

Top Business Risks in 2023

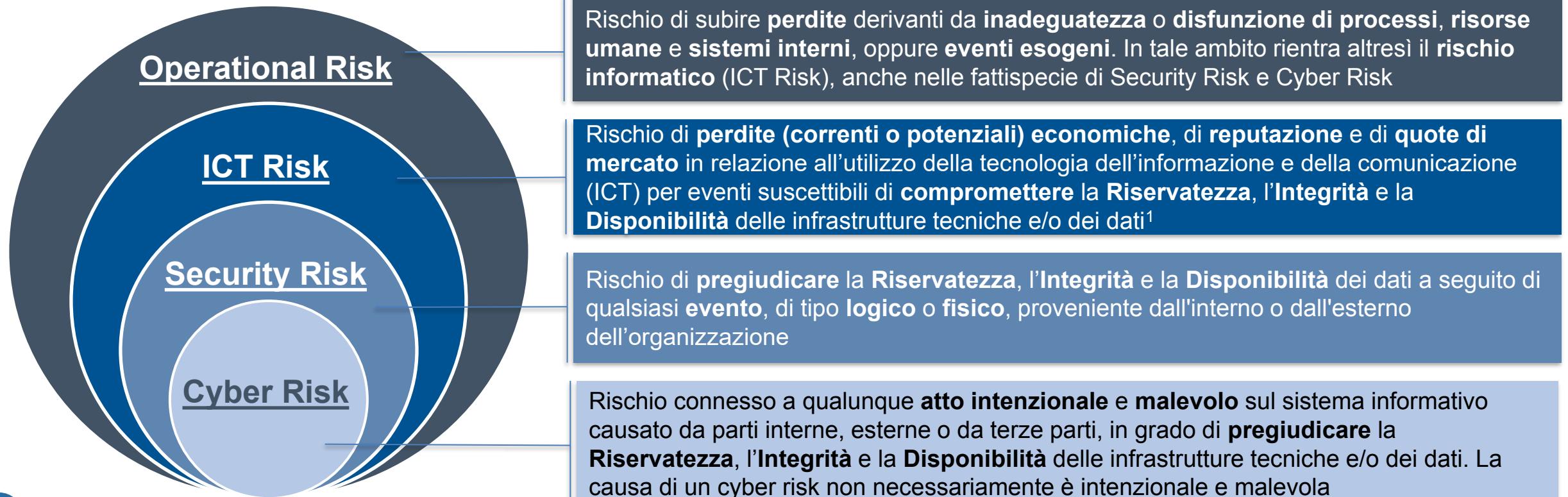
Allianz Risk Barometer 2023

Rank 2023	Risk	Rank 2022	Trend
1	Rischi informatici (e.g. cyber crime, guasti ICT, data breach, multe e sanzioni)	1	
2	Interruzione di attività (anche della catena di fornitura)	2	
3	Condizioni macroeconomiche (e.g. inflazione, deflazione, politiche monetarie, programmi di austerità)	10	
4	Crisi energetica(e.g. fornitura carenza/interruzione, fluttuazioni dei prezzi)		
5	Cambiamenti nella regolamentazione e nella legislazione (e.g. embarghi, Brexit, protezionismo, dazi)	5	
6	Catastrofi naturali (e.g. inondazioni, tempeste, terremoti)	3	
9	Incendi, esplosioni	7	

