BPER:
Banca

Mitigare il cyber risk: integrazione tra risk management e sicurezza nel Gruppo Bper

Daniele Tassile
Christian Igor Ciceri

Roma, 21/05/2016

Premessa

CRESCENTE CONSAPEVOLEZZA DEL CYBER RISK

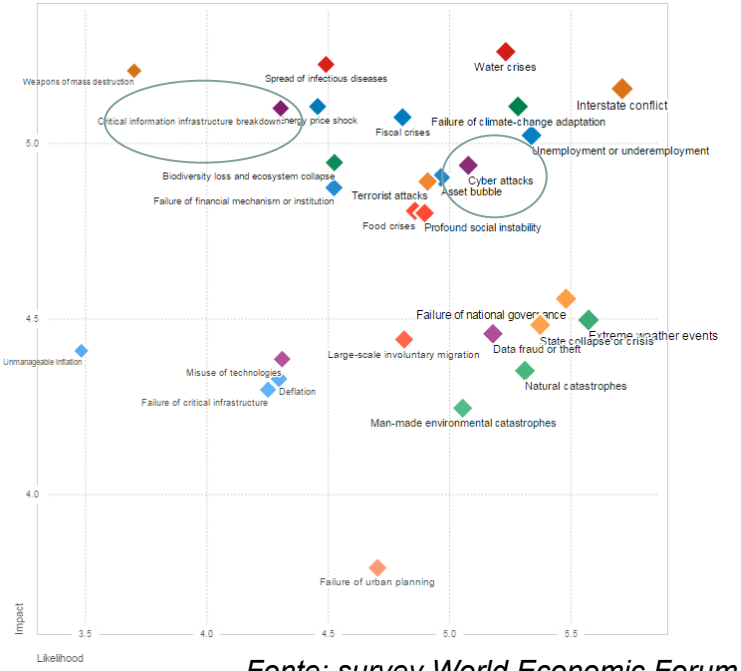
Top 10 Operational Risks for 2016

Risk.net presents the Top 10 Operational Risks of 2016, as chosen by risk practitioners

Risk Management | 20 January 2016

- ***Cyber risk classificato da risk.net nei top 10 risk nel 2015 e 2016***

Il report di Symantec *Internet Security threat report 2016*:
▪posiziona l'Italia al 13° posto a livello mondiale nella classifica delle minacce cyber.
▪indica Botnet e ransomware come le principali minacce.



Fonte: survey World Economic Forum

News | Wed May 18, 2016 7:07am EDT

SEC says cyber security biggest risk to financial system

MOODY'S INVESTORS SERVICE

Announcement: Moody's: Threat of cyber risk is of growing importance to credit analysis

Global Credit Research - 23 Nov 2015

New York, November 23, 2015 -- The threat of cyber attacks continues to rise across all sectors, and the implications could start taking a higher priority in credit analysis, according to Moody's Investors Service in a new report. Moody's views material cyber threats in a similar vein as other extraordinary event risks, such as a natural disaster, with any subsequent credit impact depending on the duration and severity of the event.

- ***La minaccia di un cyber attack rientra nelle prime 10 posizioni per probabilità di accadimento.***
- ***I guasti / avarie delle infrastrutture critiche IT sono classificate nelle prime 10 posizioni per impatto economico.***

Premessa

FREQUENZA CRESCENTE

Si verificano mediamente un numero di cyber attack quotidiani (dal furto di dati alla violazione della privacy, dall'attacco ai sistemi informatici di un'azienda alla diffusione di malware che bloccano la supply chain) compreso tra i 40.000 e i 50.000.

Fonte mappa interattiva Fire Eye

Il contesto bancario

EVOLUZIONE DEL RISCHIO OPERATIVO

- **NUOVE TECNOLOGIE**
- **INTERNET**
- **DIGITALIZZAZIONE DEI PROCESSI**

EVOLUZIONE DEL RISCHIO OPERATIVO

AUTOMAZIONE E CONTROLLI PREVENTIVI

- *Maggiore automazione dei processi e dei controlli*
- *Incremento dell'efficacia dei controlli preventivi*

