Il Cyber Risk nell'Era Digitale: identificare e gestire le nuove forme di rischi operativi emergenti

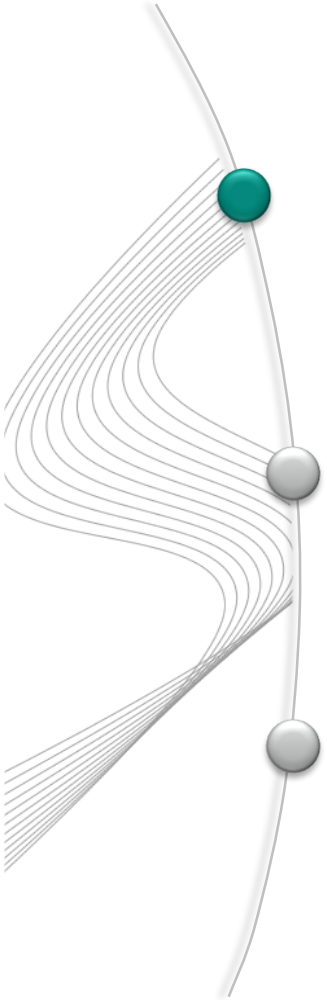
Nicasio Muscia – Senior Manager Finance & Risk Accenture

Diego Travaini – Security Senior Manager Accenture

21 Giugno 2016

Strategy | Consulting | Digital | Technology | Operations

Agenda



Contesto di riferimento

Possibile modello per la gestione del Cyber Risk

Alcune raccomandazioni

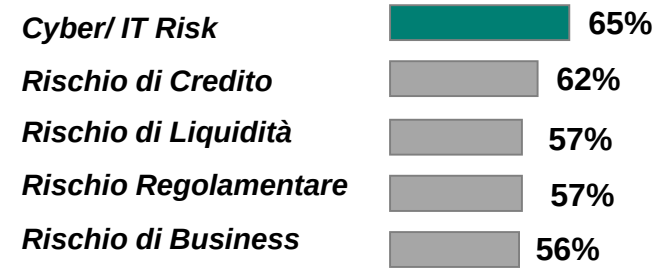
Una recente *survey* Accenture, che ha coinvolto 470 Risk Executives, evidenzia come la gestione del Cyber Risk rappresenti una priorità per le Banche

ACN Banking Risk Study 2015[1]:

ESTRATTO

Rischi

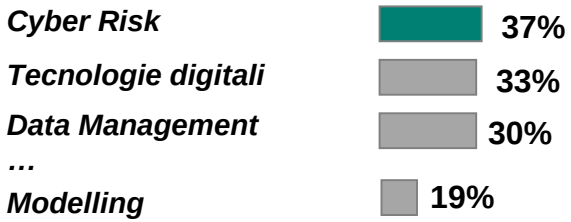
Rischi prioritari nei prox. 2 anni:



> *È necessario evolvere le capacità dell'Operational Risk di gestire le sfide del mondo digitale"*
>
> **R. Muniz, RM Director Caixa Economica Federal**

Competenze

Competenze richieste:



> *I modelli di business stanno evolvendo, è critico avere in azienda persone che pensino a soluzioni di discontinuità"*
>
> **A. Gupta, CRO American Express**

Intelligence

Realtà che utilizzano soluzioni di intelligence *(es. Risk Analytics, Big Data)*

> *L'uso di Analytics è critico nel nostro Gruppo"*
>
> **C. Palego, CRO Banco Popolare**

(1) Fonte: Survey condotta su 470 C-level di 50 Istituti Finanziari, da tre continenti differenti (America del Nord, Asia, Europa)
www.accenture.com/riskstudy2015

Il Cyber Risk può manifestarsi in una molteplicità di impatti causati da attaccanti che indirizzano gli asset/servizi aziendali

Rischio Reputazionale
- Perdita di fiducia *(interna and esterna)*
- Impatto sul Brand / Asset intangibili
- Time intensive / costo elevato di ripristino

Rischio IT e Operativo
- Indisponibilità processi e sistemi
- Discontinuità operativa

