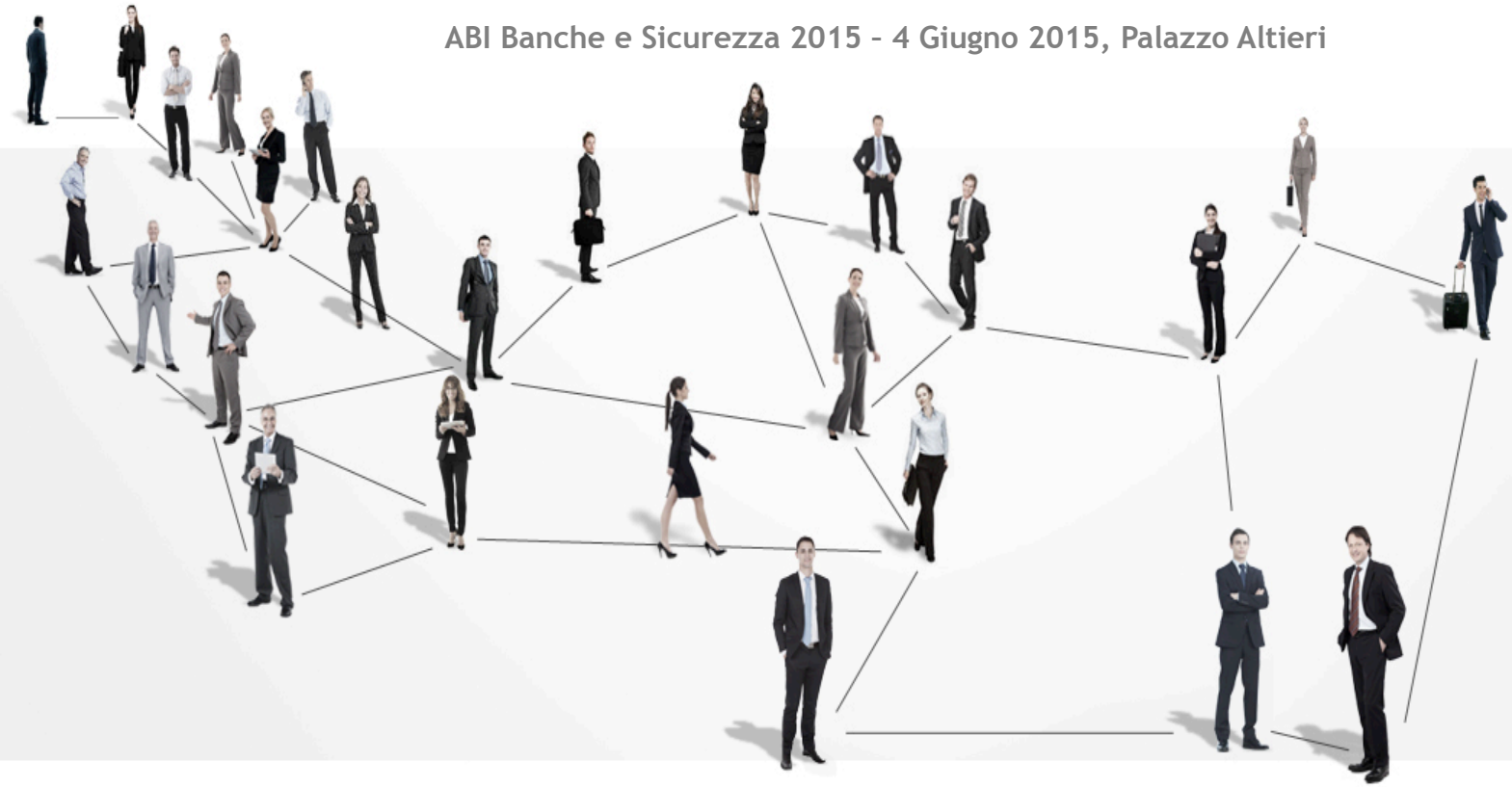
La governance della *cybersecurity* negli istituti bancari tra esigenze di conformità normativa e nuovi scenari di rischio

Ing. Andrea Agosti
Responsabile BU Sicurezza ICT e Controlli Interni

ABI Banche e Sicurezza 2015 – 4 Giugno 2015, Palazzo Altieri



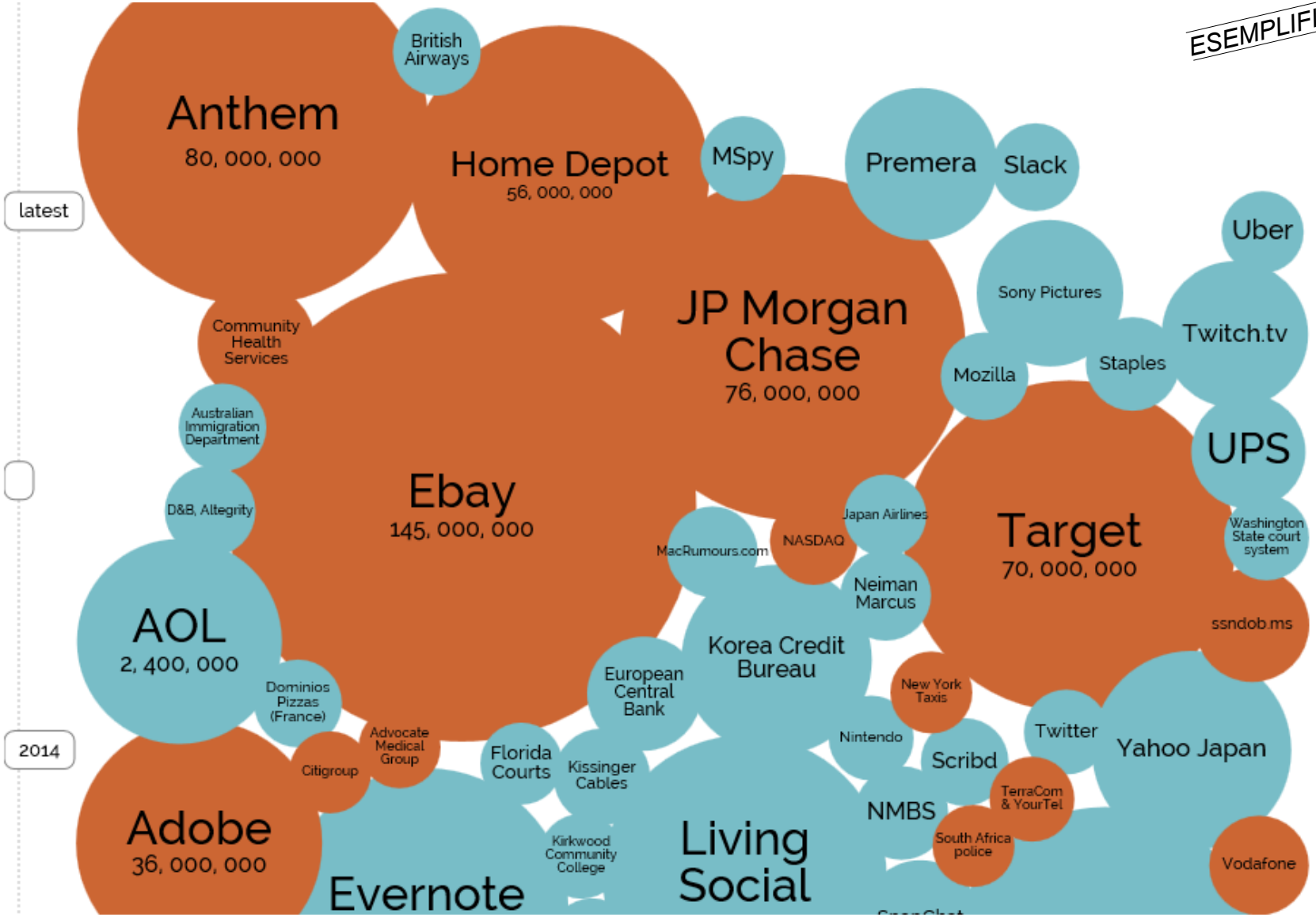
Agenda

1 ***Premessa: il contesto del cybercrime e le priorità per il settore bancario italiano***

- Come organizzarsi al meglio per gestire il rischio di *cybersecurity*: il framework CSF del NIST
- Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di *cybersecurity*
- L'impegno di OASI a supporto delle banche in tema di gestione dei rischi di *cybersecurity*

Il *cybercrime* è uno dei fenomeni criminali a maggior tasso di crescita nel biennio 2014-2015 con una crescente attenzione da parte dei media (1 / 2)

ESEMPLIFICATIVA



Il *cybercrime* è uno dei fenomeni criminali a maggior tasso di crescita nel biennio 2014-2015 con una crescente attenzione da parte dei media (2 / 2)

ESEMPLIFICATIVA

Azienda	Settore	Dettagli incidente
TARGET	Retail	• 40Mln di dati di carte di debito / credito trafugati • 70Mln di informazioni personali dei clienti sottratte
ebay	E-commerce	• 145Mln di credenziali degli utenti sottratte
JPMorgan	Financial Services	• 79Mln di informazioni personali dei clienti violate • 7Mln di dati anagrafici di piccole aziende rubati
THE HOME DEPOT	Retail	• 56Mln di dati di carte di debito / credito trafugati
SONY	Consumer eletronics	• 38Mln di informazioni personali di dipendenti e mail
	Consumer electronics	• Informazioni personali di personaggi famosi rubate dall'iCloud
	Government	• Informazioni personali del Governo statunitense sottratte dagli archivi della Casa Bianca
Anthem Health. Join In.	Health insurance	• 80Mln di informazioni personali compromesse
	Banking and finance	• 100 istituti bancari mondiali coinvolti (27 italiani) • 1Mld di dollari sottratti

A livello Europeo, cresce la preoccupazione delle Autorità di Vigilanza sui rischi IT, con particolare attenzione ai rischi legati ai *cyber attack*

