Deloitte.

Compliance e Gestione Integrata del Rischio: il ruolo del CERT in Banca

ABI, Banche e Sicurezza 2015
Roma, 4-5 Giugno – Palazzo Altieri

Fabio Battelli, CISSP, CISA, CISM, ISO 27001 LA
Senior Manager
Deloitte Enterprise Risk Services (ERS)

Agenda

1. Cyber Security: trend e rischi principali
2. Strategie ed interventi normativi per la gestione dei rischi Cyber
3. Il ruolo del CERT in Banca

© 2015 Deloitte. All Rights Reserved.

Cyber Security:
Trend e rischi principali

© 2015 Deloitte. All Rights Reserved.

Cyber Security

Trend e Rischi – Costo e redditività del Cybercrime

Costo del Cybercrime vs Mercato della Droga

Norton - Cybercrime Report

Costo del Cybercrime

388 Miliardi $

Valore che considera sia i costi in denaro diretti(*) (~30%) e costi in termini di tempo speso dalle vittime (~70%)

Valore di mercato globale per cocaina, eroina e marijuana

288 Miliardi $

Valore di mercato globale del traffico di droga

411 Miliardi $

Redditività del CyberCrime

Kaspersky – Cybercrime, Inc.: how profitable is the business

20:1 ***Rapporto medio tra profitto e costi necessari per realizzare i cyberattack***

La minaccia che genera il maggior profitto è il «Banking Trojan» che viene inviato tramite email spam

Investimento iniziale per acquistare il malware

3.000 $

Stima del profitto che una organizzazione criminale può ottenere

72.000 $

(*) denaro sottratto a causa del crimine e denaro speso per fronteggiarlo

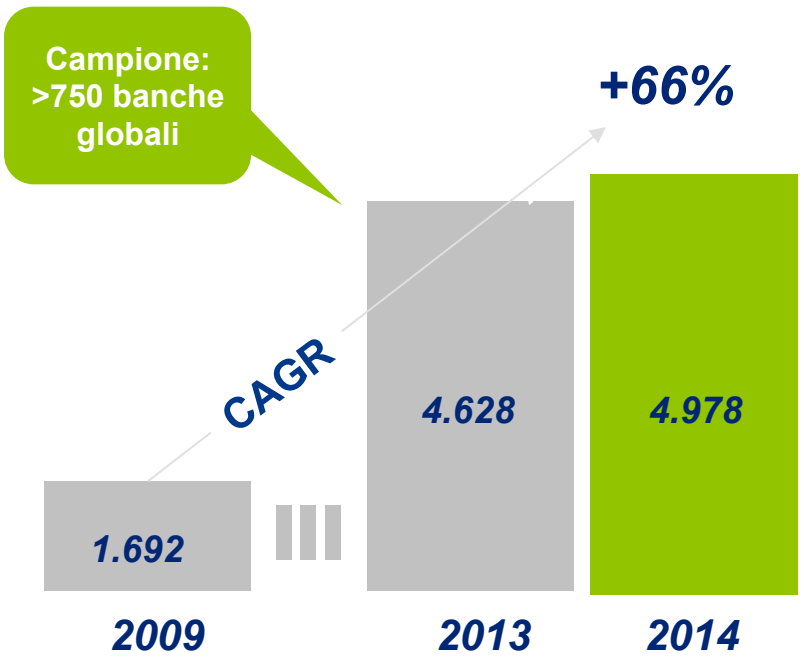
Fonte: Norton (by Symantec) - Cybercrime Report - 2011
Kaspersky – Cybercrime, Inc.: how profitable is the business?- 2014

© 2015 Deloitte. All Rights Reserved.

Cyber Security

Trend e Rischi – Incremento degli incidenti

Numero di incidenti di sicurezza informatica rilevati nel 2014



- **I rischi e gli incidenti di sicurezza informatica sono in costante crescita, confermando il trend in rialzo ormai da diversi anni**
- **Nel solo settore Finance il numero medio di incidenti di sicurezza è aumentato dell'8% rispetto all'anno precedente per un totale di 4.978 incidenti**
- **La crescita dal 2009 del numero di incidenti è pari al 66% (CAGR)**
- **L'impatto finanziario derivante dagli incidenti di sicurezza è cresciuto del 24% nell'ultimo anno**

Fonte: PWC, "The Global State of Information Security Survey 2015", September 2014

© 2015 Deloitte. All Rights Reserved.