Fraud e Financial Crime
- Mancati ricavi e profitti, costi elevati

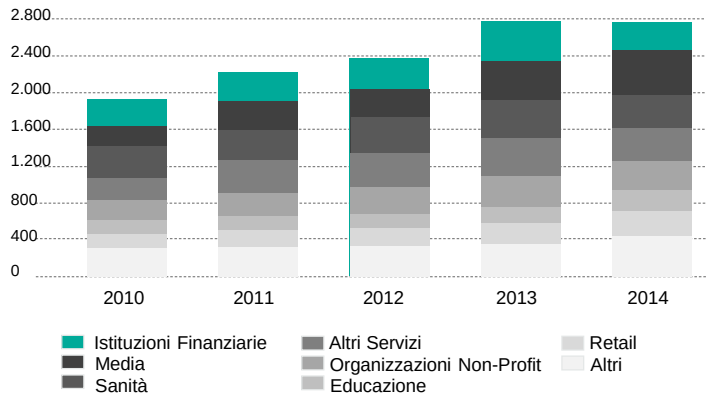
Fonti esterne del Cyber Risk
- Cybersquatter
- Hacktivism
- Hacker / lupi solitari
- Attacchi da Governi

Asset/ servizi aziendali
- Servizi digitali
- Pagamenti
- Trading elettronico
- Infrastruttura IT

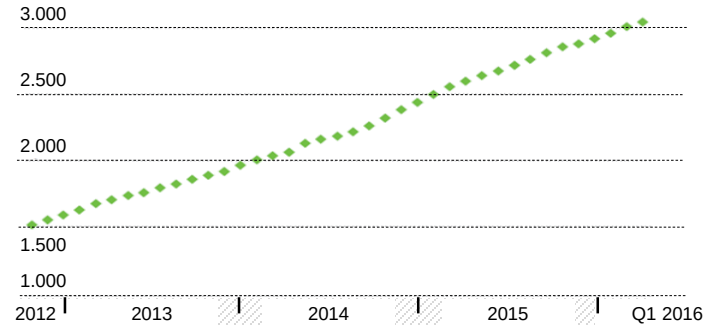
I trend di mercato confermano una numerosità degli eventi di Cyber Risk in forte crescita, cui corrisponde una stima in aumento di perdite e investimenti ad essi legati

Principali trend di mercato:

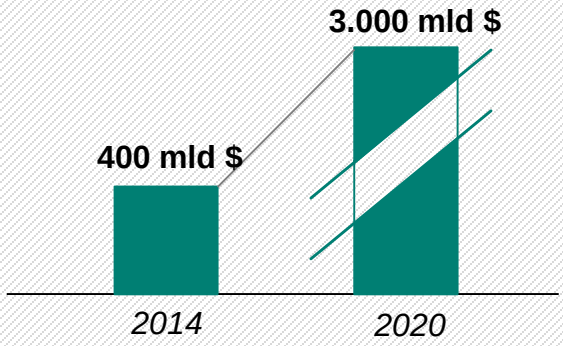
Incidenti Cyber per *industry* (1):



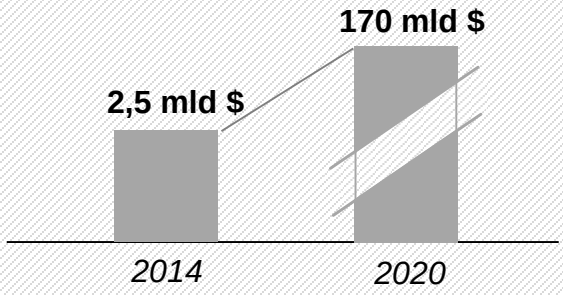
Percezione Cyber Risk dai Risk/Security Manager (2):



Stima perdite per attacchi Cyber (3):