Joint Committee of the EU Supervisory Authorities

European Banking Authority

European Insurance Authority

European Securities & Market Authority

Report on Risk in the EU Financial System *(May 2015)*

- Rispetto al precedente rapporto (Agosto 2014), i principali rischi già identificati si sono ulteriormente intensificati. Di fianco a ripresa economica debole, bassi tassi di interesse e stabilità del sistema, sono evidenziati i rischi in ambito IT, in particolare:
  - impatto negativo sui profitti da inefficienze negli investimenti IT
  - scarso collegamento la strategia IT con quella di business
  - disponibilità e continuità operativa dei sistemi
  - **cyber attacchi**, **furto di dati** e **frodi**
- Il rapporto sottolinea un interesse crescente da parte delle Autorità di Vigilanza europee sui **rischi IT** e sulla loro **sistematica integrazione** all'interno del **processo** più generale di **gestione** dei **rischi aziendali**
- Il rapporto riporta che le **Autorità** di **Vigilanza Bancaria** degli stati membri hanno identificato nei rischi di *cybersecurity* il **rischio IT** di **maggiore preoccupazione** (superiore ai rischi di continuità e outsourcing)
- Il rapporto sottolinea altresì che i requisiti di Vigilanza ai livelli nazionali sono **molto differenti** tra loro e auspica un **incremento** della **regolamentazione** e della **supervisione operativa** sui **rischi IT** a **livello Europeo** (e.g. CERT)
- *"It will be **important** to **ensure** that **spending** on **IT systems** and **security** are **maintained** at **adequate levels** and that related **internal controls** remain **robust**"*

Anatomia del *cybercrime*: un mondo variegato di crimini perpetrati con l'ausilio di Internet e delle tecnologie informatiche come strumento e/o target

Caratteristiche del Cybercrime

Il *cybercrime* comprende l'insieme dei **fenomeni criminali** che si caratterizzano per l'**utilizzo** delle **tecnologie informatiche**, in particolare della **rete Internet** *(ISO 27032)*

Il *cybercrime* è determinato da numerose e differenti motivazioni:

- guadagni illeciti
- terrorismo
- attivismo
- spionaggio governativo e industriale
- conflittualità tra nazioni

Il *cybercrime* è un fenomeno in crescita determinato dai megatrend IT in atto:

- Mobile
- Internet of Things e Cyber Physical System
- Cloud Computing
- Estensione delle supply chain
- M&A e internazionalizzazione
- Social media

Come può essere perpetrato

Le tecnologie informatiche possono essere utilizzate come **strumento** per compiere un crimine:

- attività commerciali illecite
- pirateria informatica e violazione dei diritti di autore
- furto di identità / codici di accesso
- scambio materiale illegale / osceno
- molestie, diffamazioni e false comunicazioni

Le tecnologie informatiche possono essere utilizzate come **target** di un crimine informatico (**cyber attacks**):

- Frodi
- furto di identità / codici di accesso
- violazione di sistemi di sicurezza e infrastrutture critiche nazionali
- furto di dati
- intercettazione di comunicazioni
- estorsione informatica
- interruzione / "distruzione" di servizi ICT

Il *cybercrime* comprende un **insieme variegato** ed eterogeneo di **attività criminali** condotte contro **diversi obiettivi** (persone, organizzazioni, stati) utilizzando le **tecnologie informatiche** come **strumento** / **target**. Quanto le **istituzioni finanziarie** sono un **target** del *cybercrime*?

Le minacce che rendono possibile i *cyber attacks* sono innumerevoli ed in costante evoluzione, in linea con i principali trend tecnologici in corso

Fonte

"Threat Lanscape 2014"
ENISA
(Dicembre 2014)

Stato delle minacce

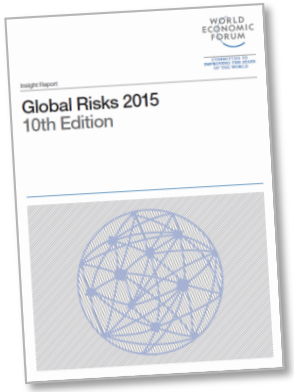
Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

- A **livello globale**, la quasi **totalità** delle **minacce** è in **crescita** nelle aree dei *megatrend* IT
- A livello di **sistema bancario** / **finanziario** italiano, le **minacce maggiori** ed in **costante evoluzione** sono quelle determinate dai ***financial malware*** (3ª generazione)
- Sono avvenuti alcuni casi di nuove minacce: **turbative** di **mercato** con attacchi di **social engineering**, attacchi *targeted* da parte di **attivisti** legati ad **EXPO**

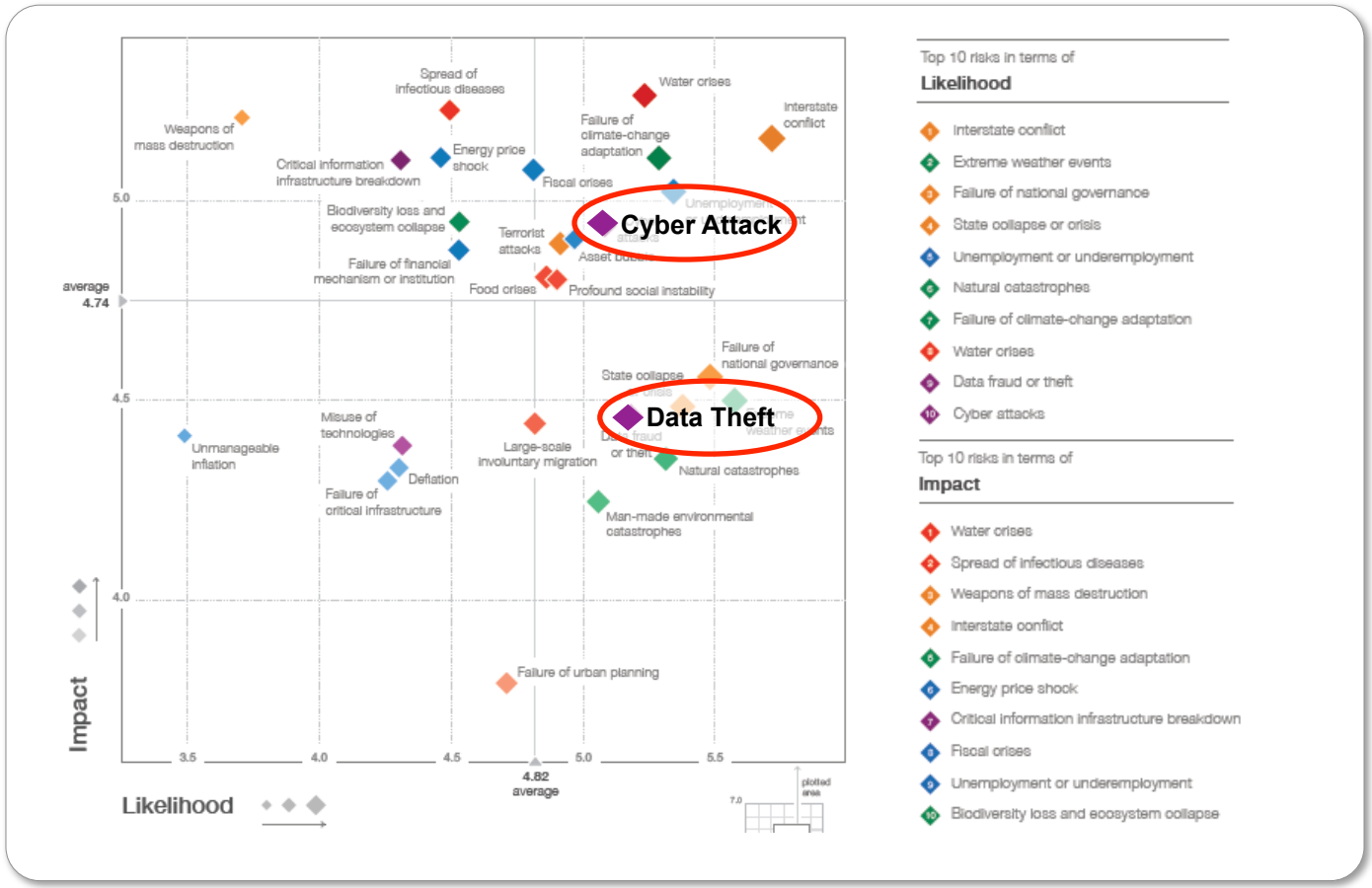
I *cyber attack e data breach* sono uno dei principali rischi all'attenzione anche presso Organizzazioni Internazionali quali il World Economic Forum (1 / 2)

Fonte

"Global Risk 2015 - 10th Edition"
World Economic Forum
(Gennaio 2015)



Mappa dei principali rischi a livello globale

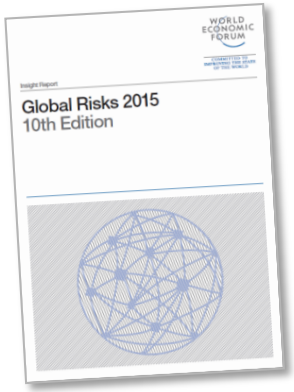


I **rischi** di *cyber attack* e *data theft* sono considerati nella **top 10** della lista dei rischi a **maggiore probabilità** di **accadimento** a **livello globale**, con i *cyber attack* **ricompresi** anche nella **lista** di quelli che hanno **impatto maggiore**

