Top Business Risks in 2021

Allianz Risk Barometer 2021

Rank 2021	Risk	Rank 2020	Trend
1	Interruzione di attività (anche della catena di fornitura)	1	↑
2	Scoppio di pandemie (*e.g.* temi di salute e sicurezza, restrizioni mobilità)	17	↑
3	Rischi informatici (*e.g.* cyber crime, guasti ICT, data breach, multe e sanzioni)	1	↓
4	Cambiamenti nei mercati (volatilità, aumento della competizione/arrivo di nuovi operatori, fusioni e acquisizioni, stagnazione e fluttuazione del mercato)	5	↑
5	Cambiamenti nella regolamentazione e nella legislazione (*e.g.* embarghi, Brexit, protezionismo, dazi)	3	↓
9	Cambiamento climatico/aumentata instabilità metereologica	7	↓
14	Furto, frode e corruzione	15	↑

Fonte: Allianz Risk Barometer 2021

Aspetti definitori

RELAZIONE TRA OPERATIONAL, ICT, SECURITY E CYBER RISK

Operational Risk

Rischio di subire **perdite** derivanti da **inadeguatezza** o **disfunzione di processi**, **risorse umane** e **sistemi interni**, oppure **eventi esogeni**. In tale ambito rientra altresì il **rischio informatico** (ICT Risk), anche nelle fattispecie di Security Risk e Cyber Risk

ICT Risk

Rischio di **perdite (correnti o potenziali) economiche**, di **reputazione** e di **quote di mercato** in relazione all'utilizzo della tecnologia dell'informazione e della comunicazione (ICT) per eventi suscettibili di **compromettere** la **Riservatezza**, l'**Integrità** e la **Disponibilità** delle infrastrutture tecniche e/o dei dati[1]

Security Risk

Rischio di **pregiudicare** la **Riservatezza**, l'**Integrità** e la **Disponibilità** dei dati a seguito di qualsiasi **evento**, di tipo **logico** o **fisico**, proveniente dall'interno o dall'esterno dell'organizzazione

Cyber Risk

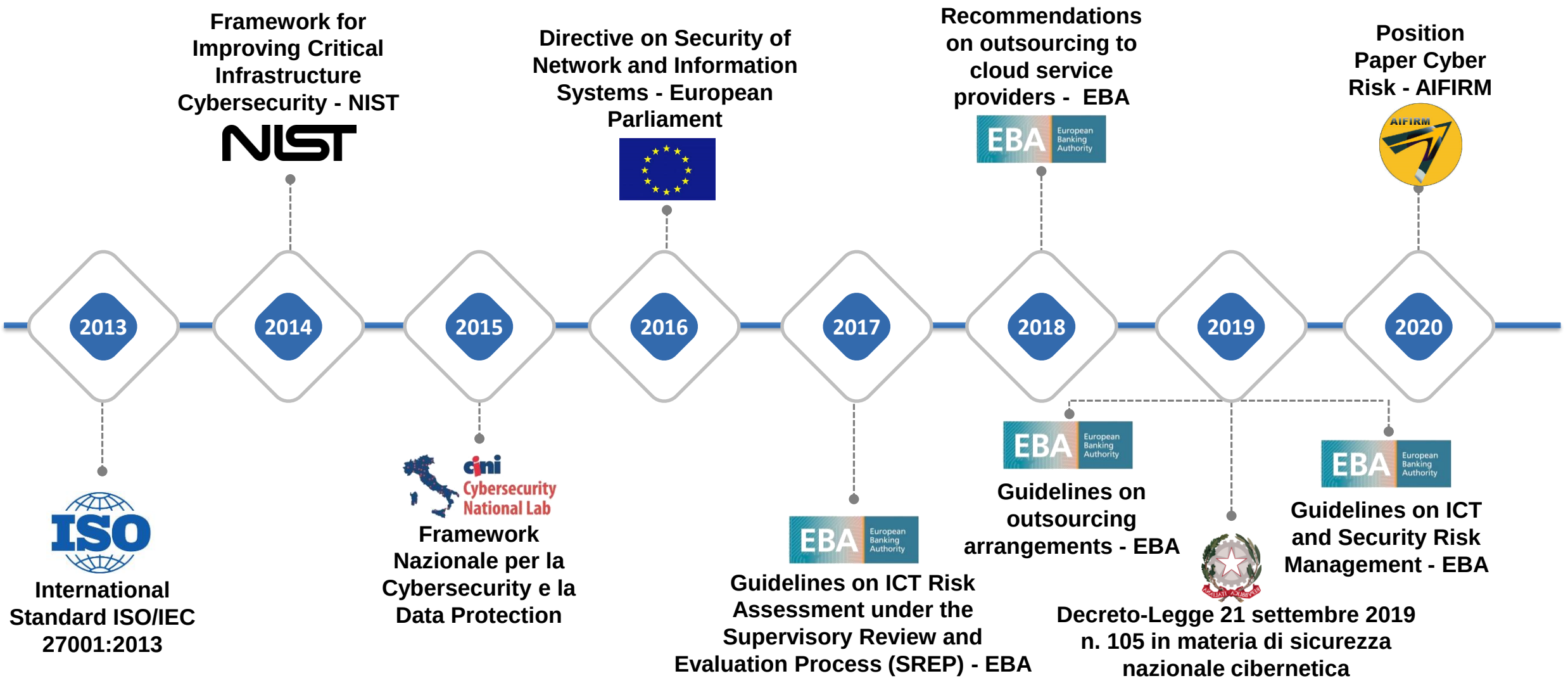
Rischio connesso a qualunque **atto intenzionale** e **malevolo** sul sistema informativo causato da parti interne, esterne o da terze parti, in grado di **pregiudicare** la **Riservatezza**, l'**Integrità** e la **Disponibilità** delle infrastrutture tecniche e/o dei dati. La causa di un cyber risk non necessariamente è intenzionale e malevola