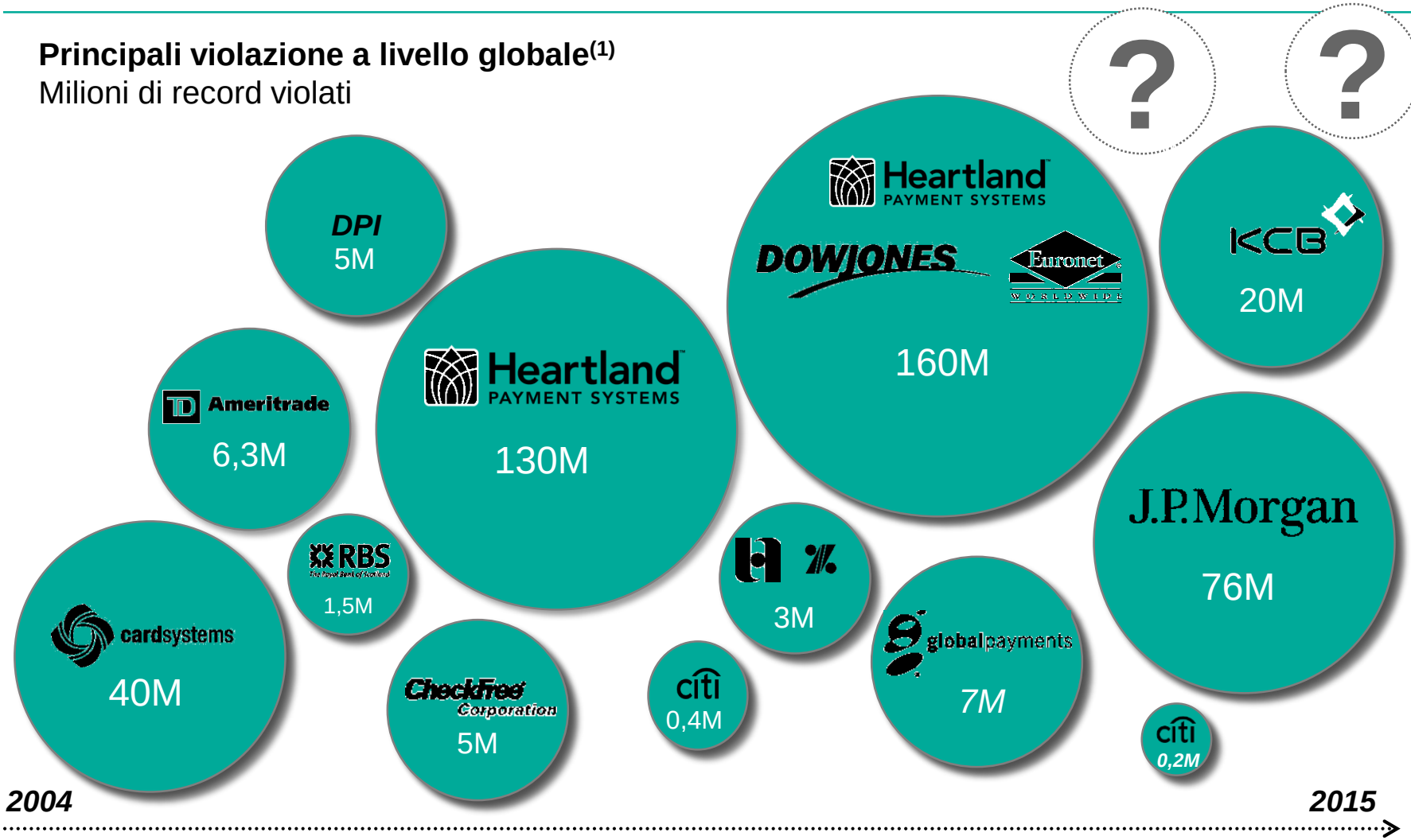
Stima investimenti per mitigazione (4):



(1) Fonte: www.cyberrisknetwork.com
(2) Fonte: www.cybersecurityindex.org
(3) Fonte: World Economic Forum - Global risks 2014 Ninth edition
(4) Fonte: Market & Markets - Cyber Security Market by Solution, Global Forecast to 2020

Di particolare rilievo per il settore finanziario sono gli attacchi informatici che hanno determinato la sottrazione/esposizione di dati (c.d. *data breach*)

