

LA SECURITY GOVERNANCE IN BANCA: I BENEFICI DI UN APPROCCIO INTEGRATO

ROBERTO LORINI

Executive Vice President VP Tech

Abstract

Il settore bancario sta attraversando una fase di profondo cambiamento, con impatti diretti anche sulla sicurezza aziendale. Il consolidamento attraverso processi di fusione e acquisizione e la ricerca di efficienze sul fronte dei costi costringono le banche a pianificare e gestire l'integrazione, standardizzando le misure di sicurezza.

Basilea 2 e le nuove normative in materia di gestione del rischio operativo impongono l'adozione di metodologie appropriate e lo sviluppo di applicativi per la sua gestione. Regolamenti della Banca d'Italia e standard internazionali spingono le banche ad individuare gli impatti di possibili eventi catastrofici (*business continuity*) e ad adottare appropriati piani di contrasto.

Nuovi progetti avviati a livello di sistema bancario (es. Carte Microcircuito e *Corporate Banking*) tendono a trasformare la sicurezza in un fattore abilitante per l'erogazione di servizi ad elevato valore aggiunto. Multicanalità e nuove tecnologie rendono infine la convergenza digitale una realtà, permettendo di fidelizzare maggiormente i clienti, ma al costo di un più elevato rischio di furto dell'identità digitale ("*phishing*").

L'esperienza VP Tech in ambito bancario dimostra che sono stati fatti molti passi in avanti per aumentare il livello di sicurezza del sistema, ma restano ancora diverse criticità. Si segnalano in particolare come aree di attenzione:

- l'esigenza di adottare sempre l'analisi dei rischi come prerequisito per l'impostazione di strategie della sicurezza;
- la necessità di applicare con rigore degli strumenti di pianificazione degli investimenti in sicurezza;
- l'esigenza di implementare sistemi di pianificazione ex-ante e controllo ex-post in merito all'efficacia e all'efficienza della contromisure di sicurezza;
- l'opportunità di aumentare il livello di integrazione della sicurezza a livello di processi e linee di business;
- l'esigenza di diffondere maggiormente il sapere tecnico e di attivare nel contempo le "comunità di *practice*" di sicurezza.

Per rispondere alle nuove sfide sollevate dall'evoluzione tecnologica e dai nuovi scenari normativi e di business, le banche devono fare lo sforzo per completare la transizione da un approccio alla sicurezza di taglio tecnologico ad uno realmente manageriale, capace d'integrare aspetti tecnologici, organizzativi e culturali. *Corporate Security*, in particolare, deve sapersi proporre come centro servizi che supporta le altre funzioni aziendali e le aiuta a ridurre i rischi collegati ai processi di business.

Corporate Security deve perciò assicurare un approccio esaustivo, coprendo le tematiche di sicurezza informatica, fisica e di *business continuity*: dalla fase di progettazione,

all'implementazione, sino all'esercizio. L'esperienza e *benchmarking* internazionali dimostrano con chiarezza che l'efficacia della gestione della sicurezza tende a migliorare se vengono implementati adeguati meccanismi e processi organizzativi e se *Corporate Security* tende ad assumere un ruolo proattivo e prossimo ai processi di business della banca.

Oltre ai meccanismi di tipo organizzativo, le banche possono migliorare il proprio profilo in termini di sicurezza adottando strumenti di *governance* quali il *Security Tableau de Bord* e il *Security Knowledge Management*, con evidenti benefici in termini di capacità di tracciare l'efficacia delle contromisure adottate, comunicazione delle informazioni, migliore reportistica di sicurezza e maggiore sensibilizzazione del personale. Soluzioni avanzate di sicurezza quali i *Security Operation Center* (SOC) permettono inoltre di gestire in modo centralizzato e in tempo reale le problematiche di sicurezza, riducendo i tempi di reazione e aumentando la capacità di risposta della banca rispetto alle minacce a cui è esposta.

E' il caso di ricordare, infine, come *Corporate Security* possa svolgere un ruolo centrale nel rendere più sicuro il business aziendale attraverso la predisposizione di efficaci misure di *business continuity* e *disaster recovery*, nonché di integrazione delle iniziative e delle tecnologie di contrasto al rischio di furto dell'identità digitale degli utenti di servizi di banca multicanale ("*phishing*").

In sintesi:

- La sicurezza è una tematica sempre meno tecnologica e sempre più di business, divenendo fattore abilitante fondamentale per l'erogazione di servizi a valore aggiunto
- Per gestire la sicurezza in modo efficace è necessario adottare un approccio manageriale, con una forte enfasi sul concetto di *security governance* (pianificazione, controllo, gestione), assicurando nel contempo la profonda conoscenza del business bancario e delle tecnologie abilitanti di sicurezza
- Il partner della banca sulle tematiche di sicurezza deve saper unire le due anime, consulenziale e tecnologica, per offrire soluzioni mirate ed *end-to-end*.

