

# Cyber Security: protezione fisica e virtuale degli asset aziendali

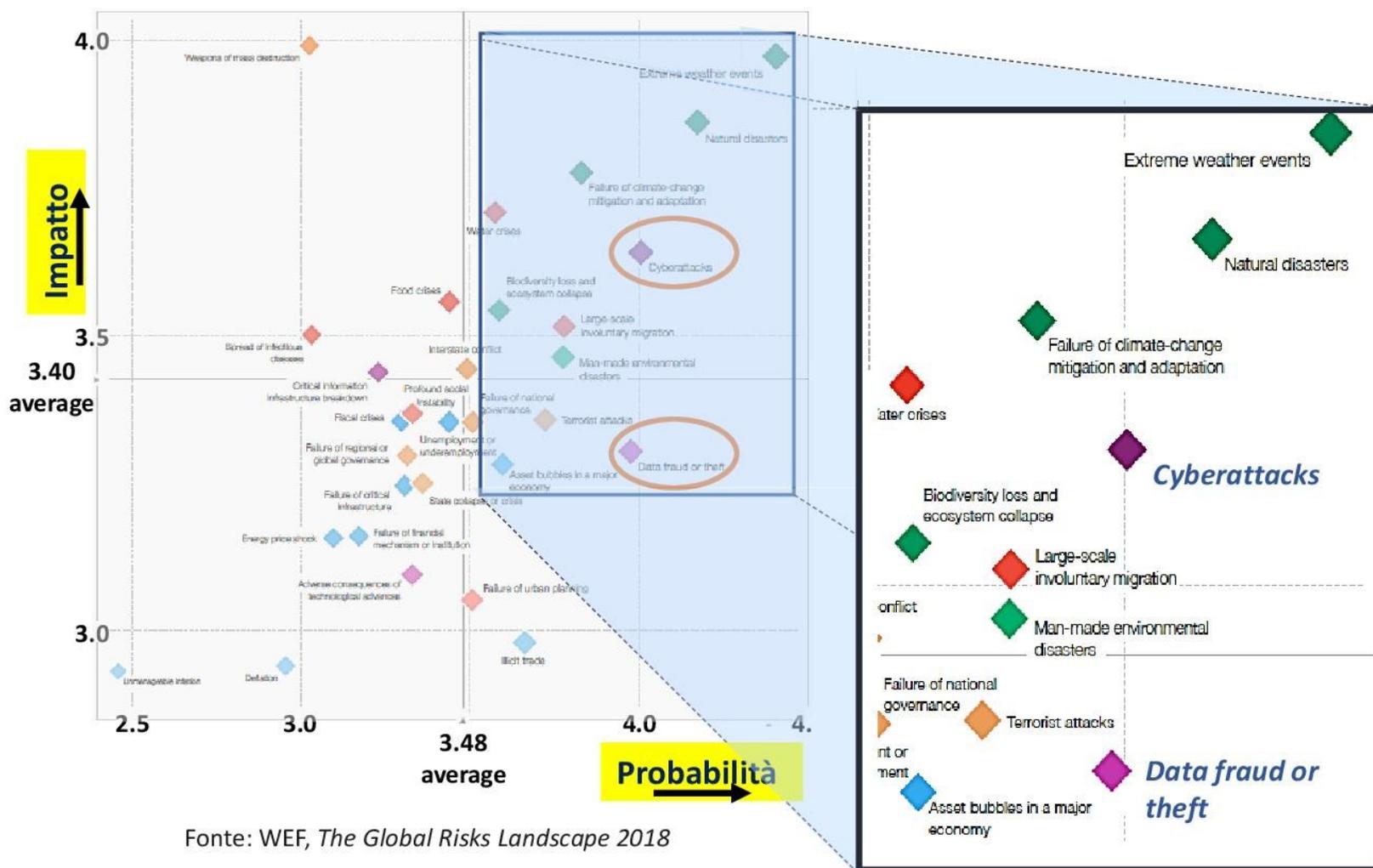
Vincenzo Calabrò



# Perché parliamo di Cyber Security?

The Global Risk Report

2018  
WORLD  
ECONOMIC  
FORUM



Cyber attacks e Data fraud or theft sono tra i primi 10 rischi del Global Risk Report 2018 del World Economic Forum:

- Sono i rischi percepiti con un livello molto elevato di impatto, in crescita rispetto al Report 2017, e che vede i **Cyber attacks al 6° posto**.
- Come probabilità di accadimento sono percepiti rispettivamente al **3° e 4° posto**, solo dietro ai disastri dovuti a condizioni climatiche estreme o a eventi naturali.

# Definizione



WIKIPEDIA  
The Free Encyclopedia

La **sicurezza informatica** (information security) è l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici; a questi tre parametri si tende attualmente ad aggiungere l'autenticità delle informazioni.