Fonte: Allianz Risk Barometer 2023

Aspetti definitori

RELAZIONE TRA OPERATIONAL, ICT, SECURITY E CYBER RISK

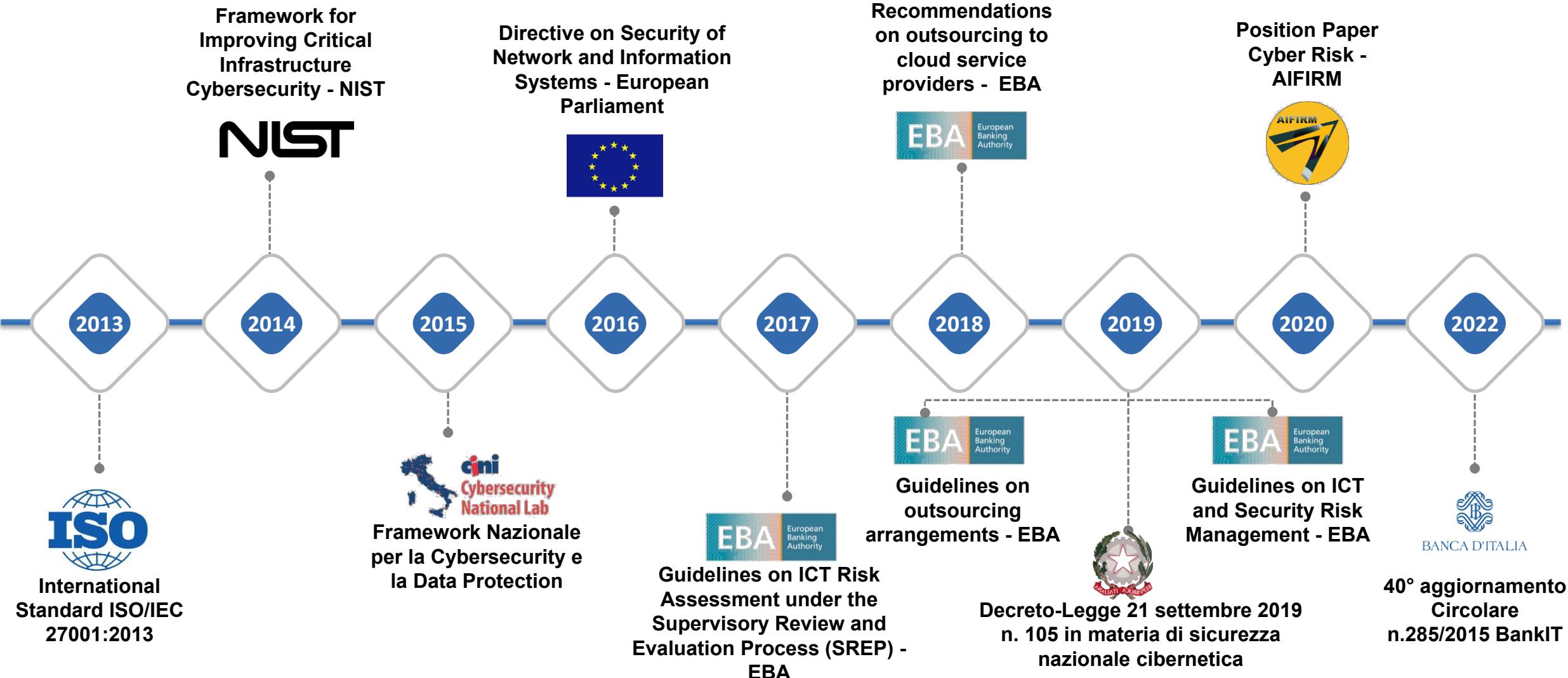


Nell'ICT Risk sono ricompresi eventi non inclusi nel Security e nel Cyber Risk (e.g. guasto/indisponibilità di un applicativo con conseguente ritardata esecuzione di attività). A sua volta, nel Security Risk sono ricompresi eventi di tipo logico (e.g. errata configurazione software con conseguente diffusione 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)**

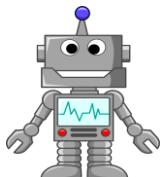
Alcune considerazioni



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

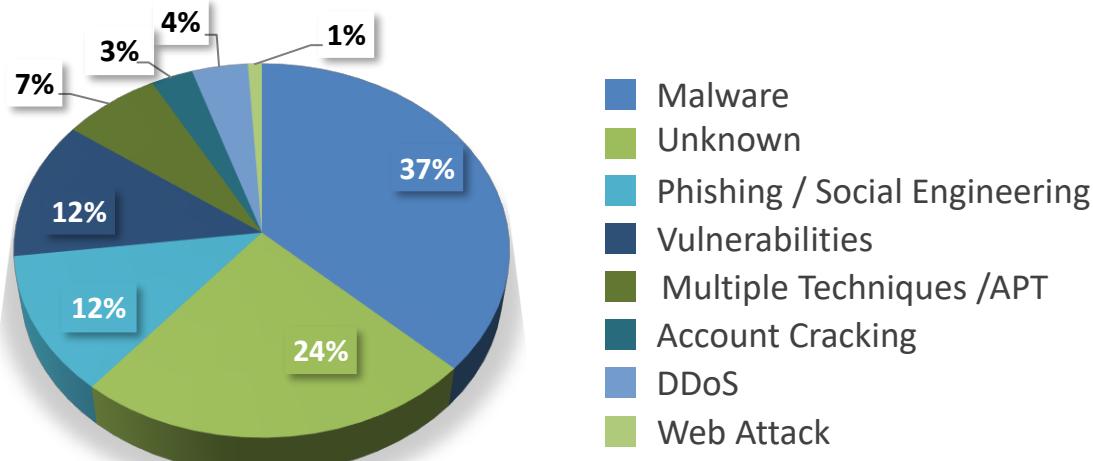


Cyber Risk

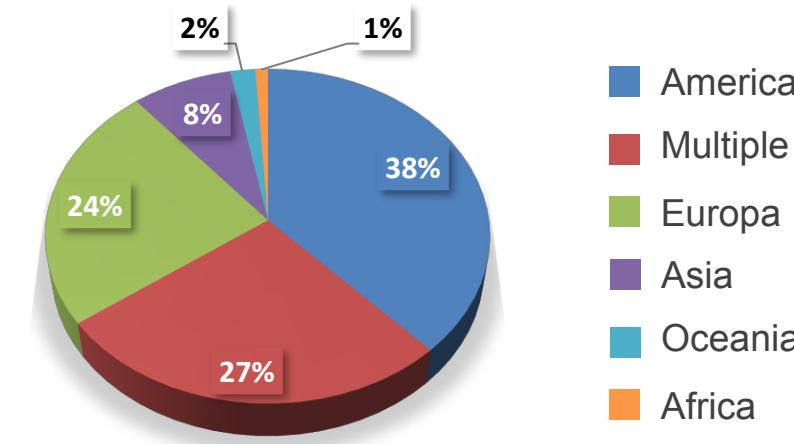
Il Cyber Risk e la sua rilevanza

(1/2)

