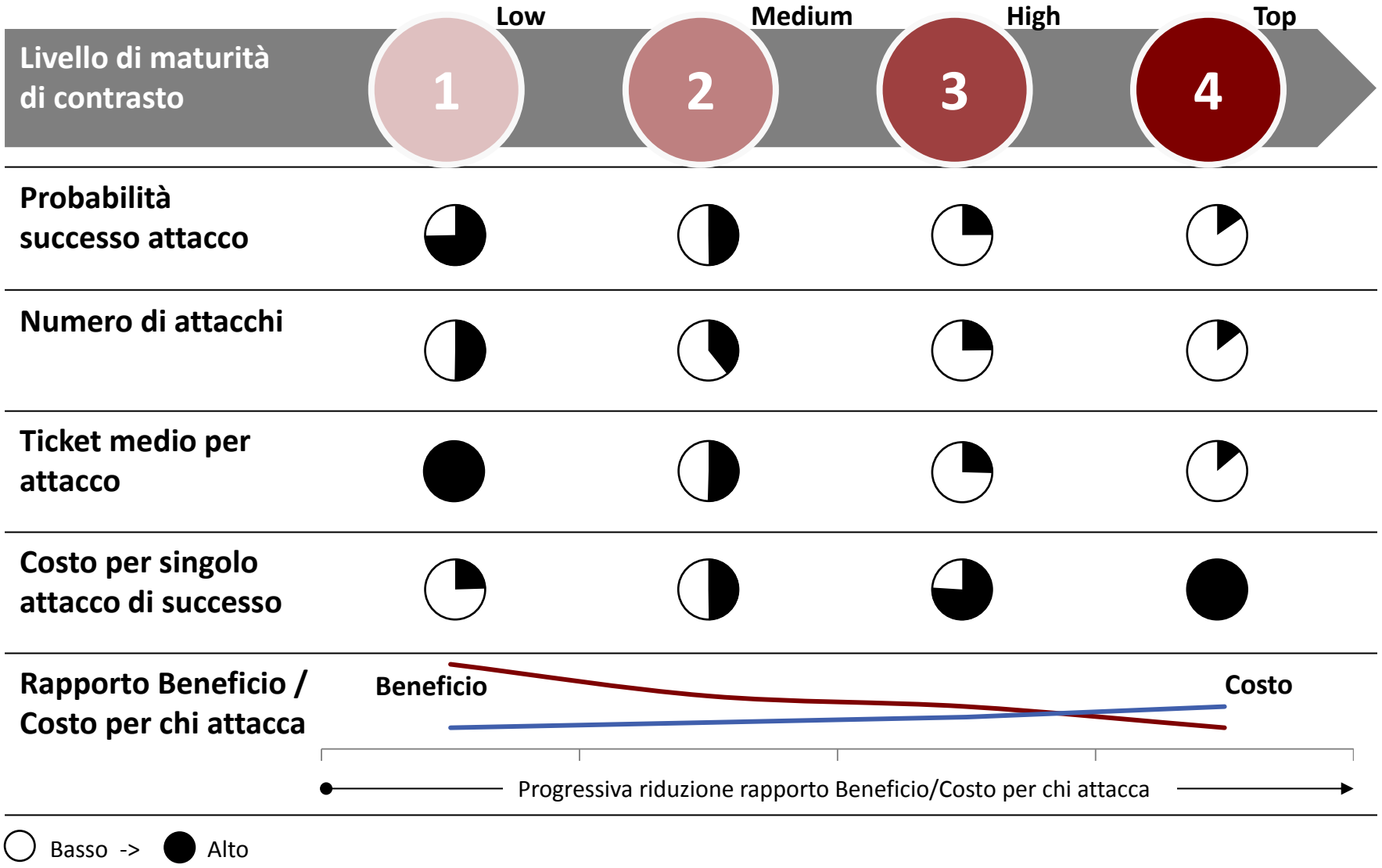
- …è un fenomeno che **non si "estirpa"**
- **…muta**, diventando sempre più sofisticata
- …segue sempre il percorso di **minor resistenza** per massimizzare beneficio/costo dell'attacco