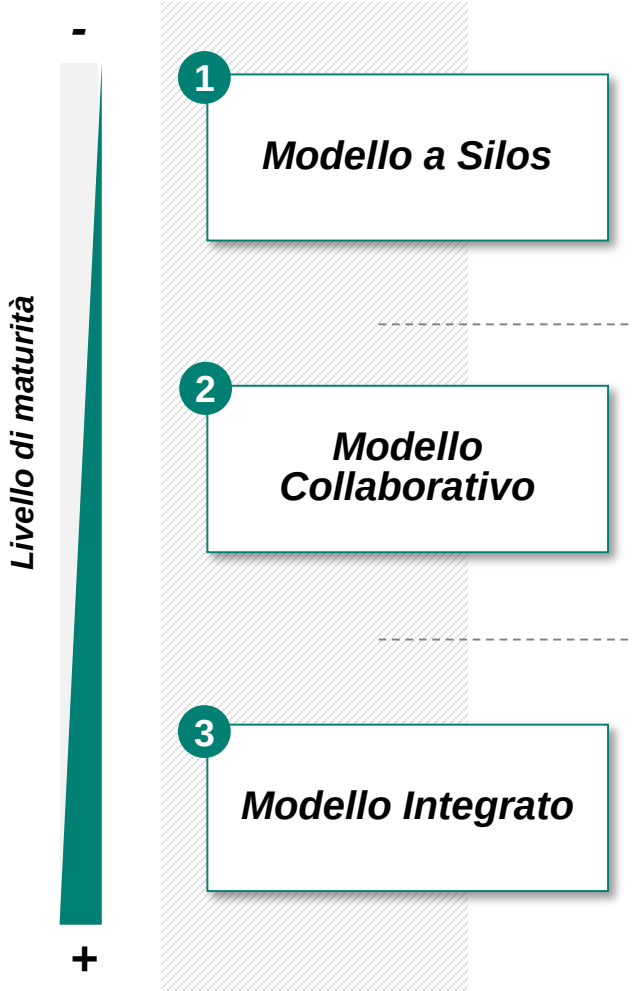
Principali violazione a livello globale[1]
Milioni di record violati



(1) Fonte: www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Ad oggi sul mercato sono presenti modelli alternativi per la gestione del Cyber Risk Management, caratterizzati da un livello di maturità ed efficacia differente

Modelli alternativi di gestione del Cyber Risk per livello di maturità:



1 *Modello a Silos*

- **Cyber Risk Management demandato ad IT/Sicurezza** *(con possibile duplicazione attività)* **e non integrato nel *framework* aziendale di Risk Management**
- **Nessun coinvolgimento strutture di business**

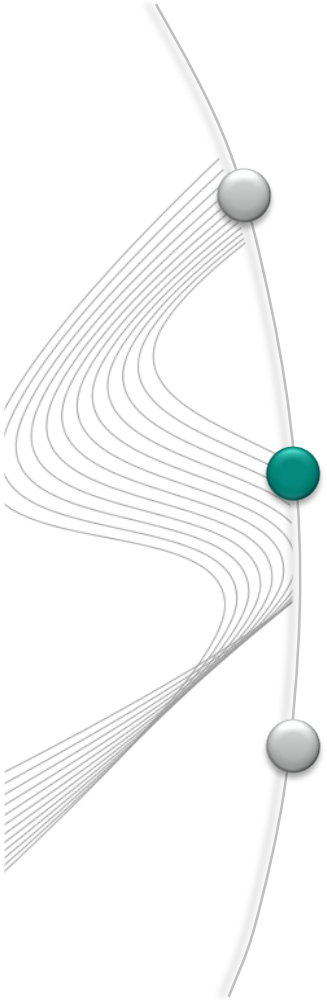
2 *Modello Collaborativo*

- **Scarso coinvolgimento del RM nella identificazione/ misurazione e mitigazione del Cyber Risk**
- **Prevenzione/monitoraggio demandati principalmente a soluzioni di Sicurezza**
- **Nessun coinvolgimento delle strutture di business**

3 *Modello Integrato*

- **Piena integrazione tra RM e IT/Sicurezza, i.e.:**
  - **linguaggio/tassonomie e *skills* comuni**
  - **coinvolgimento RM** *(a vari gradi)* **nelle fasi di (i) identificazione e misurazione; (ii) prevenzione, (iii) monitoraggio e (iv) mitigazione del rischio**
- **Coinvolgimento delle strutture di business**