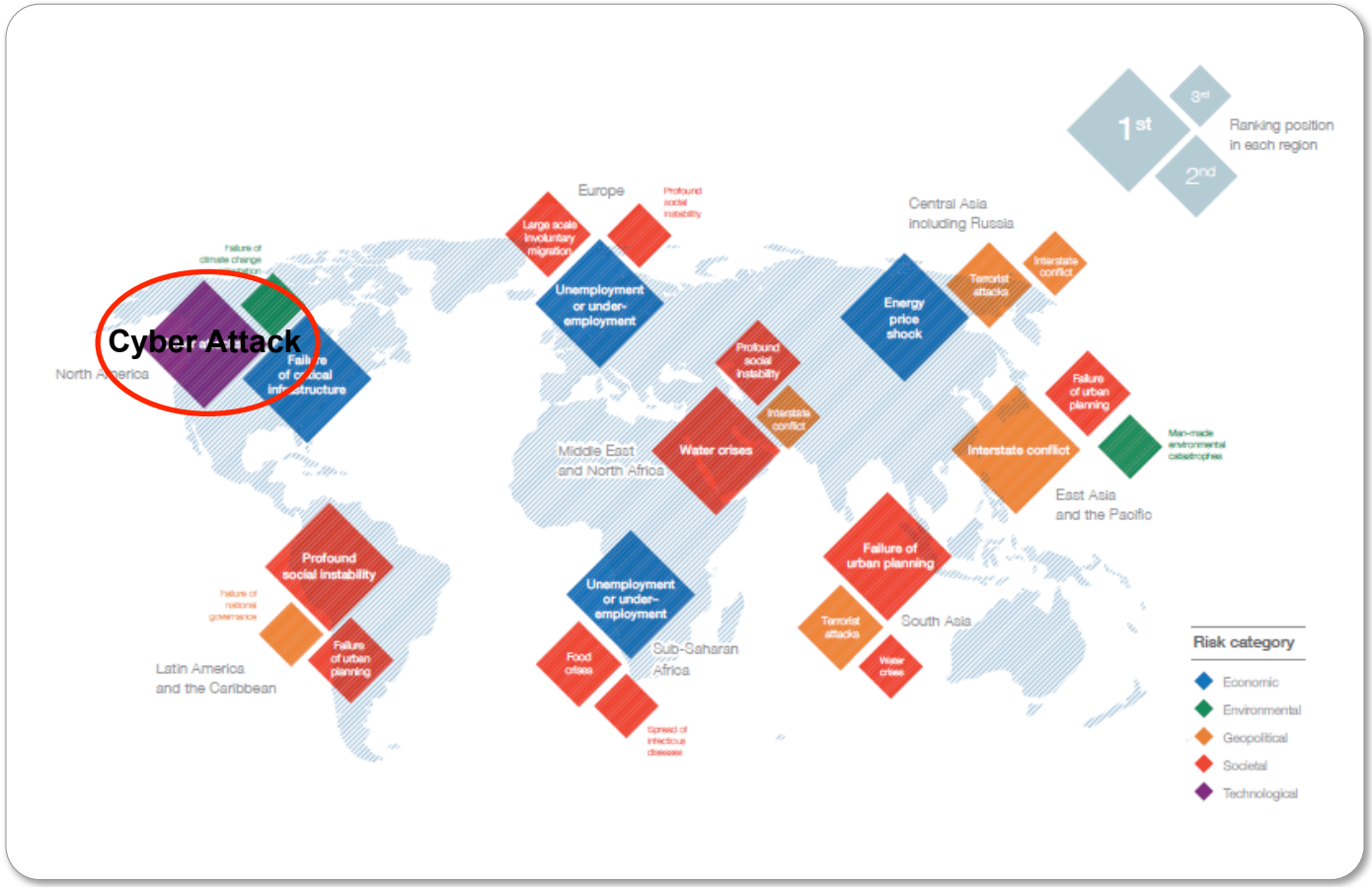
I *cyber attack e data breach* sono uno dei principali rischi all'attenzione anche presso Organizzazioni Internazionali quali il World Economic Forum (2 / 2)

Fonte

"Global Risk 2015 - 10th Edition"
World Economic Forum
(Gennaio 2015)



Livello di preparazione ai rischi a livello regionale

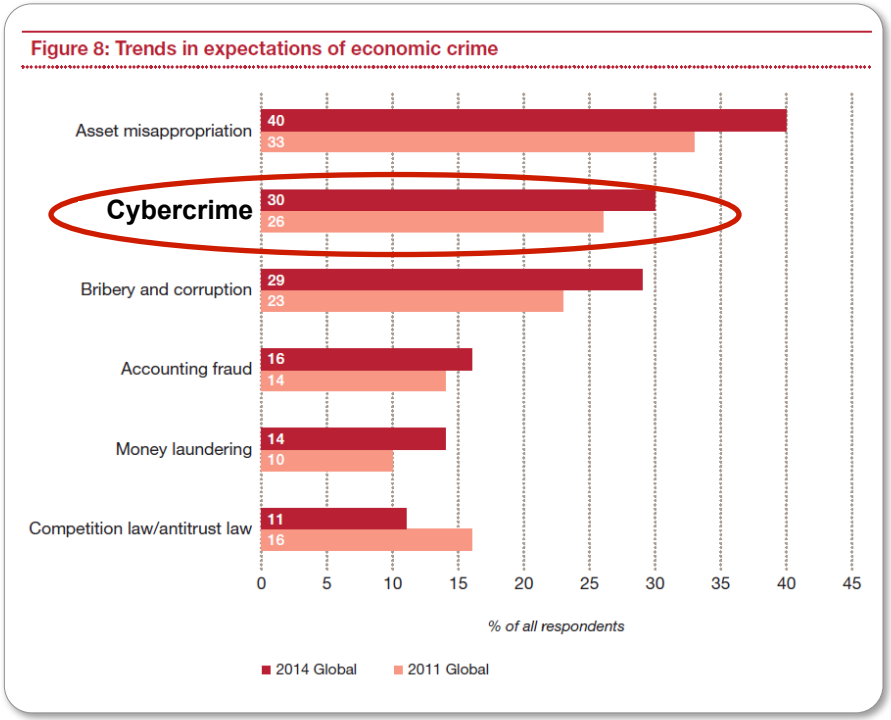


A **livello regionale**, la maggiore **percezione** di **essere impreparati** rispetto ai *cyber attack* è a livello **U.S.**, cui si aggiunge la **percezione "correlata"** di una maggiore **vulnerabilità** rispetto anche al **guasto** delle **infrastrutture critiche**

Le dimensioni del *cybercrime* e l'importanza percepita rispetto alle possibili categorie di crimini e rischi contro le attività di impresa

Cybercrime *vs* reati contro l'impresa

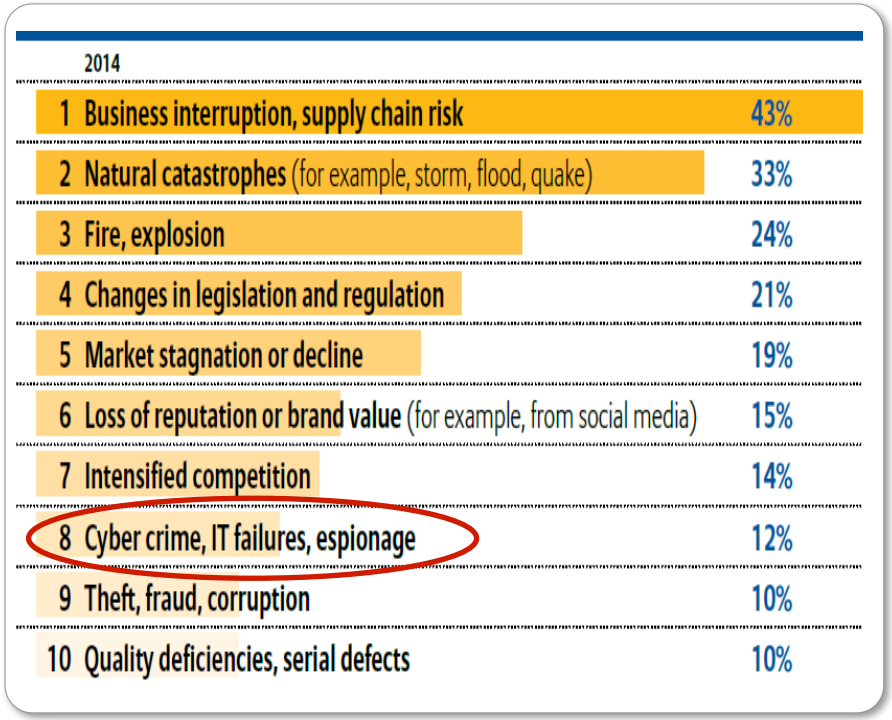
2014, Global Survey by Research Firm



- La **percezione** del *cybercrime* come **reato** contro l'impresa è al **2° posto** ed aumenta rispetto agli anni precedenti
- Il **50%** dei **CEO** intervistati nella survey afferma di essere "**preoccupato**" rispetto alle cyber minacce, con particolare **enfasi** sul **furto** di **dati personali** e **informazioni confidenziali**

Cybercrime *vs* rischi d'impresa

2014, Allianz Risk Barometer Survey



- Il rischio derivante dal *cybercrime* è salito dal 15° all'**8° posto** rispetto all'anno precedente, con una **stretta correlazione** con rischio **reputazionale**
- La **sottrazione** di **dati personali** e il furto di **proprietà intellettuale** sono i **principali rischi** percepiti

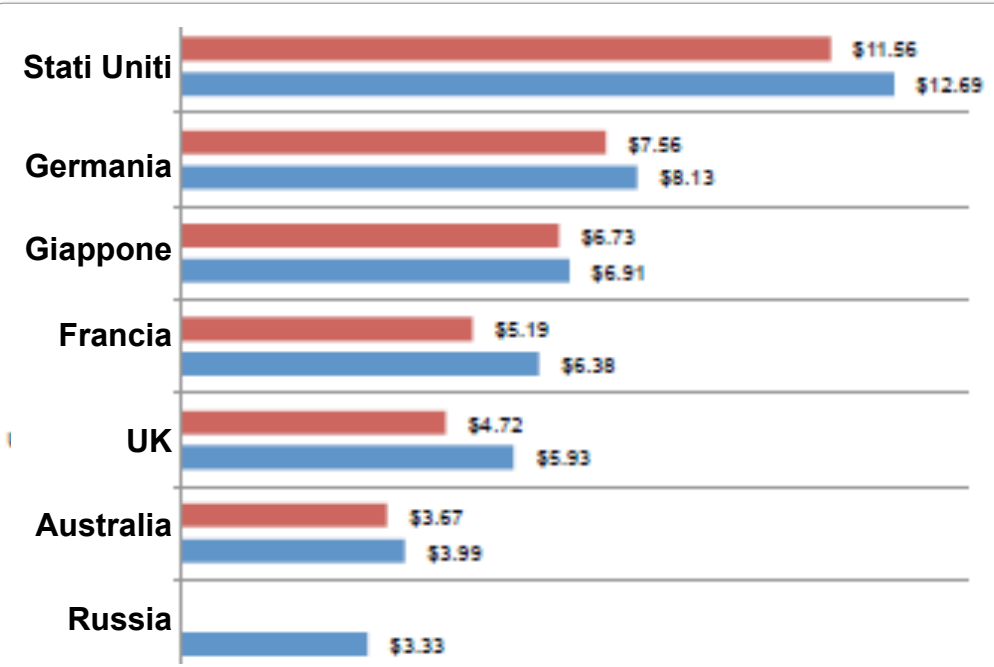
Le perdite determinate del *cyber attack* hanno raggiunto valori elevati in tutti i settori industriali a seguito di costi diretti / indiretti e costi opportunità

Fonte

"2014 Global Report on the Cost of cybercrime"
Ponemon Institute
(Ottobre 2014)

