IT Risk, Cybersecurity e nuove frontiere del Risk Management

MAURO SENATI

Chief Risk Officer UBI Banca - Gruppo Intesasanpaolo

Milano, 18 Dicembre 2020

AIFIRM – Associazione Italiana Financial Industry Risk Managers

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Il contesto

- Il ruolo sempre più determinante dei sistemi di Information and Communication Technology (ICT) nel raggiungimento degli obiettivi strategici di lungo periodo e l'ingresso nel settore di nuovi player (es. Fintech) hanno attivato una forte **evoluzione tecnologica del sistema finanziario** (crescente digitalizzazione dell'offerta commerciale, automazione dei processi operativi mediante l'introduzione della robotica e/o intelligenza artificiale)

- Tale evoluzione ha portato con sé anche un **incremento degli incidenti informatici e degli attacchi Cyber**, che continuano ad evolversi verso forme sempre più invasive

- Di fronte all'accresciuta consapevolezza di tali forme di rischio, le Istituzioni Finanziarie ed i Regulators si stanno ponendo obiettivi ambiziosi e sfidanti nel **far evolvere i propri framework di analisi e la relativa regolamentazione di riferimento** (es. PSD2, GDPR, Consultative Document del Comitato di Basilea "Principles for Operational Resilience" e "Revisions to the principles for the sound management of operational risk")

- Il contesto emergenziale determinato dalla **pandemia Covid-19** ha esacerbato ulteriormente tale necessità facendo emergere **limiti nei piani di continuità operativa** (processi/risorse incluse nel piano, durata dell'operatività in condizione di emergenza), creando nuove opportunità di social engineering e/o sfruttando più efficacemente le vulnerabilità associate all'attivazione del lavoro a distanza

Agenda

- ✓ **Di cosa stiamo parlando?**
- ✓ Analisi del contesto operativo
- ✓ Ultimi interventi del Regolatore

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Il Cyber Risk in normativa …

Nonostante la normativa vigente non preveda ancora una definizione univoca del concetto di "Cyber Risk", molti operatori si stanno interrogando sulla necessità/opportunità di considerare tale fattispecie di rischio come una componente a sé stante rispetto al Rischio Informatico

Disposizioni di vigilanza per le Banche (circ 285)	**Rischio Informatico (IT):** il rischio di perdite corrente o potenziale, dovuto all'inadeguatezza o al guasto di hardware e software di infrastrutture tecniche suscettibile di compromettere la disponibilità, l'integrità, l'accessibilità e la sicurezza di tali infrastrutture e dei dati
EBA Guidelines on ICT & Security Risk Management	**ICT & Security Risk**: il rischio di perdita dovuto alla violazione della riservatezza, alle carenze nell'integrità dei sistemi e dei dati, all'inadeguatezza o all'indisponibilità dei sistemi e dei dati o all'incapacità di sostituire la tecnologia informatica entro ragionevoli limiti di tempo e costi nel caso di modifica dei requisiti del contesto esterno o dell'attività. Questo comprende i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, compresi gli attacchi informatici o una sicurezza fisica inadeguata
Principles for Operational Resilience (Comitato Basilea)	**Cyber Risk[1]:** la combinazione della probabilità che si verifichino Cyber Incident e il loro impatto **Cyber Incident:** un evento cyber che: • mette a rischio la sicurezza informatica di un sistema informativo o delle informazioni che il sistema elabora, memorizza o trasmette • viola le politiche e le procedure di sicurezza o le politiche di utilizzo accettabile, indipendentemente dal fatto che derivi da attività dannose o meno
Guidelines on ICT Risk Assessment under SREP (ECB)	Il documento distingue le seguenti componenti: • **ICT Availability & Continuity Risk:** il rischio che le prestazioni e la disponibilità dei sistemi e dei dati ICT siano influenzati negativamente, incluso il rischio di incapacità di ripristinare tempestivamente i servizi dell'ente a causa di un guasto delle componenti ICT hardware o software; debolezze nella gestione dei sistemi ICT … • **ICT Security Risk:** il rischio di accesso non autorizzato ai sistemi e ai dati dei sistemi ICT dell'ente, dall'interno o dall'esterno (ad esempio nel caso di attacchi informatici) • **ICT Change Risk:** il rischio derivante dall'incapacità dell'ente di gestire i cambiamenti dei sistemi ICT in modo tempestivo e controllato, in particolare per quanto concerne programmi di modifica complessi e di grandi dimensioni • **ICT Data Integrity Risk:** il rischio che i dati archiviati ed elaborati dai sistemi ICT siano incompleti, inesatti o incoerenti nei vari sistemi, in seguito, ad esempio, a controlli ICT carenti o assenti durante le varie fasi del ciclo di vita dei dati ICT, tali da compromettere la capacità di un ente di fornire servizi e di produrre le informazioni finanziarie e relative alla gestione del rischio in modo corretto e tempestivo • **ICT Outsourcing Risk:** il rischio che il ricorso a una terza parte o a un'altra entità del gruppo (esternalizzazione intra-gruppo), per la fornitura di sistemi ICT o servizi connessi incida negativamente sulle prestazioni e sulla gestione del rischio dell'ente

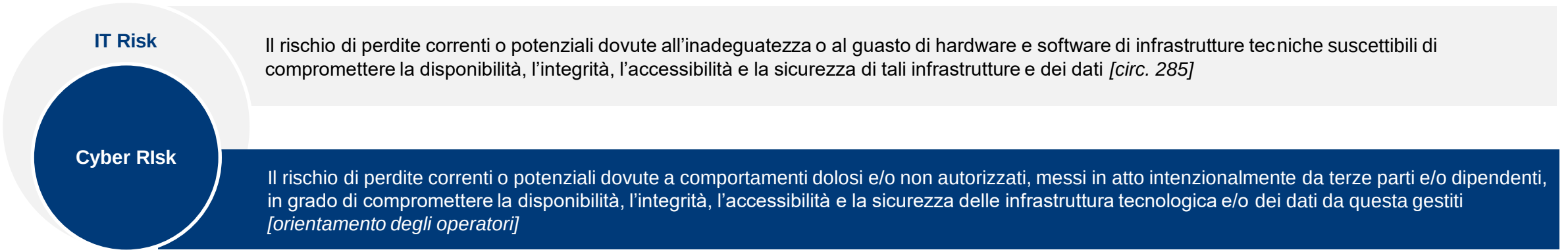
(1) Cyber Lexicon pubblicato dal Financial Stability Board (glossario dei principali termini legati alla Cyber Security e alla Resilienza operativa)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Come si stanno orientando gli operatori

- L'esigenza di definire il "Cyber Risk" come una componente a sé stante nasce dalla necessità di dover identificare e gestire tempestivamente una fattispecie di rischio con caratteristiche molto specifiche: **intenzionalità dei comportamenti, rapidità nell'evoluzione delle tecniche di attacco, trascendenza dagli asset IT della Banca** (es. credenziali carpite mediante campagne phishing indirizzate a mail dei clienti e/o bonifici disposti dai clienti stessi tratti in inganno da soggetti terzi)

- Nonostante, siamo ancora molto **lontani dall'identificazione di una definizione univoca del concetto di Cyber Risk**, i principali orientamenti sembrano essere indirizzati verso un concetto simile a quanto rappresentato nel seguente schema



- **L'IT Risk ricomprende tutti i rischi legati agli aspetti tecnici informatici** (es. malfunzionamenti, indisponibilità, change management), **di sicurezza logica e fisica** (es. gestione accessi, data management). **Il Cyber Risk viene circoscritto ai soli aspetti di sicurezza logica** (es. accessi logici, Vulnerability Management). **Il Cyber Crime** rappresenta , invece, la tipologia di attacco che può essere utilizzata per arrecare un danno (es. phishing, malware, spamming) o un disservizio (es. DDoS)