Nell'ICT Risk sono ricompresi eventi non inclusi nel Security e nel Cyber Risk (*e.g.* guasto/indisponibilità di un applicativo con conseguente ritardata esecuzione di attività). A sua volta, nel Security Risk sono ricompresi eventi di tipo logico (*e.g.* errata configurazione software con conseguente diffusione di informazioni riservate a persone non autorizzate) e di tipo fisico (*e.g.* danneggiamento involontario dell'infrastruttura con conseguente indisponibilità di dati) non inclusi nel Cyber Risk

[1] In tal senso, l'ICT Risk è focalizzato sulla prospettiva degli Asset ICT piuttosto che sulla prospettiva dei processi tipica dell'Operational Risk

Cyber Risk

Principali riferimenti normativi e best practices

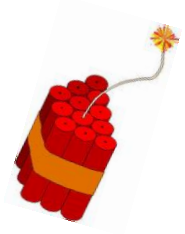


Cyber Risk

Definizione e considerazioni preliminari

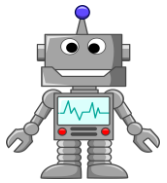
AIFIRM - Position Paper N°18 ‘Cyber Risk’: **Rischio di incorrere in perdite economiche, di reputazione e quote di mercato a seguito di interruzioni dell’operatività dei sistemi o di violazioni all’accesso dei dati in esso contenuti, generate da eventi cyber (attacchi perpetrati con finalità malevole mediante differenti tecniche e tecnologie, facendo leva sulle vulnerabilità dei sistemi ICT)**

Alcune considerazioni



Tra i rischi operativi legati ai sistemi ICT, il Cyber Risk rappresenta la sfida più grande (**elevata probabilità / alto impatto**)

Vulnerabilità zero-day (silent cyber) e **minaccia onnipresente** di attacchi alla sicurezza informatica



Investire continuamente per raggiungere (e mantenere) la frontiera tecnologica mondiale

È anche un **people risk**

Sempre più spesso le violazioni sono da ricondurre al **comportamento errato** o **doloso** di uno o più dipendenti

Oltre l’80% dei problemi di sicurezza proviene dall’interno delle organizzazioni

Cyber Risk

Un salto ‘quantico’ nei livelli di cyber-insicurezza globali

Il Re è ‘nudo’

- Non esiste un problema tecnologico quanto piuttosto **culturale** e, soprattutto, **economico**
- **‘Mutazione genetica’** delle minacce cyber
- Tema spesso ‘misterioso’ per il board (rischio di **comunicare nel modo sbagliato**)
- **Risultati** dell’attività di valutazione/ misurazione piuttosto **aleatori**
- **Filosofia ‘Zero trust’:** non fidarsi mai e verificare sempre (utenti interni ed esterni)

Alcune domande..

- In che modo si può rimediare ad un evento di Cyber Risk?
- E’ un rischio gestibile e misurabile?
- Come si mitiga l’esposizione al Cyber Risk?
- Come si misura la performance dei presìdi di sicurezza e delle misure di resilienza?
- Il livello di sicurezza dei processi core e di quelli critici per la continuità aziendale è adeguato?
- Che ruolo ha l’Operational Risk Management?

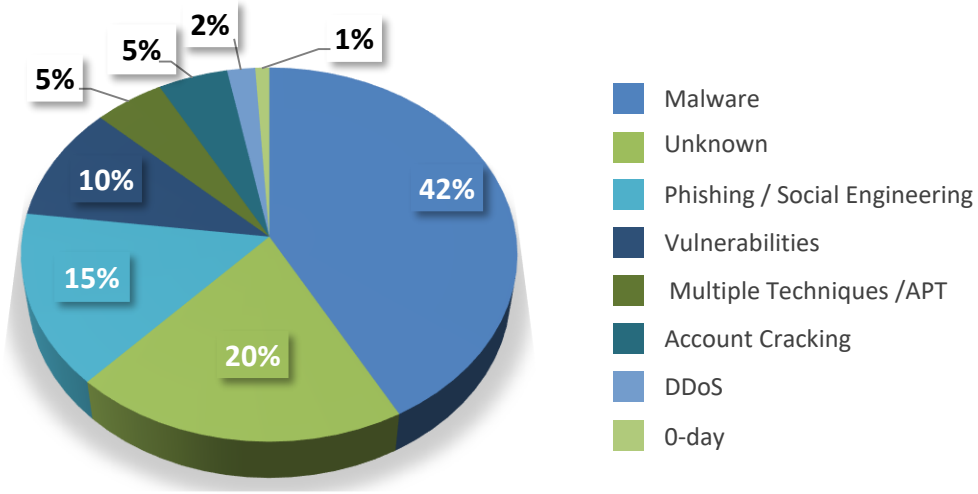
Fare previsioni a lungo termine sul Cyber Risk è particolarmente difficile