Quindi richiede un modello di contrasto:

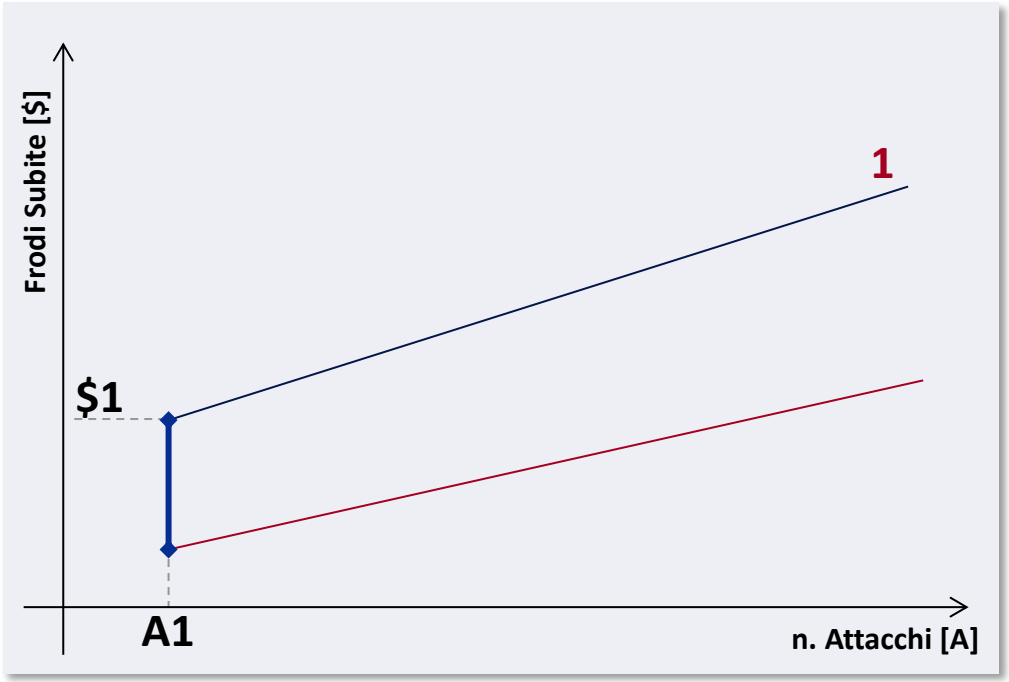
- **Definito** sulle variabili fondamentali
- **Applicabile** in pratica e in tempi celeri
- Continuamente **monitorabile** in termini di efficacia
- **Flessibile**, per potersi adattare all'evolvere delle frodi

Alla crescita della maturità di contrasto si riduce il rapporto Beneficio/Costo per chi attacca

