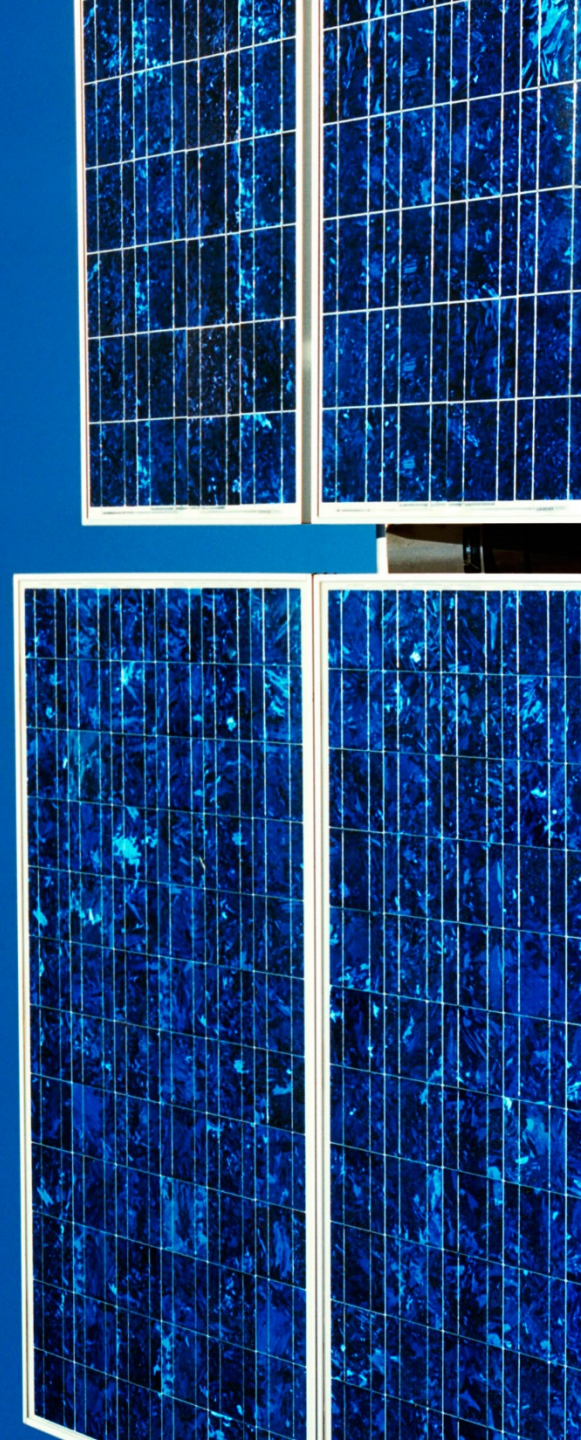
Cyber Risk Management: da problema a opportunità

KPMG Advisory S.p.A. – Andrea Zapparoli Manzoni

—

Cyber Security Day – Ancona 25 Maggio 2016



Presentazioni

Andrea Zapparoli Manzoni - Senior Manager – Head of Cyber Security

- Membro **Osservatorio per la Sicurezza Nazionale** (OSN) 2012-2014
- **CSCSS** – Center for Strategic Cyberspace + Security Science: Board Advisor
- **Assintel**: Consiglio Direttivo / Resp. GdL ICT Security
- **Clusit**: Consiglio Direttivo e docente
- Co-autore del **Rapporto Clusit** 2012, 2013, 2014, 2015, 2016…
- Co-autore del **Framework Nazionale di Cyber Security**
- Co-autore: Sicurezza Social, Frodi Online, FSN, ROSI, etc