La situazione sta rapidamente sfuggendo al controllo e diventando irreversibile

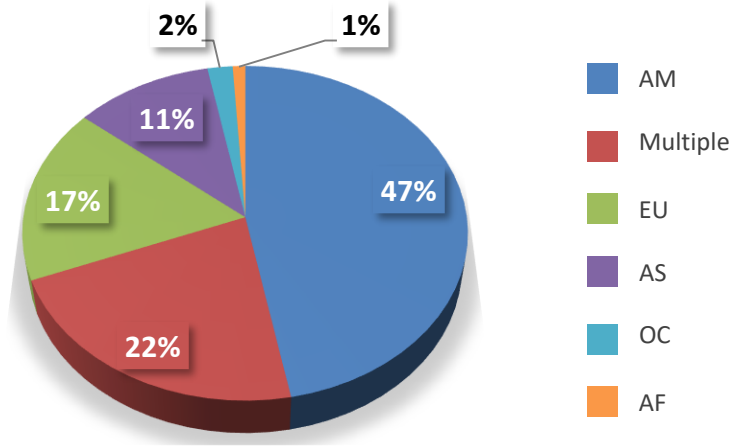
Cyber Risk

Il Cyber Risk e la sua rilevanza (1/2)

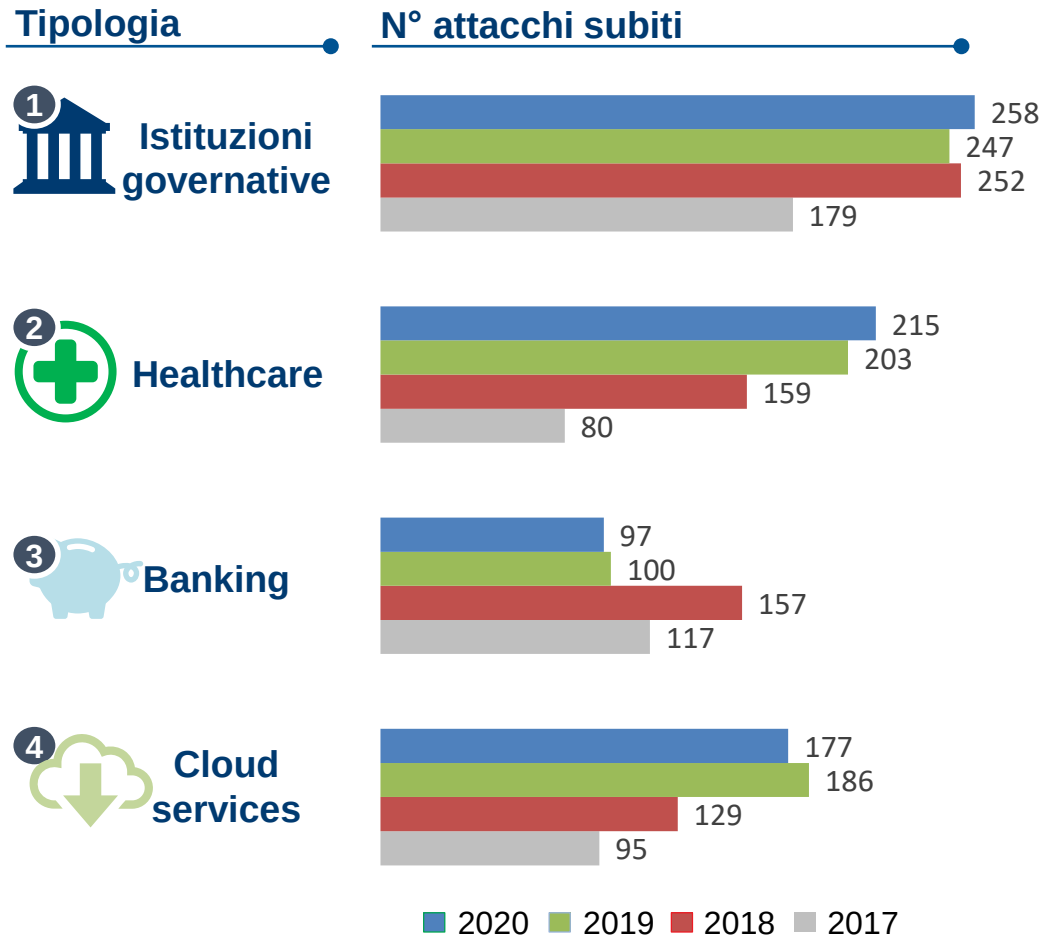
Distribuzione delle tecniche di attacco per tipologia



Distribuzione delle vittime per area geografica



Distribuzione delle vittime per settore



Fonte: Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Cyber Risk

Il Cyber Risk e la sua rilevanza (2/2)

It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it

Stéphane Nappo, 2018 Global CISO of the year

RILEVANZA CYBER RISK

12% in più di **attacchi cyber** a livello globale rispetto al 2019

NUMERO RANSOWARE

127 nuove famiglie di **ransoware** scoperte nel 2020

IMPATTO CYBER

945 MLD $ di **danni** generati dal **cybercrime**

INVESTIMENTI CYBER SECURITY

145 MLD $[1] spesa globale in ICT Security

Impatti economici che vanno **ben oltre le perdite operative…**

- **69%** **Perdita di Business**
- **55%** **Danno Reputazionale**
- **48%** **Rimborso Reclami**
- **29%** **Costi Ripristino**
- **25%** **Sanzioni e Penali**

[1] di cui 1,5 miliardi in Italia

Fonte: The Cost of Cyber Crime, 9th Edition (Accenture & Ponemon, 2019); «A costant State of Flux" (Trend Micro Report 2020; Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Cyber Risk

Eventi 2021 (1/4)

CHI

Colonial Pipeline

QUANDO

7 maggio 2021

COME

Attacco ransomware

COSA

Blocco totale dei **sistemi**

Evento

L'attacco ransomware ha costretto la Colonial Pipeline a **sospendere** le operazioni di **distribuzione del carburante** sugli oltre 8 mila km della tratta dal golfo del Messico al New Jersey per evitare che l'attacco potesse avere effetti più gravi ed espandersi ulteriormente sulla rete informatica aziendale. Il caso si è "risolto" attraverso il pagamento di un riscatto di 75 bitcoin (corrispondenti a circa 4.5 milioni di dollari) al gruppo criminale DarkSide. L'FBI è riuscita a tracciare e bloccare gran parte dei bonifici.