1



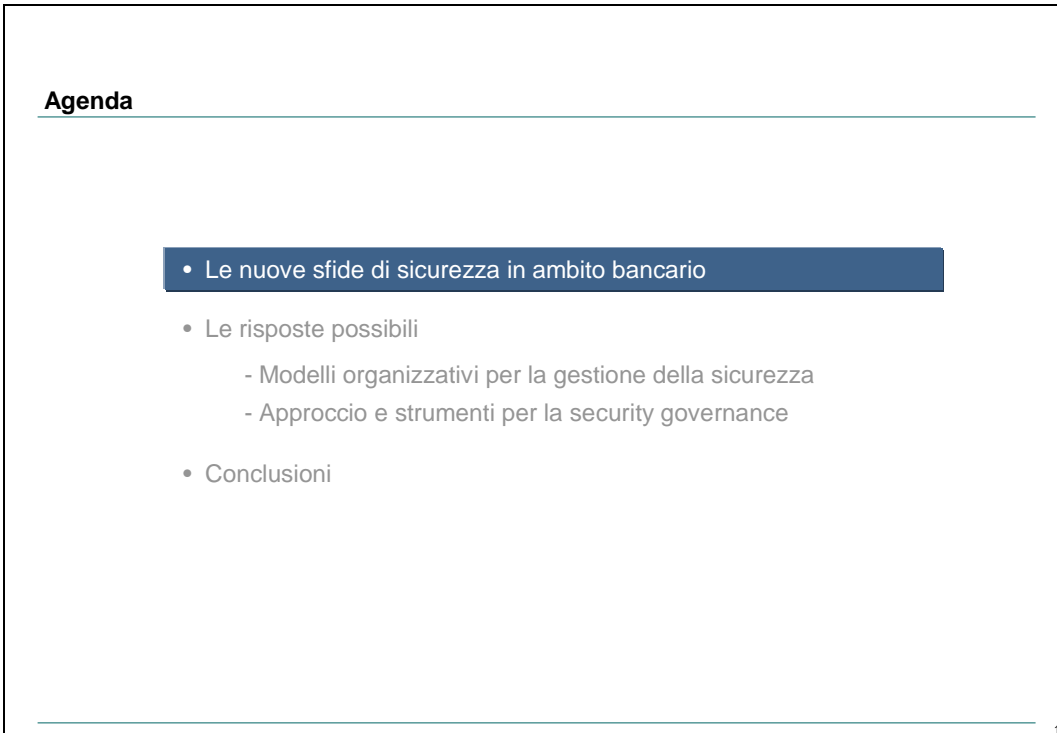

SECURITY SOLUTIONS

**La Security Governance
in banca: i benefici di un
approccio integrato**

Ing. Roberto Lorini
Executive Vice President, VP Tech

Convegno BancaSicura
Padova, 19 Ottobre 2005

2



Agenda

- Le nuove sfide di sicurezza in ambito bancario
- Le risposte possibili
 - Modelli organizzativi per la gestione della sicurezza
 - Approccio e strumenti per la security governance
- Conclusioni

3

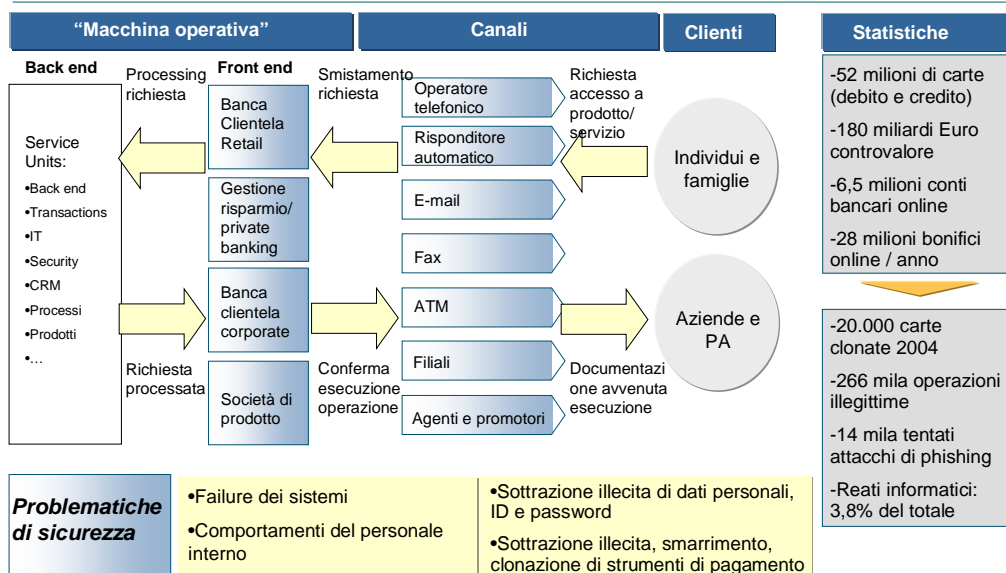
Il settore bancario sta attraversando una fase di profondo cambiamento con impatti diretti sulla sicurezza aziendale