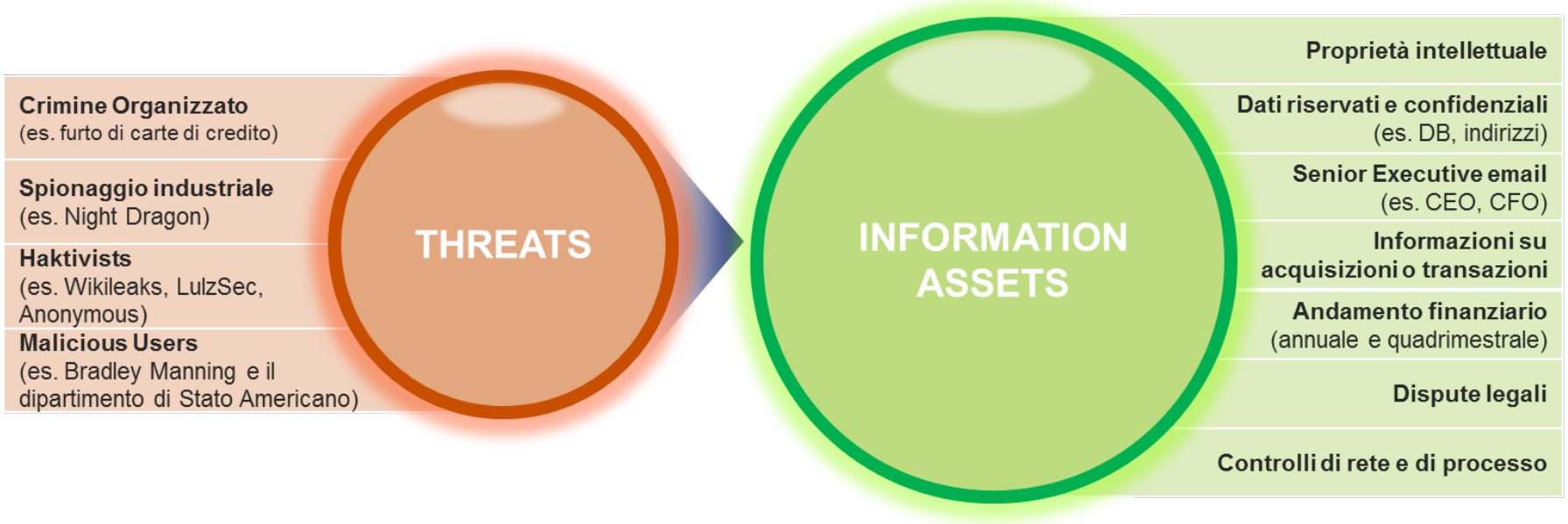
Indice

KPMG

Minacce e Rischi Cyber

Il contesto globale - IT SEC

Mentre il rischio per gli attaccanti è ancora troppo basso, il loro "ritorno dell'investimento" è elevatissimo ed è strettamente legato al crescente numero e valore degli **asset informativi** vulnerabili.



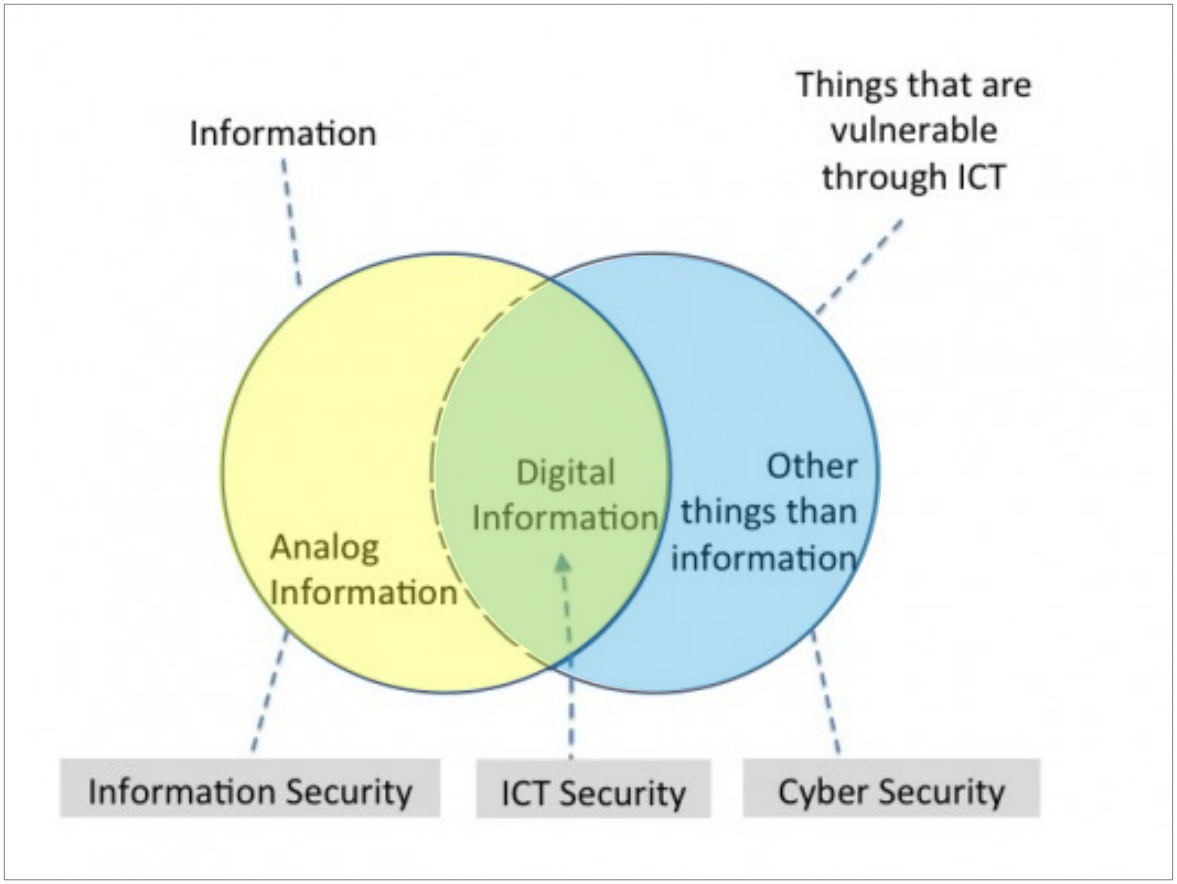
Moltiplicazione degli attori e delle capacità offensive