Cyber Risk

Eventi 2021 (2/4)

CHI

Luxottica

QUANDO

20 Settembre 2021

COME

Attacco ransomware

COSA

2GB di dati sfiltrati

Evento

L'attacco ha causato il blocco totale delle attività produttive di Luxottica negli stabilimenti di Agordo e Sedico, entrambi nel bellunese, e anche di quelle in Cina. Gli investigatori hanno potuto verificare che gli hacker sono riusciti ad entrare in possesso e a copiare esclusivamente i **file** e **materiali interni**, e quindi **nessun dato personale rilevante**. Luxottica si è **rifiutata di pagare il riscatto** nonostante alcuni dati, in particolare quelli del mercato sudafricano, siano stati rubati e quindi persi.

Cyber Risk

Eventi 2021 (3/4)

CHI

SIAE

SIAE

QUANDO

20 Ottobre 2021

COME

Attacco ransomware

COSA

60 GB di dati sfiltrati

Evento

L'attacco ha comportato il furto di dati pari a circa **28 mila documenti** (60GB) con una richiesta di **ricatto** pari a 3 milioni di euro in bitcoin, che la SIAE non **ha pagato** nonostante la pubblicazione di alcuni sample nel darweb. Successivamente, gli hacker hanno ricattato alcuni artisti e/o effettuato tentativi di phishing.
L'azienda non appena riscontrato l'attacco ha avvisato il Garante della Privacy ed effettuato una dettagliata denuncia alla Polizia Postale, che sta attualmente effettuando delle indagini.

Cyber Risk

Eventi 2021 (4/4)

CHI

San Carlo Gruppo Alimentare

QUANDO

25 Ottobre 2021

COME

Attacco ransomware

COSA

Blocco parziale dei **sistemi**

Evento

L'attacco ha comportato il **blocco parziale** di alcuni sistemi informatici ma l'operatività del gruppo è stata comunque garantita (dalla produzione, alla distribuzione e alla vendita dei prodotti). Si è trattato di un attacco di tipo **ransomware** di tipo **cryptolocker**, con il blocco dei sistemi informatici dell'azienda, a cui ha fatto seguito una **richiesta di riscatto** in criptovalute.

Cyber Risk

La comunicazione di un Cyber attack

Hydro

L'Hydro è una delle più grandi aziende **integrate dell'alluminio**, la quarta al mondo, con impianti all'estero

Attacco tramite il cryptovirus LockerGoga, un software malevolo di tipo **ransomware** in cui gli hacker bloccano i **sistemi IT**

Comunicazione

Cyber Risk & ICT Third Party Risk

Alcune riflessioni sul legame tra questi due rischi

Fornire le '**chiavi** dei sistemi ICT' a fornitori esterni aumenta i rischi di cybercrime

I dispositivi dell'Internet of Things generalmente non possiedono di default le **misure** di **protezione** di **base**

Le terze parti possono essere utilizzate come una **backdoor** (entrata secondaria) per aggirare i presìdi di sicurezza informatica

Sta aumentando sempre più il ricorso a fornitori di servizi **cloud**, che rappresentano un **target appetibile** per gli hacker

ICT Third Party Risk

Principali caratteristiche

L'ICT Third Party Risk rappresenta l'**insieme dei rischi** a cui un'azienda è esposta in relazione ai **servizi ICT esternalizzati** o **forniti** da **terze parti**

Considerato il ricorso sempre più frequente a servizi in ambito ICT forniti da terze parti, si possono verificare le condizioni per problematiche in materia di **sicurezza delle informazioni**

Alcune considerazioni

Definizione di tecniche per **valutare** e **gestire** i **rischi** connessi all'utilizzo di servizi ICT in outsourcing o forniti da terze parti

Identificazione delle esigenze aziendali in materia di **sicurezza informatica**

Conformità alle **prescrizioni normative** e **regolamentari** e alle **best practice** di settore

Possibili conseguenze

ESEMPLIFICATIVO

ICT Third Party Risk

La gestione dei rischi

Profilo di rischio

Risk assessment
La metodologia definita è efficace?

Sistema controlli interni
È effettuata una review periodica?

Business internazionale
Possibili temi di compliance?