Cyber Security

Trend e Rischi – Cybersecurity come priorità strategica nel Finance

*In accordo con lo studio **Deloitte 2015 Banking Outlook**, la **Cyber Security** è considerata tra le aree di maggior focalizzazione nello sviluppo delle priorità strategiche attese nel settore banking nel corso del 2015*

Principali aree di interesse per il settore banking nel 2015

Aree	Balance sheet efficiency	M&A	Growth	Payments transformation	Cybersecurity	Data management	Compliance and risk management
Priorità	Nuovi constraint in materia di liquidità e capitale renderanno l'ottimizzazione del profitto una priorità assoluta	Il trend di M&A in forte crescita nel 2014 continuerà anche per il 2015, in quanto funzionale al raggiungimento degli obiettivi	Per garantire competitività le grandi banche dovranno cresce in innovazione tecnologica e servizi a valore aggiunto	Nuovi player non-finance e nuove modalità di pagamento costringeranno le banche a rivedere schemi e dispositivi di pagamento	Necessità di aggiungere nuove capacità difensive, migliorando le capacità di collaborazione all'interno dell'industry	Nuove capacità di trasformazione e analisi dei dati che dovranno interessare le front-line operations e le altre funzioni core della banca	Nuove importanti regulation e regole di prudenziali richiederanno un approccio rinnovato alla gestione dei rischi

Fonte: Deloitte Center for Financial Services, "2015 Banking Outlook Boosting profitability amidst new challenges", June 2014

© 2015 Deloitte. All Rights Reserved.

Cyber Security

Trend e Rischi – Attori vs Impatti

Tipologie di Attori vs. Tipologie di Impatti

IMPATTI / ATTORI	Furti / Frodi Finanziarie	Furto di proprietà intellettuale nei piani strategici	Interruzione del business	Distruzione di infrastrutture critiche	Danno reputazionale	Minacce alla Safety / Life	Regolatorio
Criminalità organizzata							
Hacktivist							
Stati – Nazioni							
Insider							
Terze parti							
Hacker Singoli							

Molto Alto Alto Moderato Basso

© 2015 Deloitte. All Rights Reserved.

Strategie ed interventi normativi per la gestione dei rischi Cyber

© 2015 Deloitte. All Rights Reserved.

Cyber Security

Strategie ed interventi normativi – La situazione in Europa

Cyber Strategy - Situazione Attuale

- **L'EU nel 2013 ha emesso la propria Cybersecurity Strategy;**
- Anche gli stati europei sono attivi nella **definizione delle strategie nazionali di Cyber Security, ben 16 degli attuali 28 Stati membri hanno una strategia di cyber-security già formalizzata**;
- **A livello mondiale solo 30 dei 196 Stati riconosciuti sovrani hanno reso pubblica una propria cyber strategy**.

Elementi Comuni delle Cyber Strategy

1. stabilire trattati, leggi e regole di condotta nazionali e/o internazionali ad hoc
2. sviluppare i rapporti diplomatici e rafforzare le partnership internazionali
3. incrementare i livelli di sicurezza, affidabilità e resilienza delle reti e dei sistemi informatici
4. **rafforzare la condivisione delle informazioni (anche tra pubblico e privato), l'early warning e le capacità di incident response**

Fonte: Sistema di Informazione per la Sicurezza della Repubblica - I principi strategici delle politiche di cybersecurity, Dicembre 2013

© 2015 Deloitte. All Rights Reserved.

Cyber Security

Strategie ed interventi normativi – L'approccio dell'Italia

A Dicembre 2013 anche l'Italia ha pubblicato la propria strategia di **Cyber Security nazionale**, attraverso un **Quadro Strategico** e un **Piano Nazionale** (Febbraio 2014) che contengono gli obiettivi strategici e operativi della Cyber Security italiana

"In linea con quanto previsto dal DPCM del 24 gennaio 2013, il presente **Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico** individua i profili e le tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale…

"Il presente **Piano Nazionale** individua gli indirizzi operativi, gli obiettivi da conseguire e le linee d'azione da porre in essere per dare concreta attuazione al Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico…"

Indirizzi Operativi

1. ***Potenziamento capacità di Intelligence***
2. ***Coordinamento Pubblico-Privato***
3. ***Security Awarness***
4. ***Cooperazione internazionale / esercitazioni***
5. ***Operatività dei CERT***
6. **Interventi legislativi e Compliance internazionale**
7. **Compliance a standard di sicurezza**
8. **Supporto allo sviluppo industriale**
9. **Comunicazione strategia**
10. **Risorse**
11. **Information Risk Management nazionale**

© 2015 Deloitte. All Rights Reserved.