Moltiplicazione dei possibili target (public/private sector)

Scarsa efficacia delle difese tradizionali

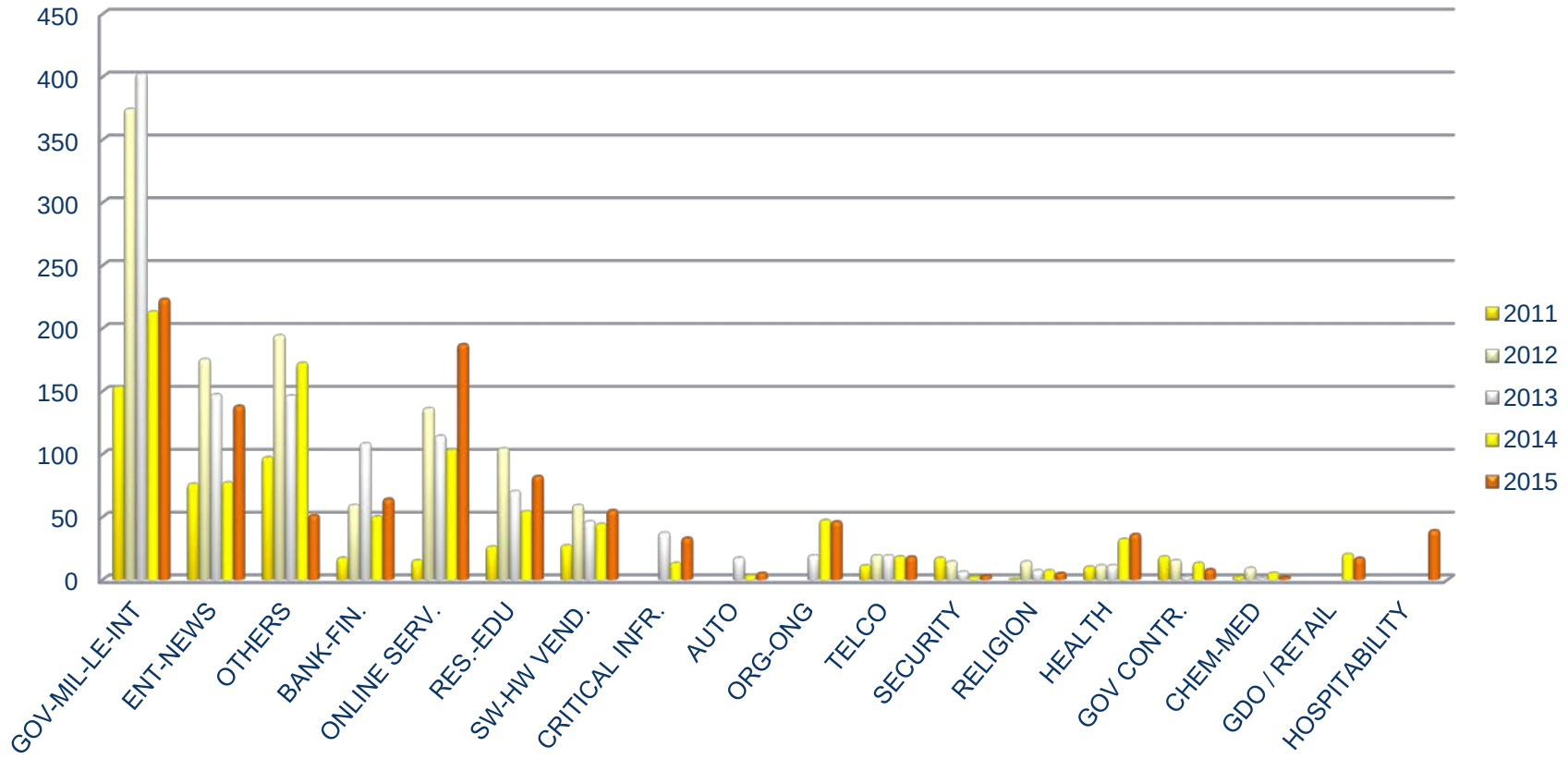
Il contesto globale - Cyber SEC

Gli asset "non-IT" che vengono oggi **resi vulnerabili tramite l'ICT** stanno