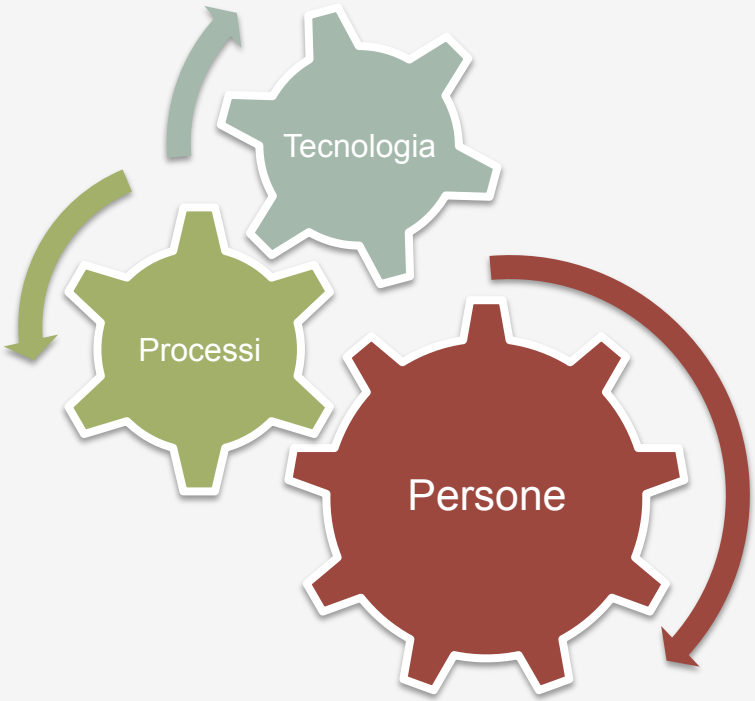
ESPOSIZIONE CRESCENTE AL CYBER RISK

- *Aumento degli incidenti*
- *Nuove minacce*
- *Protezione dei dati aziendali più costosa*

Potenziale insorgere di ulteriori rischi:
- Perdite economiche / di quote di mercato
- Maggiori costi legali ed assicurativi
- Sanzioni
- Rischi di continuità del business
- Rischi reputazionali

Cybersecurity

UNA DEFINIZIONE



La Cybersecurity è una combinazione di persone, processi e tecnologie ed è un problema dell'azienda, non solo dell'Information Technology. L'attuazione delle misure di sicurezza sulle informazioni non deve essere limitata al reparto IT, ma si deve riflettere in tutta l'azienda ed in tutte le sue componenti organizzative. Il perimetro e la visione della Cybersecurity deve comprendere quindi persone, prodotti, impianti, processi, policies, procedure, sistemi, tecnologie, dispositivi, reti ed informazioni.

Cybersecurity

ALCUNI FATTORI DI MATURITA'

Information Risk Management

Stabilire una struttura di governance efficace e determinare la propensione al rischio informatico, come accade per gli altri rischi. Mantenere informato il Board sui cyberisk.

Access Management Definire i processi di gestione degli accessi. Rispettare il criterio del "minimo privilegio". Limitare gli utenti privilegiati.	**Training & Awareness** Produrre policies che definiscano in modo chiaro l'uso in sicurezza dei sistemi aziendali. Definire un programma di formazione per gli utenti e sensibilizzarli al rischio informatico	**Incident Response Plan** Introdurre un piano di azione in caso di incidenti di sicurezza. Costituire un CSIRT. Formare le persone coinvolte nel piano. Testare ed aggiornare periodicamente l'IRP.
Collect Logs & Monitoring Implementare sistemi e processi al fine di garantire un costante monitoraggio degli output provenienti dai vari sistemi.	**Vulnerability Manag. Progr.** Analizzare continuamente le potenziali vulnerabilità del sistema informatico. Aggiornare sistematicamente sistemi e software di ogni genere.	**Intelligence** Avere in tempo reale una visione totale delle minacce e delle anomalie emergenti.
Mobile Working Sviluppare una policy per il lavoro in mobilità e formare il personale affinché la applichi. Introdurre standard di sicurezza per tutti i dispositivi. Proteggere i dati in transito e sui dispositivi.	**Distinguish Targeted Attacks** Avere chiara la differenza tra attacchi mirati e non mirati per garantire azioni di risposta proporzionate alla scala e alla complessità di attacco.	**Malware Protection** Stabilire delle difese anti-malware efficaci e applicabili a tutte le aree di business . Combinare le tecniche di difesa per mitigare i rischi.

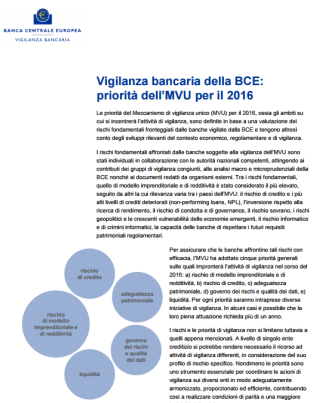
Attenzione crescente della Vigilanza (1/2)

CONTESTO DI RIFERIMENTO

Enfasi su monitoraggio continuo ed attenzione crescente anche nei confronti degli IT outosurcer

- **Rischio di criminalità informatica identificato come un tema strategico per l'attività di vigilanza nel 2015**
  - Cyber Risk questionnaire
  - Avvio attività ispettive per la verifica dei livelli di sicurezza informatica implementati dalle banche