«**The Economic impact of Cybercrime"**
Center for Strategic and International Studies
(Luglio 2013)

Costo medio dei cyber attack per azienda *($ Mln)*



- **5° anno** di rilevazione
- **257 organizzazioni** intervistate
- **17 settori** industriali (16% settore FS)
- Dimensioni da **2.000** a **125.000** dipendenti
- **Costi** diretti, indiretti e costi opportunità
- **Costi** interni e costi derivanti dalle conseguenze

- I costi del *cybercrime* sono in **aumento anno su anno**
- I costi del *cybercrime* sono differenti per settore industriale, i settori dei *financial services* e *energy & utilities* sono quelli maggiormente esposti
- I costi più elevati del *cybercrime* sono quelli determinati da ***insider* disonesti**, da **attacchi *web-based*** e da quelli di tipo ***denial of services***
- Le cause principali di **costi** associati alle **conseguenze esterne** sono determinate dall'**interruzione** delle **attività di business** e dal **furto di dati personali** e/o **informazioni sensibili**

Agenda

- Premessa: il contesto del *cybercrime* e le priorità per il settore bancario italiano

2 ***Come organizzarsi al meglio per gestire il rischio di cybersecurity: il framework CSF del NIST***

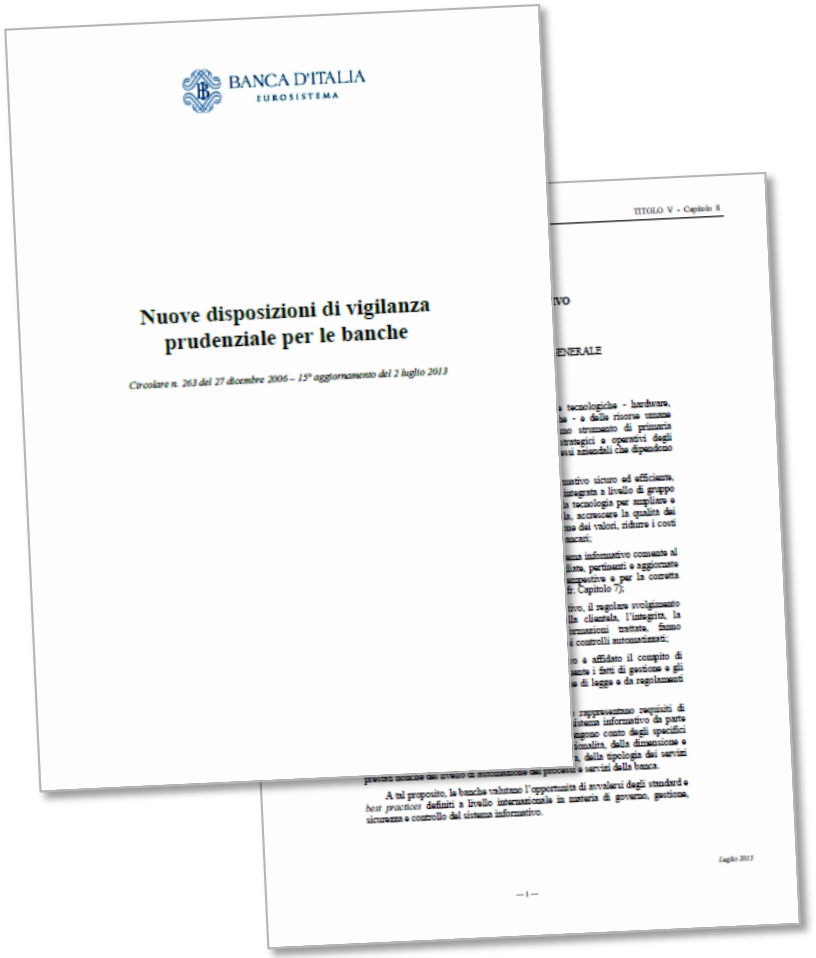
- Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di *cybersecurity*

- L'impegno di OASI a supporto delle banche in tema di gestione dei rischi di *cybersecurity*

Le Disposizioni di Vigilanza Prudenziale hanno stabilito i principi e le regole di alto livello per la gestione della sicurezza informatica all'interno delle banche

Nuove Disposizioni di Vigilanza

XV° aggiornamento, Luglio 2013



Principali indicazioni in tema di sicurezza informatica

- Coinvolgimento degli **Organi aziendali** (OFSS e OFG) nelle **decisioni chiave** e nell'approvazione dei **principali documenti** in tema di sicurezza informatica
- Istituzione di una **Funzione Aziendale** deputata allo **svolgimento** dei **compiti specialistici** in materia di **protezione** delle **risorse ICT**
- Predisposizione di una **Policy** di **Sicurezza Informatica** approvata dall'OFSS e del relativo **impianto documentale** di dettaglio operativo
- Implementazione di una serie di **misure** di **protezione** a **livello logico** e **fisico** delle **risorse ICT** (*e.g. controllo accessi logici, protezione della rete, sviluppo sicuro del codice, monitoraggio delle minacce, …*)
- **Collegamento** con il processo aziendale per l'**analisi** e la **gestione** dei **rischi informatici** al fine di stabilire l'**intensità** delle **misure** di sicurezza informatica
- Formalizzazione di un **processo** per la **gestione** degli **incidenti** di **sicurezza informatica** e modalità di cooperazione / comunicazione con le Autorità e le FFOO
- Produzione di **reportistica periodica** su base **annuale** contenente **informazioni** sullo **stato** della sicurezza informatica

Gli standard, gli approcci e le *best practice* ad oggi esistenti non sono completi in un contesto in cui le principali minacce sono derivanti dal *cybercrime*

ESEMPLIFICATIVA

ISO / IEC 27001-27002:2013


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Contenuti

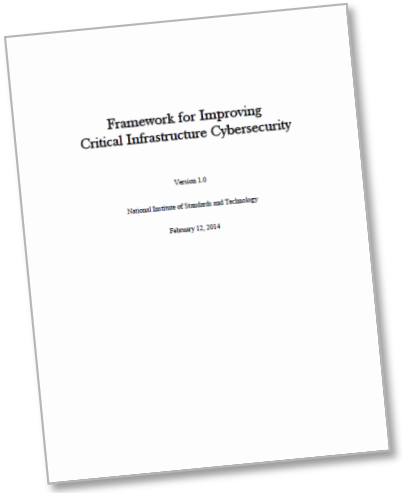
- Information security policies
- Organization of Information Security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental cecurity
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationship
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Gli **standard** attuali sono **focalizzati** sul **conseguimento** di una **adeguata «postura»** delle misure di **sicurezza informatica** del sistema informativo, tralasciando e/o trattando in maniera non adeguata le misure (preparazione, rilevazione, risposta, ripristino) per **contrastare** gli **attacchi** del *cybercrime*

Il NIST ha pubblicato di recente un framework metodologico per incrementare il livello di *cybersecurity* dei gestori delle infrastrutture critiche

Fonte

«**Framework for Improving Critical Infrastructure Cybersecurity**"
NIST
(Febbraio 2014)


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

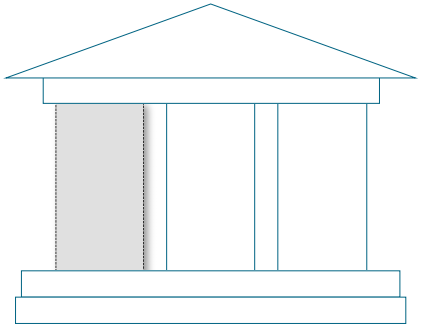
February 12, 2014

Descrizione e principali caratteristiche

- Richiesto al NIST dall'Executive Order 13636/2013 del Presidente U.S. "*Improving Critical Infrastructure Cybersecurity*" per mettere a fattor comune standard e *best practice* esistenti in un **framework *risk-based*** per la **gestione** della ***cybersecurity*** orientato alla **resilience**
- Il framework prevede che (i) le scelte in materia di *cybersecurity* siano **guidate** dalle **esigenze** di **business** e che (ii) i rischi legati alla *cybersecurity* siano **parte integrante** del **processo aziendale** di **risk management**
- Il framework è costituito da **tre parti**
  - **Framework Core**, contenente l'elenco delle «attività» per impostare un approccio alle gestione della *cybersecurity*
  - **Framework Implementation Tiers**, contenente i meccanismi per verificare e comprendere le caratteristiche dell'approccio impostato per la gestione dei rischi legati alla *cybersecurity*
  - **Framework Profile**, contenente l'elenco dei «profili» per allineare le attività di *cybersecurity* alle esigenze di business, alle risorse disponibili e al rischio accettabile
- Poiché il framework fa riferimento a **standard internazionali** in materia di *cybersecurity*, può essere utilizzato come **modello** anche da organizzazioni (specie infrastrutture critiche) **al di fuori** degli **U.S.**
- Il framework è **indipendente** da **qualsiasi scelta** relativa a **tecnologie** eventualmente utilizzate per implementare misure di *cybersecurity*

Framework metodologico del NIST per la gestione della *cybersecurity*
1. Framework Core (1 / 2)

Framework layer



Principali caratteristiche

- Contiene l'insieme delle **attività** da svolgere per proteggersi dai *cyber attacks*, organizzati in accordo ad una struttura con **5 funzioni** (Identify, Protect, Detect, Respond, Recover) **parallele** e **logicamente contigue**, suddivise poi in **22 categorie** e **97 sottocategorie**
- Costituisce un **modello** di **riferimento** di **alto livello** per la **gestione** dei **rischi** legati alla *cybersecurity*, **facilmente comunicabile** a livelli **direzionali** e **operativi** all'interno di una organizzazione
- Fa riferimento per le modalità implementative a **standard** e **linee guida / best practice** di settore quali:
  - COBIT 5
  - ISO / IEC27001:2013
  - NIST SP 800-53
  - ANSI / ISA 62443:2009
  - SANS CSC 5
- Non è una "*checklist"* di azioni da svolgere, ma bensì un modo per **rappresentare** ad **alto livello** (e rendere comparabili tra organizzazioni differenti) la **"postura" di sicurezza**, in relazione allo **specifico contesto** di **rischio** e delle **minacce**