aumentando in modo *esponenziale (IoT, connected-everything, etc)*. A rischio sono la reputazione, il business, la salute, i servizi essenziali, la vita umana, etc.



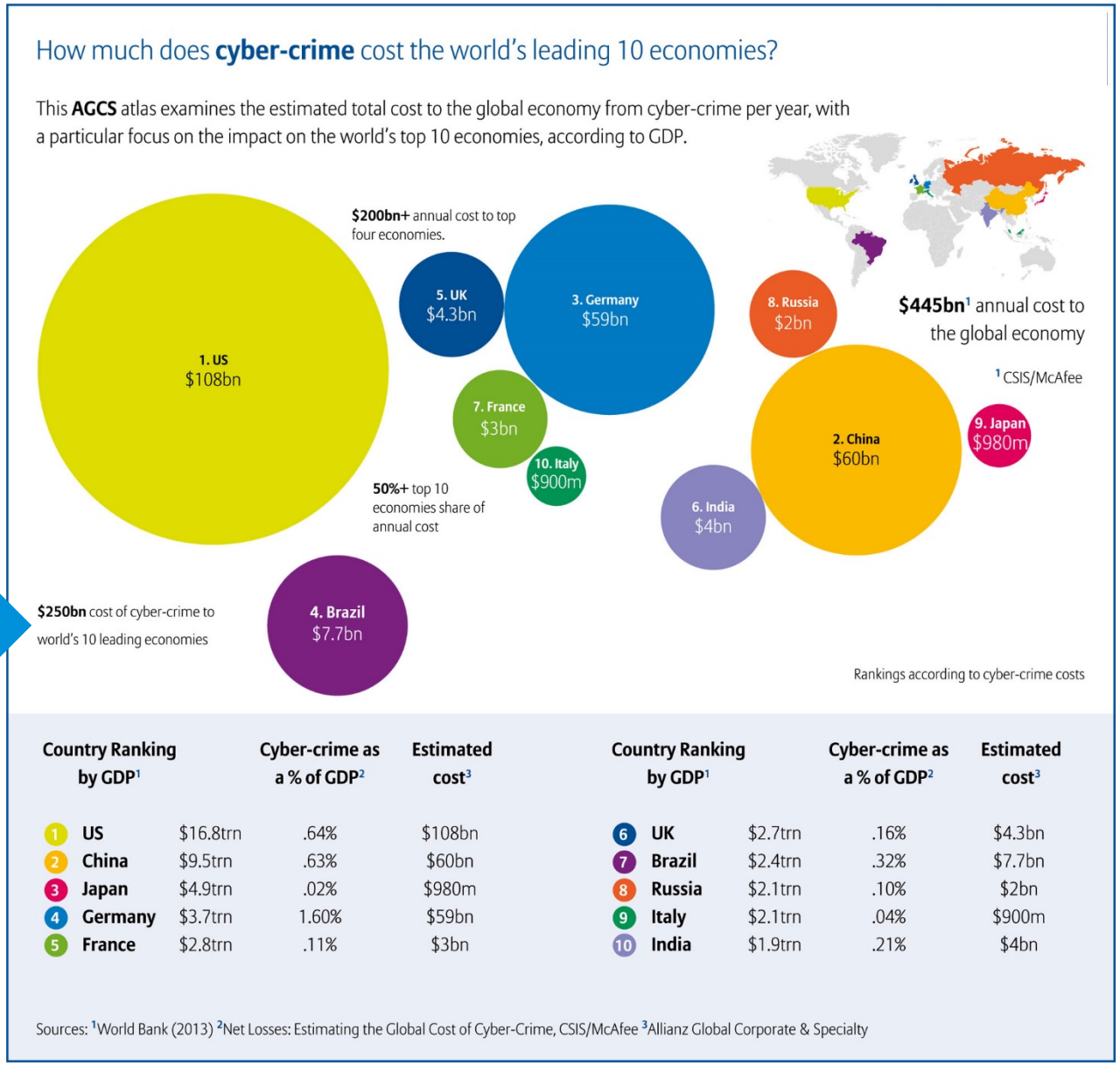
Il rischio è sistemico. Tutti sono bersagli.