	Driver del cambiamento	Implicazioni in ottica Sicurezza
Consolidamento	<ul style="list-style-type: none"> •Fusioni/acquisizioni/dismissioni •Focus su efficienza •Integrazione organizzazione/sistemi 	<ul style="list-style-type: none"> •Pianificare e gestire l'integrazione •Condividere e standardizzare le misure di sicurezza
Basilea 2	<ul style="list-style-type: none"> •Valutazione e misurazione RO •Equity capital ratios •Readiness entro 2006 	<ul style="list-style-type: none"> •Definire le metodologie di calcolo del rischio e sviluppare applicativi per la gestione del rischio operativo (e IT)
Business Continuity	<ul style="list-style-type: none"> •Guidelines Banca d'Italia •Normative e standard internazionali •Maggior attenzione eventi impattanti 	<ul style="list-style-type: none"> •Individuare possibili eventi catastrofici •Definire un piano d'azione da rivedere a scadenze regolari
Nuovi progetti	<ul style="list-style-type: none"> •EMV/ Microcircuito •Corporate Banking Interbancario 	<ul style="list-style-type: none"> •Interpretare la sicurezza come fattore abilitante per i nuovi servizi •Predispone normative e processi organizzativi mirati
Multicanalità e nuove tecnologie	<ul style="list-style-type: none"> •Accesso ai servizi finanziari multicanale •Convergenza digitale •Servizio e fidelizzazione cliente 	<ul style="list-style-type: none"> •Gestire la sicurezza, anche quando affidata a partner esterni •Negozicare contratti basati su SLA

2

4

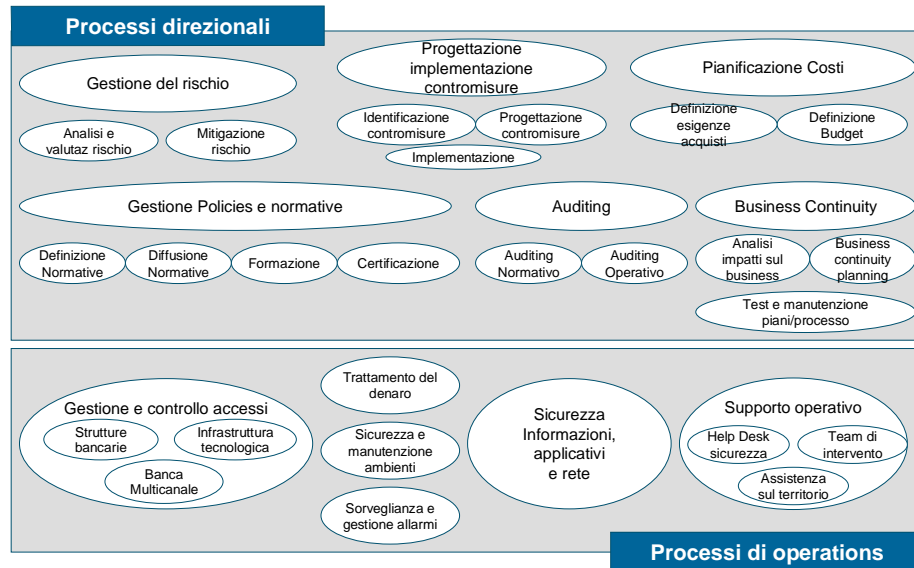
La crescente diffusione di multicanalità e nuove tecnologie accrescono i rischi di furti e frodi, rendendo il tema della sicurezza sempre più pervasivo e centrale



3

5

In un contesto di forte cambiamento è sempre più importante riuscire ad integrare i processi di sicurezza con la “macchina organizzativa” bancaria



6

Le banche hanno fatto molti passi avanti per rendere più sicura l'infrastruttura e l'erogazione del servizio, tuttavia permangono delle criticità non pienamente risolte

Aree di attenzione	Criticità riscontrate con maggior frequenza
Conoscenza dei rischi reali	•Analisi dei rischi come prerequisito per l'impostazione di strategie della sicurezza non sempre implementata con il dovuto rigore
Pianificazione e controllo	•Logica e strumenti di pianificazione degli investimenti in sicurezza non sempre applicati con chiarezza
Gestione operativa	•Implementazione e valutazione di efficacia ed efficienza della contromisure di sicurezza spesso non misurate
Sicurezza e processi di business	•Sicurezza non sempre integrata a livello di processi e linee di business
Cultura della sicurezza	•Diffusione del sapere e attivazione di comunità di practice di sicurezza ancora insufficienti