Definizione di un modello a 4 livelli



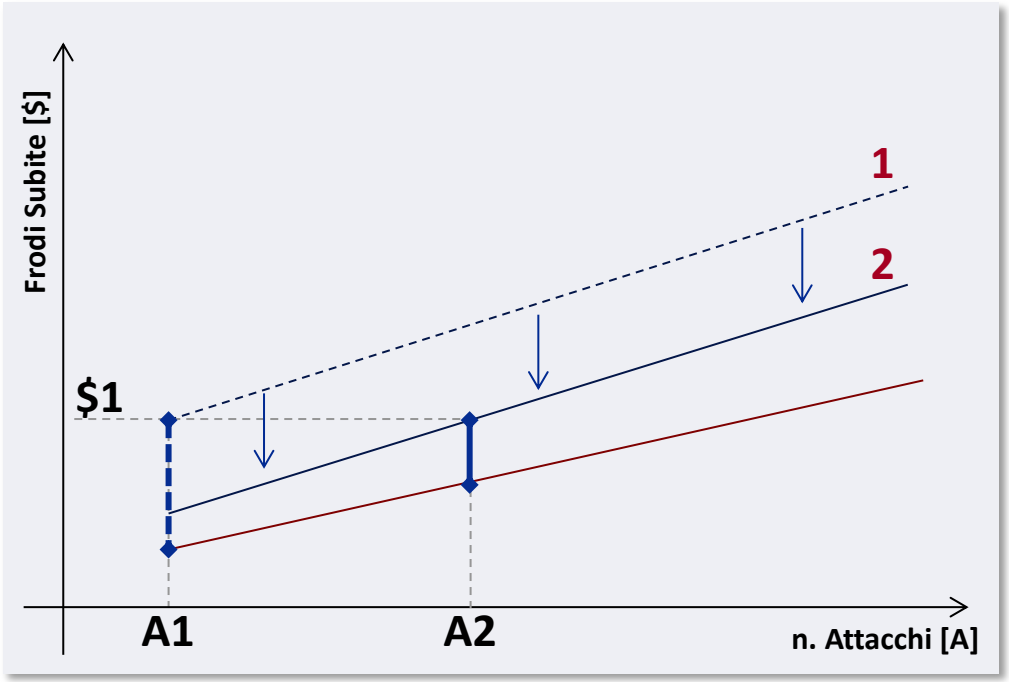
Maturità 1: Livello di contrasto ‘’Low’’



- Comprensione parziale del fenomeno
- Difese non adeguate
- Ridotta collaborazione IT-Sicurezza e Business
- Alta probabilità di successo dell’attacco
- Medio numero di attacchi
- Alto Ticket medio per attacco
- Massimo Beneficio/Costo per l’attaccante

L’attaccante guadagna quanto più attacca

Maturità 2: Livello di contrasto ‘’Medium’’

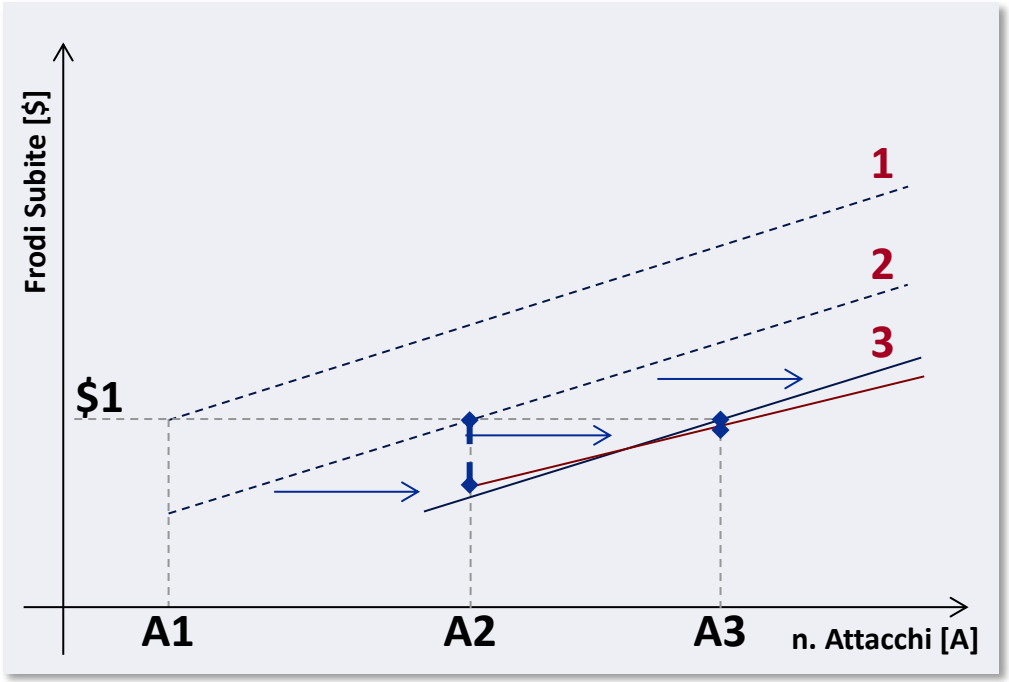


Curva ricavi frodatore
Curva costi frodatore
Margine frodatore: > 0 ma ridotto

- Maggiore comprensione del fenomeno
- Rafforzamento delle difese informatiche
- Relazione collaborativa IT-Sicurezza e Business per azioni congiunte di contrasto
- Minore probabilità di successo dell’attacco
- Ridotto numero di attacchi e Ticket medio per attacco
- Medio Beneficio/Costo per l’attaccante

L’attaccante guadagna quanto più attacca.
Ma meno!