Agenda



Contesto di riferimento

Possibile modello per la gestione del Cyber Risk

Alcune raccomandazioni

Un efficace gestione del Cyber Risk prevede l'adozione del Modello Integrato che richiede una convergenza delle *capabilities* di Risk Management e Sicurezza per la gestione congiunta del Cyber Risk

Modello Integrato

Descrizione attività e contributo Risk

1
- ***Analisi e classificazione delle Minacce di sicurezza e cyber*** *(Cyber Threat Intelligence)*
- ***Lessons learnt su Incidenti e valutazione degli impatti***

2 ***Definizione dei controlli e attività di prevenzione*** *(es. Vulnerability Assessment/ Penetration Tests, ecc.)*

3 ***Monitoraggio del profilo di rischio attraverso metriche dedicate*** *(es. KPI/ KRIs)*

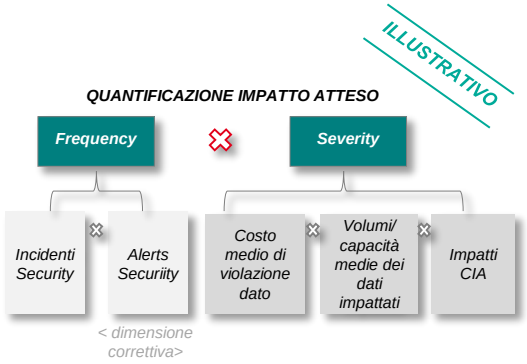
4 ***Azioni e strategie per ridurre/ eliminare/ trasferire il rischio***

Contributo Funzione RM:

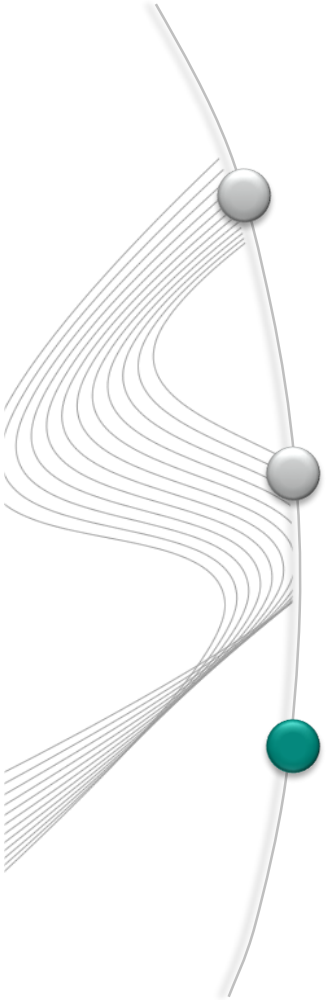
Basso | Medio | Medio-Alto | Alto | Molto Alto

Focus nella prossima slide

Nella fase di Identificazione e Misurazione del rischio, la Banca dovrà mettere a fuoco le possibili minacce di attacco e stimarne i relativi impatti al fine di prioritizzare gli interventi di mitigazione

Elementi Chiave	Principali attività	Esempi
Identificazione del Cyber Risk	▪ **Definizione Tassonomie di Rischio** per una più efficace identificazione/ classificazione degli eventi ▪ **Analisi e classificazione Incidenti/Minacce di Sicurezza** considerando, ove disponibili**, fonti informative qualificate** *(compresa 'Cyber Threat Intelligence')*	
Misurazione del Cyber Risk	▪ **Stima impatti attesi**, attraverso: 1. analisi storico **incidenti di sicurezza** in considerazione di **asset/dati impattati** 2. stima **volumi dei dati impattati** 3. stima **costo di violazione del dato** ▪ **Stima impatti potenziali** sulla base di eventi storici, attualizzati in base ai volumi in essere *('Scenario Analysis')*	