Fonte: VP Tech 2005

7

Agenda

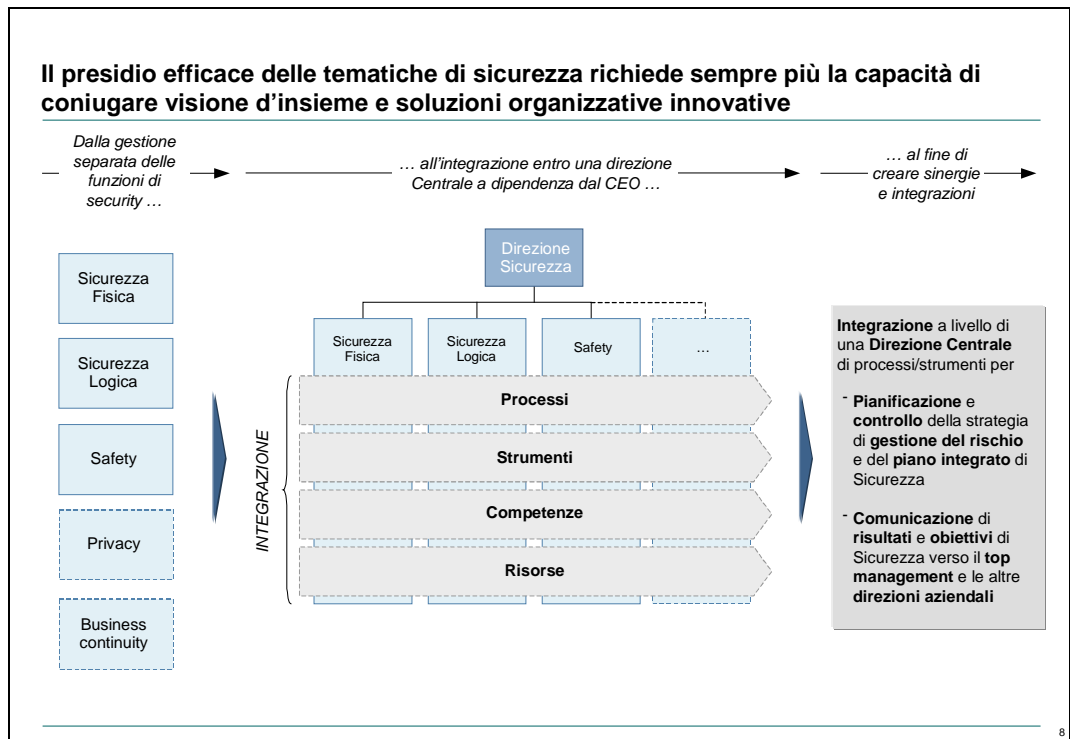
- Le nuove sfide di sicurezza in ambito bancario
- Le risposte possibili
 - Modelli organizzativi per la gestione della sicurezza
 - Approccio e strumenti per la security governance
- Conclusioni

8

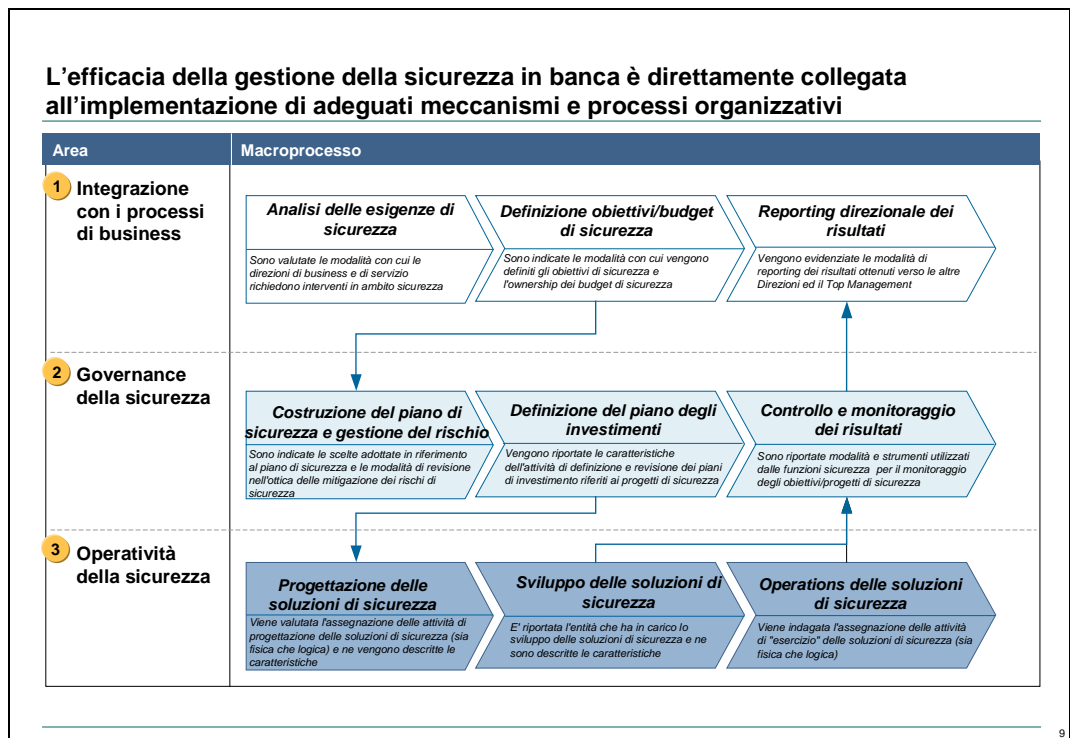
Corporate Security diviene un centro servizi cruciale verso le altre funzioni aziendali della banca al fine di ridurre i rischi collegati a processi di business

Processi bancari	Esigenze di business	Aspetti critici	Ruolo centrale per Sicurezza Aziendale
Processi direzionali Strategia Controllo di gestione Comunicazione istituzionale	Verso il mercato	Frodi verso i clienti	-La Sicurezza aziendale è una tematica trasversale -E' un interlocutore importante per le altre direzioni aziendali -Eroga servizi di integrità, disponibilità, riservatezza delle informazioni a supporto di funzioni e processi aziendali
Gestione del rischio Rischio di mercato Rischio di credito Rischio operativo	Verso la macchina operativa	Business continuity	
Processi di marketing Piano di marketing Sviluppo prodotti Rete commerciale Customer service	Verso l' area legale	Compliance	
Processi di operations Servizi di sportello Monetica Incassi e pagamenti Fiscalità e previdenza Finanza e credito	Verso la protezione	Tutela della proprietà intellettuale	
Processi a supporto Organizzazione e personale Sistemi informativi Amministrazione e legale	Verso le risorse umane e l'organizzazione	Politiche aziendali	
SICUREZZA			