Distribuzione delle tecniche di attacco per tipologia



Distribuzione delle vittime per area geografica



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**



TEMPO MEDIO DATA BREACH

257 giorni
(191 gg per
identificazione e 66
gg per contenimento)



PERDITA MEDIA MEGA BREACHES

332 MLN \$
(tra i 50 e i 60 mln
di record impattati)



PERDITA MEDIA DATA BREACH (MONDO)

4.45 MLN \$



PERDITA MEDIA DATA BREACH (ITALIA)

145 MLD \$¹ spesa
globale in ICT
Security

Alcuni numeri chiave...

33%

**N° data breach
identificati da team
interni di sicurezza**

51%

**Aziende che stanno
aumentando
investimenti in
cybersecurity**

82%

**Breach che
riguardano dati in
cloud**

16%

**Attacchi in cui il
phishing è il vettore
iniziale**

¹ di cui 1,5 miliardi in Italia

Cyber Risk

Eventi 2023

(1/4)

CHI



Azienda
ospedaliera
universitaria
integrata Verona

QUANDO



24 ottobre
2023

COME



Distributed
Denial of
service

COSA



Interruzione
del sistema
informatico

Evento

Il 24 ottobre 2023 alcuni hacker, ancora non identificati hanno avviato un attacco nei confronti dell'azienda ospedaliera integrata Verona, bloccandone tutto il sistema informatico. L'attacco ha causato il blocco del Centro unico prenotazioni, delle casse automatiche, degli sportelli per pagamenti, del sistema di ritiro dei referti, del sito web dell'azienda, delle reti telefoniche ed internet dell'azienda



Cyber Risk

Eventi 2023

(2/4)

CHI



Poliambulatorio
ViLAB

QUANDO



22 ottobre
2023

COME



Defacement

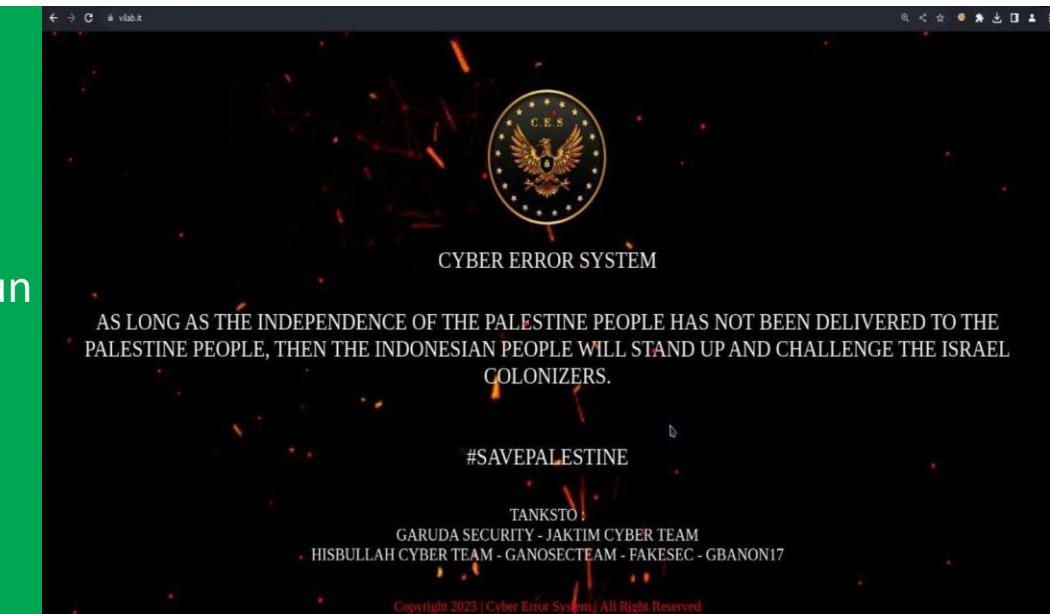
COSA



Modifica sito
web

Evento

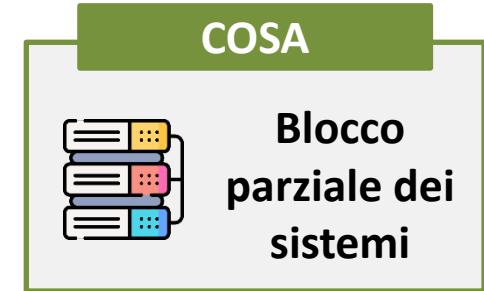
Il 22 ottobre 2023 hacktivisti cibernetici del gruppo CYBER ERROR SYSTEM, pro Palestina, hanno colpito il poliambulatorio ViLab con un attacco di defacement che ha alterato la pagina web aziendale con messaggi politici



Cyber Risk

Eventi 2023

(3/4)