Agenda

- ✓ Di cosa stiamo parlando?
- ✓ **Analisi del contesto operativo**
- ✓ Ultimi interventi del Regolatore

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Overview

Negli ultimi 40 anni, si è assistito ad una progressiva e rapida evoluzione dei fenomeni di Cybercrime, non sempre accompagnata dall'evoluzione dei sistemi di Cybersecurity delle aziende: oltre metà degli attacchi è indirizzata alle PMI che non dispongono di risorse finanziarie e competenze per potersi difendere adeguatamente

	1980s	1990s	2000s	2010s	2020s
Obiettivi	Personal Computer	Rete Internet	Applicazioni	Attacchi Misti	Attacchi su larga scala e multi settore
Attaccanti	Principalmente adolescenti che operano per puro divertimento e/o sfida	Iniziano ad organizzarsi e a comunicare attraverso il Web. Iniziano i primi episodi di Cybercrime	Diventano più organizzati, meno interessati alla notorietà e più attratti dai soldi	Raggiungono livelli di raffinatezza tali da renderli veri e propri professionisti	Organizzazioni industriali dotate di competenze ed esperienze specifiche. Offrono propri social network, malware in licenza con relativo supporto tecnico, botnet in affitto, servizi pay-for-play
Tecniche di attacco	Prima forme di Virus	Rapida e ampia diffusione dei software malevoli	Dalla diffusione randomica dei virus ad una strategia mirata allo sfruttamento delle vulnerabilità	Esfiltrazione di dati, spionaggio internazionale, interruzioni su larga scala effettuate su commissione	Il livello di personalizzazione dei malware è tale da consentirgli di infiltrarsi e proliferare rapidamente e silenziosamente in tutto il sistema
Strumento di diffusione	Floppy disk	Connessioni di rete	Vulnerabilità associate all'infrastruttura IT	Codici malevoli nascosti nei file e/o supporti removibili (es. allegati mail, USB)	Phishing, Business E-mail Compromise, Social Media, SMiShing, Vishing, USB. Tecniche di Social Engineering sempre più sofisticate che impiegano strumenti di Intelligenza Artificiale
Contromisure	Prime soluzioni di Antivirus	Sviluppo dei primi Firewall di Rete	Sviluppo di sistemi rilevazione e prevenzione degli attacchi a vulnerabilità note (Intrusion Detection System e Intrusion Prevention System)	Introduzione di nuove tecnologie basate sull'ispezione preventiva dei file in ingresso (es. anti-botnet, sandbox)	Integrazione del sistema di Cybersecurity nel Framework complessivo di gestione dei rischi (cfr. slide successive)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Dimensione globale degli attacchi di nuova generazione

Nonostante non siano disponibili dati complessivi sulla dimensione globale dei tentativi di attacco, di seguito si riportano alcune statistiche estrapolate dal Kaspersky Security Bulletin 2019[1]

20%

utenti che hanno rilevato almeno un Malware e/o Attacco Web nel corso dell'anno

Web-Based Attacks

976 mln

attacchi web rilevati

25 mln

oggetti dannosi rilevati (script, exploit, file eseguibili, ecc.)

274 mln

URL bloccati da antivirus

Crypto-Ransomware

755.485

utenti attaccati da Encryptors

46.156

sistemi di Encryptors oggetto di modifica (rappresentano nuove minacce)

2,2 mln

utenti che hanno subito attacchi durante transazioni in criptovaluta

Banking malware

766.728

utenti che hanno subito almeno una tentata sottrazione di denaro dai conti bancari mediante software malevolo

Phishing[2]

55%

percentuale delle aziende che hanno subito almeno un attacco di Phishing nel 2019 (Spear Phishing, Business E-mail Compromise, Social Media, SMiShing, Vishing, USB)

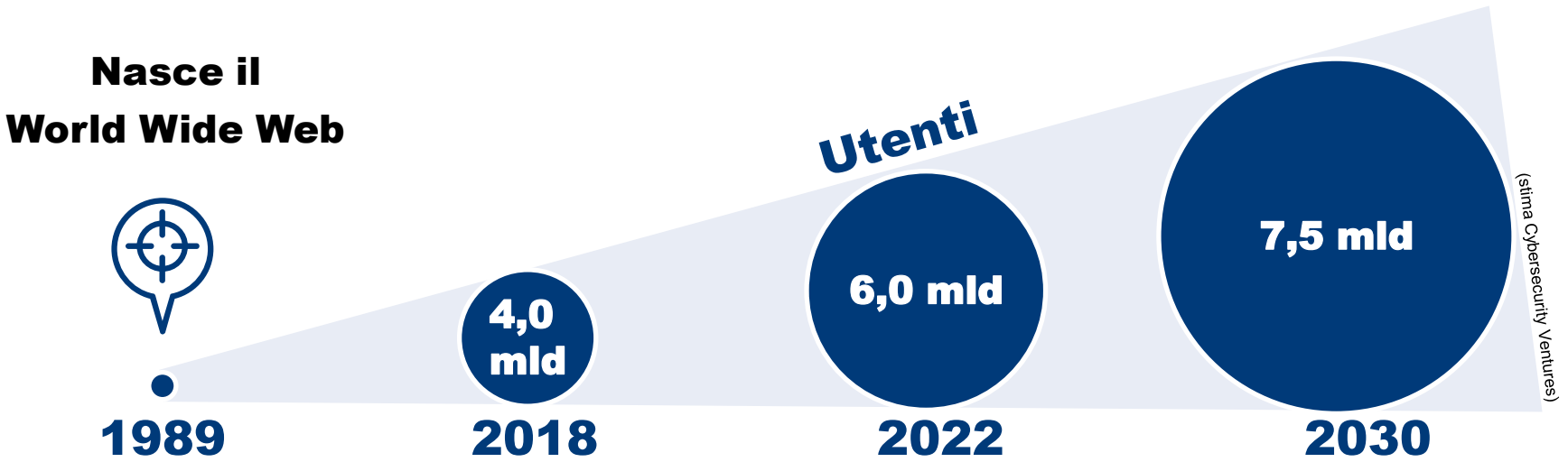
1) Evidenze raccolte dai sistemi di antivirus distribuiti da Kaspersky nel periodo novembre 2018 - ottobre 2019

2) Survey condotta da Proofpoint (primaria società di sicurezza informatica mondiale) su 600 professionisti di sicurezza informatica

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Complessità della Cybersecurity legata all'evoluzione del contesto

La complessità nel difendersi da possibili attacchi cresce in proporzione al numero di fattori che possono essere sfruttati (es. nuovi attaccanti, minacce emergenti, numero di utenti, aumento dei dispositivi interconnessi, crescita esponenziale della quantità di dati che devono essere protetti)



100

moltiplicatore di crescita dei dispositivi IoT tra il 2006 e il 2020 (da 2 mld a 200 mld - stima Cybersecurity Ventures)

111 mld

linee di nuovo codice software prodotto ogni anno (stima Gartner)

50

moltiplicatore di crescita del volume di dati on line dal 2016 al 2025 (da 2 mld a 200 mld di terabyte - stima Microsoft)

100

moltiplicatore di crescita della quantità di dati che saranno archiviati in cloud entro il 2021 (stima Cybersecurity Ventures)