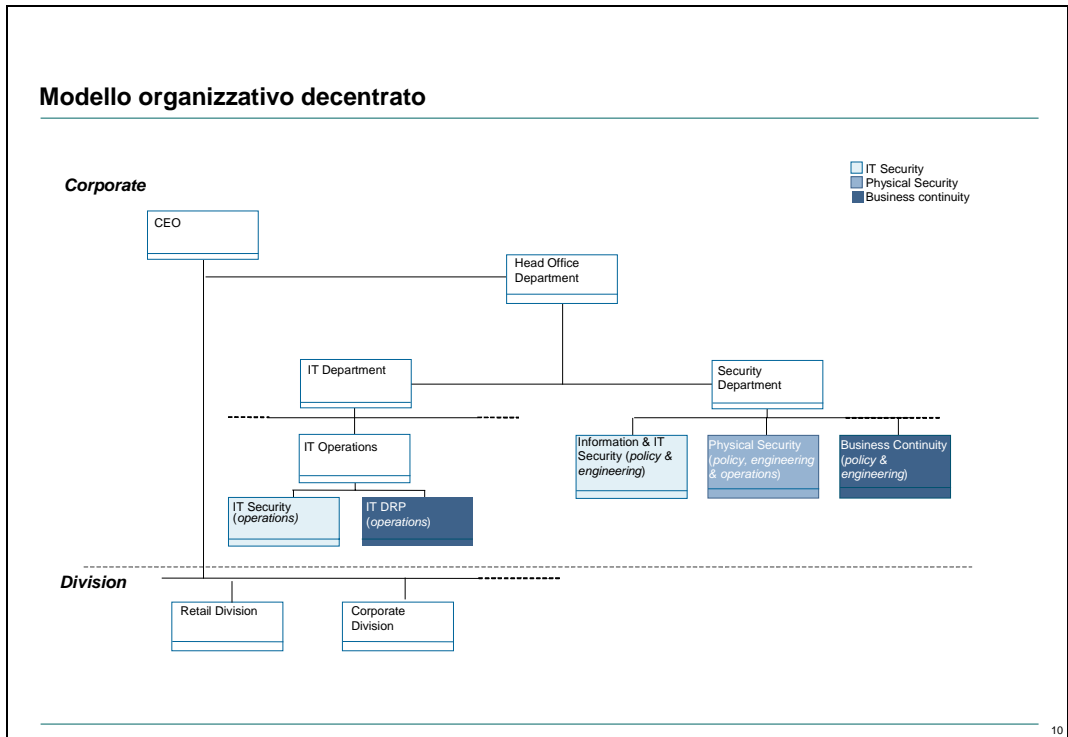
9



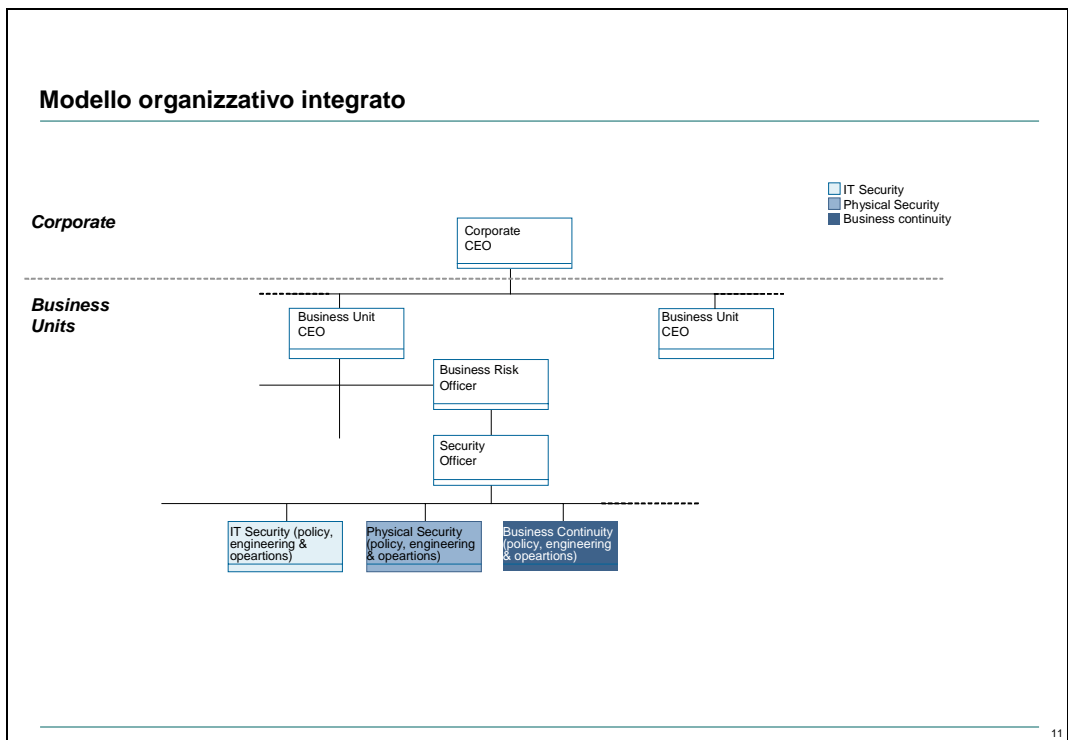
10



11



12



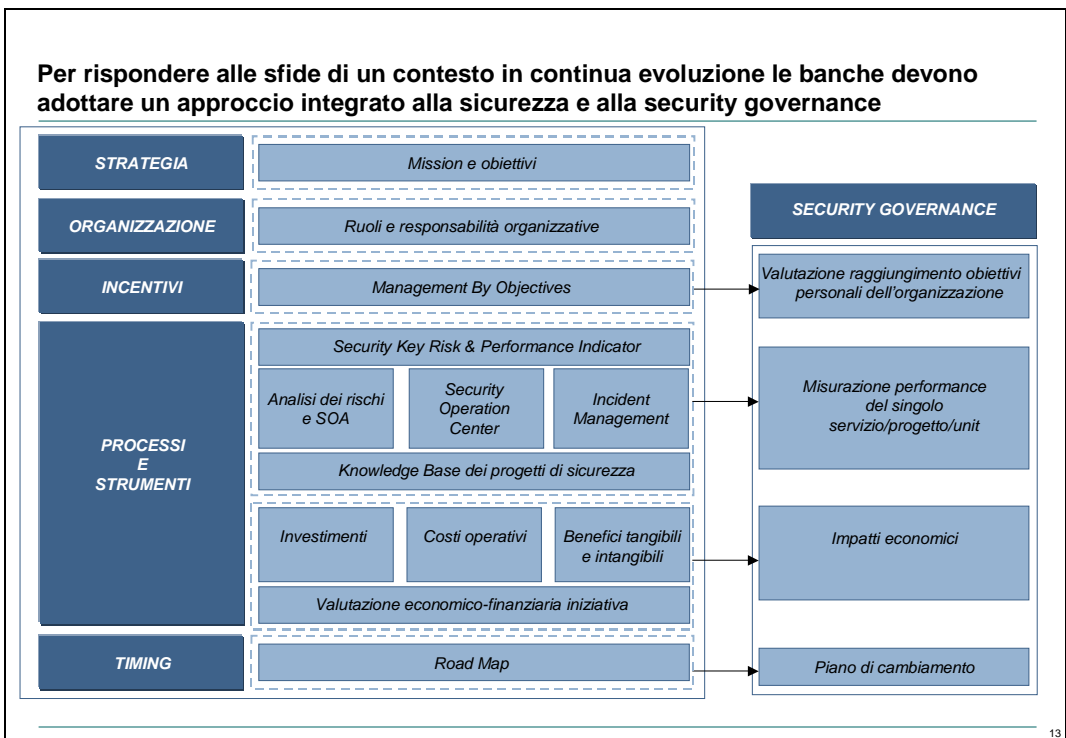
13

Agenda

- Le nuove sfide di sicurezza in ambito bancario
- Le risposte possibili
 - Modelli organizzativi per la gestione della sicurezza
 - Approccio e strumenti per la security governance
- Conclusioni

12

14



13

15

I Key Performance Indicators (KPIs) possono essere uno strumento efficace di pianificazione e gestione della sicurezza all'interno della banca

Adottando una **metodologia di gestione della sicurezza** come da standard **ISO 17799** ...

... è possibile costruire un sistema di **raccolta sistematica** di misurazioni di **rischio e performance** ...

... al fine di ricavarne **indicatori specifici (KRI, Key Risk Indicator e KPI, Key Performance Indicator)** da inserire negli **event type** del rischio operativo di **Basilea II**

- 1 Caratteristiche generali del governo della sicurezza
- 2 Policy di Sicurezza
- 3 Organizzazione della Sicurezza
- 4 Classificazione e controllo degli Assets
- 5 Sicurezza del personale
- 6 Sicurezza fisica ed ambientale
- 7 Gestione della comunicazione e dell'operatività
- 8 Controllo degli accessi
- 9 Sviluppo e manutenzione dei sistemi
- 10 Gestione della Business Continuity
- 11 Compliance

Key Risk Indicators
Key Performance Indicators

"Internal fraud" risk

"External fraud" risk

"System failure" risk

14

16

Il sistema di indicatori permette di realizzare un Security Tableau de Bord, con la possibilità di tracciare il positioning dell'azienda in tempo reale