Distribuzione delle vittime di attacchi gravi di dominio pubblico - 2011 - 2015



© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia

Cyber Risk Management: da problema a opportunità



Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]
1 US	$16.8trn	.64%	$108bn
2 China	$9.5trn	.63%	$60bn
3 Japan	$4.9trn	.02%	$980m
4 Germany	$3.7trn	1.60%	$59bn
5 France	$2.8trn	.11%	$3bn

Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]
6 UK	$2.7trn	.16%	$4.3bn
7 Brazil	$2.4trn	.32%	$7.7bn
8 Russia	$2.1trn	.10%	$2bn
9 Italy	$2.1trn	.04%	$900m
10 India	$1.9trn	.21%	$4bn

Sources: [1]World Bank (2013) [2]Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee [3]Allianz Global Corporate & Specialty

Cyber Risk Management: da problema a opportunità

Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]	Country Ranking by GDP[1]		Cyber-crime as a % of GDP[2]	Estimated cost[3]
1 US	$16.8trn	.64%	$108bn	6 UK	$2.7trn	.16%	$4.3bn
2 China	$9.5trn	.63%	$60bn	7 Brazil	$2.4trn	.32%	$7.7bn
3 Japan	$4.9trn	.02%	$980m	8 Russia	$2.1trn	.10%	$2bn
4 Germany	$3.7trn	1.60%	$59bn	9 Italy	$2.1trn	.04%	$900m
5 France	$2.8trn	.11%	$3bn	10 India	$1.9trn	.21%	$4bn

Sources: [1]World Bank (2013) [2]Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee [3]Allianz Global Corporate & Specialty

KPMG

Cyber Risk Management

Il Framework Nazionale di Cyber Security

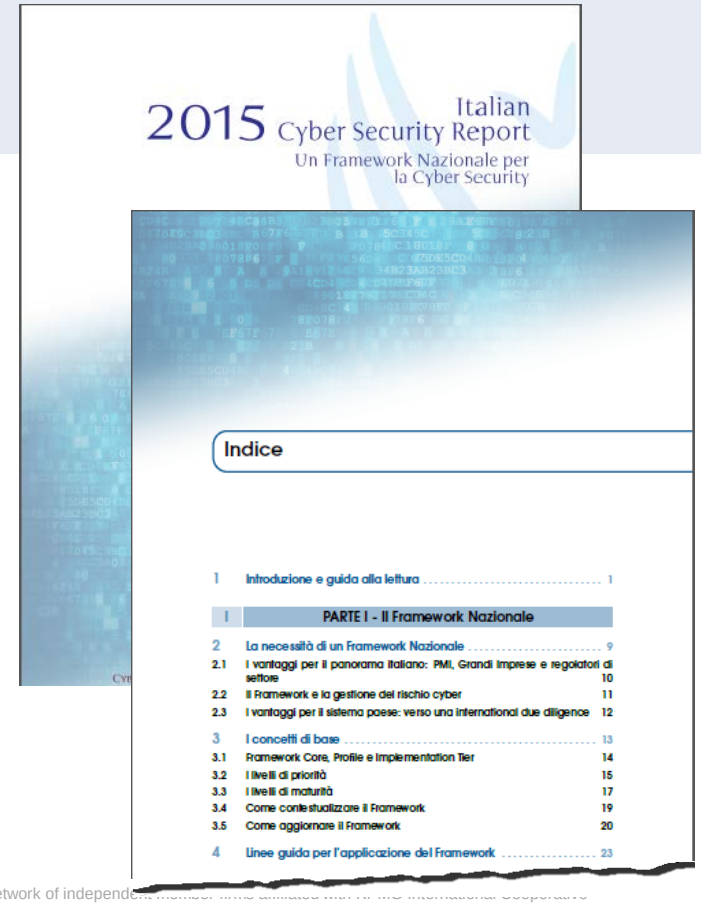
Con l'adozione del **DPCM 24 gennaio 2013** il Governo Italiano ha posato le **pietre miliari** di un cammino evolutivo finalizzato alla protezione e alla tutela della sicurezza nazionale relativamente alle infrastrutture critiche materiali e immateriali.