Controls	Items to consider	Score 1-4	Rationale and Supporting documentation
IDENTIFY			
1 Asset Management		2 - Partially implemented	
	* Software platforms and applications within the organization are inventoried	2 - Partially implemented	The applications inventory for server components, workstations and laptops is carried out through TEM (Tivoli Endpoint Management). An official list of authorized software and the relative versions is not yet available.
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy	* Maps of network resources, connections with external and mobile resources and data flows are created and updated	2 - Partially implemented	The regulatory framework for the management and updating of the IT systems has been defined. The mapping project has been implemented in order to populate a CMDB and keep it updated.
	* Resources (e.g., hardware, devices, data, and software) are prioritized for protection based on their sensitivity and business value	2 - Partially implemented	The regulatory framework for the classification of the IT resources has been defined. The support documentation is "Manuale per la classificazione delle informazioni" (Manual for the classification of data). The regulatory framework in support of current operating practices is in the process of being implemented.
3 Governance		2 - Partially implemented	
	* Outsourced IT resources comply with the same requirements as inhouse resources (and processes are in place to manage that)	2 - Partially implemented	A regulatory framework has been applied to processes which define the methodology for outsourcing services and the controls to be carried out, also in relation to cybersecurity. The prompt adoption of the regulations on the part of the suppliers is in the course of being verified.
PROTECT			
6 Access Control		2 - Partially implemented	
	* Access permissions are managed, incorporating the principles of least privilege and separation of duties	2 - Partially implemented	There is an access authority which manages all the access requests and which, through a structured process and an automatic technological infrastructure (via Active Directory, LDAP) guarantees the disablement or revocation of accounts. The assignment of access to resources and data according to principles of least privilege are regulated through specific rules. A specific activity is underway in order to remap user profiles according to their company roles.
8 Data Security			A Data Loss Prevention system which will allow the protection of data which transits through outgoing emails is in the process of


BANCA CENTRALE EUROPEA
VIGILANZA BANCARIA

Vigilanza bancaria della BCE: priorità dell'MVU per il 2016

Le priorità del Meccanismo di vigilanza unico (MVU) per il 2016, ossia gli ambiti su cui si incentrerà l'attività di vigilanza, sono definite in base a una valutazione dei rischi fondamentali fronteggiati dalle banche vigilate dalla BCE e tengono altresì conto degli sviluppi rilevanti del contesto economico, regolamentare e di vigilanza.

I rischi fondamentali affrontati dalle banche soggette alla vigilanza dell'MVU sono stati individuati in collaborazione con le autorità nazionali competenti, attingendo ai contributi dei gruppi di vigilanza congiunti, alle analisi macro e microprudenziali della BCE nonché ai documenti redatti da organismi esterni. Tra i rischi fondamentali, quello di modello imprenditoriale e di redditività è stato considerato il più elevato, seguito da altri la cui rilevanza varia tra i paesi dell'MVU. Il rischio di credito e i più alti livelli di crediti deteriorati (non-performing loans, NPL), l'inversione rispetto alla ricerca di rendimento, il rischio di condotta e di governance, il rischio sovrano, i rischi geopolitici e le crescenti vulnerabilità delle economie emergenti, il rischio informatico e di crimini informatici, la capacità delle banche di rispettare i futuri requisiti patrimoniali regolamentari.

Per assicurare che le banche affrontino tali rischi con efficacia, l'MVU ha adottato cinque priorità generali sulle quali improntera l'attività di vigilanza nel corso del 2016: a) rischio di modello imprenditoriale e di redditività, b) rischio di credito, c) adeguatezza patrimoniale, d) governo dei rischi e qualità dei dati, e) liquidità. Per ogni priorità saranno intraprese diverse iniziative di vigilanza. In alcuni casi è possibile che le loro piena attuazione richieda più di un anno.

I rischi e le priorità di vigilanza non si limitano tuttavia a quelli appena menzionati. A livello di singolo ente creditizio si potrebbe rendere necessario il ricorso ad attività di vigilanza differenti, in considerazione del suo profilo di rischio specifico. Nondimeno le priorità sono uno strumento essenziale per coordinare le azioni di vigilanza sui diversi enti in modo adeguatamente armonizzato, proporzionato ed efficiente, contribuendo così a realizzare condizioni di parità e una maggiore incisività della vigilanza.

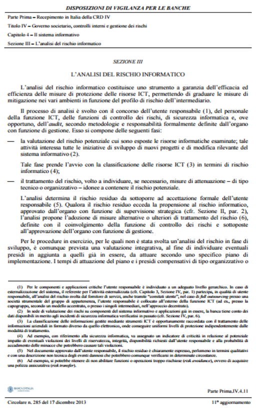
- **Cyber risk tra le priorità 2016 della Vigilanza**
  - Questionnaire on IT outsourcing and cloud computing

Attenzione crescente della Vigilanza (2/2)

CONTESTO DI RIFERIMENTO ITALIANO

- **15° Aggiornamento della Circolare Banca d'Italia 263 nel 2014 (successivamente confluita nella circolare 285/2013)**

  - **Monitoraggio continuo degli applicativi in uso e analisi preventiva per le iniziative di sviluppo o per l'aggiornamento rilevante del sistema informativo**



DISPOSIZIONI DI VIGILANZA PER LE BANCHE

Parte Prima – Recepimento in Italia della CRD IV
Titolo IV – Governo societario, controlli interni e gestione dei rischi
Capitolo 4 – Il sistema informativo
Sezione III – L'analisi del rischio informatico

SEZIONE III

L'ANALISI DEL RISCHIO INFORMATICO

L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT, permettendo di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio dell'intermediario.

Il processo di analisi è svolto con il concorso dell'utente responsabile (1), del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove opportuno, dell'*audit*, secondo metodologie e responsabilità formalmente definite dall'organo con funzione di gestione. Esso si compone delle seguenti fasi:

— la valutazione del rischio potenziale cui sono esposte le risorse informatiche esaminate; tale attività interessa tutte le iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo (2).