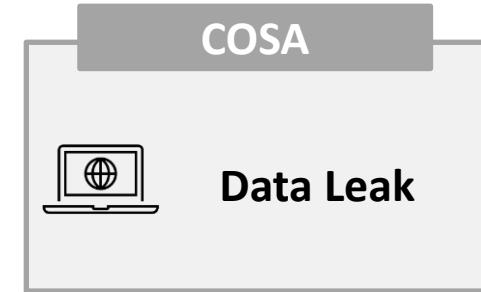
L'attacco ha riguardato i siti web di Roma Capitale gestiti da Zetema Progetto Cultura che li ha resi completamente inaccessibili. Si è trattato di un attacco di tipo ransomware che ha cifrato le infrastrutture IT dell'azienda, rendendo di fatto inutilizzabili i sistemi che ospitavano le infrastrutture del Comune di Roma. Dalle notizie che circolano in rete, sembrerebbe che gli hacker criminali abbiano richiesto un riscatto per fornire la chiave di decifratura che permetta di ripristinare il danno creato. La richiesta ammonta a ben 1.000.000 di euro da versare dall'azienda in Bitcoin sui wallet dei criminali informatici.



Cyber Risk

Eventi 2023

(4/4)



La banda criminale di Medusa ransomware, nella giornata di ferragosto, rivendica un attacco ransomware alle infrastrutture della Postel SpA sul suo Data Leak Site (DLS). Nel post pubblicato viene riportato un countdown ad 8 giorni, 14 ore e 13 minuti e 48 secondi, data di quando la cybergang inizierà a pubblicare i dati sul suo sito underground qualora il riscatto non sia stato pagato dall'azienda. All'interno del post viene pubblicato che il costo del riscatto è fissato a 500.000 dollari. Oltre ai dati esfiltrati, anche il sito di Postel è stato messo offline dagli attaccanti.

MEDUSA BLOG

0 8 1 4 1 2 1 7

Postel SpA

Postel SpA offers computer software for sale. The Company provides software products and management services including document management, direct marketing, and e-procurement software and related services. Postel operates throughout Italy, the company's head office is located at 5 Via Ricerca Scientifica, Padova, Veneto, 35127, Italy

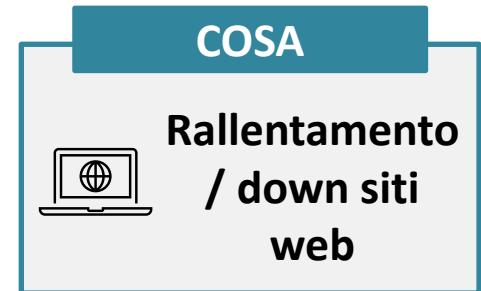
Add time 1 day Delete All Data Download data now!

10000\$ 500000\$ 500000\$

Cyber Risk

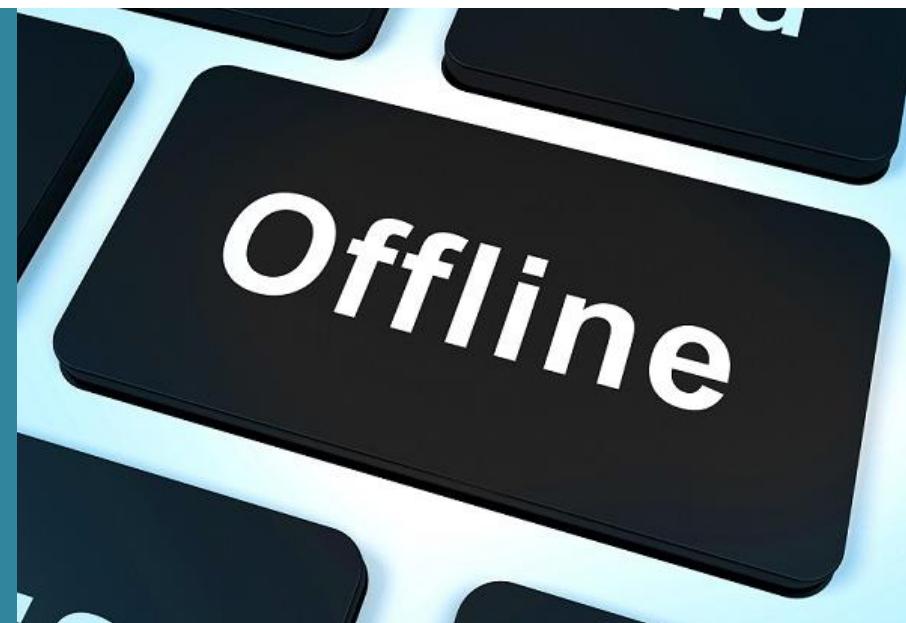
Eventi 2022

(1/4)



Evento

Il 20 maggio 2022 hacker russi del Gruppo Legion hanno avviato un attacco nei confronti di alcuni siti web istituzionali - tra cui quelli di Ministero degli Esteri, Consiglio Superiore della Magistratura, Senato, Ministero della Difesa, alcuni dei principali aeroporti - hanno subito grandi rallentamenti e/o indisponibilità con conseguenti disservizi. Il timore degli esperti di cybersecurity è che si tratti solo di accenni e che potrebbero verificarsi attacchi ben più gravi nei prossimi giorni.