IL DPCM prevede due principali strumenti di programmazione:

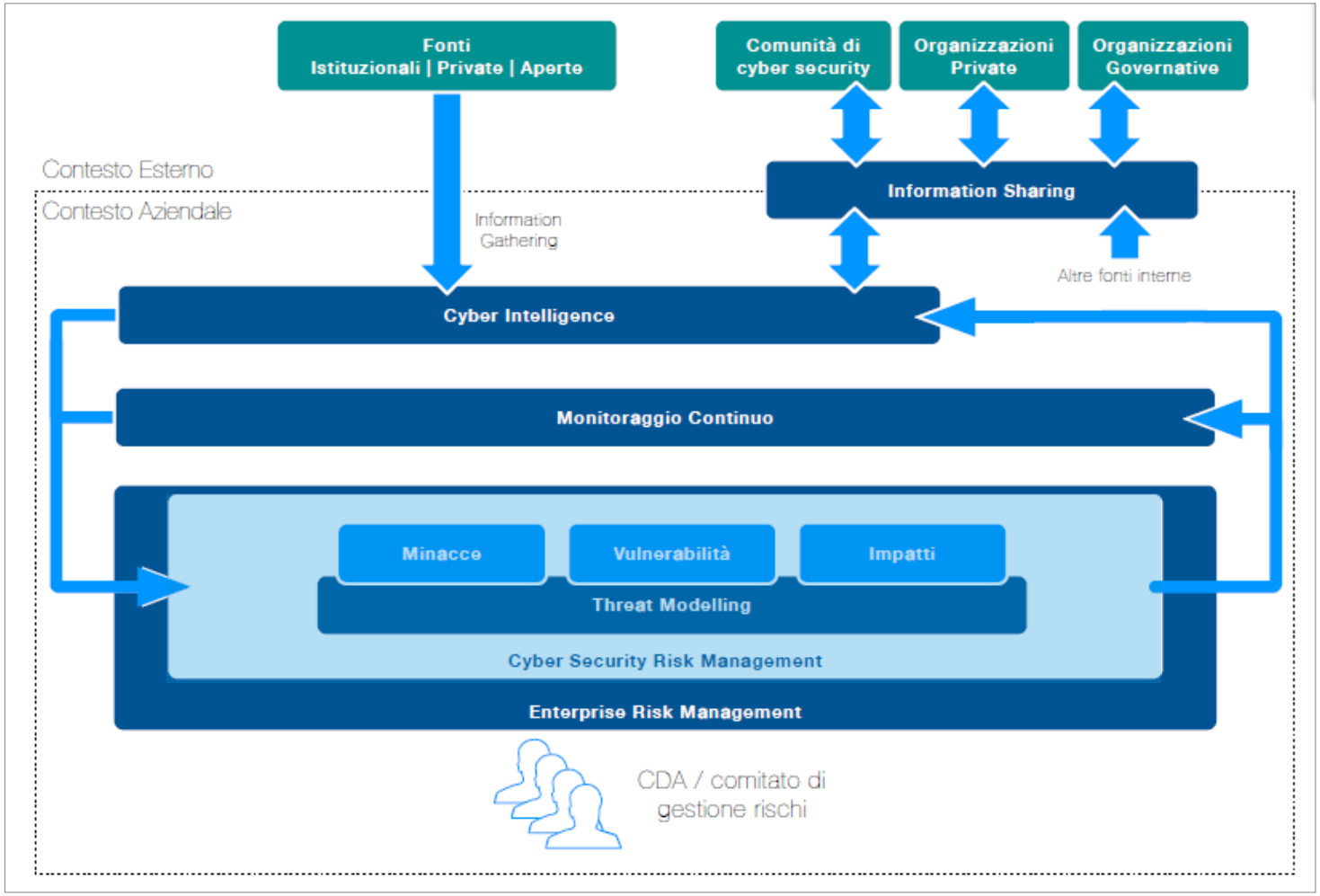
"Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico" (2013) finalizzato alla definizione degli indirizzi strategici;

"Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica" (2013) che definisce gli indirizzi operativi, i relativi obiettivi specifici e linee di azione.