Tale fase prende l'avvio con la classificazione delle risorse ICT (3) in termini di rischio informatico (4);

— il trattamento del rischio, volto a individuare, se necessario, misure di attenuazione – di tipo tecnico o organizzativo – idonee a contenere il rischio potenziale.

L'analisi determina il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile (5). Qualora il rischio residuo ecceda la propensione al rischio informatico, approvato dall'organo con funzione di supervisione strategica (cfr. Sezione II, par. 2), l'analisi propone l'adozione di misure alternative o ulteriori di trattamento del rischio (6), definite con il coinvolgimento della funzione di controllo dei rischi e sottoposte all'approvazione dell'organo con funzione di gestione.

Per le procedure in esercizio, per le quali non è stata svolta un'analisi del rischio in fase di sviluppo, è comunque prevista una valutazione integrativa, al fine di individuare eventuali presidi in aggiunta a quelli già in essere, da attuare secondo uno specifico piano di implementazione. I tempi di attuazione del piano e i presidi compensativi di tipo organizzativo o

(1) Per le componenti e applicazioni critiche l'utente responsabile è individuato a un adeguato livello gerarchico. In caso di esternalizzazione del sistema, il referente per l'attività esternalizzata (cfr. Capitolo 3, Sezione IV, par. 1) partecipa, in qualità di utente responsabile, all'analisi del rischio svolta dal fornitore di servizi, anche tramite "comitati utente"; nel caso di *full outsourcing* presso una società strumentale del gruppo di appartenenza, l'utente responsabile è collocato all'esterno della funzione ICT (ad es., presso la capogruppo, secondo un modello accentrato, o presso i singoli intermediari, nell'approccio decentrato).

(2) In sede di valutazione dei rischi su componenti del sistema informativo e applicazioni già in essere, la banca tiene conto dei dati disponibili in merito agli incidenti di sicurezza informatica verificatisi in passato (cfr. Sezione IV, par. 6).

(3) La classificazione delle informazioni gestite mediante strumenti ICT è opportunamente raccordata con il trattamento delle informazioni aziendali in formato diverso da quello elettronico, onde conseguire uniformi livelli di protezione indipendentemente dalle modalità di trattamento.

(4) Ad esempio, con riferimento alla sicurezza informatica, va assegnato un indicatore di criticità in relazione al potenziale impatto di eventuali violazioni dei livelli di riservatezza, integrità, disponibilità richiesti dall'utente responsabile e alla probabilità di accadimento delle minacce che potrebbero causare tali violazioni.

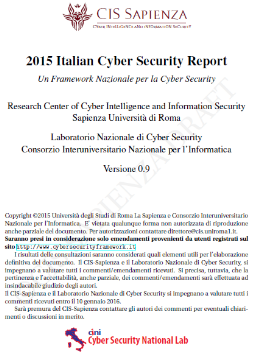
(5) Nel documento approvato dall'utente responsabile, il rischio residuo è chiaramente espresso, perlomeno in termini qualitativi e con una descrizione non tecnica degli eventi dannosi che potrebbero comunque verificarsi in determinate circostanze.

(6) Ad esempio, si potrebbe ritenere di non abilitare funzioni o operazioni troppo rischiose (*risk avoidance*), ovvero di acquisire una polizza assicurativa (*risk transfer*).

Parte Prima.IV.4.11

Circolare n. 285 del 17 dicembre 2013 — 11° aggiornamento

- **16° aggiornamento del 17 maggio 2016 alla Circolare n. 285 del 17 dicembre 2013 recante «Disposizioni di Vigilanza per le banche» introduce una Sezione che disciplina gli obblighi imposti alle banche che prestano servizi di pagamento tramite canale internet**



CIS Sapienza
Cyber Intelligence and Information Security

2015 Italian Cyber Security Report

Un Framework Nazionale per la Cyber Security

Research Center of Cyber Intelligence and Information Security
Sapienza Università di Roma

Laboratorio Nazionale di Cyber Security
Consorzio Interuniversitario Nazionale per l'Informatica

Versione 0.9

Copyright ©2015 Università degli Studi di Roma La Sapienza e Consorzio Interuniversitario Nazionale per l'Informatica. E' vietata qualunque forma non autorizzata di riproduzione anche parziale del documento. Per autorizzazioni contattare direttore@cis.uniroma1.it. **Saranno presi in considerazione solo emendamenti provenienti da utenti registrati sul sito** http://www.cybersecurityframework.it

I risultati delle consultazioni saranno considerati quali elementi utili per l'elaborazione definitiva del documento. Il CIS-Sapienza e il Laboratorio Nazionale di Cyber Security, si impegnano a valutare tutti i commenti/emendamenti ricevuti. Si precisa, tuttavia, che la pertinenza e l'accettabilità, anche parziale, dei commenti/emendamenti sarà effettuata ad insindacabile giudizio degli autori.
Il CIS-Sapienza e il Laboratorio Nazionale di Cyber Security si impegnano a valutare tutti i commenti ricevuti entro il 10 gennaio 2016.