ESEMPLIFICATIVO

MOCK-UP DEL SISTEMA

BANCA XX
Key Performance Indicators

Giorno XX Mese YY Anno 200X
| English Version | Contatti |

Banca XXX > **Key Performance Indicators > Access Control**

BENVENUTO Livello di performance complessivo

Livello 1

Livello 2

Livello 3

Livello 4

Processi

Internet Banking

ATM Cash Dispensing

Human Resource Management

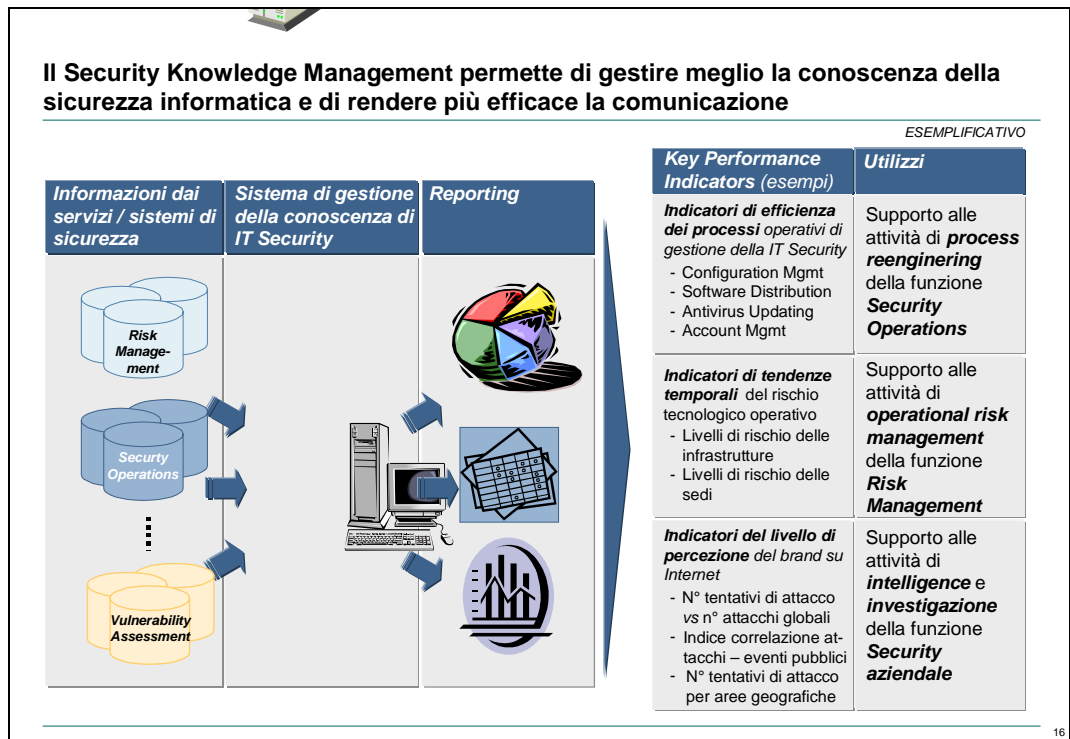
Investor Relation

...

	User Access Management	Network Access Control	System Access Monitoring	Application Access Control	Operating system access control	...
Andamento						
Valore	20	50	35	70	42	...
Obiettivo	40	75	50	200	50	...
Performance	50%	67%	70%	35%	84%	...
Frequenza	Mensile	Giornaliero	Settimanale	Settimanale	Trimestrale	...
K.P.I.						