95%

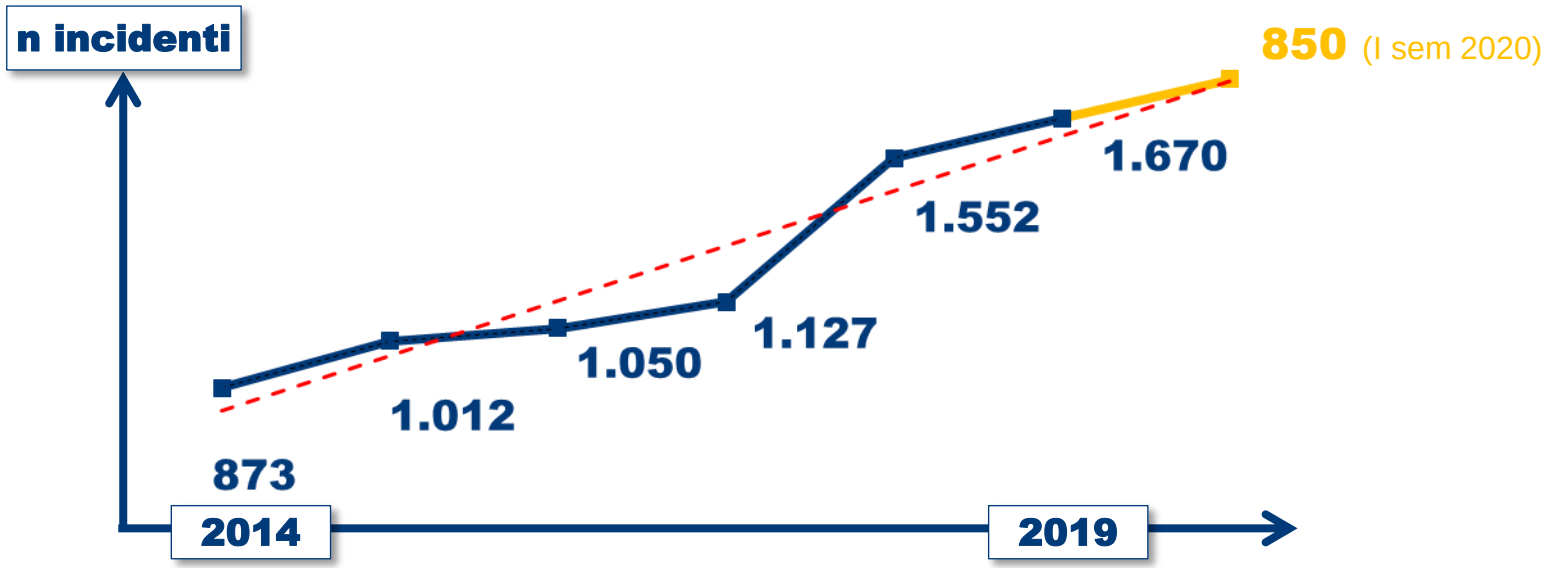
percentuale di traffico dei data center che sarà gestita in cloud entro il 2021 (stima Cisco)

(fonte: rapporto Clusit 2020)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Analisi del trend mondiale dei gravi incidenti provocati da un attacco

Secondo il rapporto Clusit 2020 tra il 2014 ed il 2019 il contesto operativo mondiale è in netto deterioramento



91%

aumento del numero di attacchi ***«gravi»*** registrato dal 2014 al 2019 (1.670 del 2019 vs 873 del 2014)

7%

aumento del numero di attacchi ***«gravi»*** registrato nei primi 6 mesi del 2020 (850 vs 796 del I sem 2019)

- Nel periodo si registra un forte ***aumento delle azioni messe in atto dalle organizzazioni di Cybercrime (+163%)***, ormai vere e proprie multinazionali con ampia disponibilità di mezzi tecnologici, ***e dei fenomeni di «Espionage» ed «Information Warfare» (+115%)***
- Secondo gli esperti Clusit, l'incremento dei fenomeni di «Espionage» ed «Information Warfare» potrebbe essere interpretato come un **possibile cambiamento di strategia** (attacchi più discreti ma prolungati nel tempo)

Fonte: rapporto Clusit 2020 – il report illustra gli esiti dell'analisi dei più gravi cyber attacchi di dominio pubblico avvenuti nel mondo a partire dal gennaio 2014. Il rapporto è pubblicato dall' associazione italiana Clusit (associazione nata presso il Dipartimento di Informatica dell'Università degli Studi di Milano, attualmente rappresenta più di 600 organizzazioni appartenenti a settori diversi)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

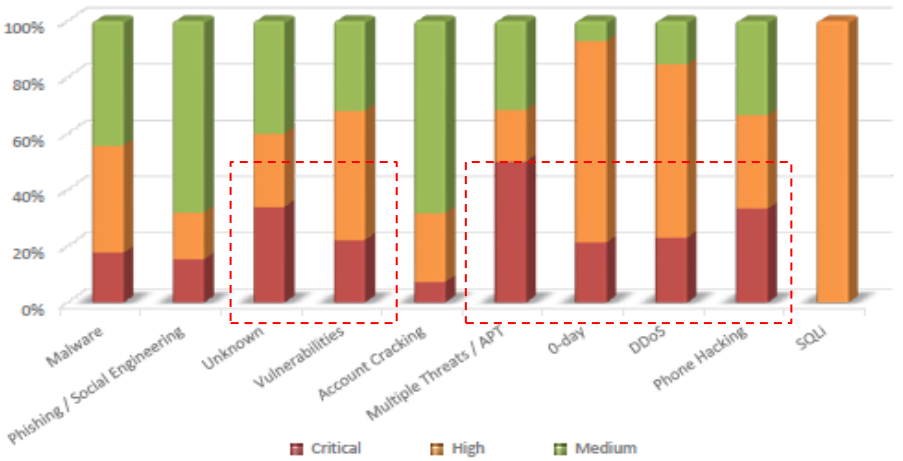
Analisi delle tecniche di attacco a livello mondiale

Tipologia di Attacco	2014	2015	2016	2017	2018	2019	2020	Δ 2014-2019
Malware	127	106	229	446	585	730	346	475%
Unknown	199	232	338	277	408	317	153	59%
Vulnerabilities	195	184	136	127	177	126	72	-35%
Phishing/Social Engineering	4	6	76	102	160	291	169	7.175%
Multiple Techniques/APT	60	104	59	63	98	65	38	8%
Account Cracking	86	91	46	52	56	86	41	0%
DDoS	81	101	115	38	38	23	13	-72%
0-Day	8	3	13	12	20	30	14	275%
Phone Hacking	3	1	3	3	9	1	3	-67%
SQL Injection	110	184	35	7	1	1	1	-99%
Totale	873	1.012	1.050	1.127	1.552	1.670	850	91%

- Gli Advanced Persistent Treath (APT), Phone Hacking, Unknown, DDoS e 0-day presentano una maggiore Severity
- Nonostante siano più numerosi, gli attacchi Malware semplici, Phishing/Social Engineering e Account cracking, mediamente hanno un livello di Severity più basso

- Grazie ai bassi costi di produzione (piccole modifiche a codici preesistenti o minime sofisticazioni alle tecniche di Phishing possono garantire ampi margini di profitto), ***Malware, Phishing e Social Enginnering si confermano le tecniche più utilizzate dai Cyber Criminali***
- L'aumento degli attacchi «Unknow» e «0 Day» evidenzia come ***le tecniche di attacco si stiano evolvendo***

Distribuzione della Severity associata agli incidenti



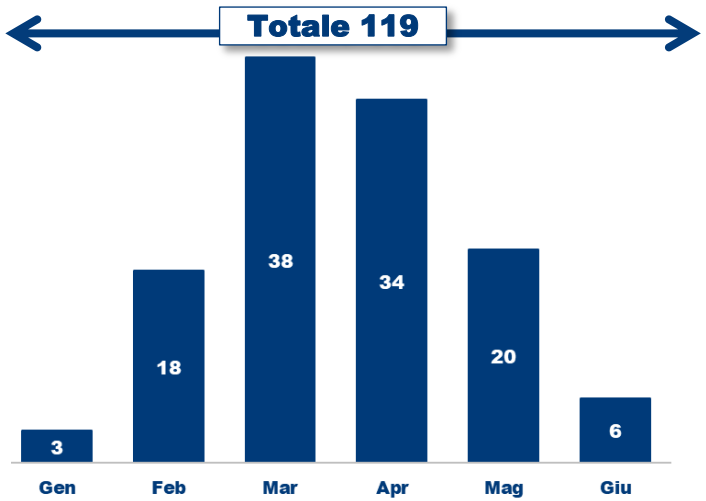
(fonte: rapporto Clusit 2020)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Gestione dell'emergenza pandemia Covid 19 a livello mondiale (parte 1 di 2)