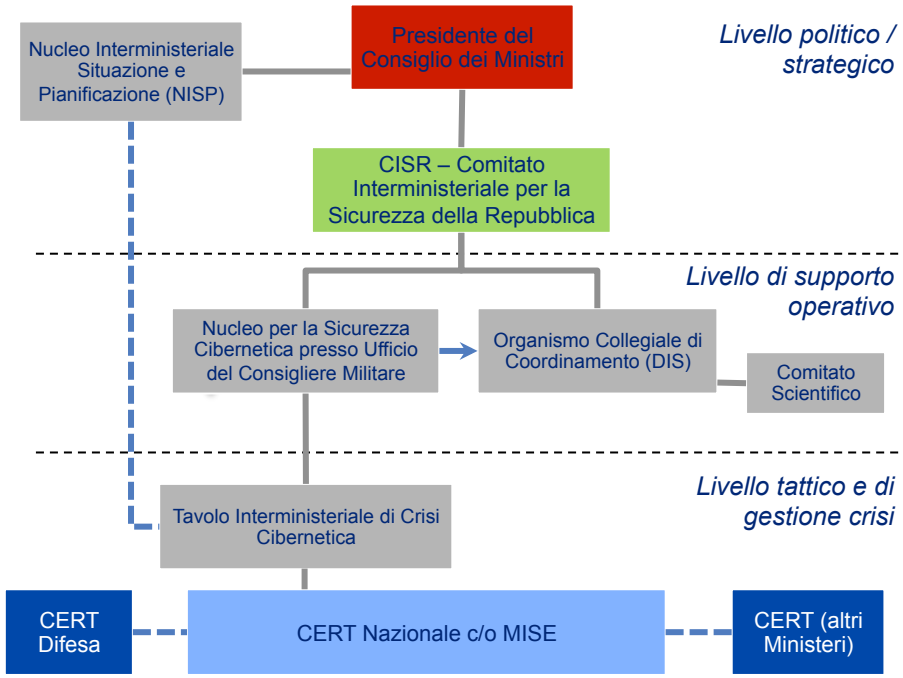
Cyber Security

Strategie ed interventi normativi – La governance in Italia

Il DPCM del 24 gennaio 2013 contiene gli "Indirizzi per la Protezione Cibernetica e la Sicurezza Informatica Nazionale" con l'obiettivo di riorganizzare l'architettura istituzionale nel settore della cyber-security, attraverso una graduale e progressiva razionalizzazione di ruoli, strumenti e procedure

All'interno del processo istituzionale disegnato, gli operatori privati assumono un ruolo primario:

- gli operatori che gestiscono infrastrutture critiche di rilievo nazionale devono comunicare ogni significativa violazione della propria sicurezza…
- …e devono adottare le misure di sicurezza predisposte dall'Organismo Collegiale di Coordinamento