Rischi da mitigare

ESEMPLIFICATIVO

- **Security Risk**
  Sicurezza dei dati e dei sistemi

- **Reputational Risk**
  Attenzione ai danni d'immagine

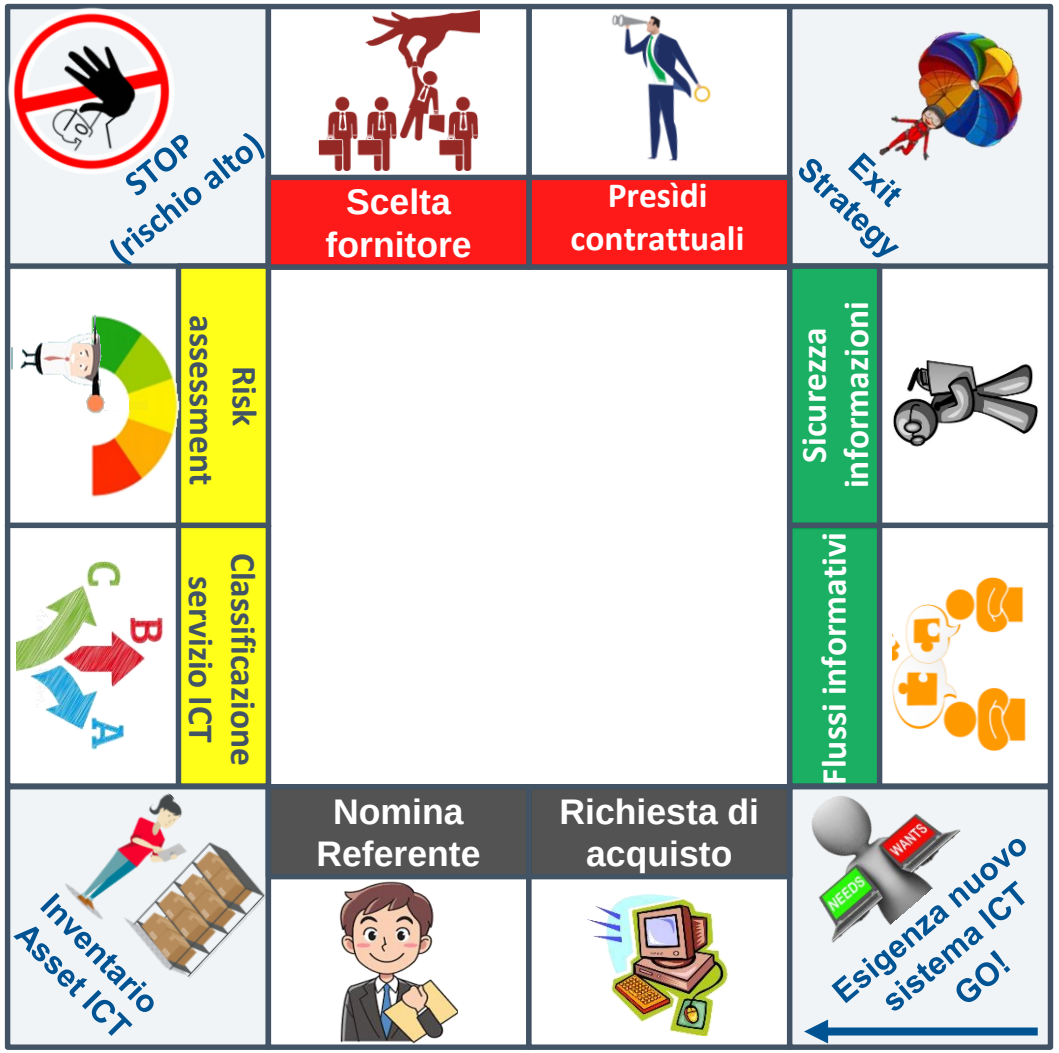
- **Sub-outsourcing risk**
  Monitorare la catena di fornitura

L'attività di due diligence è commisurata al rischio associato all'attività?

Il processo di risk management è integrato con quello di gestione degli acquisti?