Con l'inizio dell'emergenza pandemica le aziende hanno attivato piani di continuità emergenziali basati sul lavoro a distanza, con poco tempo a disposizione per una valutazione preventiva delle ripercussioni. La conseguenza è stata una catena di incidenti spesso causati proprio da azioni estemporanee non incluse in un piano strategico per la gestione delle emergenze

Trend dei gravi incidenti rilevati nel I semestre 2020 direttamente riconducibili alla gestione pandemica



14%

percentuale di attacchi ***«gravi»*** registrati nel primo semestre 2020 direttamente riconducibili alla gestione pandemica (119 vs 850)

Distribuzione per tecnica di attacco dei gravi incidenti rilevati nel I semestre 2020 direttamente riconducibili alla gestione pandemica

72%

percentuale di attacchi perpetrati da Cyber Criminali

28%

percentuale di attacchi perpetrati per finalità di spionaggio e Information Warfare

Sfruttando la nuova consapevolezza acquisita durante la pandemia, le organizzazioni dovranno rivedere le proprie Policy interne in modo da tener conto dei seguenti elementi:

- i lavoratori possono svolgere le proprie mansioni da remoto, in spazi fisici e con strumenti tecnologici non sempre soggetti a presidi di sicurezza aziendale, pertanto, non è più sufficiente mettere in sicurezza i server per proteggere i dati aziendali e/o dei clienti

(fonte: rapporto Clusit 2020)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Gestione dell'emergenza pandemia Covid 19 a livello mondiale (parte 2 di 2)

I 119 ***«gravi»*** incidenti si sono registrati principalmente nella fase immediatamente successiva alla dichiarazione di lockdown e sono riconducibili alle seguenti rischiosità

1

Phishing e Social Engineering

Tecniche già ampiamente diffuse prima dell'avvio della pandemia, ma riadattate al nuovo contesto emergenziale. Le campagne sono state caratterizzate da contenuti estremamente simili, veicolate attraverso canali differenti (mail, SMS, piattaforme di instant messaging e social) e con l'unico intento di indurre gli utenti a cliccare su link malevoli o rivelare informazioni riservate

2

Rischi connessi all'operatività a distanza

Forte incremento delle scansioni per l'identificazione di nuovi Remote Desktop Protocol (RDP) esposti. Dopo aver rilevato un nuovo RDP, gli attaccanti hanno provato ad accedere ai sistemi utilizzando metodi di brute force (tecnica che utilizza un numero elevato di password differenti fino all'individuazione di quella corretta) o sfruttando altre vulnerabilità note (soprattutto ransomware)

3

Espionage ed Information Warfare

Rilevati anche casi di "CEO Fraud", in cui l'attaccante fingendosi l'Amministratore Delegato o altra figura apicale, invia una mail ad un dipendente autorizzato ad effettuare transazioni finanziarie
Le organizzazioni dovrebbero esserne consapevoli e adottare le contromisure appropriate, ad esempio rafforzando le procedure di autorizzazione interne o sensibilizzando il personale su come riconoscere tentativi di frode

Altre rischiosità potenziali

- Con il fine di limitare le possibili ripercussioni del lavoro a distanza su produttività e benessere dei lavoratori, numerose organizzazioni si sono dotate di strumenti di monitoraggio (es. applicazioni da installare sullo smartphone, auto-certificazioni, rilevazioni stato di salute)
- Strumenti utili ma che possono dare origine a rischi legati alla riservatezza dei dati e al relativo trattamento (es. sanzione di 35 milioni di euro inflitta dall'Autorità garante tedesca al colosso H&M per un'attività di profilazione illecita del proprio personale)

(fonte: rapporto Clusit 2020)

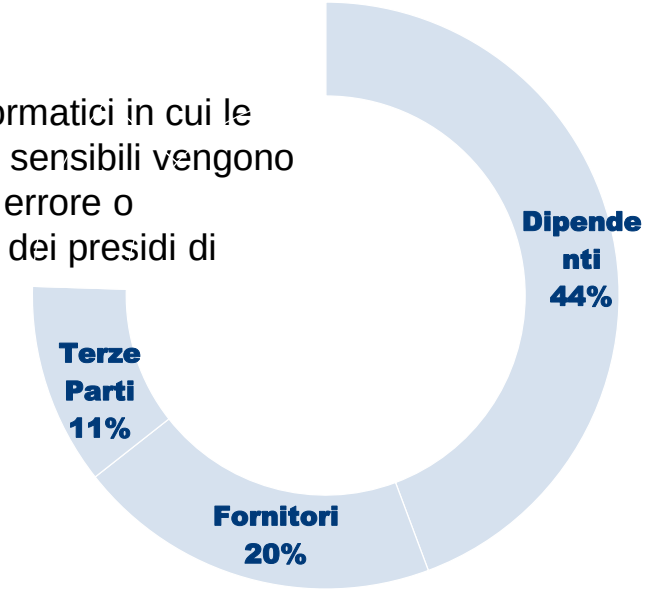
IT Risk, Cybersecurity e nuove frontiere del Risk Management

Priorità di intervento identificate dai Risk Manager

Secondo il Global Fraud & Risk Report 2020[1] i primi due rischi a cui si sentono esposti i principali esperti di Risk Management mondiali sono: ***Data Leak*** e ***Data Theft***

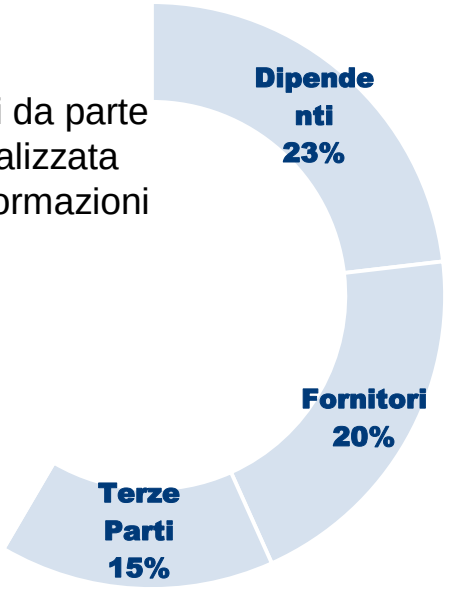
1

Data Leak
incidenti informatici in cui le informazioni sensibili vengono esposte per errore o vulnerabilità dei presidi di sicurezza



2

Data Theft
violazione dei sistemi da parte di Cyber Criminali finalizzata alla sottrazione di informazioni



I Data Leak e Data Theft molto spesso sono di origine endogena. Nella metà dei casi tali azioni sono realizzate senza l'ausilio di strumenti informatici, ma sfruttando comunque carenze dei presidi di sicurezza informatica. Ciò evidenzia la necessità di integrare la sicurezza informatica nella strategia complessiva di gestione del rischio