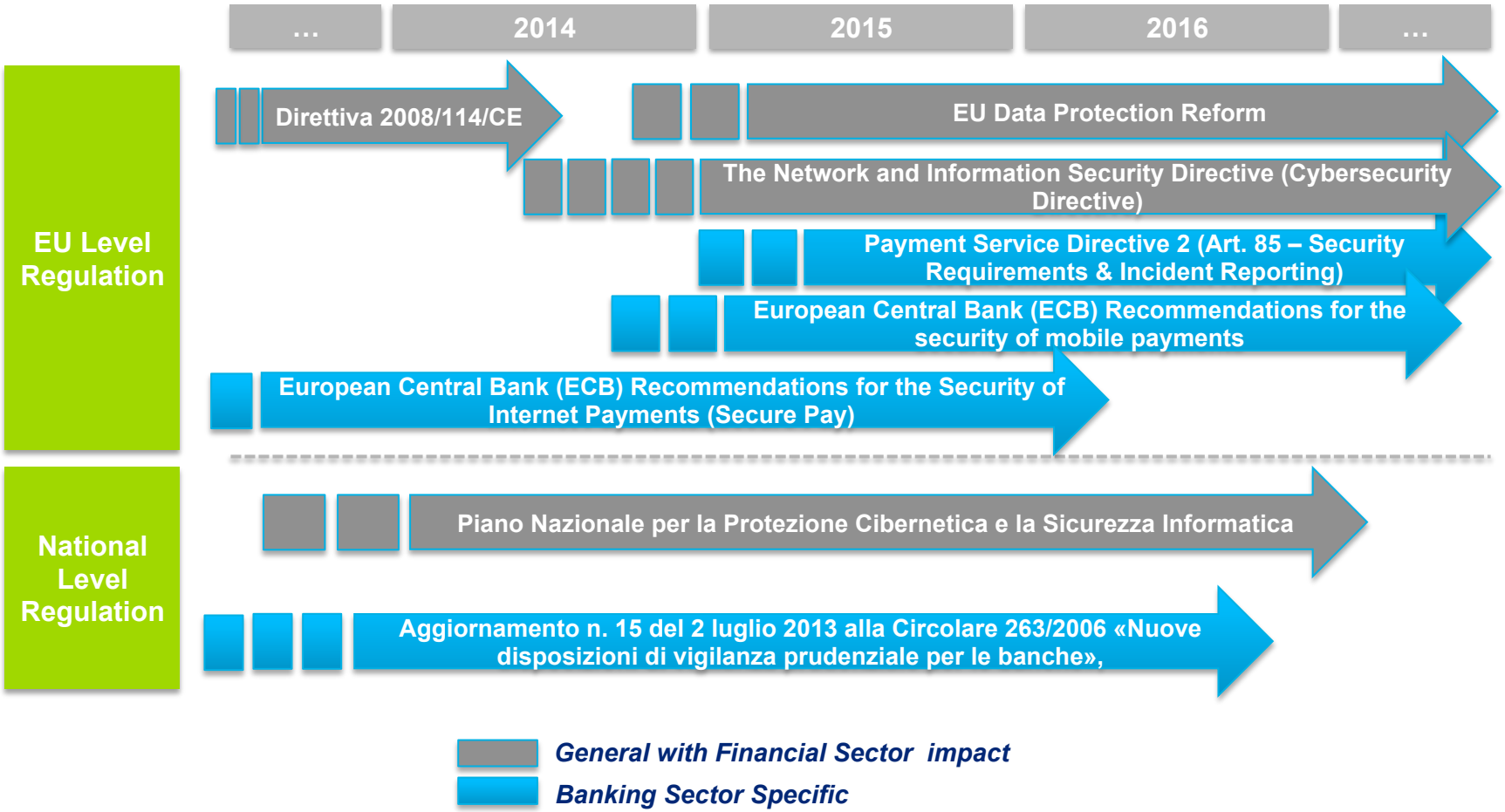


© 2015 Deloitte. All Rights Reserved.

Cyber Security

Strategie ed interventi normativi – Compliance e Cyber Security

Esempi di Compliance con impatti sulla Cyber Security



© 2015 Deloitte. All Rights Reserved.

Cyber Security

Strategie ed interventi normativi – Circolare 263 e Gestione degli Incidenti

Le recenti disposizioni di vigilanza prudenziale di Banca d'Italia impongono una riflessione sul modello di **gestione degli incidenti di sicurezza informatica,** richiedendo attività che sono tipicamente svolte da un **CERT**

BANCA D'ITALIA
EUROSISTEMA

Nuove disposizioni di vigilanza prudenziale per le banche

Circolare n. 263
del 27 dicembre 2006
15° aggiornamento
del 2 luglio 2013

Processo di Gestione

- …procedure **formalmente definite**, con l'obiettivo di **minimizzare l'impatto** di eventi avversi e garantire il **tempestivo ripristino** del regolare funzionamento dei servizi e delle risorse ICT coinvolti.
- …funzioni a cui **comunicare l'incidente** sono individuate secondo un'opportuna **procedura di escalation**;

Monitoraggio integrato

- Il processo si **raccorda** con il **monitoraggio di sistemi, accessi e operazioni** nonché con la **gestione** dei **malfunzionamenti** e delle **segnalazioni di problemi** da parte degli utenti interni ed esterni, favorendo l'assunzione di iniziative di prevenzione
- A seguito **dell'analisi degli incidenti di sicurezza informatica** e dei relativi rilievi delle funzioni di **audit e della compliance** sono **definite e monitorate le azioni correttive**

Cooperazione e Condivisione

- Le procedure definite per gravi incidenti di sicurezza informatica includono la cooperazione con le **forze dell'ordine** preposte e con **gli altri operatori o enti coinvolti**, anche in caso di **fuoriuscite di informazioni**.
- I gravi **incidenti** di sicurezza informatica sono **comunicati tempestivamente** alla **Banca d'Italia,** con l'invio di un rapporto sintetico…

© 2015 Deloitte. All Rights Reserved.