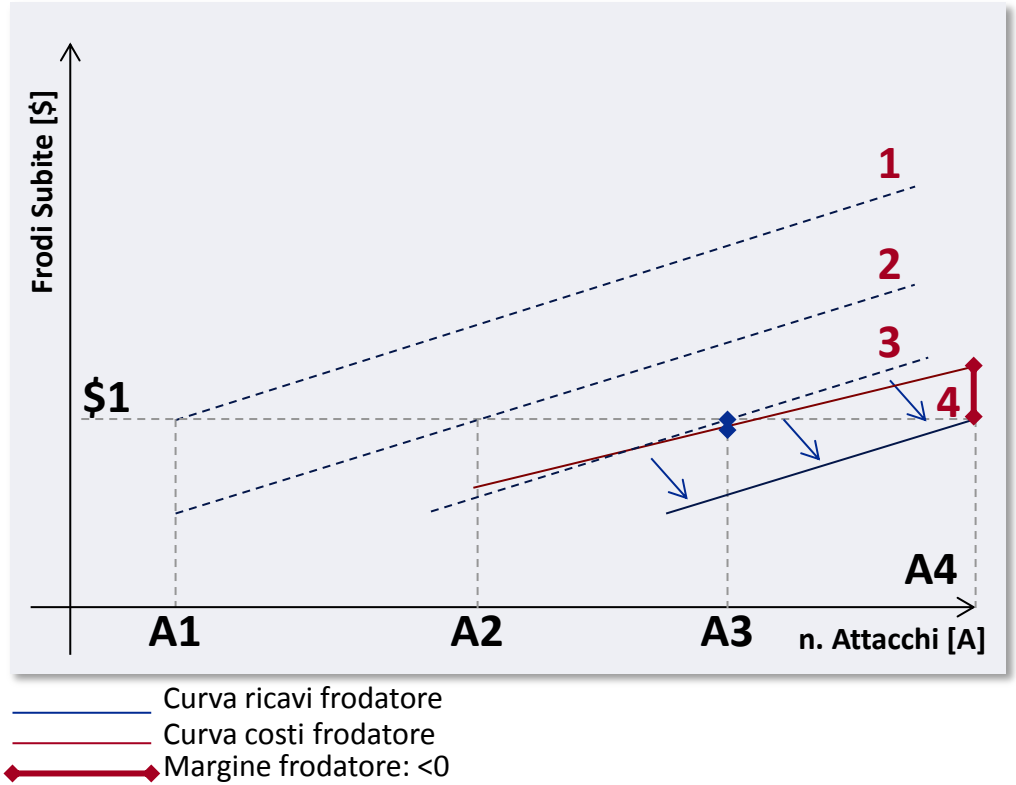
Maturità 3: Livello di contrasto ‘’High’’



- Ottima comprensione del fenomeno
- Attivazione di strumenti di monitoraggio evoluto e collaborativo (es: OF2CEN)
- Progressivo rilascio di azioni congiunte IT-Sicurezza e Business
- Bassa probabilità di successo dell’attacco
- Ridotto numero di attacchi e Ticket medio per attacco
- Minimo Beneficio/Costo per l’attaccante (~1)

L’attaccante guadagna quanto più attacca.
Ma meno e meno volte!