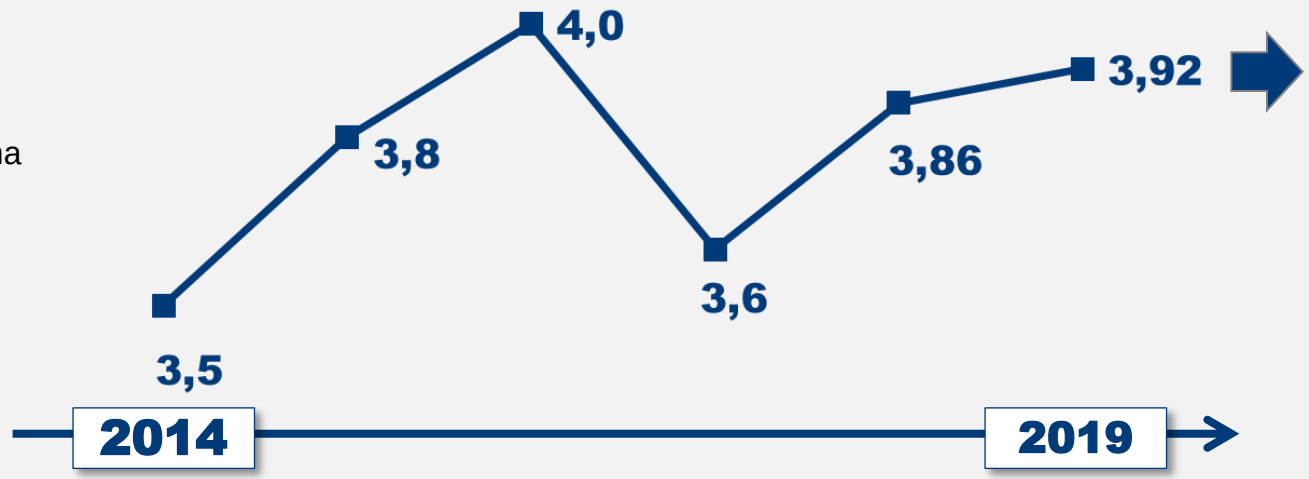
(1) Rapporto redatto da Kroll (società leader globale nelle investigazioni complesse e nella sicurezza informatica), rappresenta una delle più complete analisi sul nuovo panorama dei rischi globali. L'analisi ha visto il coinvolgimento di 588 Manager con ruolo attivo nella definizione delle strategie di gestione del rischio di società provenienti da 13 paesi diversi, operanti in più di un paese e appartenenti a 10 settori differenti. L'analisi è stata condotta tra marzo e aprile 2019

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Cost of a Data Breach (parte 1 di 3)

+12%

aumento del costo medio di una Data Breach dal 2014 al 2019 (mln USD)



Composizione

- **36%** Loss Business Cost
- **31%** Detection & Escalation
- **27%** Post Breach Cost
- **6%** Notification

279gg

- *206 gg per identificare*
- *73 gg per contenere*

Numero di giorni medi impiegati per identificare e contenere un Data Breach *(+ 4,9% vs 266 del 2018)*

25.575

Numero medio di records di un Data Breach

150$

Costo medio per records

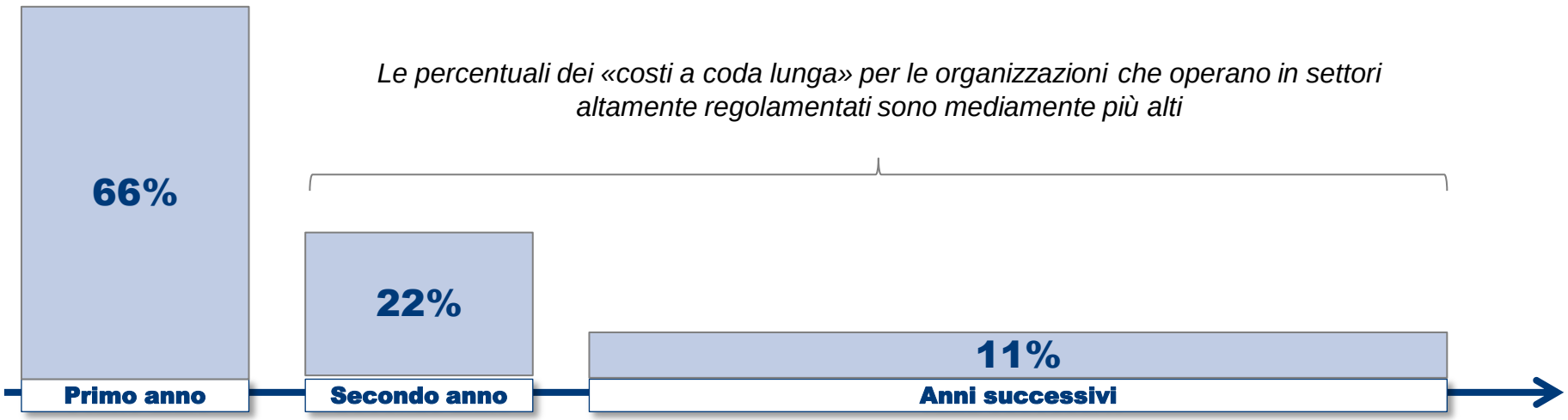
Data Breach con un ciclo di vita < 200 gg registrano il 37% di costi in meno rispetto a quelli con ciclo di vita ≥ 200 gg

(fonte: Cost of a Data Breach Report 2019 redatto dall' IBM Security e Ponemon Institute sulla base di una survey su più di 500 aziende di tutto il mondo che hanno subito una violazione dei dati tra luglio 2018 e aprile 2019)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

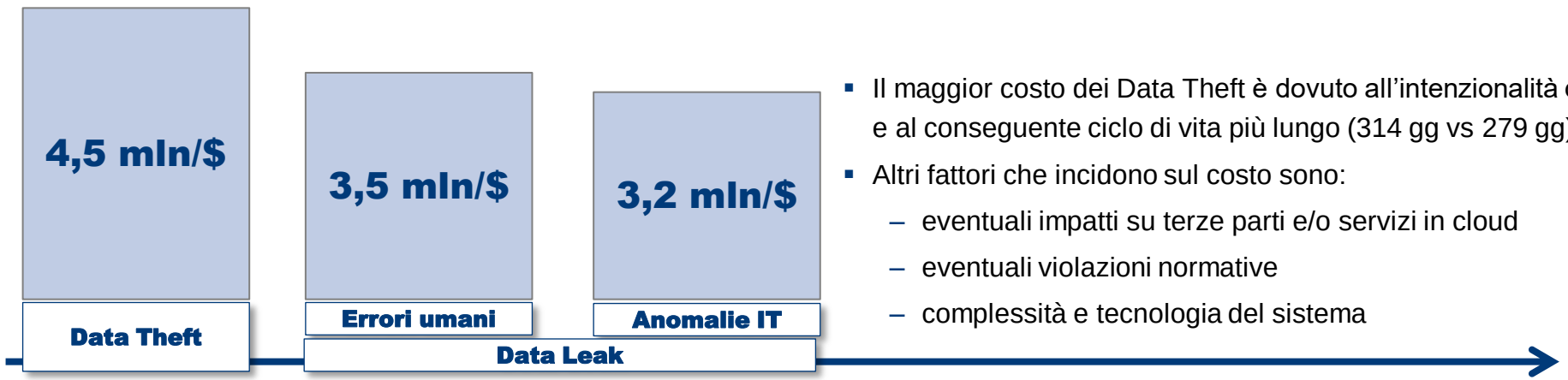
Cost of a Data Breach (parte 2 di 3)

I costi di un Data Breach incidono per anni



Le percentuali dei «costi a coda lunga» per le organizzazioni che operano in settori altamente regolamentati sono mediamente più alti

Un Data Theft è mediamente più costoso di un Data Leak



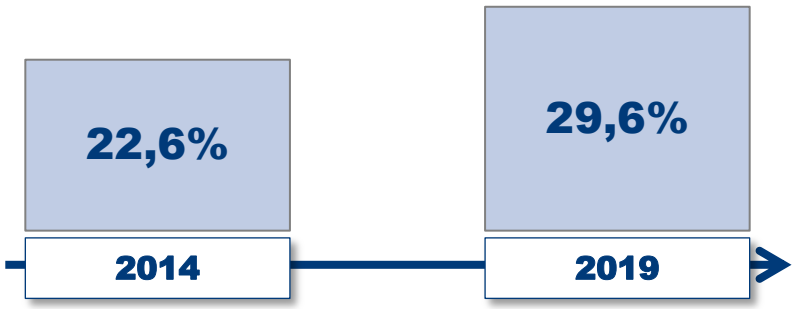
- Il maggior costo dei Data Theft è dovuto all'intenzionalità dell'attacco e al conseguente ciclo di vita più lungo (314 gg vs 279 gg)
- Altri fattori che incidono sul costo sono:
  - eventuali impatti su terze parti e/o servizi in cloud
  - eventuali violazioni normative
  - complessità e tecnologia del sistema