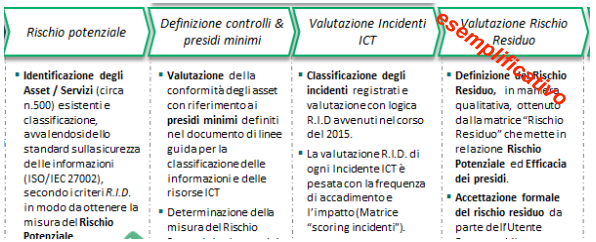
Sarà premura del CIS-Sapienza contattare gli autori dei commenti per eventuali chiarimenti o discussioni in merito.

cini Cyber Security National Lab

Framework nazionale per la cyber security realizzato da CIS-Sapienza e dal Laboratorio Nazionale di Cyber Security offre alle organizzazioni un approccio omogeneo per affrontare la cyber security

Ruolo del Risk Management

ADOZIONE DI UN FRAMEWORK



- Adozione di un approccio integrato al cyber risk che favorisca il confronto tra Risk e Sicurezza, dalla definizione ed implementazione del framework di gestione alla condivisione della normativa interna e dei principali processi di gestione (es. incident management)

- Monitoraggio continuo all'interno e verso terze parti (fornitori, clienti, consulenti ecc.)
  - catalogo delle minacce e attività di threat modeling
  - valutazione del grado di rischio degli asset informatici, con particolare riferimento a quelli critici
  - processi di incident management (la domanda non è più se ma quando..)
  - definizione di una soglia di tolleranza e di azioni di mitigazione per ridurre i rischi che eccedono la soglia di tolleranza definita dal CdA o trasferimento dei rischi all'esterno
  - reporting al Top management e al Consiglio di Amministrazione

La Cybersecurity nel Gruppo BPER

IL MODELLO IMPLEMENTATO

Il Gruppo BPER ha definito un **modello di presidio della sicurezza informatica,** intesa come l'insieme dei *processi*, dei *presidi* e delle *misure di natura tecnologica*, *organizzativa, procedurale e normativa*, volto a garantire un livello di protezione e controllo del rischio lungo l'intero ciclo di vita delle risorse informatiche e delle informazioni da esse gestite, in relazione ai requisiti di:

Riservatezza	Integrità	Disponibilità	Tracciabilità	Verificabilità
capacità di rendere disponibili o rivelare le informazioni solo e soltanto a individui, entità o processi autorizzati ad accedervi	capacità di salvaguardare l'autenticità e la completezza delle informazioni	capacità di rendere accessibili e utilizzabili le informazioni secondo tempi e modi richiesti da un'entità autorizzata	capacità di attribuire in maniera univoca gli accadimenti sul sistema informativo al fine di garantirne il non ripudio	garanzia di poter ricostruire, all'occorrenza e a distanza di tempo, eventi connessi all'utilizzo del sistema informativo e al trattamento di dati

Il modello è definito tramite il **«Sistema di Gestione della Sicurezza Informatica»** ed è formalizzato all'interno del Gruppo tramite un impianto normativo composto da *Policy*, *Regolamenti* e *Procedure Organizzative*. Il modello è presidiato direttamente da parte del **Chief Information Officer** in quanto responsabile dell'ICT a livello di Gruppo ed è stabilito presso la Capogruppo.

Sistema di Gestione della Sicurezza Informatica

Impianto Normativo

- *Policy di Gruppo*
- *Regolamenti*
- *Procedure Organizzative*

Principali attori coinvolti

- *Chief Risk Officer* (**CRO**)*e Chief Information Officer* (**CIO**) di Gruppo

- Ufficio *Rischi Operativi* e Ufficio *Architetture e Sicurezza Informatica*

Fattori di rischio

PRINCIPALI EVIDENZE

- Il 57% degli incidenti di sicurezza sono da ricondurre a cause interne
- Il 35 % degli incidenti di sicurezza sono il risultato di un errore umano
- I crimini informatici più costosi per l'azienda sono quelli provocati dal personale interno

MINACCE

Le minacce fanno sempre più leva sulle vulnerabilità umane e su comportamenti non conformi alle regole e alle comuni prassi di sicurezza

RISORSE UMANE

Fattore di rischio maggiormente impattato

AZIONI DI MITIGAZIONE

Necessità di azioni preventive per diffondere la cultura e awarness, formazione e sensibilizzazione del personale

Azioni di mitigazione

TRASFERIMENTO DEL RISCHIO

- Anche l'azienda con i migliori presidi di sicurezza si troverà ad affrontare una violazione alla sicurezza: la domanda è quando, non se.

- La spesa sostenuta dal comparto bancario per il trasferimento all'esterno del rischio cyber occupa una fascia bassa rispetto ad altre industry.