Il ruolo del CERT in Banca

© 2015 Deloitte. All Rights Reserved.

Il ruolo del CERT in Banca

Le funzioni SOC e CERT per la gestione dei rischi Cyber

Come evidenziato in precedenza, il ruolo del del **Computer Emergency Response Center** (**CERT**) risulta sempre più strategico per la gestione dei rischi Cyber nelle Organizzazioni

Security Operations e Gestione degli Incidenti Cyber

SOC
(Security Operations Center)

Il SOC rappresenta il **punto nevralgico** per il **controllo** ed il **governo** della sicurezza. É il luogo, fisico e logico, in cui convergono tutte le informazioni di sicurezza provenienti dall'infrastruttura e necessarie a **gestire**, **controllare** e **monitorare proattivamente** la sicurezza in modo **centralizzato** e **globale**

CERT
(Computer Emergency Response Team)

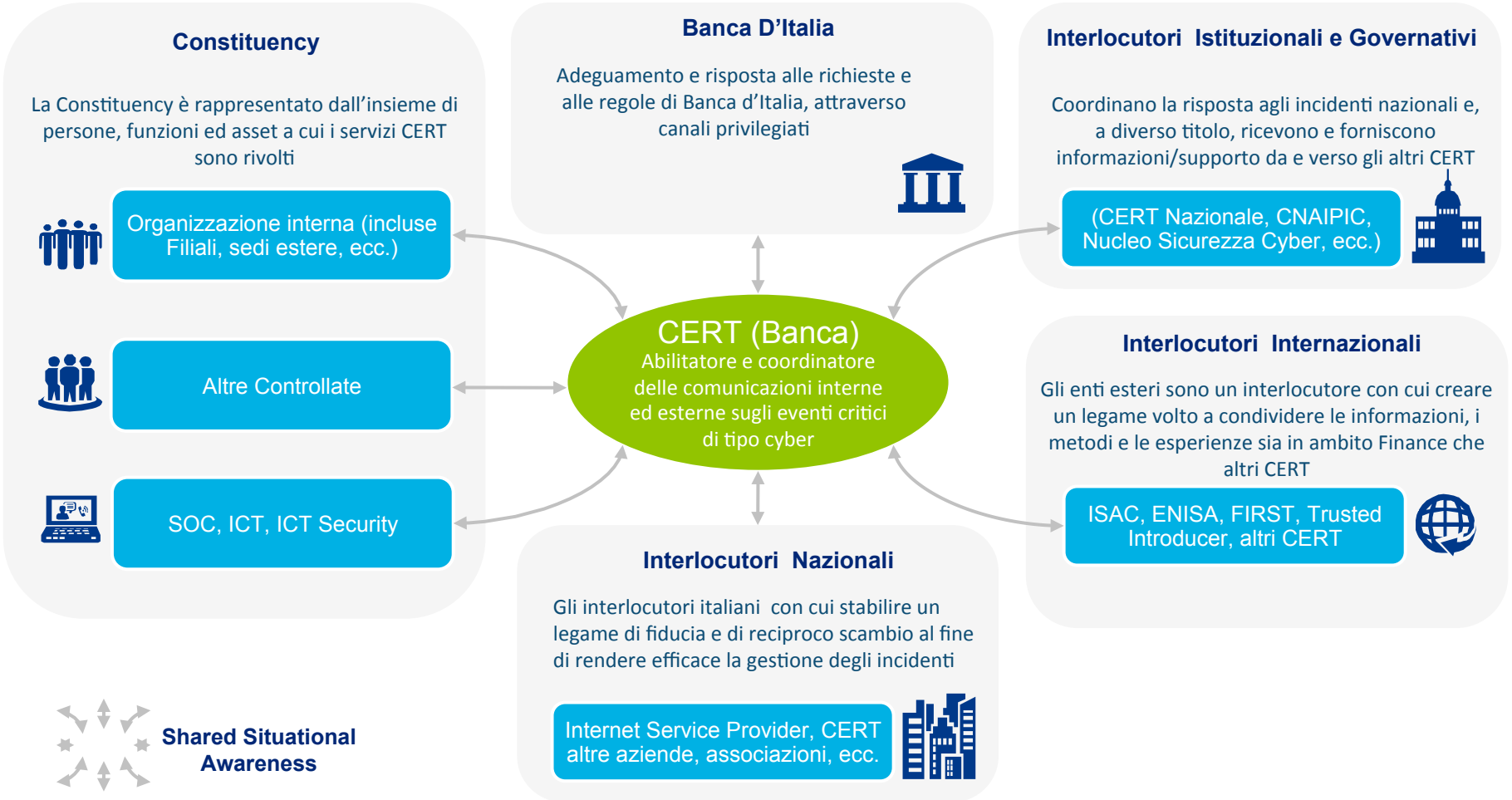
In collaborazione con il SOC (o parte stessa del SOC) è l'unità operativa che si occupa di gestire gli **eventi critici di tipo Cyber** (**Incidenti**). **Coopera** inoltre con l'intera **Community di sicurezza** (altri CERT, Istituzioni, ecc.) al fine di **prevenire** ed **individuare** tempestivamente i **rischi**