(fonte: Cost of a Data Breach Report 2019 redatto dall' IBM Security e Ponemon Institute sulla base di una survey su più di 500 aziende di tutto il mondo che hanno subito una violazione dei dati tra luglio 2018 e aprile 2019)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Cost of a Data Breach (parte 3 di 3)

Le probabilità di accadimento sono in aumento



+31%

percentuale di aumento rispetto al 2014 della probabilità attesa di un Data Breach entro due anni

L'automazione della sicurezza riduce i costi

-95%

percentuale di riduzione dei costi registrati dalle Organizzazioni che hanno automatizzato la propria sicurezza, rispetto a chi non lo ha fatto

- **Big data and analytics**
- **Artificial intelligence**
- **Machine learning**
- **Robotic process automation**

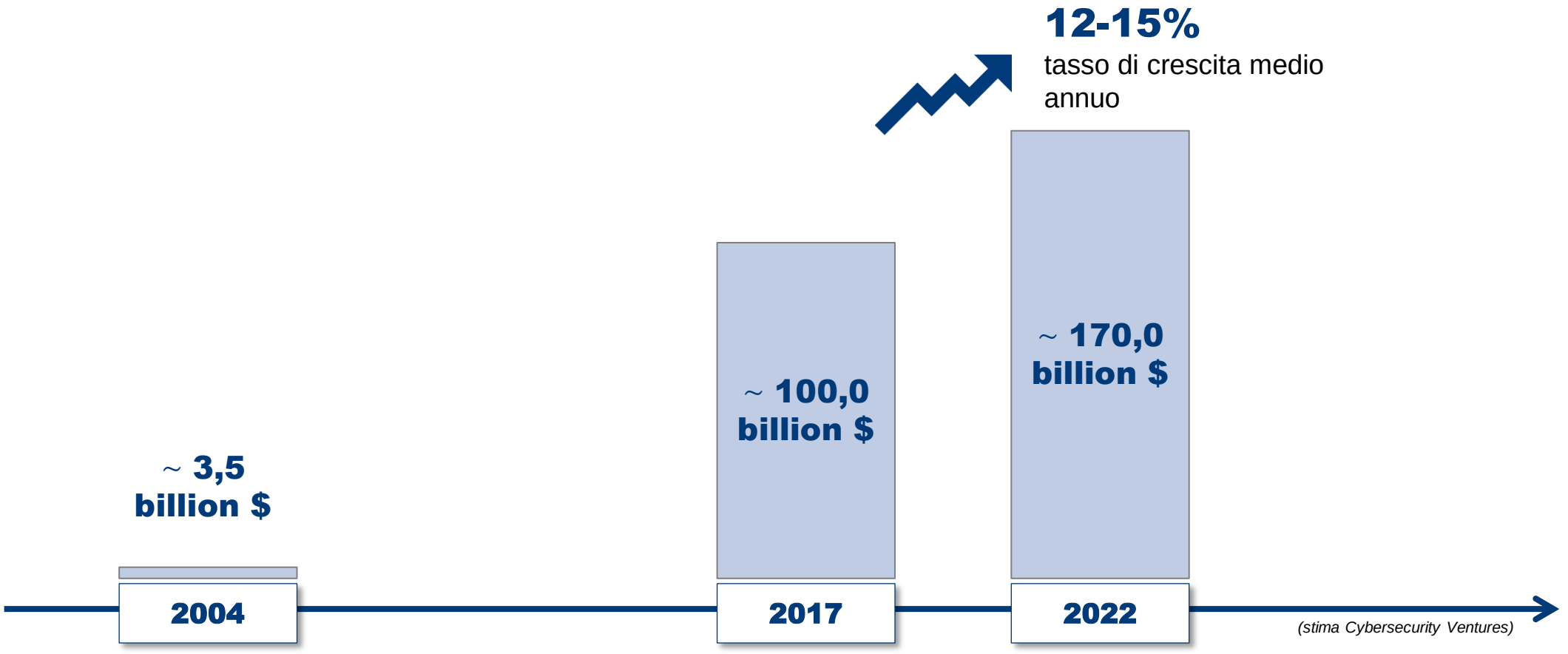
I presidi di Security Operation Center, Incident Management, Threat intelligence e Business Continuity si stanno dotando di strumenti di analisi e gestione molto più sofisticati

(fonte: Cost of a Data Breach Report 2019 redatto dall' IBM Security e Ponemon Institute sulla base di una survey su più di 500 aziende di tutto il mondo che hanno subito una violazione dei dati tra luglio 2018 e aprile 2019)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Investimenti globali in Cybersecurity

Nel 2004, il mercato globale della sicurezza informatica valeva 3,5 miliardi di dollari. Nel 2018 ha superato i 100 miliardi e si stima che crescerà fino a 170 miliardi nel 2022



IT Risk, Cybersecurity e nuove frontiere del Risk Management

Analisi del settore bancario italiano

La survey 2020 sulle frodi informatiche 2019 condotta dal CERTFin[1] per il settore bancario italiano conferma le evidenze rilevate a livello globale

Frodi

84%

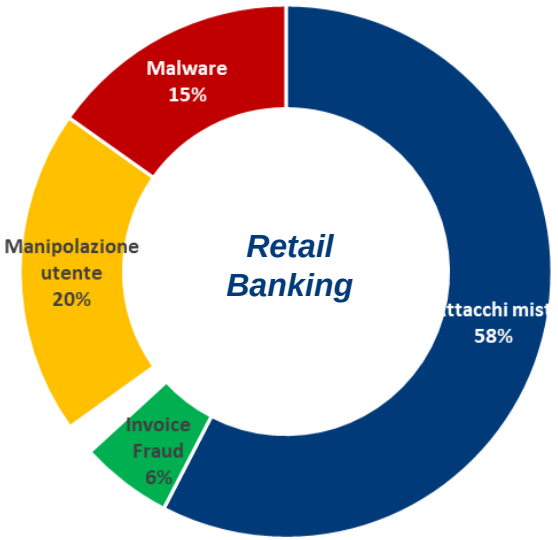
percentuale dei tentativi di frode che hanno interessato il segmento Retail Banking

Data Breach

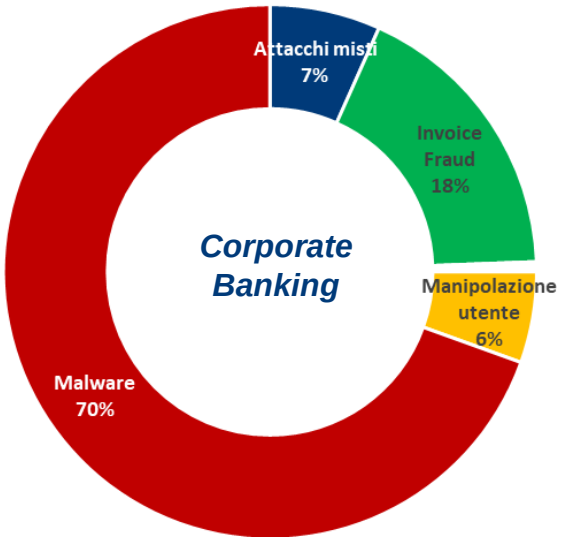
33%

percentuale di Banche intervistate che hanno dichiarato di aver ricevuto attacchi mirati al furto di dati (4 casi di «successo»)

I fenomeni frodatori presentano caratteristiche differenti a seconda del segmento di clientela