Framework metodologico del NIST per la gestione della *cybersecurity*

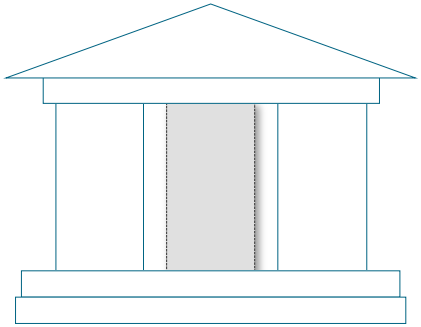
1. Framework Core (2 / 2)

Security Posture

Funzioni	Identify	Protect	Detect	Respond	Recover
Obiettivi	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.	Develop and implement the appropriate activities to maintain plans for resilience and to restore any services that were impaired due to a cybersecurity event
Categorie	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications
Sottocategorie	23	35	18	15	6

Framework metodologico del NIST per la gestione della *cybersecurity*
2. Framework Implementation Tier (1 / 2)

Framework layer



Principali caratteristiche

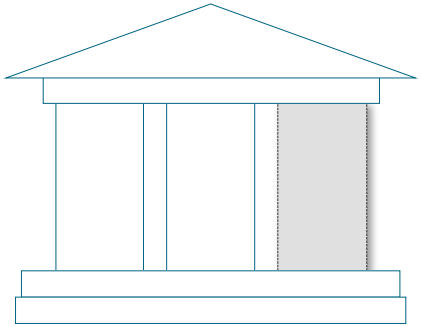
- Contiene l'elenco dei **4 livelli** (*Implementation tier*) con cui descrivere**,** ad un **livello** di **rigore** e **sofisticazione crescenti,** le **pratiche** adottate per **gestire** i **rischi** di *cybersecurity*, in particolare:
  - Tier 1: **Partial**
  - Tier 2: **Risk Informed**
  - Tier 3: **Repeatable**
  - Tier 4: **Adaptive**
- Permette di **contestualizzare** le modalità con cui un'organizzazione **gestisce** i **rischi** di *cybersecurity* e i **processi** adottati per **mitigare** tali **rischi**
- La **selezione** del *tier* per un'organizzazione considera elementi quali il **contesto** delle **minacce**, le **pratiche** correnti di **risk management**, i **requisiti** di **conformità** e gli **obiettivi** di **business**
- Il *tier* **selezionato** deve essere in linea con gli **obiettivi** dell'organizzazione, deve essere **fattibile** e in grado di **ridurre** i **rischi** di *cybersecurity* agli asset critici ad un **livello accettabile**
- I *tier* **non rappresentano livelli** di **maturità**, il passaggio a *tier* superiori è consigliato quando tale cambiamento implichi una **riduzione** dei **rischi** di *cybersecurity* a **costi accettabili**

Framework metodologico del NIST per la gestione della *cybersecurity*
2. Framework Implementation Tier (2 / 2)

Ambito	Descrizione	Tier 1	Tier 2	Tier 3	Tier 4
1 Risk Management Process	– Le attività di *cybersecurity* sono allineate agli obiettivi di rischio, alle esigenze di business e al contesto delle minacce		√	√	√
	– Le attività di *cybersecurity* sono aggiornate regolarmente sulla base di un processo di risk management formalizzato			√	√
	– Le attività di Cybersecurity sono adattate anche in funzione delle *lesson learned*, di KPI / KRI relativi alle attività passate / presenti al contesto evolutivo delle minacce e delle tecnologie				√
2 Integrated Risk Management Program	– Esiste una consapevolezza dei rischi legati alla cybersecurity e sono formalizzati processi e procedure operativi		√	√	√
	– La gestione dei rischi legati alla *cybersecurity* è estesa a tutta l'organizzazione ed organizzata in accordo a policy *risk-based*			√	√
	– La gestione dei rischi legati alla *cybersecurity* fa parte della cultura aziendale ed è continuamente sostenuta sulla base delle *lesson learned* e della condivisione delle informazioni				√
3 External Partecipation	– Conoscenza del proprio ruolo nell'ecosistema di appartenenza in termini di partner e relative dipendenze		√	√	√
	– Ricezione di informazioni / collaborazione con i partner in relazione ad eventi di *cybersecurity*			√	√
	– Condivisione di informazioni accurate e tempestive con i partner, anche prima dell'accadimento di eventi di *cybersecurity*				√

Framework metodologico del NIST per la gestione della *cybersecurity*
3. Framework Profile (1 / 2)

Framework layer

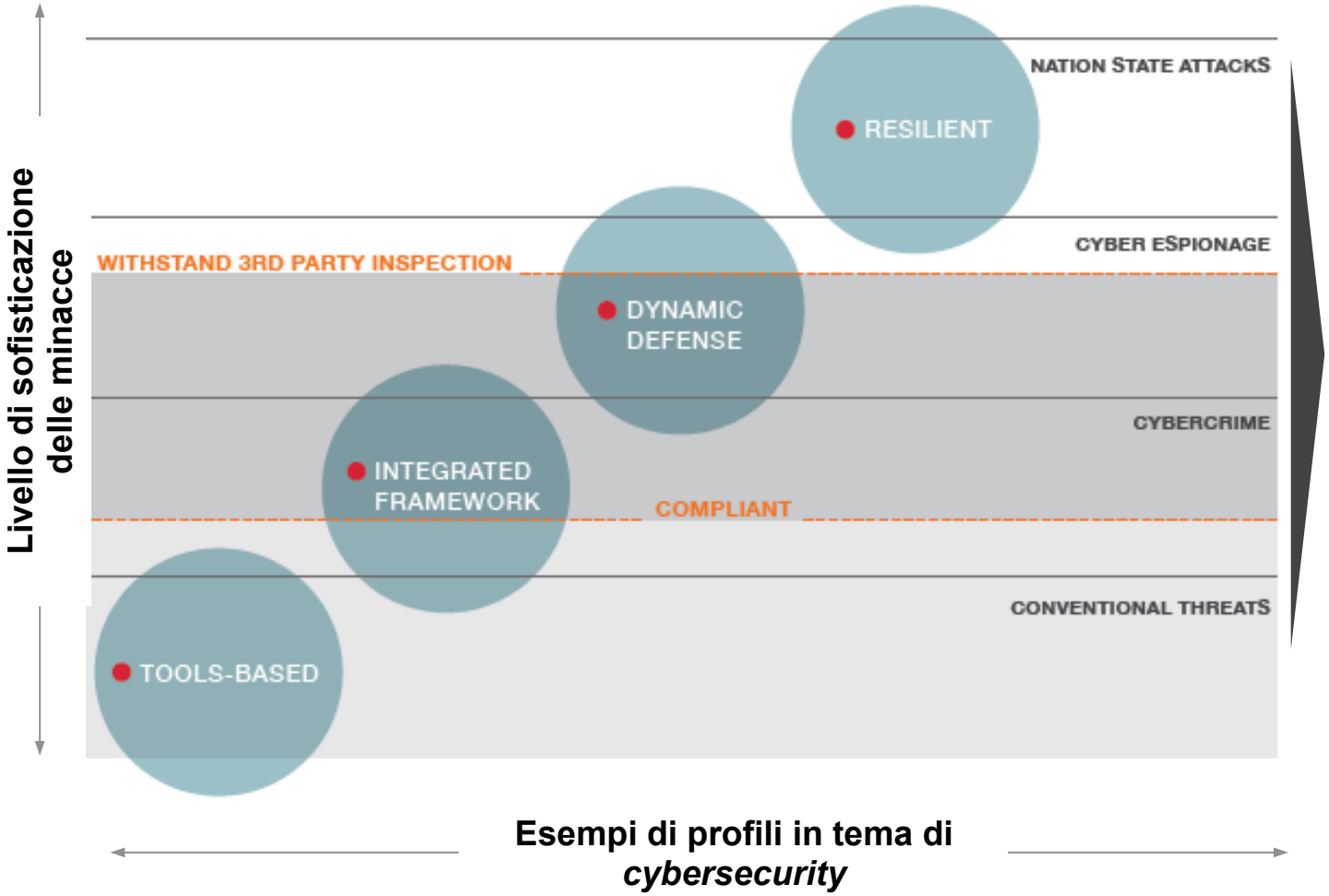


Principali caratteristiche

- Un **profilo** rappresenta l'allineamento delle **funzioni**, **categorie** e **sottocategorie** del *framework core* ai **requisiti** di **business**, alla **tolleranza** al **rischio** ed alle **risorse** dell'organizzazione
- Sono previsti **2 profili**: il **profilo corrente**, che contiene i risultati attualmente conseguiti in tema di *cybersecurity*, e il **profilo target**, che contiene i risultati necessari per ottenere gli **obiettivi** in tema di *cybersecurity* derivanti dall'attività di risk management
- La **comparazione** tra profilo **corrente** e profilo **target** potrebbe rilevare degli **scostamenti** in relazione agli obiettivi di gestione dei rischi di *cybersecurity*, a cui far conseguire un **piano** degli **interventi**
- Il successo dell'implementazione del *framework* è basato sul **conseguimento** dei **risultati** descritti nel **profilo target** dell'organizzazione e non nella determinazione del *tier*. Non sono previsti template per la descrizione dei profili

Framework metodologico del NIST per la gestione della *cybersecurity*
3. Framework Profile (2 / 2)

