

# Kick Off Gruppo di Lavoro AIIC

## Cyber Insurance

Roma 8 giugno 2016

**Coordinatori: Luisa Franchina, Fabrizio Loppini, Giuliano Merlo**



# Agenda

---

- Obiettivi del gruppo di lavoro
- Approccio metodologico
- Attività proposte
- Risultati attesi
- Organizzazione del Gruppo di lavoro
- Tempi
- Pianificazione operativa prossimi step

# Obiettivi del Gruppo di lavoro

- Obiettivo di breve periodo
  - Creare una mappa del mercato in termini di offerte di prodotti assicurativi sottolineando attuali punti di forza e debolezza
- Obiettivo di lungo periodo
  - Individuazione dell'approccio strategico più appropriato (proattivo, reattivo, mix) a fine di corretta valutazione dei cyber risk da un punto di vista di stima e copertura assicurativa
- Tali obiettivi sono in linea con gli indirizzi operativi del «Piano Nazionale per la protezione cibernetica e della sicurezza informatica», tra i quali viene evidenziata la copertura assicurativa come elemento integrante di una strategia volta alla gestione del rischio cyber

# Approccio reattivo - scenario post sinistro:

1. Identificazione delle figure coinvolte da una problematica Cyber Risk
2. impatto economico - costi (gestione della crisi, consulente informatico - sicurezza, ricostruzione immagine aziendale)
3. impatto economico - Business Interruption (perdita di fatturato e relativo Margine di Contribuzione, aumento costi connessi)
4. impatto assicurativo - quali coperture possono intervenire e come integrarle

# Approccio proattivo - scenario pre sinistro:



1. Definizione del tavolo di lavoro interno all'azienda - unità Cyber Risk con identificazione dei ruoli
2. impatto economico - definizione di budget destinato alla gestione del Cyber Risk
3. impatto economico - simulazione (tramite modellazione ed analisi) di costi e danni da Business Interruption
4. impatto assicurativo - adeguamento o integrazione del piano assicurativo aziendale
5. Fornire alle assicurazioni un metodo per valutare polizze e riserve tecniche tramite implementazione del Framework Nazionale

# Attività e metodologia

---

- Raccolta informazioni sui prodotti assicurativi attualmente presenti nel mercato italiano
- Raccolta di casi e di approcci al cyber risk all'interno di realtà italiane con l'obiettivo di approfondire come le aziende valutano gli impatti conseguenti agli attacchi cyber
- A seguito di analisi saranno formulati principi guida sulla adozione dello strumento assicurativo a integrazione della strategia cyber risk management

- Documento di mappa del mercato in termini di offerte di prodotti assicurativi sottolineando attuali punti di forza e debolezza
- Discussione sui questionari e sui casi raccolti
- Determinazione delle modalità preferite dalle aziende su come affrontare problematiche di cyber-insurance
- Individuazione dei principi base per la implementazione dei due approcci
- Sessioni aperte di condivisione e confronto per approfondimenti verticali su specifiche tematiche di Sicurezza

# Struttura Organizzativa del Gruppo di Lavoro



## **Coordinatori GDL**

*Luisa Franchina  
Fabrizio Loppini  
Giuliano Merlo*

## **Core Team**

*Paolo Giudice  
Cesare Burei  
Michele Kidane  
Roberto De Sortis  
Riccardo Scalici  
Luca Montanari  
Stefano Armenia  
Alessio Pennasilico  
Andrea Zapparoli Manzoni  
Raffaella d'Alessandro*

## **Team Esteso**

*Dursi Elenio, Alessandro Lazari, Fabio De Paolis,  
Marcello Pistilli, Roberto Setola, Manuel Cacitti,  
Sergio Casagrande, Federico Franchina, Andrea  
Castellano, Pio Lauda*



# Tempi

---

- Ipotizziamo di produrre primi risultati per fine ottobre
  - Condivisione e discussione dei risultati
- Progettazione della fase ulteriore del GdL sul tema degli approcci da seguire nella cyber insurance (approccio reattivo versus approccio proattivo)

# Pianificazione Operativa dei prossimi passi

- Raccolta informazioni sui prodotti assicurativi attualmente presenti nel mercato italiano (entro fine agosto)
- Redazione del documento di mappa del mercato in termini di offerte di prodotti assicurativi sottolineando attuali punti di forza e debolezza (settembre - ottobre)
- Predisposizione del questionario e raccolta delle risposte dall'azienda in merito all'approccio reattivo o proattivo, Analisi materiale ricevuto (ottobre - novembre)
- Elaborazione dei principi guida sulla adozione dello strumento assicurativo a integrazione della strategia cyber (da novembre)
- Sessioni aperte di condivisione e confronto per approfondimenti verticali su specifiche tematiche di Sicurezza ( a seguire)
- **Prossima data per incontro: TBD Fine giugno**

# Q&A