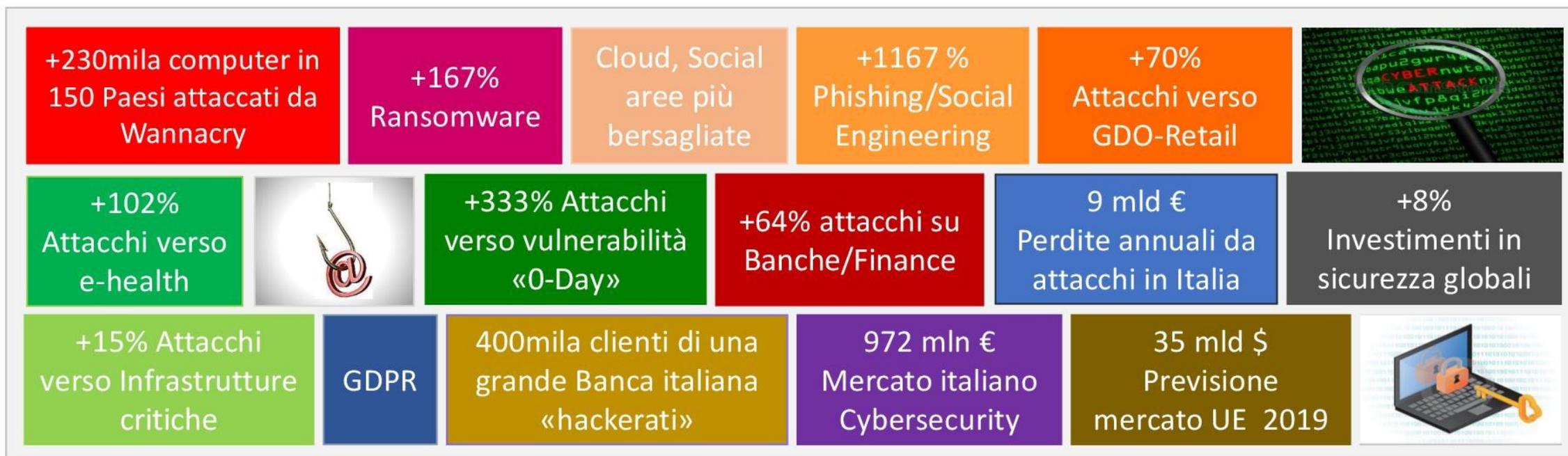
La **cybersecurity** rappresenta la sottoclasse della sicurezza informatica che dipende solo dalla tecnologia informatica.

La Cyber Security è in sintesi l'insieme di attività, ruoli e responsabilità, approcci, metodologie e tecnologie finalizzati a proteggere le informazioni e tutto ciò che dipende da risorse ICT ed è **vulnerabile** e a **rischio**, attraverso attività di **prevenzione, rilevazione e risposta** ad attacchi provenienti dal cyberspazio

**Obiettivo:** assicurare l'integrità e la difesa dalle **minacce** interne ed esterne con un approccio olistico che miri ad una **gestione del rischio** ritenuta accettabile

# Scenario

Il mercato dell'information security in Italia (concentrata nelle **grandi imprese, per il 78%**) ha raggiunto nel 2017 un valore di **1,09 miliardi di Euro**, in crescita rispetto ai 12 mesi precedenti.



# Use Case



**PROTEZIONE ASSET**

- Identità digitali
- Mobile
- End point
- Rete/Network
- Posta elettronica
- Sistemi produttivi
- Web application

**Azienda di sviluppo soluzioni SW/consulenza:**

Realizzazione di un progetto per la fornitura ai propri dipendenti di strumenti di Office Automation «sicuri» tra cui PC con gestione centralizzata della Software distribution e delle Patch, Posta elettronica, SmartPhone e palmari con MDM (Mobile device Management)



**SICUREZZA DATI**

- Certificazione dato filiera
- Dati e applicazioni in cloud
- Backup/DR
- Protezione informazioni

**Azienda di apparati medicali**

Prodotto medico che inietta insulina nel paziente sulla base delle informazioni ricevute dai sensori indossati dal paziente stesso (IoT). Cifratura dei flussi di comunicazione e dei dati memorizzati; certificazione della corretta identità dei sensori e dell'applicazione centralizzata



**COMPLIANCE**

- Fatturazione elettronica
- eIDAS (firma digitale, PEC)
- GDPR
- Normative Privacy ITA

**Laboratorio di analisi cliniche**

Migrazione verso servizi in Cloud per demandare al provider dei servizi la gestione dei dati in linea con le direttive del GDPR; campagna informativa verso i Clienti per fornire la corretta informazione sulle modalità di trattamento dei dati.

# Componenti essenziali



# Principali Benefici

- Business Continuity
- Protezione da Frodi
- Data Breach prevention
- Resilienza
- Disponibilità ed integrità delle informazioni

Questi rappresentano solo alcuni tra i principali benefici che una corretta gestione del rischio può portare alle aziende. E' sicuramente importante avere chiaro che anche nel mondo della Cyber Security **prevenire è meglio che curare.**

# Sinergie

La diffusione di elementi connessi aumenta notevolmente la superficie di attacco ed anche la numerosità dei potenziali attaccanti (Botnet).

IoT, Cloud, Big Data fondano la loro esistenza sulla garanzia che i servizi, i Dati e le infrastrutture siano Sicure, di conseguenza la Cyber security rappresenta un elemento comune a tutte. E' per questo che tale argomento sta assumendo nel tempo sempre più importanza.

# Da dove partiamo?

- Definire **COSA abbiamo** di prezioso **da proteggere** sul Cyberspazio
- **Individuare** le principali **Minacce** a cui siamo esposti (Sicurezza e compliance)
- Avere chiara la nostra **Propensione al Rischio**
- Individuare le **soluzioni migliori** in termini di rapporto costo-beneficio per le nostre esigenze (prodotti e servizi di sicurezza)
- Investire molto sulla **Consapevolezza** dei nostri dipendenti ( qualsiasi strumento implementeremo sarà inutile se non usato correttamente)

# Grazie

Vincenzo Calabrò

LinkedIn \ vincenzocalabro

[vincenzocalabro.it](http://vincenzocalabro.it)