Cyber Risk

Eventi 2022

(2/4)

CHI	Polizia di Stato

QUANDO	17 Maggio 2022

COME	Phishing

COSA	Rischio furto dati personali

Invio massivo di migliaia di mail di phshing da parte del collettivo russo Killnet da indirizzi mail fake apparentemente istituzionali (ad esempio ‘scuolasuperiorepolizia.ufficiostudi@poliziadistato.it’). Si ipotizzano due tipologie di impatti, vale a dire possibili furti di dati personali e blocco dei sistemi degli utenti nel caso in cui gli allegati contenessero ransomware.

La Polizia di Stato, peraltro, aveva subito pochi giorni prima un attacco Distributed Denial of Service dal medesimo collettivo russo con conseguente indisponibilità - durata qualche ora - del sito istituzionale www.poliziadistato.it

Evento



Cyber Risk

Eventi 2022

(3/4)



Evento

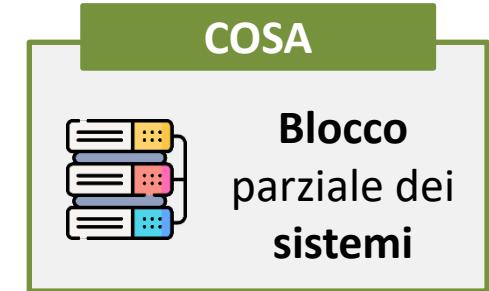
Un attacco informatico (si ipotizza un ransomware) ha messo fuori gioco i sistemi informatici degli ospedali Sacco, Fatebene, Buzzi e Macedonio Melloni di Milano nella giornata di domenica primo maggio e il sito internet istituzionale dell'Azienda Socio Sanitaria Territoriale. Il personale medico, vista l'indisponibilità delle cartelle cliniche digitali, ha dovuto ricorrere a carta e penna per varie attività (registrazione di pazienti, cure e medicinali somministrati)



Cyber Risk

Eventi 2022

(4/4)



Evento

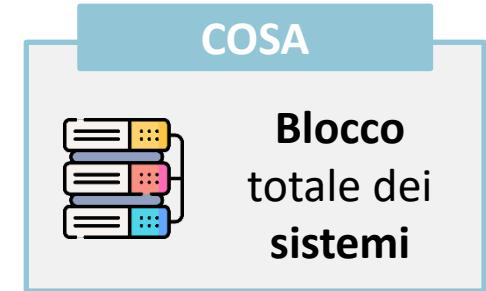
HIVE ransomware è un attacco di tipo cryptolocker che ha l'obiettivo di cifrare i sistemi informatici, effettuare un leak dei dati e chiedere un riscatto, in criptovalute, per il recupero delle chiavi di cifratura. L'attacco ha comportato il **blocco dei sistemi di biglietteria del gruppo ed un parziale blocco dell'operatività aziendale**.



Cyber Risk

Eventi 2021

(1/4)



Evento

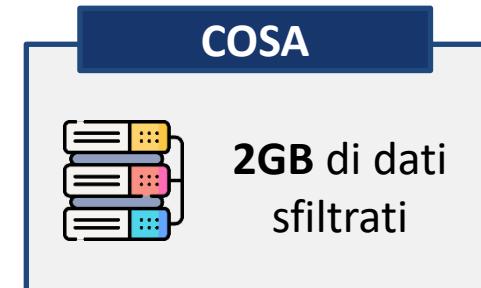
L'attacco ransomware ha costretto la Colonial Pipeline a **sospendere** le operazioni di **distribuzione del carburante** sugli oltre 8 mila km della tratta dal golfo del Messico al New Jersey per evitare che l'attacco potesse avere effetti più gravi ed espandersi ulteriormente sulla rete informatica 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)



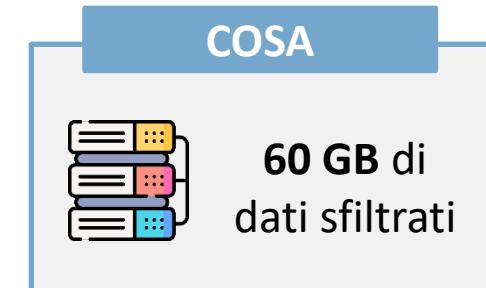
L'attacco ha causato il blocco totale delle attività produttive di Luxottica negli stabilimenti di Agordo e Sedico, entrambi nel bellunese, e anche di quelle in Cina. Gli investigatori hanno potuto verificare che gli hacker sono riusciti ad entrare in possesso e a copiare esclusivamente i **file e materiali 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)



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.

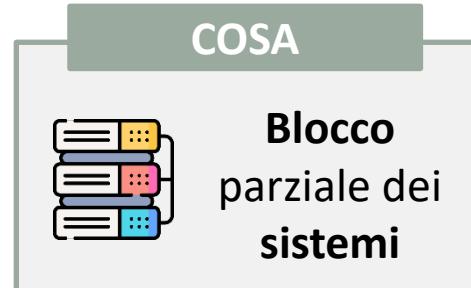
L'azienda non appena riscontrato l'attacco ha avvisato il Garante della Privacy ed effettuato una dettagliata denuncia alla Polizia Postale, che sta attualmente effettuando delle indagini.