Agenda



Contesto di riferimento

Possibile modello per la gestione del Cyber Risk

Alcune raccomandazioni

Per un efficace gestione del Cyber Risk, è necessario (i) rafforzare alcuni ambiti specifici della Banca e (ii) favorire la diffusione della cultura e degli *standards* per la gestione del rischio nel settore

Possibili aree di miglioramento

Per i singoli Istituti Finanziari:

Organizzazione:

Rafforzare il coinvolgimento dell'organo di supervisione e la collaborazione tra Risk Management e Sicurezza

Cyber Intelligence:

Adottare soluzioni di Cyber Intelligence per favorire il monitoraggio pro-attivo delle minacce interne/esterne

Misurazione del Rischio:

Considerare gli impatti del Cyber Risk nelle valutazione di nuove iniziative di business (es. nuovi prodotti)

Per il Sistema Bancario:

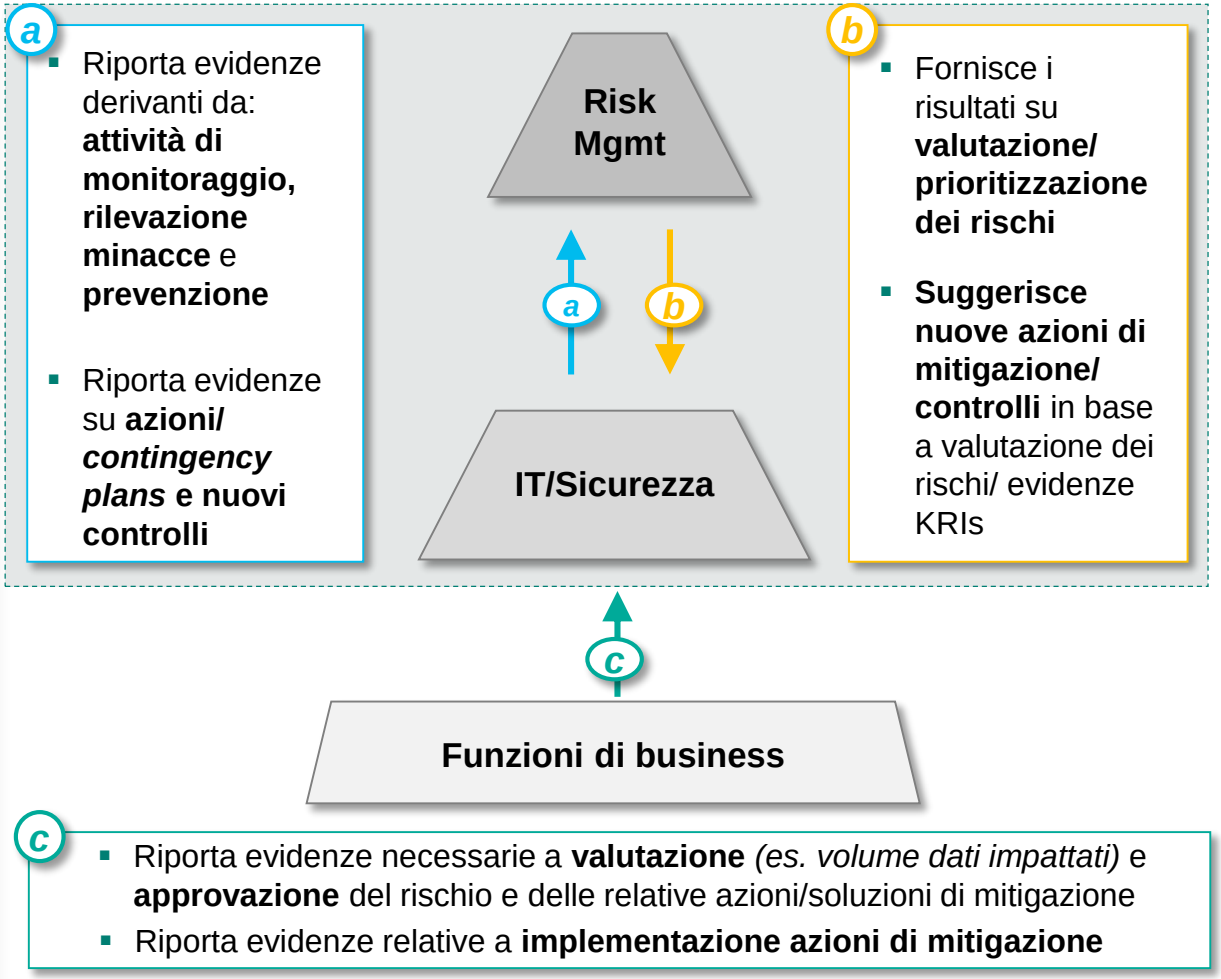
- Stabilire un **Cyber Forum** per sviluppare dialogo/ *best practices*
- Incoraggiare l'**utilizzo di Cyber Risk Management *standards***
- Aprire un tavolo per **detassare gli investimenti** in Cyber Risk Mgmt