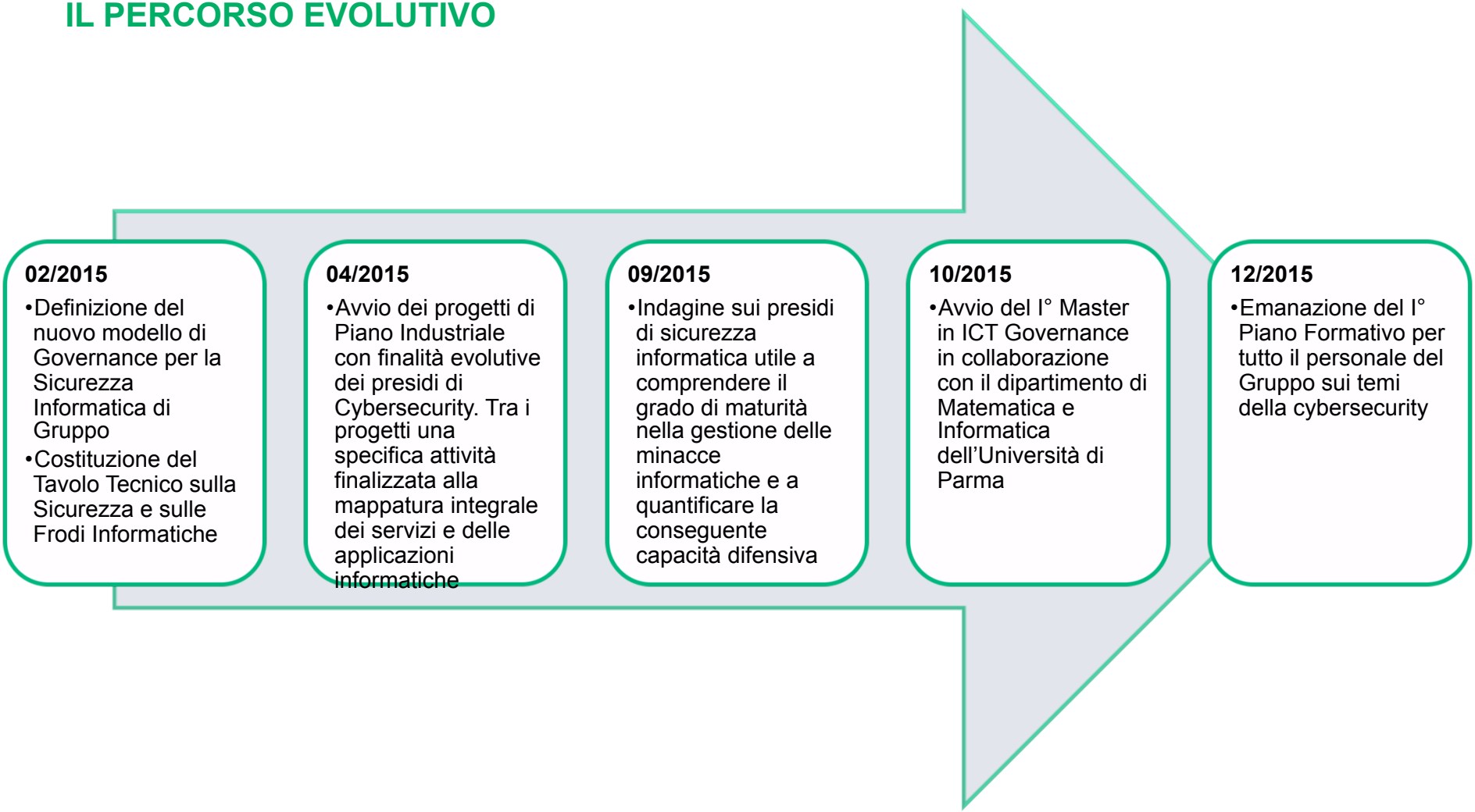
- Il Gruppo Bper ha deciso, nell'ambito della gestione del rischio cyber, di trasferire parte del rischio all'esterno ed è stato tra i primi Gruppi Bancari Italiani a sottoscrivere una polizza Cyber con la Compagnia ACE.

- Coperture previste per eventi che possono colpire il comparto dati:
  - perdite finanziarie;
  - costi di ripristino dati (es. ricostituzione dati e archivi digitali, spese per «bonifica», business interruption, costi derivanti da comunicazioni ai clienti, spese legali, consulenti ecc.).

    - La copertura copre sia dolo che frodi interne ed esterne (intrusioni nel sistema e attacchi informatici).

La Cybersecurity nel Gruppo BPER

IL PERCORSO EVOLUTIVO



Cybersecurity Assessment

VALUTAZIONE DEL LIVELLO DI MATURITA' RAGGIUNTO

Con la collaborazione di uno dei principali esperti mondiali nei servizi di consulenza sulla Cybersecurity, il Gruppo BPER ha condotto un'indagine sui presidi di sicurezza informatica utile a comprendere il grado di maturità nella gestione delle minacce informatiche e a quantificare la conseguente capacità difensiva.