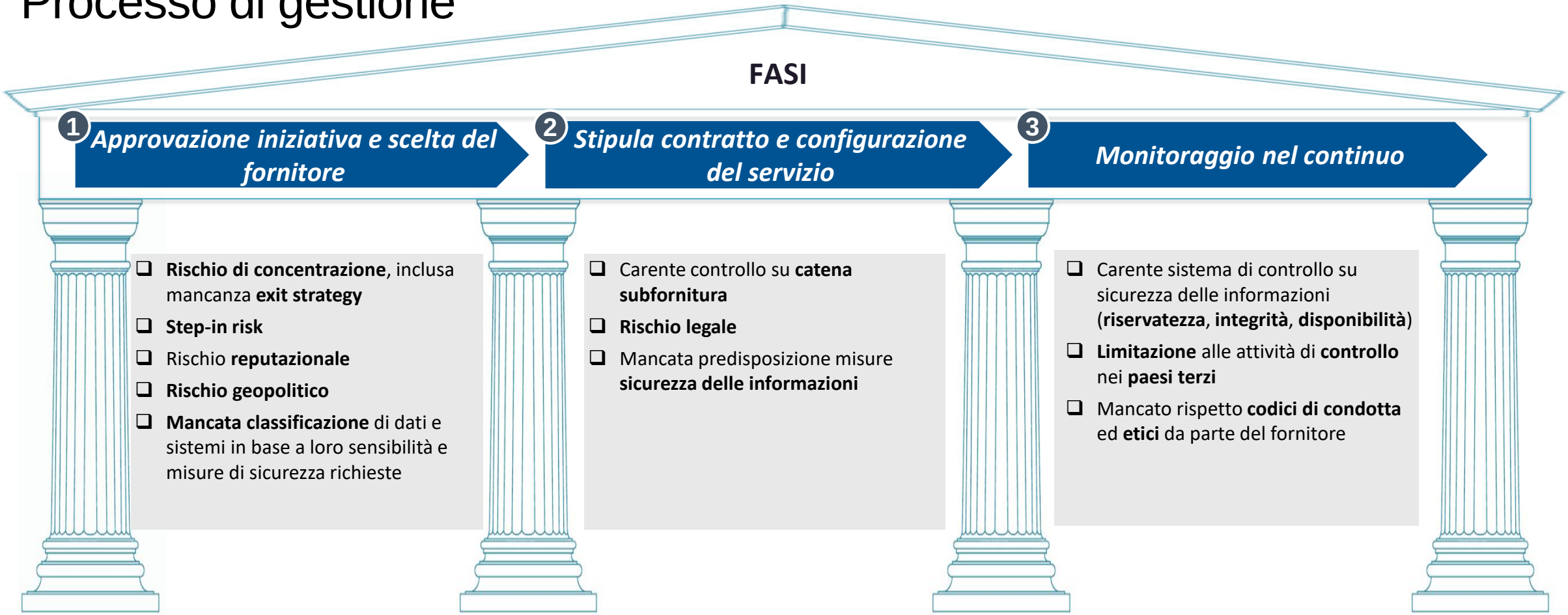
ICT Third Party Risk

Processo di fornitura di un servizio ICT



ICT Third Party Risk

Processo di gestione

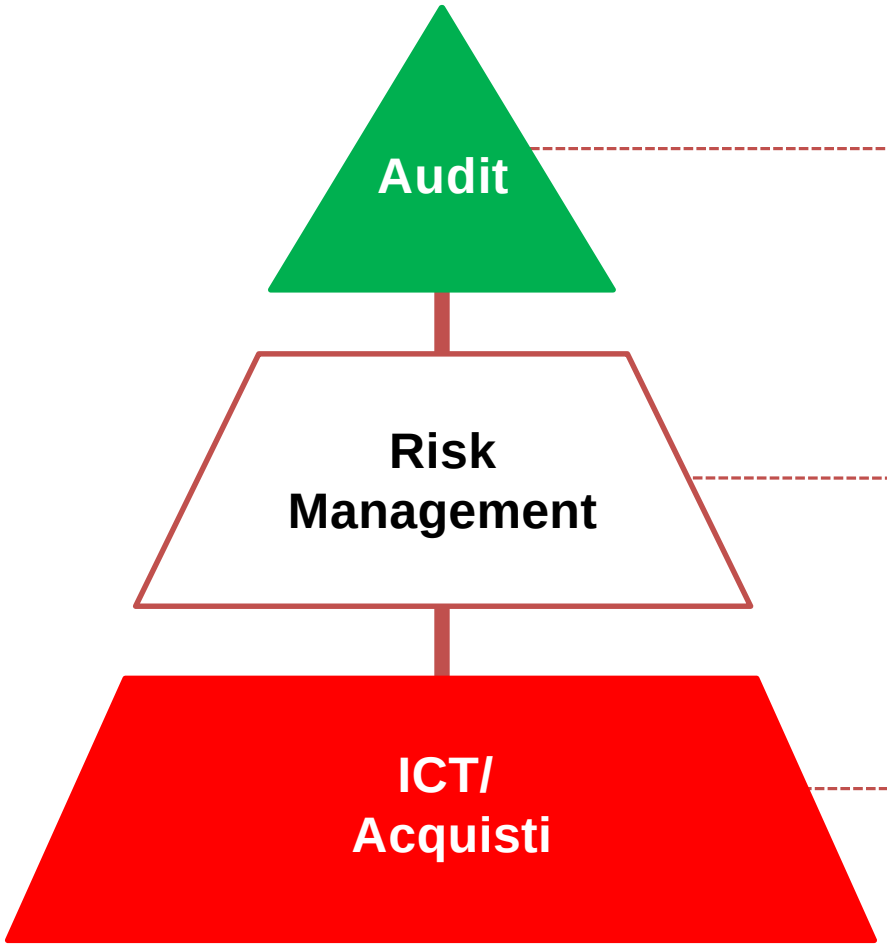


- Rischi di fuoriuscita di informazioni e di utilizzo non autorizzato di strumenti aziendali a seguito di attacco cyber
- Controlli anche in caso di ricorso a terze parti per servizi ICT che non assumono la qualifica di esternalizzazione

ICT Third Party Risk

Governance del modello di gestione del rischio

Governance | **Ruoli e responsabilità**



- Esecuzione di audit sul **processo di selezione** e **monitoraggio** del fornitore e sulla **metodologia di valutazione dei rischi**
- Facoltà di **ispezione presso il fornitore**

- **Definizione** della **metodologia** di Risk Assessessment preliminare
- **Analisi** dei **flussi informativi** sull'attività di monitoraggio nel continuo ricevuti da ICT

- **ICT**: (i) Individuazione del **Referente** per l'attività esternalizzata, (ii) **classificazione** del servizio ICT, (iii) esecuzione del **Risk Assessment preliminare** e (iv) **monitoraggio** nel continuo
- **Acquisti**: **contrattualizzazione** del servizio ICT

ICT Third Party Risk

Tematiche e contromisure

Perché è complesso? Possibili sfide

1. Rischio difficile da **misurare** e **quantificare**
2. Il **risk appetite non** è **semplice** da **definire**
3. È possibile un **risk appetite diverso da zero?**
4. La natura complessa del rischio richiede **misure forward looking**
5. Non sempre è diffusa la **consapevolezza** aziendale sui **rischi di sicurezza**

Cosa fare? Possibili contromisure

Due diligence sui fornitori

Policy e procedure formalizzate

Schemi contrattuali standard

Risk assessment ex-ante

Monitoraggio nel continuo

ICT Third Party Risk

Una lista (non esaustiva) di mitigant

Requisiti di conformità (*e.g.* data protection)

Polizze assicurative

Attività di Vetting

Piani di risposta

Revisione dei forma contrattuali

Risk assessment

Le aziende devono rafforzare i propri presìdi di controllo per monitorare le terze parti

Un approccio olistico

Interrelazioni tra le funzioni aziendali

Obiettivo

Attuare le misure di sicurezza sulle informazioni in tutte le componenti organizzative dell'azienda

Approccio

Prevedere un **approccio multidisciplinare**, **integrato** e **cooperativo** tra le diverse funzioni aziendali

People risk

Oltre l'80% dei problemi di sicurezza proviene dall'interno delle organizzazioni

Alcune considerazioni

Rischi operativi

- **Rafforzare** la gestione dei rischi operativi
- Valutare **nuovi scenari di rischio**