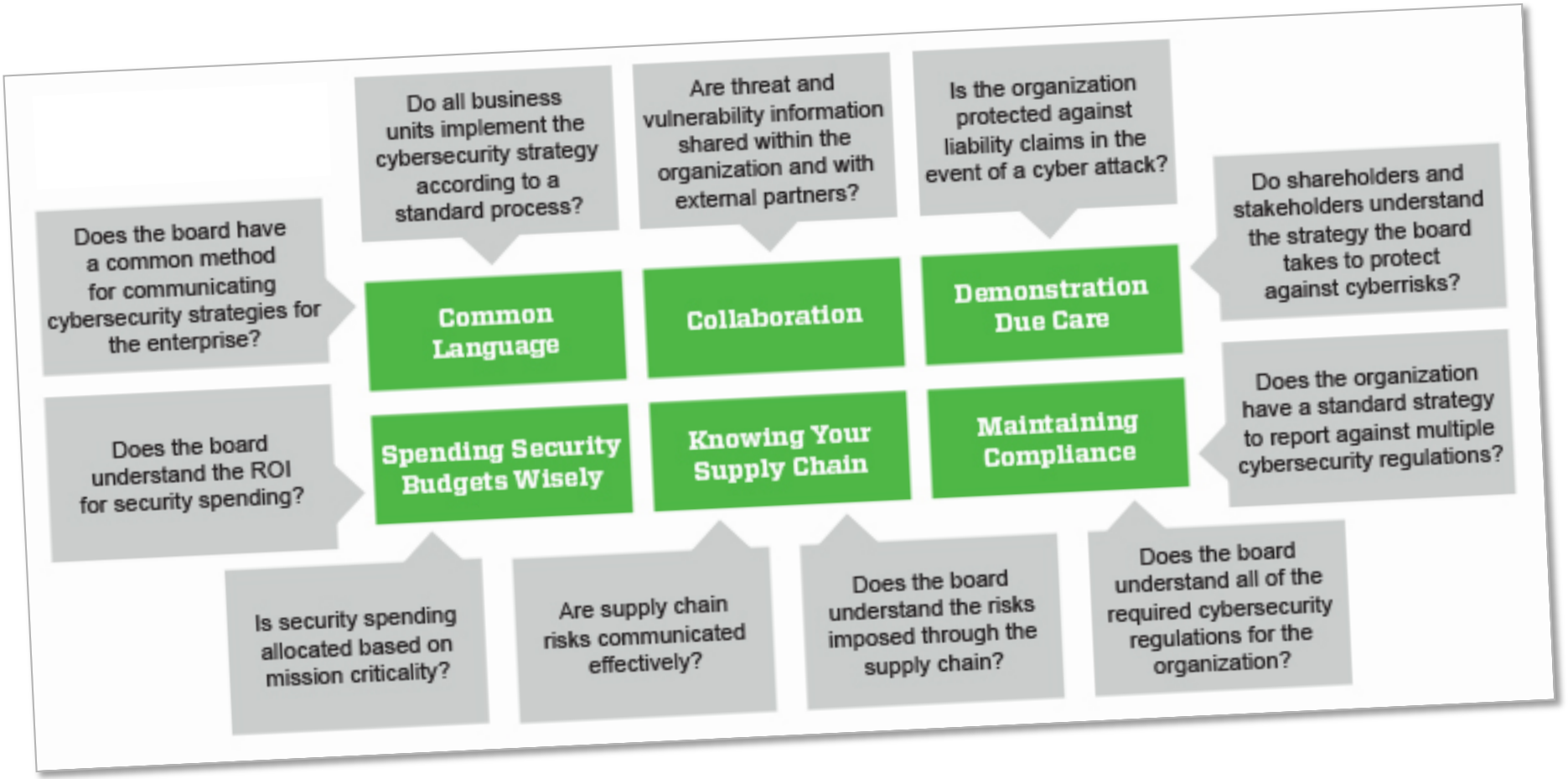
Esempio di profili



Evidenze

- Approccio **tool based** (e.g. AV, IDS, firewall) per le **minacce convenzionali**
- **Integrated framework** per garantire la **compliance** (e.g. PCI DSS), **senza certezza** di subire **attacchi**
- **Dynamic Defense** e **Resilient** per minacce sofisticate e attaccanti motivati, per cui le esigenze di **intelligence** sono **fondamentali** per **scoprire** e **bloccare attacchi**

L'adesione ad un framework di gestione dei rischi di *cybersecurity* basato sullo standard CSF del NIST consente di conseguire una serie di benefici



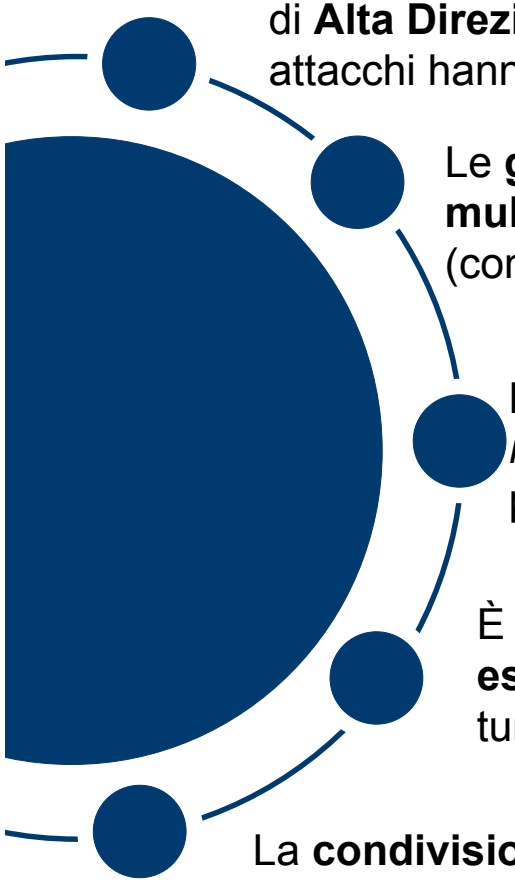
Agenda

- Premessa: il contesto del *Cybercrime* e le priorità per il settore bancario italiano
- Come organizzarsi al meglio per gestire il rischio di *cybersecurity*: il framework CSF del NIST

3 ***Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di cybersecurity***

- L'impegno di OASI a supporto delle banche in tema di gestione dei rischi di *cybersecurity*

La *cybersecurity* non è più un problema tecnologico per la Funzione ICT, è un soprattutto un problema strategico da affrontare a livello di Alta Direzione



La **responsabilità** "ultima" della *cybersecurity* deve essere stabilita a livello di **Alta Direzione** e di **Organi Aziendali**, gli impatti derivanti dai *cyber* attacchi hanno un rapporto diretto con il **brand** e il **valore** per gli **azionisti**

Le **gestione** della *cybersecurity* deve essere assicurata da un **team multidisiciplinare** con competenze **non sono soltanto tecnologiche** (comunicazione, legale, assicurativo, risk management)

Le **istituzioni finanziarie** sono **sotto attacco**, pensare che i *cyber risk* non siano una minaccia reale oppure che non interessino la propria realtà è un **errore** che può avere **gravi conseguenze**

È importante conoscere il proprio **contesto** in termini di **minacce** e di **esigenze** di **protezione**, focalizzando l'attenzione non solo sulla "postura" di *cybersecurity* ma sulla reale **capacità** di **difesa** e **resilienza**

La **condivisione** delle **informazioni** è fondamentale a **livello di sistema** per garantire una **rapida risposta** e **capacità** di **ripristino** a seguito di gravi incidenti in tema di *cybersecurity*

Prepararsi all'inevitabile: per proteggersi dai rischi *cyber* cresce l'interesse delle polizze assicurative specifiche per la *cybersecurity* (1 / 2)

	Evento	Danni diretti *(1st party losses)*	Danni verso terzi *(3rd party losses)*
1	Danneggia-mento di dati	• Recupero / ricostru-zione dei dati	• Danni contrattuali
2	Furto/perdita di dati	• Intellectual Property • Sanzioni amministrative • Obblighi normativi	• Danni contrattuali (e.g. PCI DSS) • Obblighi normativi
3	Interruzione di servizio	• Perdita ricavi	• Danni contrattuali
4	Estorsione / frode	• Sottrazione denaro	• Furto di identità
5	Multimedia liability	• Danno di reputazione	• Violazione IP / diritti di autore di terzi

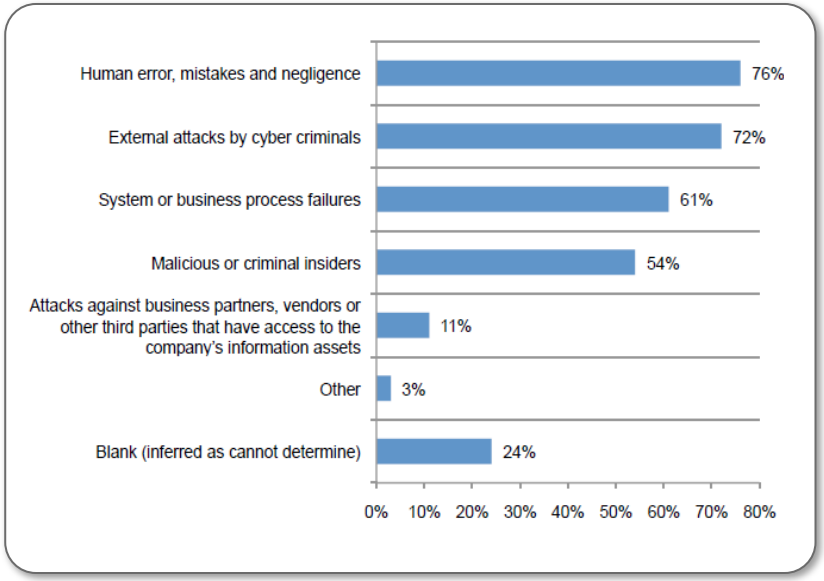
Consulenza specialistica ambito investigativo, legale, IT e PR

Responsabilità civile verso terzi (singoli e/o aziende)

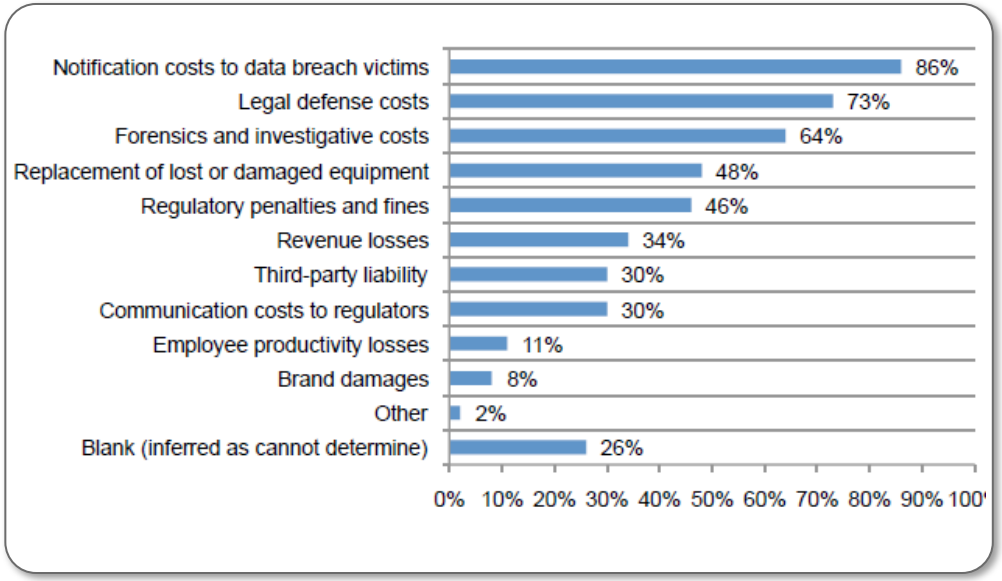
Le **polizze assicurative tradizionali** (e.g. All Risk) in genere sono in grado coprire soltanto i **danni diretti** relativi al **danneggiamenti** dei **dati** causati da **errori umani** e/o **di sistema**, le **polizze cyber** coprono invece altre cause (attacchi esterni, dipendenti infedeli) ed **altre tipologie** di **eventi** (e.g. furto di dati, estorsioni)