© 2015 Deloitte. All Rights Reserved.

Il ruolo del CERT in Banca

Obiettivi e Relazioni del CERT

Il CERT eroga servizi alla propria **Constituency** ed interagisce esternamente con l'intera **Community** al fine di ottenere e contribuire ad avere una visione complessiva delle minacce e degli incidenti che si stanno verificando a livello locale e globale (**Shared Situational Awarness**)



© 2015 Deloitte. All Rights Reserved.

Il ruolo del CERT in Banca

Alcune sfide tipiche nello sviluppo del CERT

L'applicazione degli standard e delle best practice di riferimento rappresentano solo il primo passo per la definizione e realizzazione di un CERT. L'esperienza conferma la necessità di modellare accuratamente tali Fuzioni in relazioni agli obiettivi e alle caratteristiche specifiche dell'Organizzazione

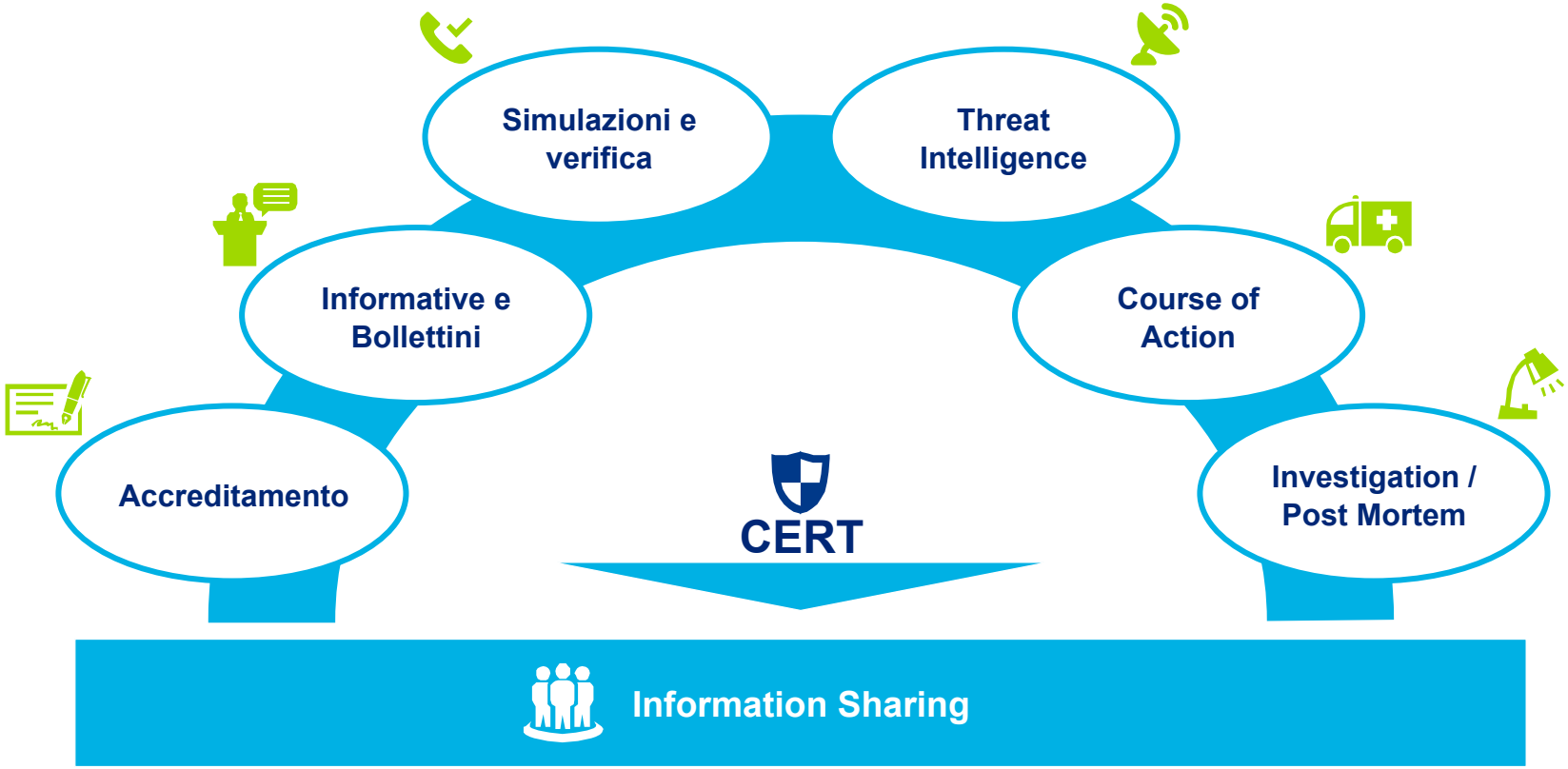
Obiettivi e Strategia	• Quali sono gli obiettivi del CERT per l'Organizzazione ? • E' richiesto l'accreditamento della struttura ? • Quale è la Constituency a cui si rivolge ? • Quali mandati specifici deve recepire ? (Compliance, politiche interne, internazionalizzazione, ecc.)