- 2019 caratterizzato dall'aumento delle frodi sui bonifici istantanei (più del 50% dei tentativi di frode)
- Nonostante le Banche siano state in grado di bloccare circa l'85% dei bonifici sospetti, dovranno essere ricercati nuovi strumenti di detection
- Tale segmento è principalmente caratterizzato da tecniche di attacco miste, nuovi schemi frodatori e manipolazione degli utenti. In tale ambito si segnala un forte incremento dei casi di SIM SWAP



- Nonostante riceva meno attacchi, tale segmento fa registrare maggiori perdite
- Tale segmento soffre della maggiore sofisticazione dei malware che sono arrivati a essere la principale tipologia di attacco
- Un ulteriore elemento di criticità è rappresentato dall'incremento delle «Invoice Fraud» (c.d. *truffa della fattura)*
- Il segmento Corporate è meno esposto alla tecnica SIM SWAP in quanto meno propenso ad utilizzare il canale mobile

(1) CERT Finanziario Italiano è un'iniziativa cooperativa pubblico-privata (ABI, ABI Lab, Banca d'Italia, IVASS e ANIA) finalizzata a innalzare la capacità di gestione del rischio informatico e la cyber resilience del sistema finanziario italiano

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Come stanno reagendo le aziende (parte 1 di 2)

- La coesistenza di metodiche tradizionali associate all'utilizzo di strumenti informatici sta spingendo le organizzazioni a rivedere le proprie strategie di valutazione e gestione del rischio IT. Si sta passando infatti **da un approccio di tipo reattivo**, guidato tradizionalmente dalle strutture specialistiche di primo livello, **ad una visione di più ampio respiro** in cui la sicurezza informatica è componente integrate del framework complessivo di gestione del rischio

- L'attuazione di questo nuovo approccio richiede una maggiore consapevolezza dei rischi, un'approfondita conoscenza dell'intera organizzazione ed un **coordinamento trasversale di molteplici funzioni aziendali** (CIO, CISO, CRO, CCO, CGC, CAE, CCoO,…)

- Tale riposizionamento della sicurezza informatica consente di cogliere in modo più puntuale le caratteristiche dei fattori di rischio associati alle diverse minacce/asset aziendali, modulare i presidi di sicurezza in funzione del rischio associato a ciascun asset ed **assicurare un profilo di rischio coerente con il Risk Appetite Framework**

- Il processo evolutivo avrà successo solo se associato ad una **crescente «maturità» delle Organizzazioni**. Infatti, i presidi di sicurezza sono efficaci solo se associati ad altri elementi abilitanti (es. un sistema di rilevazione di minacce cyber di ultima generazione sarà di scarsa utilità senza un numero adeguato di risorse qualificato in grado di rispondere rapidamente agli alert generati da quel sistema e di porre rimedio agli eventuali danni arrecati)

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Come stanno reagendo le aziende (parte 2 di 2)

Per aumentare la propria «**maturità**» le organizzazioni si stanno muovendo sulla base dei seguenti fondamentali:

1

Strategia IT

- Sviluppo di una strategia informatica coerente con il RAF e pienamente integrata nel piano industriale (OSI ECB)
- Allocazione di adeguate risorse per l'implementazione della stessa
- Implementazione di processi e procedure di supporto

2

Governance

Definizione di meccanismi di risoluzione dei conflitti tra:

- politiche di sicurezza e costi di implementazione
- priorità di intervento nelle diverse aree

3

Controllo

- Allocazione di adeguate risorse per la verifica ex ante e ex post del framework complessivo e per il monitoraggio delle performance dei sistemi di sicurezza
- Monitoraggi basati su misure quantitative e non solo su valutazioni soggettive
- Misurazioni effettuate in tempo reale
- Simulazioni in situazioni di emergenza in modo da testare la tenuta delle persone e dei sistemi anche in condizioni estreme

Agenda

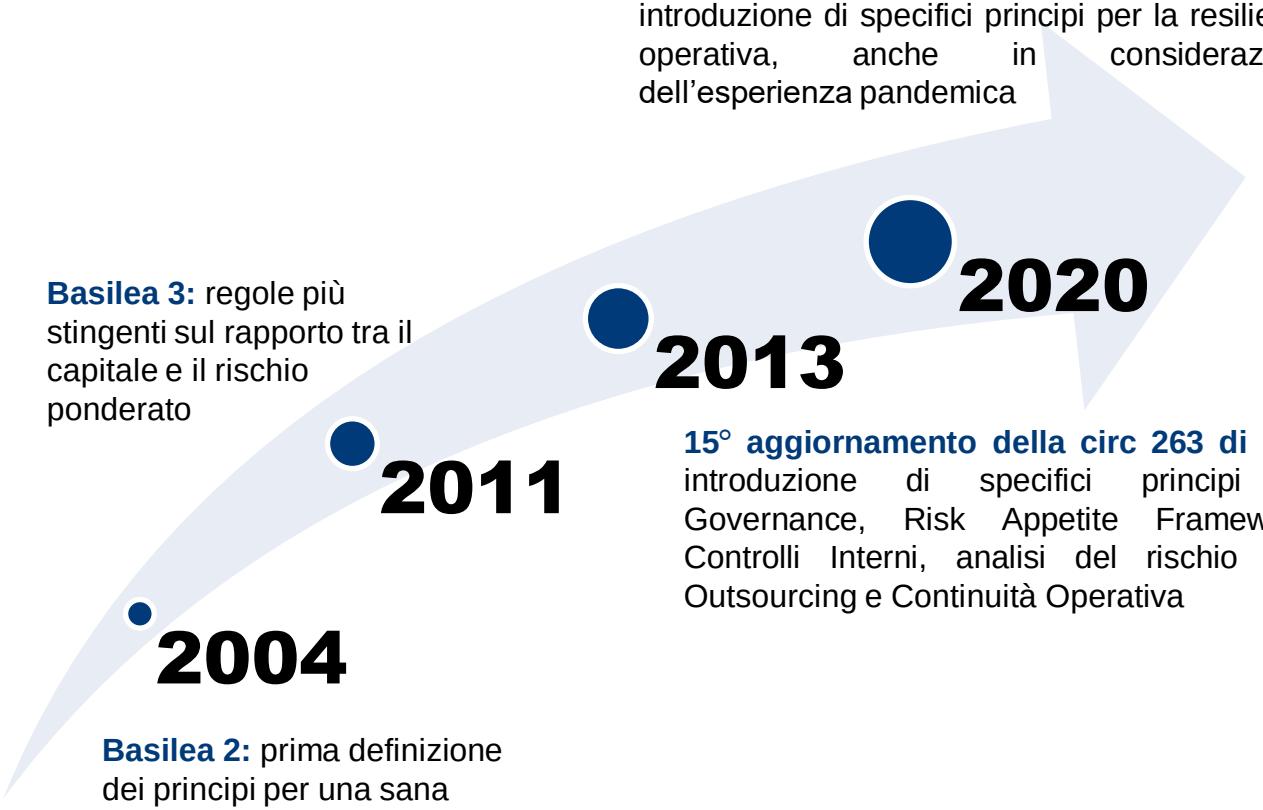
- ✓ Di cosa stiamo parlando?
- ✓ Analisi del contesto operativo
- ✓ **Ultimi interventi del Regolatore**

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Percorso evolutivo

- Riconoscendo il maggior rischio potenziale di interruzioni significative dovute a pandemie, disastri naturali, incidenti di sicurezza informatica distruttivi o guasti tecnologici, il Comitato di Basilea sta introducendo specifici principi per la ***resilienza operativa*** e contestualmente aggiornando i ***principi per la sana gestione del rischio operativo***

- Tali principi sono in gran parte derivati e adattati da linee guida già esistenti (es. principi per la sana gestione del rischio operativo, Governance Aziendale per le Banche, esternalizzazione di funzioni aziendali, Continuità Operativa)