Maturità 4: Livello di contrasto ‘’Top’’



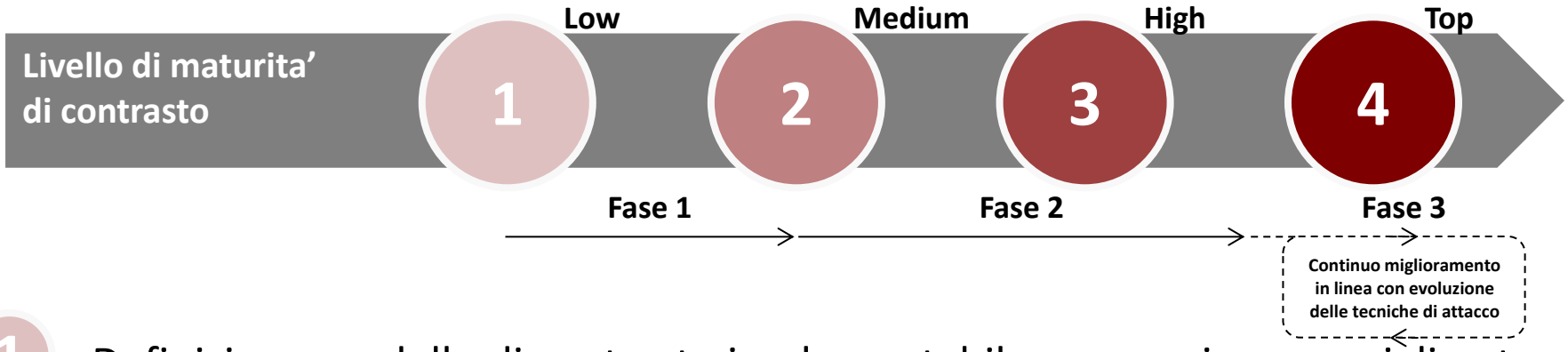
- Comprensione adattativa del fenomeno
- Ottimizzazione/autoapprendimento strumenti di monitoraggio basati su correlazioni
- Minima probabilità di successo dell’attacco e minimo numero di attacchi e ticket medio
- Rapporto Beneficio/Costo unitario o <1

L’attaccante guadagna meno, meno volte, a costi crescenti fino a rendere l’attacco non remunerativo.

Raggiunto il livello 4 di maturità è necessario proseguire in un azione di continuo miglioramento

Lista non esaustiva

I passi per evolvere da 1 a 4



1. Definizione modello di contrasto implementabile per passi sequenziali auto consistenti
2. Introduzione/miglioramento filtri paesi a rischio/ soglie (disposizioni estere)
   Introduzione/miglioramento White/Black list (disposizioni estere e Italia)
3. Introduzione/evoluzione di soluzioni automatica di monitoraggio e alerting End User, Internet/Mobile Banking e Core Banking
   Adesione a gruppi di collaborazione cross organizzazione per sharing informazioni (es: Polizia Postale OF2CEN)
4. Continuo miglioramento degli strumenti e degli algoritmi di monitoraggio e alerting

Lesson learned: una lista in continuo aggiornamento

Lesson learned

- Avere una corretta comprensione del fenomeno e definire un modello strutturato di contrasto
- Definire team di lavoro cross funzionali specializzati e dedicati all'analisi e al contrasto delle frodi informatiche
- Condividere le informazioni internamente alla Banca (Security-IT-Business) per accrescere la maturità del modello di contrasto a livello di Sistema Banca
- Condividere delle informazioni esternamente alla Banca (Polizia Postale, OF2CEN,…) per definire un modello collaborativa di contrasto a livello di Sistema Interbancario
- Adottare e adeguare nel tempo gli strumenti informatici e di processo di monitoraggio e alerting
- Investire nell'educare i Clienti ad un utilizzo sicuro di Internet Banking e Mobile Banking

Evolvere il modello da Reactive a Predictive

Prossimi passi

Riconoscere attacco e relativa frode prima che l'evento avvenga e la Banca subisca il danno finanziario

Grazie per l'attenzione!

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Primo Trebbi

Chief Technology Officer
Banca Monte dei Paschi di Siena S.p.A.

Siena – Via Ricasoli, 60
E-mail: primo.trebbi@mps.it

MPS: Prevenzione delle frodi Internet Banking

Roma, 05 Giugno 2015

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

ABI Lab