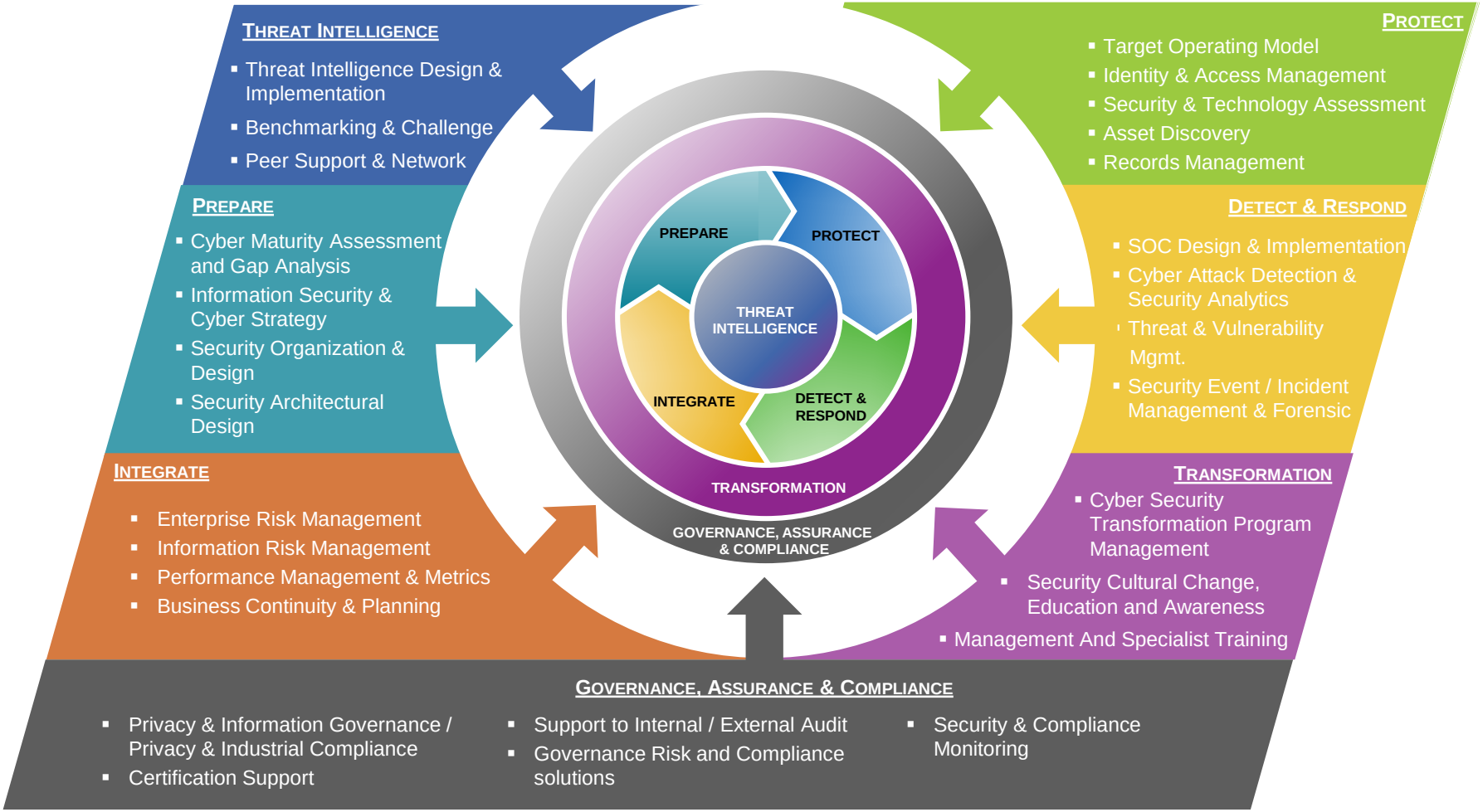
In questo contesto, **il FRAMEWORK NAZIONALE PER LA CYBER SECURITY (FNCS) del 2016,** redatto con un significativo contributo di KPMG, formalizza un quadro di riferimento **Risk-based** che le organizzazioni possono utilizzare per comprendere il proprio livello di preparazione e ridurre i rischi legati alle minacce "cyber".