Prepararsi all'inevitabile: per proteggersi dai rischi *cyber* cresce l'interesse delle polizze assicurative specifiche per la *cybersecurity* (2 / 2)

Eventi* coperti da polizze *cyber*



Danni* coperti da polizze *cyber*



- Le **perdite** determinate da un ***cyber incident*** sono la **principale motivazione** per **valutare** una **polizza assicurativa** contro i *cyber attack*
- Le **3 principali motivazioni** che determinano la scelta di **non sottoscrivere** una **polizza assicurativa *cyber*** sono determinate dal **prezzo troppo elevato** (52%), dalle **troppe esclusioni / restrizioni** sugli eventi (44%) oppure perché ritengono le **polizze in essere** già **adeguate** (38%)
- Tipicamente, sono coperte le **principali cause** di **eventi** che determinano un ***cyber incident*** (errori / negligenze umane, attacchi esterni da criminali e malfunzionamenti) e i **principali costi** sostenuti a **seguito** di un **incidente** (notifiche, spese per consulenze legali, informatiche, investigative)

(*) Fonte: «Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age», Ponemon Institute, Agosto 2013

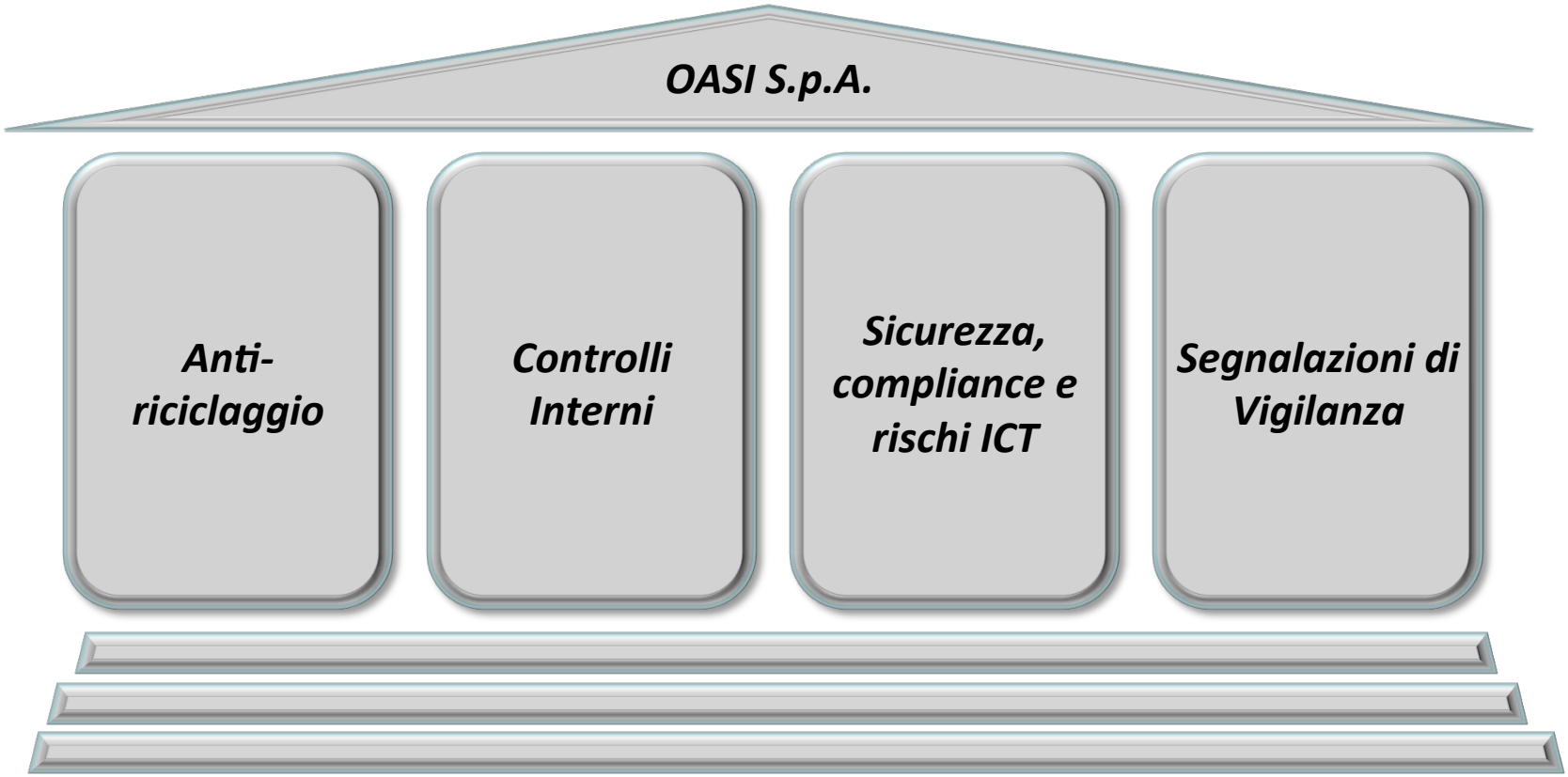
Agenda

- Premessa: il contesto del *Cybercrime* e le priorità per il settore bancario italiano
- Come organizzarsi al meglio per gestire il rischio di *cybersecurity*: il framework CSF del NIST
- Conclusioni e raccomandazioni per gli Istituti Bancari italiani in tema di *cybersecurity*

4 ***L'impegno di OASI a supporto delle banche in tema di gestione dei rischi di cybersecurity***

OASI è la società del Gruppo ICBPI specializzata nello sviluppo / integrazione di soluzioni informatiche e nei servizi di consulenza, outsourcing e formazione

OASI – Outsourcing Applicativo e Servizi Innovativi S.p.A. è la società del gruppo ICBPI leader nelle soluzioni, nella consulenza, nei servizi innovativi e nell'outsourcing in tema di antiriciclaggio, controlli interni, sicurezza, rischi e compliance ICT, Segnalazioni di Vigilanza e Formazione



Oasi S.p.A. ha predisposto un'offerta completa di servizi e soluzioni innovative in materia di *cybersecurity*, compliance e rischi ICT

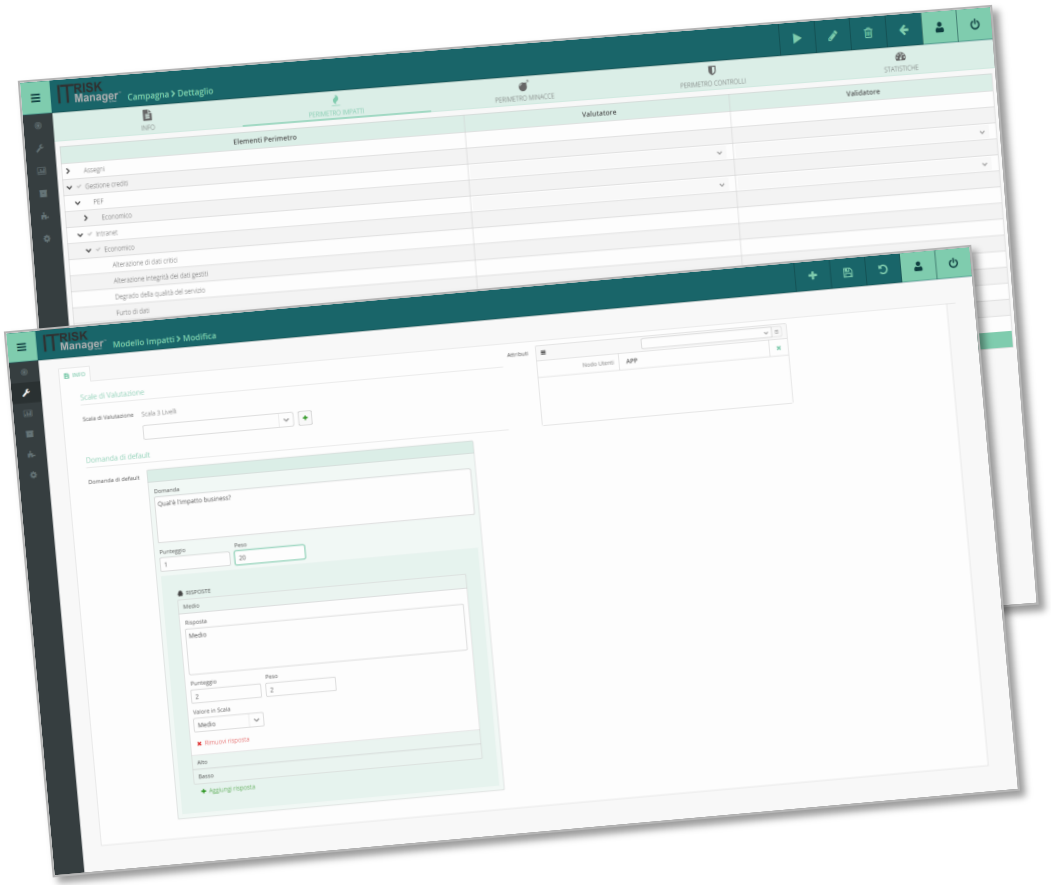
Ambito	Consulenza	Soluzioni	Servizi / outsourcing
Cyber Security	- Policy e procedure - Gestione rischio informatico - Conformità Privacy - Certificazioni ISO 27001 - Adeguamenti Circ. 263/2006 - Assessment FW Cybersec. NIST - Revisione contrattualistica - IT auditing - Sistemi di reportistica	- Gestione dei log di sicurezza - Classificazione delle informazioni - Data Loss Prevention - Protezione degli endpoint - Prevenzione APT - IT Risk Manager	- Monitoraggio della sicurezza IT - Computer forensics - Vulnerability / penetration test - Revisione del codice sorgente
Antifrode e-payments	- Policy e procedure - Gestione rischio frode - Verifiche di conformità - Conformità Circ. 263/2006 - Conformità Racc. BCE / LG EBA	- Strong Authentication - Transaction monitoring	- Anti Phishing / Anti malware - Active Fraud Prevention - Monitoraggio canale CBI - Threat Intelligence
Business Continuity	- Analisi degli impatti - Piani di Continuità Operativa - Piani di Disaster Recovery - Verifiche conformità - Certificazioni ISO 22301 - Revisione contrattualistica - Conformità Circ. 263/2006	← - SW per la gestione del piano di BC - SW per la gestione delle crisi →	
Trust Services	- Policy e procedure - Modelli Organizzativi - Verifiche di conformità - Accreditamento	- Dematerializzazione - Identità Digitale	- Firme elettroniche - Marcatura temporale - Conservazione a norma