Servizi erogati	• Quale servizi (catalogo) il deve erogare alla propria Constituency ? Solo reazione o anche prevenzione ? • Quali ruoli e responsabilità tra il CERT e le altre funzioni (IT Security, Risk Management, ecc.), soprattutto nel monitoraggio e nella gestione degli incidenti ?
Strumenti e Tecnologia	• Quali soluzioni tecnologiche sono richieste per l'erogazione dei servizi ? (Ticketing, Dashboarding, Knowledge Base, ecc.) ? • Quale livello di integrazione con le altre soluzioni in uso presso altre funzioni ? (ICT, Risk Management, ecc.) ?
Organizzazione / Modello Operativo	• Quale modello operativo è richiesto ? Distribuito, centralizzato, virtuale, ecc. ? • Quanto personale deve essere impiegato nel CERT ? Quali profili ? Dedicato o part-time ? • Quanto personale deve essere impiegato nel CERT?

© 2015 Deloitte. All Rights Reserved.

Il ruolo del CERT in Banca

Servizi ed attività principali

L'efficacia del CERT è fortemente condizionata dalla capacità di strutturare ed erogare servizi alla propria **Constituency**, ma al tempo stesso di contribuire attivamente all'intera **community** impegnata nell'individuazione e nel contrasto tempestivo dei rischi Cyber