Cyber Risk

Eventi 2021

(4/4)



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

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 presidi 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

Furto di dati



Contenziosi

Errori operativi



Frodi



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

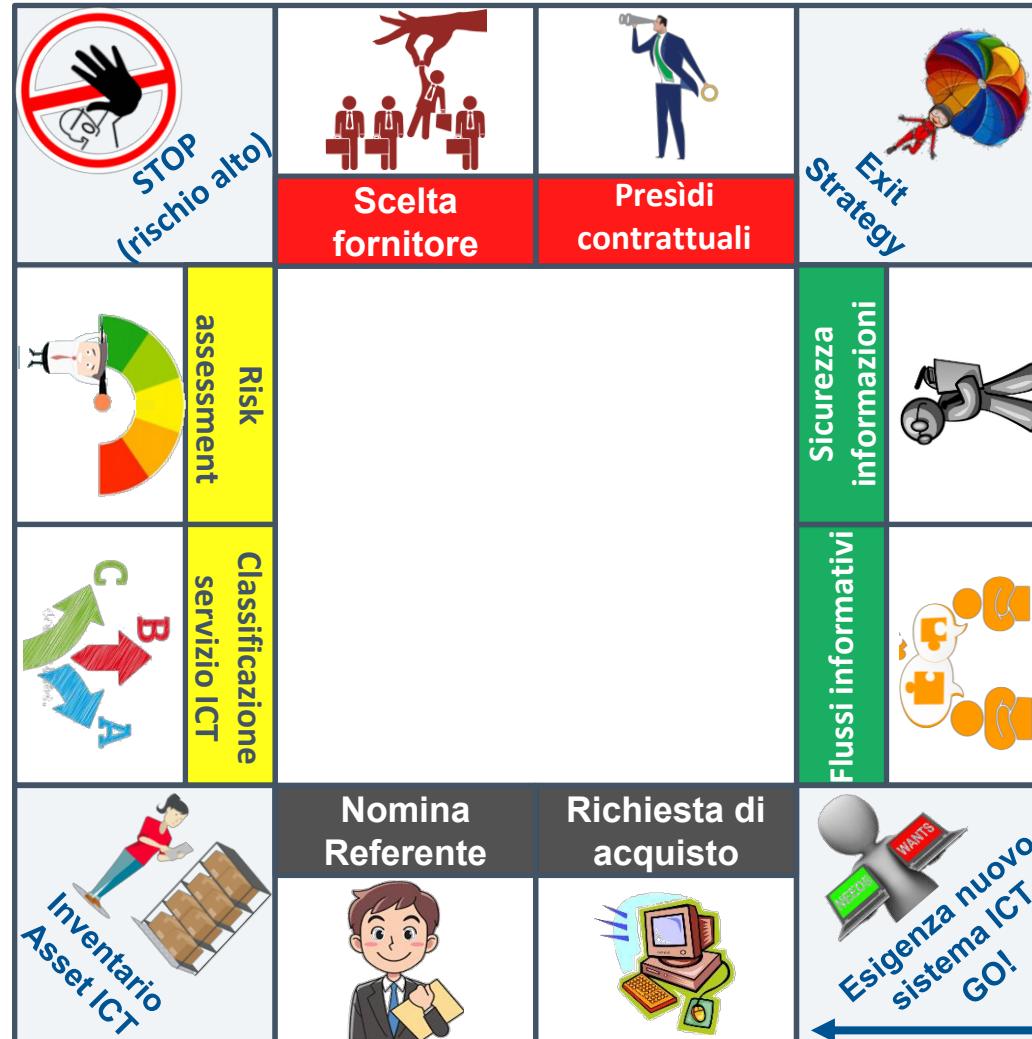


L'attività di due diligence è commisurata al rischio associato all'attività?