FASE I

- Analisi del modello organizzativo e operativo
- Comprensione della governance aziendale
- Verifica dele policies e delle procedure interne
- Comprensione dei presidi tecnologici e di intelligence

FASE II

- Valutazione delle specifiche capacità delle UO coinvolte nella gestione delle minacce
- Valutazione delle capacità e della maturità raggiunta nella gestione degli incidenti
- Focus su metriche, rilevazione, contenimento e risposta agli attacchi

FASE III

- Simulazione realistica di attacco
- Confronto verbale sulle azioni intraprese durante l'attacco
- Valutazione della capacità di risposta del CIRT rispetto all'Incident Response Plan aziendale

FASE IV

- Report di sintesi e di dettaglio delle evidenze riscontrate
- Definizione delle raccomandazioni e della roadmap implementativa

LE FUNZIONI AZIENDALI COINVOLTE

COO, CIO, Sicurezza Informatica, Divisione IT, Risk Management, Internal Audit, Compliance, Organizzazione

Formazione e Governance

IL TAVOLO TECNICO SULLA SICUREZZA E FRODI INFORMATICHE

Formulare proposte in ordine all'evoluzione della strategia di sicurezza informatica;

Valutare le soluzioni progettuali e i piani di sviluppo più significativi

Monitorare i livelli di servizio in collaborazione con le funzioni aziendali preposte ai controlli, verificando periodicamente l'efficacia e l'efficienza dei presidi posti in essere

Analizzare periodicamente gli incidenti di sicurezza informatica e i tentativi di frode al fine di condividere le azioni difensive e i possibili scenari evolutivi

1
incontro mensile

18
n° medio partecipanti

Formazione e Governance

LE ATTIVITA' PER I CLIENTI E PER IL PERSONALE

Awareness della clientela

Pillole di Sicurezza Informatica

4 Video Tutorial di circa 1 minuto pubblicati sull'Home Banking e su You Tube

Affrontano i temi della sicurezza sul Web, sui dispositivi mobili, sulla protezione delle credenziali di accesso e sul phishing

+ 65.000 Visualizzazioni

Formazione al personale

Corsi di Formazione obbligatori online

5 differenti corsi per 5 diversi campioni d'utenza

Conoscenze di Sicurezza Informatica, Cybersecurity Awareness, Sicurezza delle Informazioni, best practice di sicurezza per amministratori di sistema e best practice OWASP per programmatori

+ 11.000 colleghi coinvolti

Formazione e Governance

LA COLLABORAZIONE CON L'UNIVERSITA' DI PARMA

I discenti, selezionati tra diversi tecnici provenienti da BPER Banca e da altre aziende specializzate nell'Information and Communication Technology, sono stati coinvolti in un percorso di studio della durata di 4 mesi, per 45 ore complessive di formazione. Le lezioni hanno approfondito temi relativi alla gestione e al miglioramento di moderni sistemi informatici e sono state arricchite anche da una parte pratica con analisi di case-study.