Zero - Day attack

- Silent cyber
- Vulnerabilità non ancora note/risolte

Zero Trust

- Ambiente ostile, non si distingue tra utenti interni ed esterni
- Non fidarsi mai e verificare sempre

L'utilizzo sempre più invasivo di tecnologia nei processi produttivi richiede una maggiore attenzione da parte del Management al rischio di frodi e attacchi informatici, per i relativi danni e costi di ripristino

Un approccio olistico

Il Cyber Risk in un mondo sempre più regolamentato

Rischio	Punti di attenzione
A **Cyber Risk** *(Asset IT: dati e sistemi)*	– Integrità – Riservatezza – Disponibilità
B **Rischio privacy (Dati personali)**	– Accesso – Falsificazione – Alterazione – Divulgazione – Perdita – Distruzione

- Adozione di **metodi e strumenti** di rilevazione e valutazione dei rischi **coerenti tra loro**

- **Condivisione** delle situazioni di rischio e delle azioni di rimedio
- **Scale di valutazione** comuni o raccordabili

I principali rischi che gravano sui dati, direttamente o indirettamente, sono danneggiamento o indisponibilità dei sistemi hardware e software, intercettazione di messaggi, intrusioni mirate e attacchi vandalici

Cyber Risk

Un possibile framework

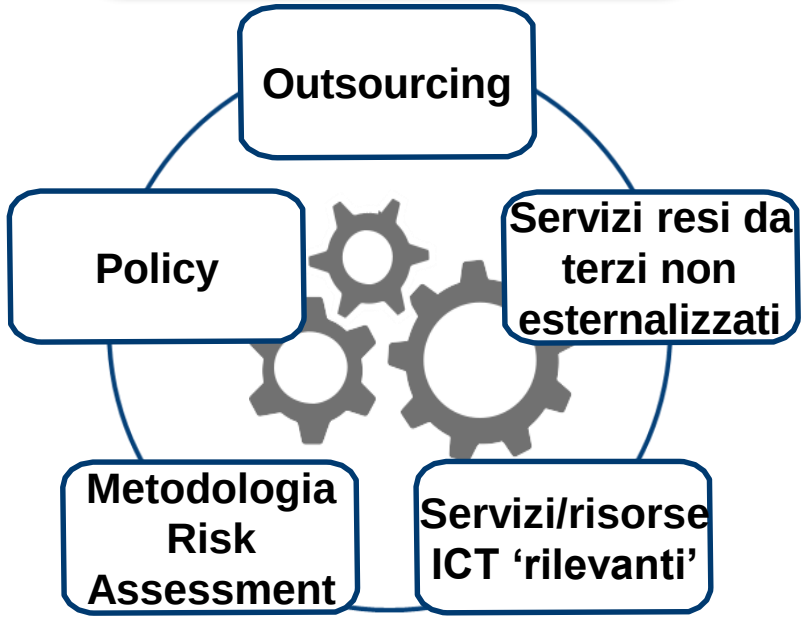
Prospettive

A. Awareness

- A parità di sistemi, la vulnerabilità al Cyber Risk dipende dalla **consapevolezza** degli utenti
  - Programma di '**Security Awareness**'
  - Training mirato (**e-learning**, **formazione in aula)**

Rischio correlato

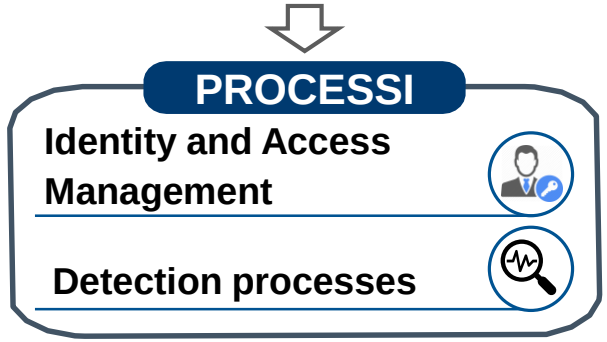
B. ICT Third Party Risk



'AS IS' *vs* 'TO BE'

C. Resilienza strutturale

- **Capacità intrinseca dell'architettura ICT** di far fronte a situazioni sfavorevoli, rendendo difficili gli attacchi cyber e resistendo ad essi



'Cyber - resilience: Range of practices' (Basilea, Dicembre 2018)