Il processo di Cyber Risk Management nel FNCS



Un processo integrato di Cyber Security



Un (piccolo) esempio di Threat Vector Risk Analysis

High Risk
High-Medium Risk
Medium Risk

		Threat Actors									
		Hacker	Employee Resistance to Change	Disgruntled Insider	Disgruntled Contractor	Contractor with I.P.	Compliancy Failure	Careless Insider	Illegal Use of Corporate Assets	Organized Crime / Syndicates	General Public (i.e., PA Citizen)
Data Loss Threat Vectors	Non-Company Devices	X	X	X	X	X	X	X		X	
	Web Traffic	X	X	X	X	X	X	X	X	X	X
	Webmail	X	X	X	X	X	X	X	X	X	
	Company Devices	X	X	X	X	X	X	X	X	X	
	Outbound Email	X	X	X	X	X	X	X	X	X	X
	Internal Email		X	X	X		X	X	X		
	Data Replication		X	X	X	X	X	X	X		
	User Download			X	X	X	X	X	X		
	Network Storage		X	X	X	X	X	X	X		X
	Peer-to-Peer		X	X	X		X	X	X		

Problemi

Oggi le **vulnerabilità endemiche**, **l'impreparazione del fattore umano** e **l'assenza di processi efficaci di Cyber Risk Management** sono tre elementi che, combinati tra loro, **facilitano enormemente** le attività degli attaccanti. **Non possiamo più permettercelo.**

Solo un approccio dinamico, risk-based, pro-attivo ed informato consente di guidare con efficienza la definizione delle strategie e l'allocazione dei budget, e di controllarne strettamente l'efficacia nel tempo.

Sono tre i **principali elementi di trasformazione** necessari per implementare un processo di Cyber Risk Management che consenta di realizzare attività di Cyber Security economicamente sostenibili ed efficaci:

- **creare una mentalità risk-based in tutta l'organizzazione**,
- **implementare un modello operativo basato su una costante attività di Cyber Risk Management,**
- **definire processi di decision-making basati sull'analisi puntuale dei rischi "cyber", continuamente aggiornata**.

La vera **sfida** del Cyber Risk Management sta nel dover **conciliare ed armonizzare la difesa contemporanea** di asset appartenenti a dominii fino ad oggi gestiti separatamente (p.es. i record del database dei clienti ed il valore in Borsa dell'azienda, l'account Facebook del figlio del CEO e la continuità dei processi produttivi, la fiducia degli Stakeholders e la Compliance, etc).

In assenza di ciò, oggi si può mettere in gioco la sopravvivenza dell'organizzazione nel suo complesso.

Opportunità

Siamo giunti ad un **bivio** importante, che rappresenta una **forte discontinuità** con il recente passato.

La Cyber Security ha lo scopo di gestire rischi "cyber" (ICT e non) che oggi possono impattare anche gravemente su processi di business e/o asset preziosi (anche non IT, p.es. la reputazione o la delivery di servizi "core"). **Data la numerosità e la pericolosità delle minacce, questi rischi se non controllati e mitigati possono causare effetti potenzialmente deleteri per i singoli, le aziende, le Istituzioni e la collettività in generale.**

Possiamo continuare a vedere la Cyber Security come un problema, un costo da sopportare (e minimizzare) o una "tassa" crescente, indotta anche da maggiori oneri futuri di compliance (NIS, Privacy europea, eIDAS, etc), oppure possiamo **sfruttare strategicamente i vantaggi competitivi** forniti da un buon processo di Cyber Risk Management per:

- **Differenziare l'organizzazione dalla concorrenza,**
- **Rassicurare gli Stakeholders (azionisti, top management, utenti, clienti, partner, fornitori),**
- **Abilitare e rendere sostenibili nuovi business (digitali e non), altrimenti resi antieconomici / troppo rischiosi,**
- **Sopravvivere e prosperare in un contesto globale dinamico, in rapido cambiamento e sostanzialmente ostile.**

Cogliere questa opportunità è una delle principali sfide dei prossimi mesi / anni.

KPMG

Grazie

Andrea Zapparoli Manzoni
KPMG Advisory S.p.A. - Senior Manager
azapparolimanzoni@kpmg.it
3463087235

kpmg.com/socialmedia

kpmg.com/app