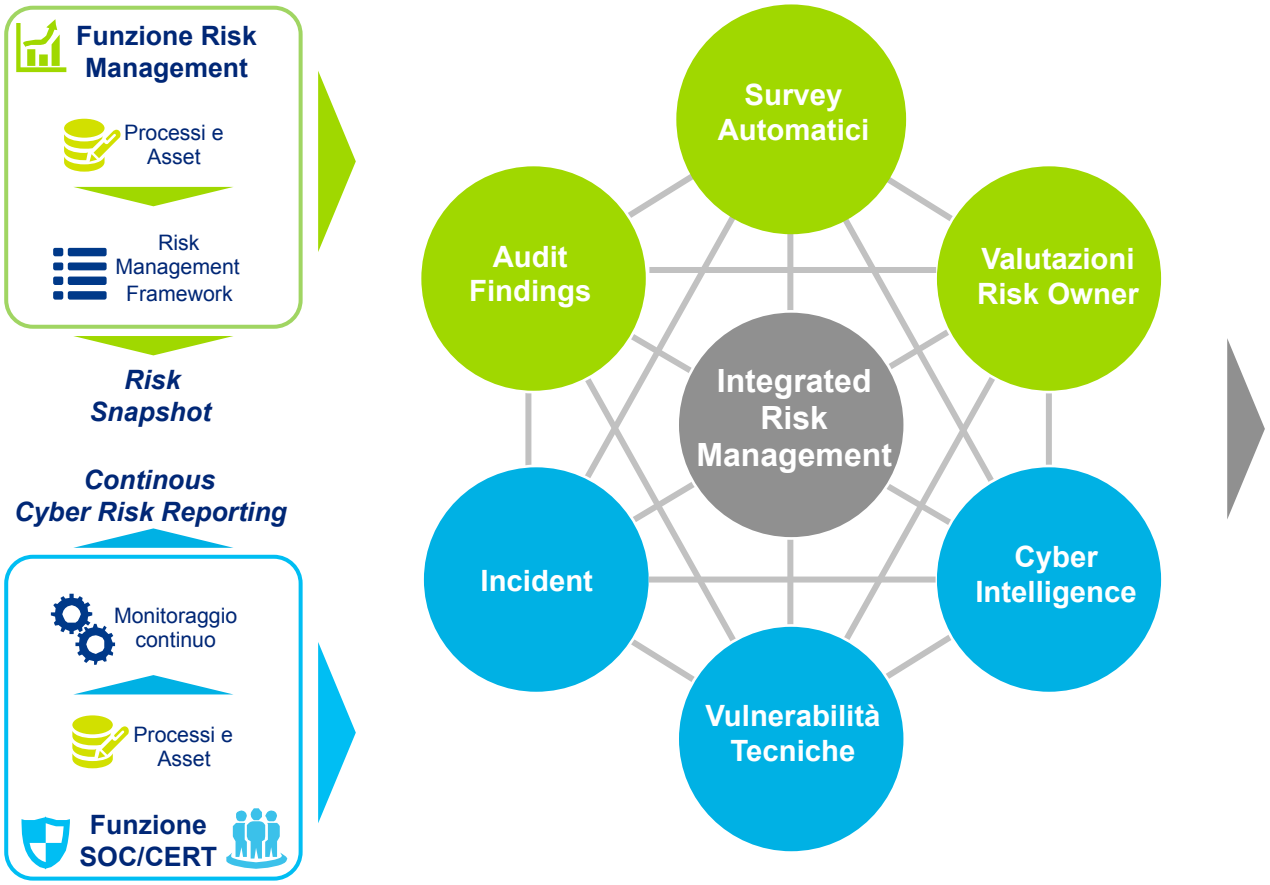


© 2015 Deloitte. All Rights Reserved.

Il ruolo del CERT in Banca

La gestione integrata e “dinamica" dei Rischi

In un’ottica **integrata** le attività di **Gestione Incidenti** del **CERT** avranno un ruolo sempre più **determinante** nell’individuazione "**dinamica**" dei rischi a cui l’Organizzazione è sottoposta



Integrated Risk Management

- La valutazione tradizionale del rischio (**snaphshot**) è arricchito da **indicatori reali (dinamici)** provenienti dalle funzioni SOC/ CERT
- La valutazione del rischio **residuo** (dopo il trattamento) è ricalcolato misuando **l’efficacia reale** delle contromisure applicate sulla base dei dati forniti dal SOC/CERT

© 2015 Deloitte. All Rights Reserved.

Deloitte, the largest professional services network in Italy, first started its activity in this country in 1923 and boasts century old roots, combining a tradition of quality with avant garde methods and technological expertise. Deloitte's professional services, which include audit, tax, consulting and financial advisory, are rendered by various separate and independent firms, specialised in the single professional areas, which are all part of the Deloitte network. Today, the Italian network employs over 2,900 professionals who help their clients excel thanks to the confidence in the high level of service, in our multidisciplinary offering and our widespread geographical coverage.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's about 200,000 professionals are committed to becoming the standard of excellence.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see deloitte.com\about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.