Basilea 2: prima definizione dei principi per una sana gestione del rischio operativo

Basilea 3: regole più stingenti sul rapporto tra il capitale e il rischio ponderato

15° aggiornamento della circ 263 di BdI: introduzione di specifici principi su Governance, Risk Appetite Framework, Controlli Interni, analisi del rischio ICT, Outsourcing e Continuità Operativa

Consultative paper Comitato di Basilea: introduzione di specifici principi per la resilienza operativa, anche in considerazione dell'esperienza pandemica

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Principali elementi di novità

Focalizzando l'attenzione sugli elementi di novità, è possibile cogliere quali saranno le caratteristiche essenziali del Framework di valutazione e gestione dei rischi di nuova generazione

Principles for operational resilience	Revisions to the principles for the sound management of Operational Risk
• La funzione di gestione del rischio operativo delle banche dovrebbe lavorare insieme alle altre funzioni competenti per gestire e affrontare gli eventuali rischi che minacciano l'esecuzione delle operazioni critiche • Ai fini della resilienza operativa, un coordinamento appropriato tra piano di Continuità Operativa, gestione della dipendenza da Terze Parti, Recovery & Resolution planning e altri framework di gestione del rischio può generare una crescente armonizzazione degli approcci all'interno dell'azienda (art 21)	• I principi di Governance, Risk Management, Information and communication technology, Business Continuity planning & the Role of disclosure dovrebbero essere componenti integrati del framework di gestione del rischio operativo e del framework di gestione dei rischi complessivo di Gruppo, inclusa la resilienza operativa (Cap 2) • Ulteriori elementi di novità riguardano potenziamenti delle fasi di identificazione e valutazione dei rischi (sempre più basati su rilevazioni oggettive effettuate in tempo reale, potenziamento dei processi di Change Management, nuovi prodotti ed esternalizzazione di funzioni aziendali) ed il relativo sistema di reporting (artt 34 -51)

> ***"La funzione di controllo dei rischi operativi ricoprirà un ruolo sempre più centrale nella valutazione e gestione dei rischi informatici e della Resilienza Operativa"***

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Framework di Operational Risk Management di nuova generazione

Il Framework di Operational Risk Management di nuova generazione sarà basato sull'evoluzione della relazione esistente tra la prima e la seconda linea di difesa in modo da farla evolvere verso una ***"partnership di pensiero e competenze"***

Primo livello

- sarà responsabile dell'identificazione e valutazione dei rischi operativi (in condizioni normali e di stress)
- effettuerà le proprie valutazioni sulla base di KRI monitorati in tempo reale e verificando l'esistenza di correlazioni con i Rischi Operativi utilizzando strumenti di analisi avanzata
- rendiconterà periodicamente la funzione di controllo di II livello sulla base di KRI e KP condivisi

Secondo livello

- metterà in discussione le valutazioni effettuate dalla prima linea di difesa
- monitorerà tutte le fasi dei processi di Change Management, nuovi prodotti/servizi, esternalizzazione di funzioni aziendali, garantendo il coinvolgimento di tutte le funzioni competenti
- monitorerà l'efficacia del sistema dei controlli e degli interventi di mitigazione

Strategia IT

Sulla base di tali evidenze la funzione di controllo dei rischi in coordinamento con le strutture specialistiche, potrà indirizzare in maniera consapevole la strategia IT, a supporto delle funzioni competenti

Fattori abilitanti

Evoluzione delle conoscenze e competenze della funzione di controllo dei Rischi

Data la trasversalità, pervasività e mutevolezza di tale fattispecie di rischio, la seconda linea di difesa dovrà dotarsi di:

- risorse con esperienza e competenze specialistiche
- strumenti di analisi avanzata
- Capacità costante di adattamento

Sistema di Reporting

Il Sistema di Reporting della funzione di controllo dei rischi operativi dovrà essere integrato in modo da garantire:

- un approccio multidisciplinare nella gestione del rischio
- un riscontro tangibile dell'azione della funzione di controllo

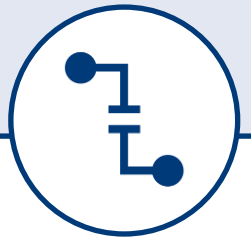
IT Risk, Cybersecurity e nuove frontiere del Risk Management

Principali aree di intervento

Le indicazioni del Comitato di Basilea identificano in modo chiaro gli ambiti su cui i nuovi framework dovranno focalizzarsi

Rischi di Condotta
(incluse frodi interne e pratiche commerciali scorrette)

Resilienza Operativa



Rischi informatici
(inclusi Cyber Risk e Change Management)

Rischio associato a Terze Parti

Rischi associati all'attivazione di nuovi Prodotti/Servizi
(inclusi rischi informatici associati)

Frodi esterne

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Evoluzione normativa

I nuovi principi per la resilienza operativa e l'aggiornamento dei principi per la sana gestione del rischio operativo andranno a consolidare il processo evolutivo che ha caratterizzato le strutture dei Risk Management negli ultimi 30 anni:

	1998 Basilea I	2004 Basilea II	2011 Basilea III	2013 Basilea IV	2021 Next Generation
Framework	Introduzione del requisito patrimoniale minimo	Introduzione dei Rating, dei Rischi Operativi[1] e strumenti finanziari a basso impatto sul capitale	Regole più stingenti sul rapporto tra il capitale e il rischio ponderato	Introduzione dei principi per la misurazione e gestione del rischio IT e di Data Governance	Introduzione dei principi per la Resilienza Operativa
Tecnologia	Processi manuali e assenza di serie storiche dei dati	Processi manuali non supportati da fonti dati comuni e con bassa qualità	Il rafforzamento del "risk management information System» come priorità	Introduzione di Strumenti di Data Mining e Data Analysis	Big data, Machine learning, AI e Robotic process automation
Competenze	Assenza di competenze su Rischi Operativi ed Informatici	Introduzione risorse specialistiche su Rischi Operativi	Aumentano le risorse e le competenze su Rischi Operativi	Introduzione risorse specialistiche su IT Risk e Data Governance	Risorse con competenze trasversali e specialisti di Analisi Avanzata
Integrazione	Regolamentazione non focalizzata su temi di Operational / IT / Cyber risk	Gestione del rischio per silos	Logica della "redditività corretta per il rischio"	Sviluppo di un approccio di collaborazione con le altre funzioni	Approccio multidisciplinare nella gestione del rischio

(1) Il rischio IT è ancora considerato solo come manifestazione di perdita associata ad errori e/o malfunzionamenti IT

IT Risk, Cybersecurity e nuove frontiere del Risk Management

Conclusioni

- Siamo in presenza di **rischi emergenti con tassi di crescita potenziali e variabilità nelle tipologie mai sperimentati** in precedenza

- In tale contesto le funzioni di controllo dovranno avere **piena visibilità dei rischi e delle vulnerabilità** associati a tutte le unità organizzative, al fine di indirizzare in maniera consapevole le priorità di intervento

- I nuovi principi per una sana gestione dei rischi operativi prevedono che Governance, Risk Management Environment, Information & Communication Technology (ICT) ed il Business Continuity Planning debbano essere **componenti integrate del framework di gestione del rischio**: la funzione di controllo dei rischi in coordinamento con le strutture di Business potrà indirizzare nuove opportunità di investimento aiutando la Banca a raggiungere i propri obiettivi strategici in coerenza con il Risk Appetite Framework

- La partnership instaurata con le funzioni di Business e la prima linea di difesa consentiranno inoltre alla funzione di controllo dei rischi di integrare il proprio sistema di reporting con una serie di informazioni gestionali (es. indicatori di performance dei processi, indicatori di efficacia del sistema dei controlli) e di **garantire un approccio multidisciplinare nella gestione del rischio** ed avere un riscontro tangibile dell'azione della funzione di controllo