39
partecipanti professionisti del settore

45
ore di formazione in 4 mesi

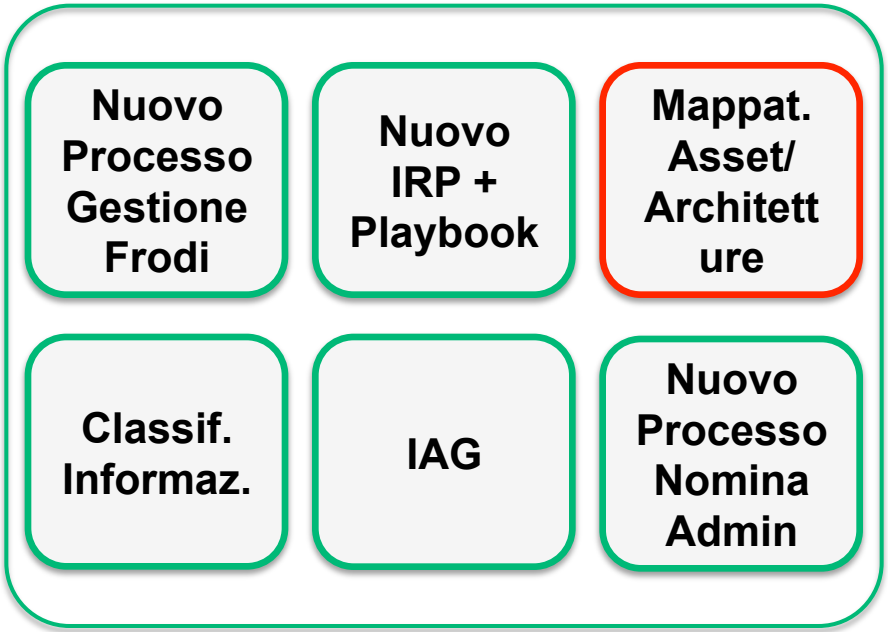
13
docenti tra BPER e UNIPR

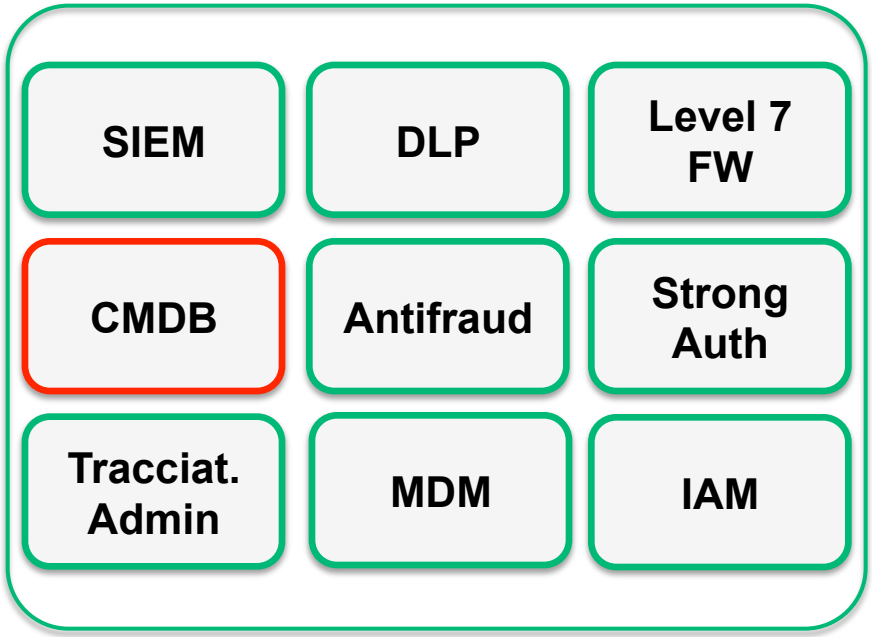
Cybersecurity, IT Risk, Fraud Prevention, Incident Management tra i temi trattati

Iniziative Progettuali

INIZIATIVE IN CORSO

Nel corso del 2015 BPER Services ha avviato una serie di iniziative progettuali finalizzate al rafforzamento dei presidi di sicurezza informatica e incluse nel Piano Industriale di Gruppo.
Tra queste il Configuration Management DataBase (CMDB), strumento funzionale all'adozione delle best practice di governance del sistema informativo che consente, in un sistema integrato di architettura informatica, di mappare e gestire le relazioni tra servizi erogati, applicazioni e sistemi gestiti. Il CMDB è funzionale, oltre alle attività di governance del sistema informativo, anche all'efficacia delle attività aziendali che richiedono la possibilità di ricostruire le catene tecnologiche sottostanti i processi di business delle Banche e delle Società del Gruppo, tra cui la Business Impact Analysis svolta a fini di continuità operativa e di analisi del rischio informatico.





Focus: Mappatura e gestione asset ICT

CONFIGURATION MANAGEMENT DATABASE

Il CMDB (Configuration Management DataBase) è una base di dati che contiene informazioni su ogni componente tecnico del sistema informativo. Il Gruppo BPER sta implementando una soluzione che consentirà di rilevare gli asset attivi sulla rete, le loro configurazioni e relative relazioni di interdipendenza.

Funzionalità

- **Visibilità**
  - ✓ cosa è installato
  - ✓ con che cosa è connesso
- **Controllo**
  - ✓ monitorare la configurazione con funzionalità di reportistica
  - ✓ tracciare i cambiamenti delle configurazioni
- **Analisi**
  - ✓ accelera il processo di troubleshooting degli incidenti
  - ✓ eseguire l'analisi d'impatto dei cambiamenti

Benefici

- **Discovery**
  - ✓ inventario delle applicazioni costruendo un inventario topologico di dettaglio
  - ✓ mappatura AS-IS degli asset di rete
- **Supporto ai processi operativi e di governo**
  - ✓ controllo delle dipendenze tra i componenti (applicazioni, sistemi & network)
  - ✓ awareness di anomalie tra interdipendenze
  - ✓ evidenza di eventuali lacune nei presidi di sicurezza
  - ✓ controllo dei cambiamenti e storicizzazione
  - ✓ analisi dell'evoluzione dell'infrastruttura in essere

Focus: Mappatura e gestione Asset ICT

ENTERPRISE ARCHITECTURE

L'inventario degli asset proveniente dalla soluzione CMDB verrà poi integrato in una soluzione di Enterprise Architecture al fine di consentire un miglior governo del patrimonio informatico.

Funzionalità

- **Mappare gli asset in funzione dei servizi di business**
  - ✓ descrizione delle diverse rappresentazioni
  - ✓ inserimento di modelli di servizio
- **Ottimizzare gli asset per raggiungere gli obiettivi target**
  - ✓ valutazione delle strutture obiettivo (To-be)
  - ✓ implementazione della strategia di business
- **Permette di valutare l'impatto di cambiamenti nell'architettura e dei rischi**
  - ✓ su infrastruttura IT
  - ✓ sui dati e sulle funzionalità

Benefici

- **Architettura IT**
  - ✓ importazione e mappatura delle normative
  - ✓ ottenere una visione complessiva conforme alle normative IT e definire un Action Plan
  - ✓ definizione di un IT framework di riferimento
  - ✓ calcolo della pertinenza degli asset
- **Sicurezza IT**
  - ✓ identificazione e monitoraggio dei rischi e creazione di una risk library
  - ✓ mappatura dei rischi in relazione al contesto (processi di business e U.O.)
  - ✓ calcolo della pertinenza dei livelli di rischio

BPER:
Banca

Per approfondimenti contattare

Daniele Tassile
daniele.tassile@bper.it
Telefono 059 20.21.111

Christian Igor Ciceri
Christian.ciceri@bperservices.it
Telefono 059 20.21.118