(*) limitato ai clienti del servizio CBI di ICBPI

Focus on: la soluzione OASI *IT Risk Manager*™ a supporto del modello di gestione dei rischi informatici e di cybersecurity in conformità alla 263/2006

ILLUSTRATIVA

IT Risk Manager™



Benefici attesi

- **Conformità** con i requisiti della Nuove **Disposizioni** di **Vigilanza** Prudenziale per le Banche (Capitolo 8, aggiornamento n°15 Circ. BdI 263/2006), con flessibilità di **estensione** ad altri modelli e requisiti specifici (e.g. analisi dei rischi CAI, analisi dei rischi ISO 27001, …)
- **Supervisione** da parte di un **Comitato degli Esperti** costituiti dagli IT Risk Manager di alcune delle principali banche italiane e organizzazione di user group periodici per lo scambio di best practice esperienze tra *peer*
- **4 moduli funzionali** per la gestione di **tutti i requisiti** in materia di gestione del rischio informatico:
  - Modellistica del rischio ICT
  - Workflow processi / procedure
  - Reportistica
  - Amministrazione

Focus on: assessment rispetto al Framework NIST per la gestione dei rischi di *cybersecurity* e formalizzazione dei profili *current / target*

ILLUSTRATIVA

NIST Cybersecurity Framework Assessment

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Benefici attesi

- Predisporre una **modalità** di gestione dei **rischi** di *cybersecurity* in linea con il nuovo **approccio BCE**
- Spingere ulteriormente la modalità di **gestione** dei **rischi** di *cybersecurity* in una **logica *risk based***
- Possibilità di **confrontarsi** con ***peer*** per verificare l'**adeguatezza** del programma di *cybersecurity*
- Valorizzare le **attività** e gli **investimenti** già effettuati per l'adeguamento alla **263/2006** e ad **altri standard**
- Focalizzarsi sugli **aspetti** di **reazione** (rilevazione, risposta, ripristino) agli **incidenti** di **sicurezza informatica**
- Migliorare la **capacità** di **gestire** i **rischi** di *cybersecurity* emergenti dalla ***supply chain*** dei fornitori utilizzati
- In **partnership** con **azienda U.S.** che ha **partecipato** alla predisposizione del **framework**

Focus on: l'impegno di OASI all'approfondimento delle tematiche legate alla gestione dell'identità digitale degli utenti dei servizi di e-banking

ILLUSTRATIVA

Attività di ricerca in tema di identità digitale

Benefici attesi

- **Aumentare** in generale la **fiducia** dei **cittadini** nei **servizi Internet**, ivi inclusi i sistemi di pagamento online
- **Ottimizzare** lo **sviluppo** di **servizi digitali**, separando la parte di identificazione e autorizzazione da quella di funzionalità dei servizi
- **Ridurre** le **basi dati** contenenti **dati personali** dei cittadini con accesso "autorizzato" solo ai dati di cui si ha bisogno per erogare il servizio
- **Incrementare i livelli di sicurezza** utilizzando modello decentrati e cooperanti dell'architettura SPID
- **Sfruttare** al massimo le **tecnologie disponibili** pei i metodi per la verifica delle identità
- **Sviluppare** un **mercato** per i **servizi** di **gestione** dell'**identità digitale**, con conseguente riduzione dei costi

Focus on: soluzioni per la *cybersecurity* degli impianti di sicurezza fisica delle filiali nel contesto dell'integrazione *physilogical* dei sistemi

ILLUSTRATIVA

Monitoraggio traffico CEI-ABI

Benefici attesi

- Approccio **non intrusivo** per monitorare **impianti** di **sicurezza fisica** delle **filiali** sempre più "aperti" su reti dati TCP/IP
- Capacità di **rilevazione** in **tempo reale** di "infezioni" da **malware** / **APT** e di rilevazione **attività sospette**
- Capacità di **comprendere** e **decodificare** i **protocolli CEI ABI** per il colloquio tra centro e periferia
- **Profilatura comportamentale** di ogni **oggetto** del sistema di sicurezza fisica (e.g. sensori, videocamere) tramite algoritmi di **machine learning**
- Livello di **protezione** ispirato alle soluzioni per il **monitoraggio** delle reti e sistemi **SCADA** per il **controllo industriale**

Focus on: i servizi di CERT e di SOC* per il monitoraggio degli attacchi e il supporto alla risposta agli incidenti di *cybersecurity*

ILLUSTRATIVA

Security Operation Center

Benefici attesi

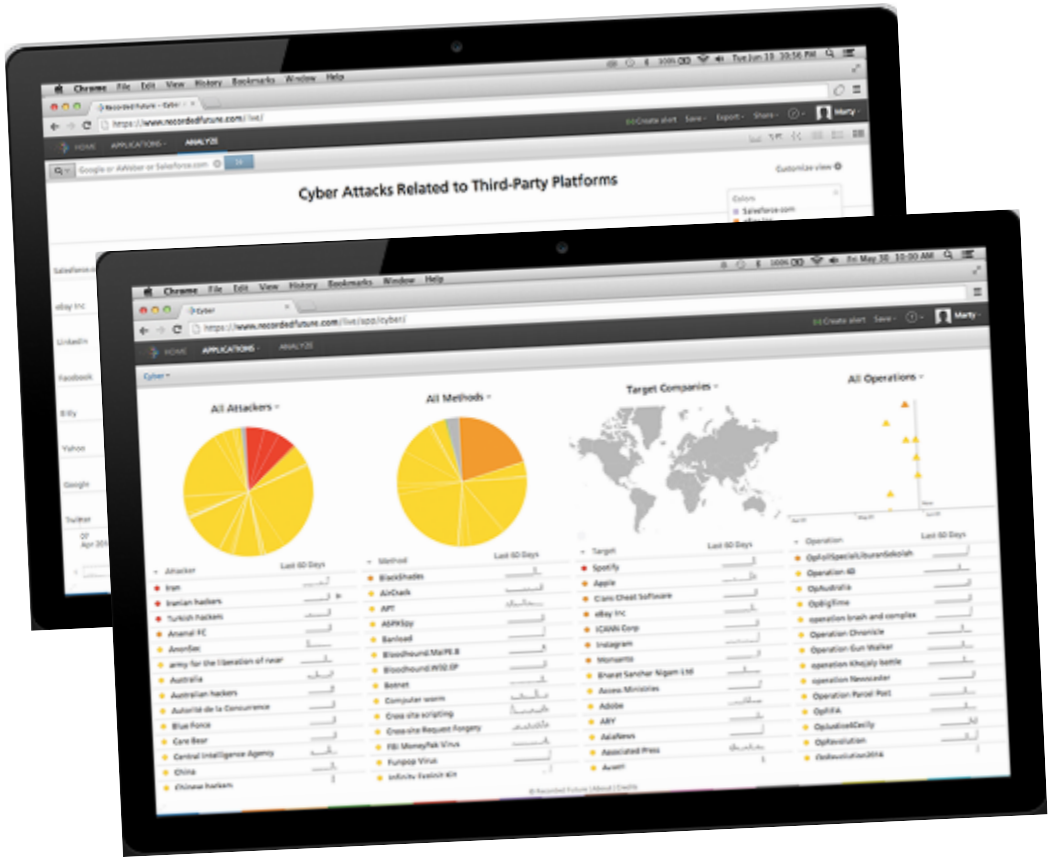
- **Completezza** dei **servizi** di **sicurezza** gestiti: **SOC**, **CERT**, **gestione** dei dispositivi di **sicurezza**, contrasto agli attacchi DoS / DDoS
- Garantisce la **prossimità territoriale** ai clienti sul territorio italiano, con una **copertura** del servizio **flessibile**
- Elevata **focalizzazione** su **minacce** ed esigenze dei clienti del **settore bancari** e **finanziario** (*e.g. phishing, malware, brand buse, rogue app*)
- Team di **personale** con **competenze specialistiche uniche** e **certificazioni** di alto livello
- **Garanzia** di **funzionamento H24** tramite soluzioni e piani di Business Continuity e Disaster Recovery
- Utilizzo di un mix di **tecnologie proprietarie** e delle migliori in ambito **commerciale**

(*) Erogati in partnership con Communication Valley

Focus on: servizio di open source intelligence* per il monitoraggio del livello di esposizione alle minacce derivanti dal *cybercrime*

ILLUSTRATIVA

Open Source Intelligence



Benefici attesi

- Servizio di **Web Open Source Intelligence** (OSINT) basato sull'analisi in tempo reale di **650.000+ sorgenti** open in 7 lingue
- Identificazione e notifica di **credenziali rubate**, **monitoraggio** di **"menzioni" sospette** su domini / indirizzi IP di proprietà
- **Monitoraggio** di **informazioni** su **attacchi** / **data breach** relative a clienti, fornitori e partner
- **Sintesi periodiche** dei **trend** di attacco in relazione a **dimensioni** di **interesse** (e.g. per settore industriale, per minaccia, per area geografica)
- Possibile **integrazione** con servizio di **HUMINT** (Human Intelligence) per servizi di **intelligence** più specifici

(*) Erogati in partnership con Communication Valley

Oasi
GRUPPO ICBPI

Grazie per l'attenzione

Andrea Agosti
Responsabile BU Sicurezza ICT e Controlli Interni

Oasi

OASI – Outsourcing Applicativo e Servizi Innovativi S.p.A.
Azienda del Gruppo Bancario Istituto Centrale delle Banche Popolari Italiane
Corso Europa, 18 - 20122 Milano - Tel. +39 02 77051
Cell.:**+39 335 7365157** Ufficio: **02 7705326** Mail: **a.agosti@oasi-servizi.it**