Un adeguato assetto organizzativo prevede una stretta collaborazione tra RM e IT/Sicurezza oltre che un continuo coinvolgimento del business nella gestione del Cyber Risk

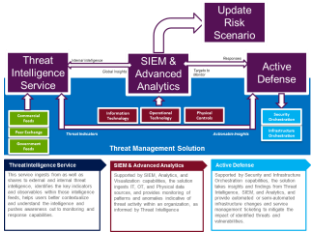
Raccomandazioni

1. **Coinvolgimento dell'Organo di Supervisione nella definizione del Framework**
2. **Scambio continuo flussi informativi tra gli attori coinvolti**
3. **Allineamento processo per strategie/ azioni di mitigazione**
4. **Definizione di tassonomie / linguaggi comuni**

Principali flussi informativi



Il nuovo paradigma per la Cyber Security sfrutta tutte le informazioni disponibili su minacce per intervenire proattivamente per il contenimento degli impatti

Soluzione	Descrizione	Esempi
Cyber Threat Intelligence	▪ **Raccoglie info relative a minacce / eventi esterni** *(da terze parti, enti Governativi, associazioni di categoria e peers)* ▪ **Evidenzia *alert* significativi** per supportare interventi proattivi di contenimento/mitigazione del rischio Cyber	*Report Threat Intelligence* ILLUSTRATIVO 
Advanced Security Analytics	▪ **Consolida e correla informazioni da fonti interne** *(log applicativi, DLP, SIEM)* **ed esterne** *(feed Cyber Threat Intelligence)* ▪ **Fornisce indicazioni sull'attività delle minacce** *(analisi di pattern e anomalie)* **nel contesto aziendale**	*Report Analytics* ILLUSTRATIVO 
Active defense	▪ **E' alimentato da evidenze *Cyber Threat Intelligence e Advanced Sec. Analytics*** ▪ **Permette azioni di difesa / contenimento semi-automatizzate / automatizzate** *(es. blocco traffico malevolo, isolamento postazioni, scansione antivirus)*	Struttura *Active Defense* ILLUSTRATIVO 

La misurazione del Cyber Risk è fondamentale al fine identificare preventivamente i rischi connessi a nuove iniziative di business e indirizzare le opportune azioni correttive

La misurazione del Cyber Risk per le nuove iniziative di business:

Fasi	*Descrizione*	*Esempio*
Analisi Preliminare	▪ **Raccolta e analisi delle informazioni** legate all'iniziativa **per identificare l'approccio da seguire per la valutazione del profilo di rischio**	***Valutazione lancio nuovo prodotto Carta Contactless*** ***Raccolta delle caratteristiche chiave*** *dell'iniziativa* ***tramite Check-list/ Questionari*** *(e.g. Canali utilizzati, dati gestiti, Interfacce / soluzioni architetturali, modalità di accesso, etc.)*
Project Risk Assessment	▪ **Stima quantitativa e qualitativa dei rischi** *(incluso Cyber Risk),* **associati all'iniziativa, secondo una logica *''rischio-rendimento"***	***Valutazione Quantitativa dell'impatto*** *in termini di:* ▪ *Perdite attese sulla base dello storico a disposizione* ▪ *RWA Atteso* ▪ *Analisi di Scenario* ***Valutazione qualitativa dei rischi non quantificabili*** *(es. reputazionale, di conformità)*