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

ICT Third Party Risk

Processo di fornitura di un servizio ICT



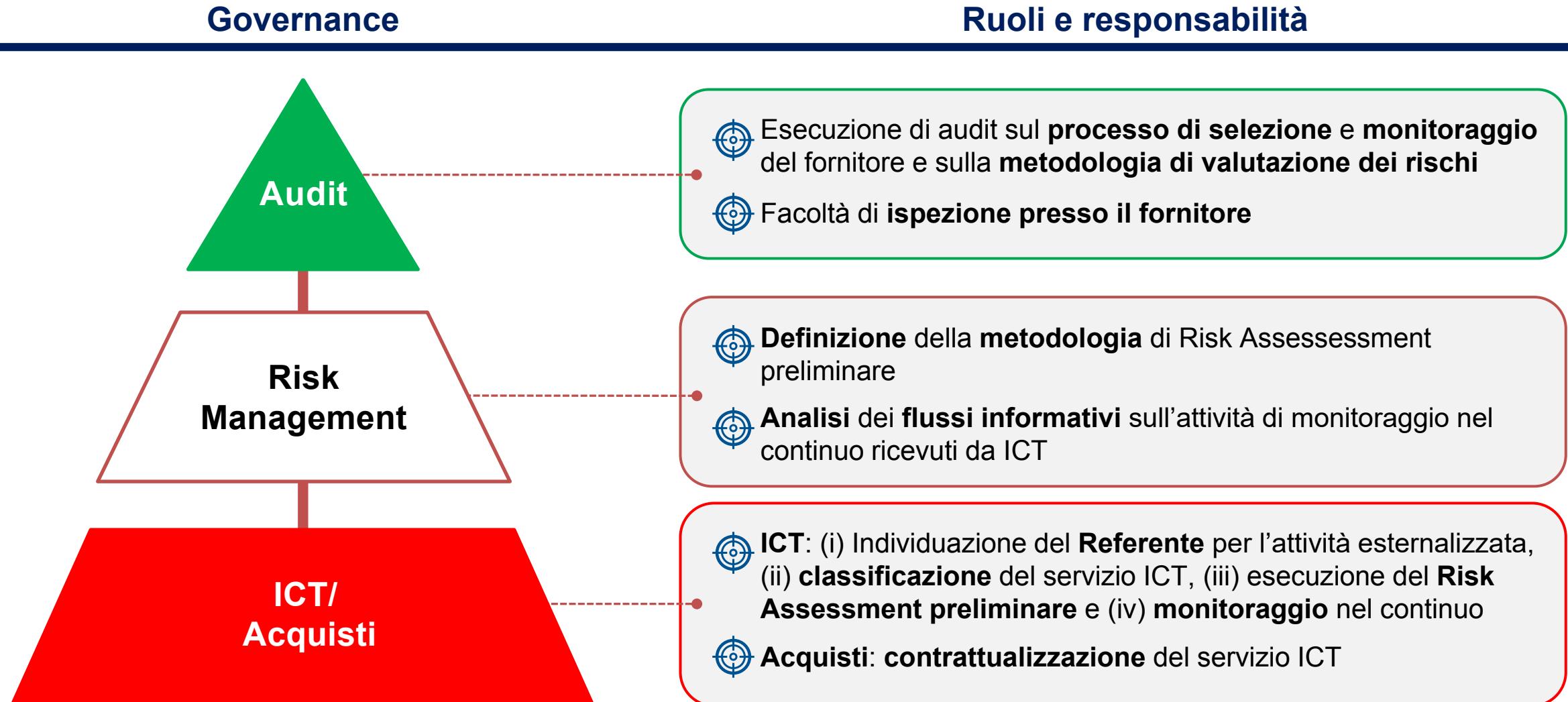
ICT Third Party Risk

Processo di gestione



ICT Third Party Risk

Governance del modello di gestione del rischio



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)