15

17



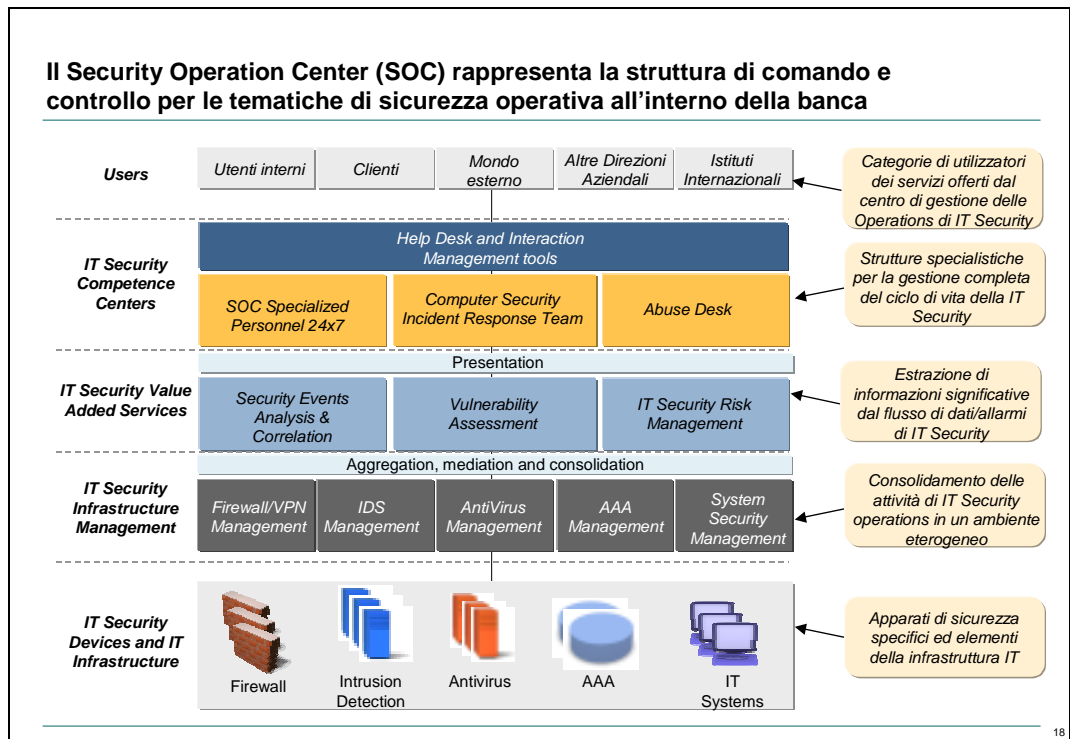
18

Esempio di Security Knowledge Management System

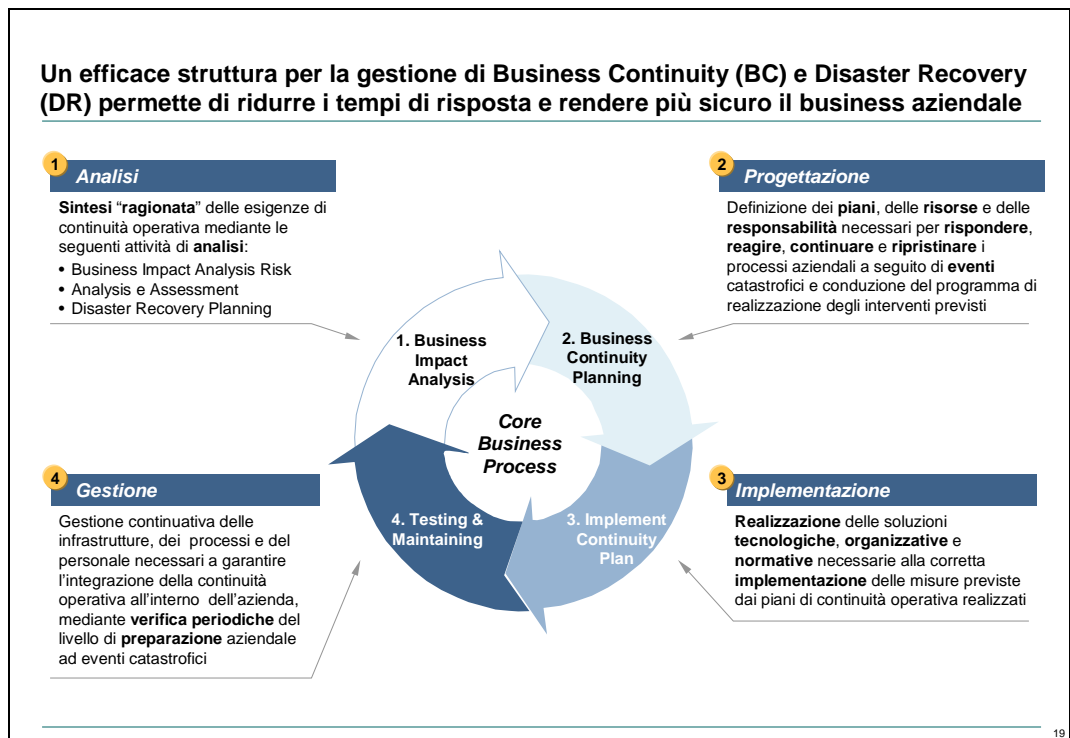
ESEMPLIFICATIVO

17

19



20



21

Soluzioni di sicurezza già disponibili possono permettere di contrastare con successo i rischi legati al furto dell'identità digitale nel multichannel banking

Le **soluzioni** per contrastare il fenomeno del phishing esistono, è necessario un piano organico che coinvolga tutti gli elementi che compongono la **catena tecnologica** necessaria per l'erogazione dei servizi di e-banking, partendo dalle banche fino ad arrivare ai **clienti finali** con l'ausilio di un **impianto legislativo** adeguato a prevenire e contrastare tale attività illecita

- Sicurezza bidirezionale delle comunicazioni banca-cliente**

È necessario **certificare l'identità** della banca nelle sue comunicazioni elettroniche verso i clienti
- Sistemi di autenticazione forti a due fattori**

Bisogna adeguare i **sistemi di autenticazione** con soluzioni più strong rispetto alle semplici credenziali username/password
- Formazione, sensibilizzazione verso i clienti finali**

Il cliente deve essere **educato sui rischi** e sensibilizzato sulle azioni da intraprendere in presenza di casi anomali
- Indicatori di rischio e di prestazione per la misura del fenomeno**

Il fenomeno deve essere **misurato** per comprendere le **aree di efficienza** e **orientare gli investimenti** laddove i risultati sono migliori

20

22

Agenda

- Le nuove sfide di sicurezza in ambito bancario
- Le risposte possibili
 - Modelli organizzativi per la gestione della sicurezza
 - Approccio e strumenti per la security governance
- **Conclusioni**

21

23

In sintesi

La sicurezza è una tematica sempre meno tecnologica e sempre più di business

La sicurezza è una componente abilitante fondamentale nel business bancario e per l'erogazione di servizi a valore aggiunto

Per gestire la sicurezza in modo efficace è necessario adottare un approccio manageriale, con una forte enfasi sul concetto di security governance

- pianificazione, controllo degli obiettivi
- disegno e gestione dei processi
- integrazione di soluzioni tecnologiche e organizzative in un'ottica bancaria

Il partner della banca sulle tematiche di sicurezza deve saper unire le due anime, consulenziale e tecnologica, per offrire soluzioni mirate ed end-to-end

22