Cyber Risk

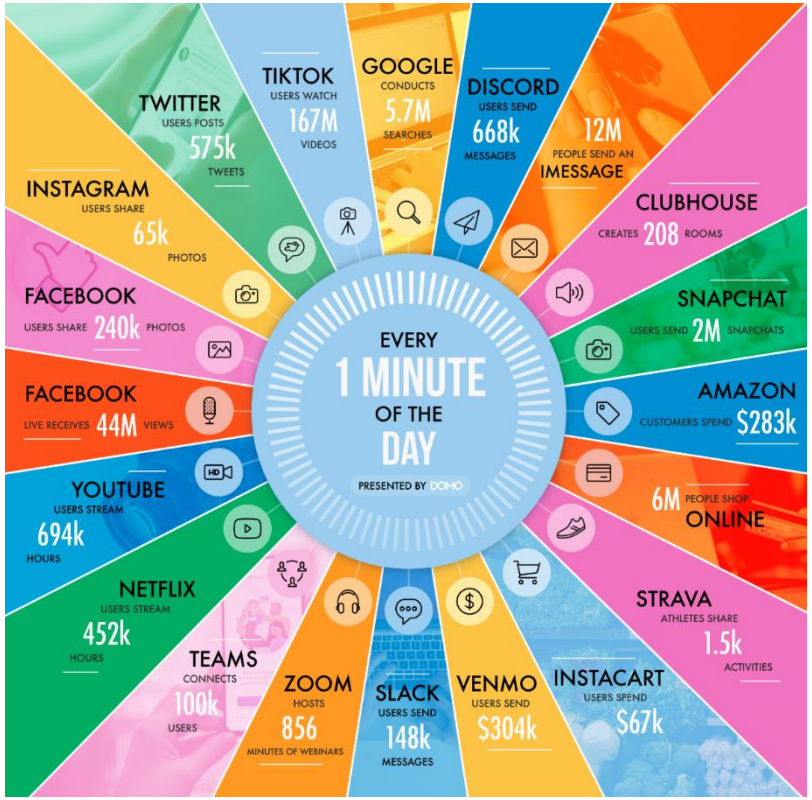
A. Awareness

60 Secondi

5.2 MLD persone

Le azioni del singolo utente potrebbero avere un forte impatto sull'azienda, con ripercussioni anche sulla capacità di generare reddito

2021: what happens in an internet minute..



Fonte: www.visualcapitalist.com

La consapevolezza è sempre la miglior difesa

Firewall 'umano'

Cyber Risk

B. ICT Third Party Risk

Contesto

ICT Third party risk

Un attacco cyber ad un fornitore potrebbe comportare il rischio di

- **fuoriuscita di informazioni**
- **utilizzo non autorizzato di strumenti aziendali**

BANCA D'ITALIA

Invito di Banca d'Italia (2018) a tutti gli intermediari finanziari a **rafforzare i controlli** sui servizi ICT esternalizzati o forniti da terze parti

Piano d'azione

Misure di sicurezza e **presìdi di controllo** nelle fasi del processo di outsourcing/ fornitura da terze parti:

approvazione dell'iniziativa e scelta del fornitore

stipula del contratto e configurazione del servizio

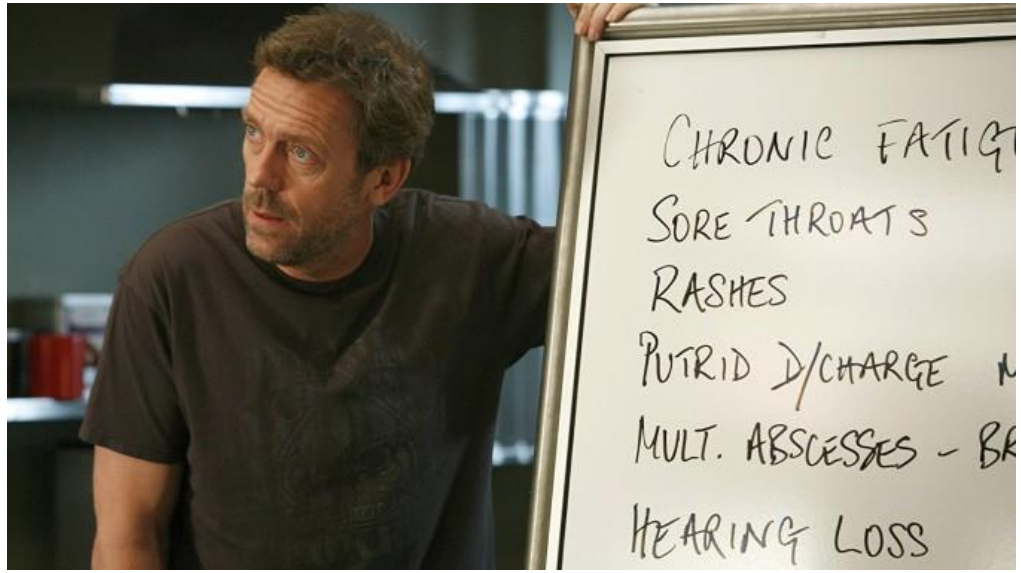
processo di monitoraggio nel continuo

Cyber Risk

C. Resilienza strutturale (1/4)

Un'azienda che subisce un evento di Cyber Risk è come un paziente che non conosce ancora la sua diagnosi…

…inoltre, anche l'evento apparentemente più banale potrebbe comportare gravi conseguenze (anche a distanza di anni)



Operational risk managers are paid to be paranoid
(S. Scandizzo)

Cyber Risk

C. Resilienza strutturale (2/4)

Non esiste un modo per rendere totalmente immune un'azienda dagli attacchi cyber
Essere resilienti consente di prevenire e/o di limitare i danni del Cyber Risk

Definizione di resilienza

<<The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents>>

Presidential Policy Directive - Critical Infrastructure Security and Resilience (12 febbraio 2013)

Cosa vuol dire essere cyber-resilient?

R.it *14 gennaio 2017*

Hacker russi, blitz contro l'Aeronautica a caccia dei segreti dell'F-35

HUFFPOST *28 maggio 2013*

F-35: hacker cinesi rubano i progetti di aerei militari e altre armi Usa

The Telegraph *5 agosto 2018*

Honeytrap hacker attempted to steal RAF fighter jet secrets using Tinder

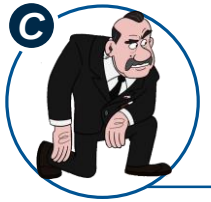
Cyber Risk

C. Resilienza strutturale (3/4)

Risk Assessment

Talent gap
Come sta andando il recruiting?

Zero Trust
Abbiamo blindato gli accessi logici?



Servizi di intelligence
Collaboriamo con agenzie esterne?

Rappresentazione

- **Modello as is**
  Dove siamo: qual è l'esposizione

- **Modello to be**
  Cosa stiamo facendo

- **Gap analysis**
  Confronto as vs to be e mitigant

Processo di apprendimento continuo (c.d. life-long learning)