Attività di Vetting



**Revisione dei forma
contrattuali**



Polizze assicurative



Piani di risposta



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

Rischi operativi

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

Zero - Day attack

- Silent cyber
- Vulnerabilità non ancora note/risolte

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

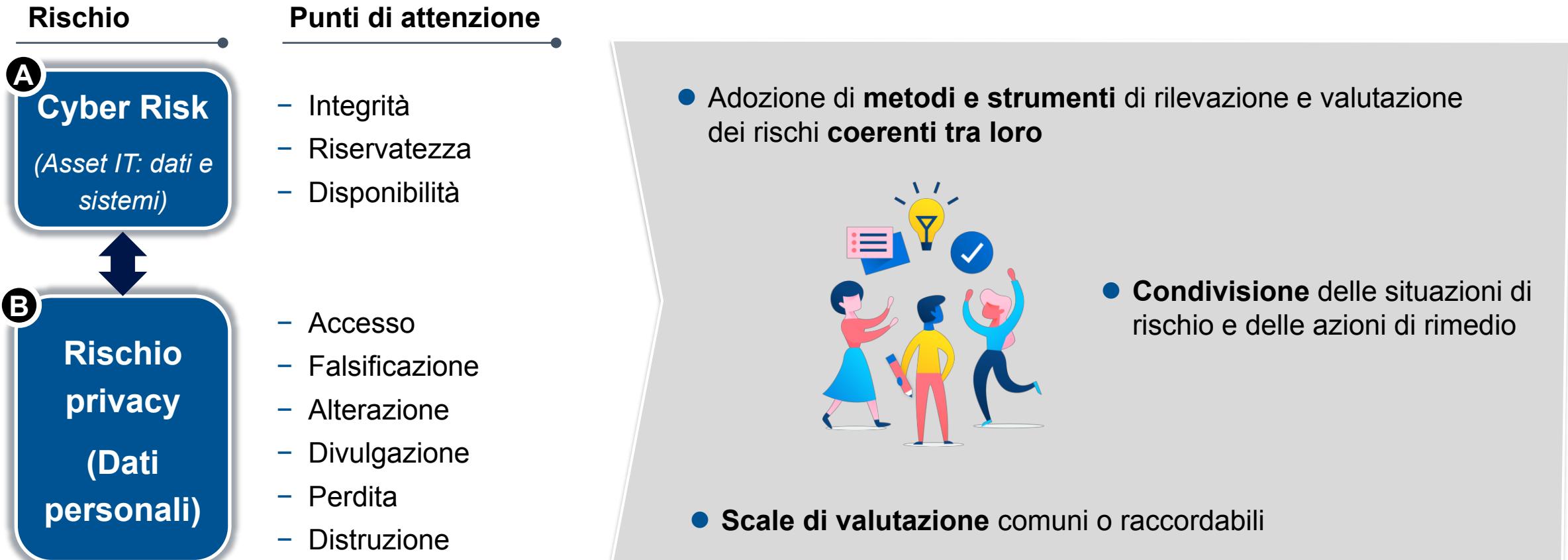
Alcune considerazioni



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



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



PROCESSI

Identity and Access Management



Detection processes

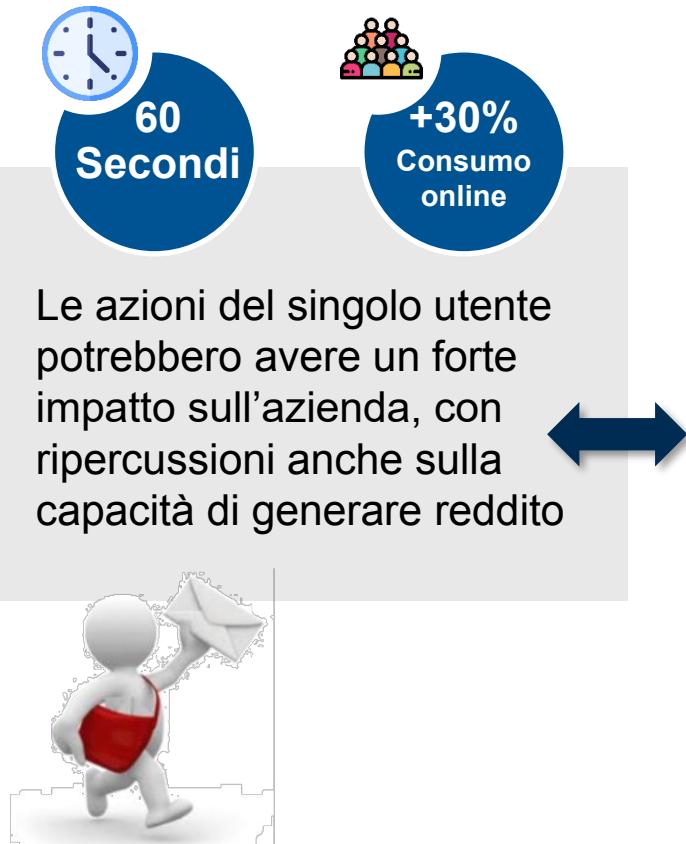


'Cyber - resilience: Range of practices' (Basilea, Dicembre 2018)

Cyber Risk

A. Awareness

2022: what happens in an internet minute..



La consapevolezza è sempre la miglior difesa



Firewall
'umano'

Fonte: <https://ediscoverytoday.com/2023/04/20/2023-internet-minute-infographic-by-ediscovery-today-and-ltmg-ediscovery-trends/>

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 presidi 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

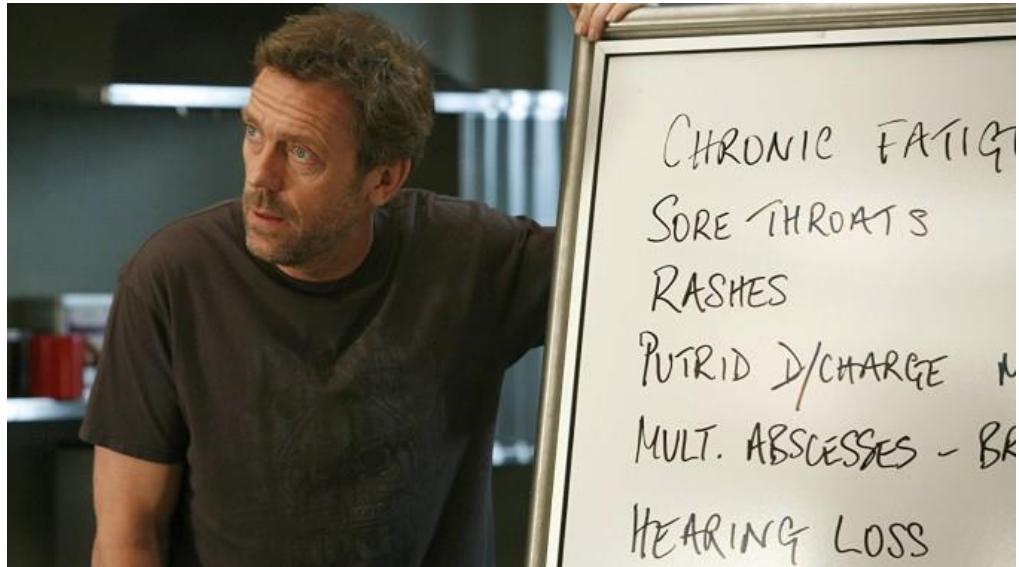
Cyber Risk

C. Resilienza strutturale

(1/3)

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

(2/3)

**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

(3/3)

Risk Assessment



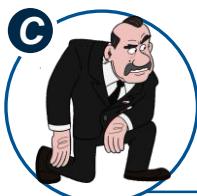
Talent gap

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)