POLITECNICO DI TORINO

Facoltà di Ingegneria

Corso di Laurea Magistrale in Ingegneria Gestionale

Tesi di Laurea Magistrale

Cybercrime e finanza: una ricerca empirica sul cyber-risk nel mondo bancario

Relatore
Prof Varetto Franco

Candidato
Giovine Andrea Serena

Anno Accademico 2019/2020

Ad Anna,
mamma, amica ed esempio di vita.

Sommario

I Indice Figure

II Indice Tabelle

III Indice degli acronimi

AIC	Akaike's Information Criterion
AMA	Advanced Measurement Approches
APT	Advanced Persistent Threat
ASA	Metodo Standardizzato Alternativo
BIA	Basic Indicator Approach
BIS	Bank for International Settlements
BRI	Banca dei Regolamenti Internazionali
CBVB	Comitato di Basilea per la Vigilanza Bancaria
DDoS	Distributed Denial of Service
DoS	Denial of Service
DR	Disaster Recovery
ERP	Enterprise Resource Planning
GDPR	Regolamento Generale sulla Protezione dei Dati
GITC	General IT Controls
ICT	Information and Communications Technology
IMA	Internal Measurement Approach
IoT	Internet of Things
IRM	Information Risk Management
IT	Information Technology
ITAC	IT Application Controls
KAM	KPMG Audit Methodology
MID	Margine di Intermediazione
Oms	Organizzazione Mondiale della Sanità
PT	Penetration Test
SIA	Standardised Indicator Approach
SQL	Structured Query Language
TA	Total Asset
VA	Vulnerability Assesment
VAR	Value At Risk
WCGW	What Could Go Wrong

IV Abstract

Tutte le società che ricorrono a sistemi informativi nella gestione della propria attività sono costrette a fronteggiare il pericolo di attacchi informatici. Questo fenomeno è conseguenza della sempre crescente digitalizzazione che sta investendo tutti i principali settori dell'economia. Un processo di *Risk Management* efficiente può aiutare le aziende a ridurre il rischio e a circoscrivere i danni derivanti.

Nel presente elaborato è stata calcolata l'esposizione al rischio del settore finanziario nel suo complesso tramite la stima del valore a rischio. A causa della asimmetria informativa che caratterizza il settore, è stato dapprima necessario costruire una base dati sulla quale è stato possibile effettuare attente analisi. Dopo aver constatato assenza di correlazione tra i dati, sono state individuate due distribuzioni di probabilità che rappresentassero bene i valori di frequenza e di severità degli attacchi individuati. È stata dunque eseguita una simulazione Montecarlo per la quale sono stati generati 10.000 scenari. La simulazione ha così permesso di ottenere in *output* una distribuzione di severità cumulata sulla base della quale è stato calcolato un valore a rischio al 99-esimo percentile di 0,039404175.

Il risultato ottenuto permette di affermare che, nel 99% dei casi, il settore finanziario subirà a causa di reati informatici, nell'arco di un trimestre, danni che incidono al massimo per il 3,9% del valore del settore nel suo complesso.

V Introduzione

Il crescente sviluppo delle tecnologie informatiche ha portato innumerevoli cambiamenti in ogni settore della vita dell'uomo. Questa tecnologia offre, da un lato, enormi opportunità sul piano sociale, economico e lavorativo ma porta con sé una serie di debolezze intrinseche che sono terreno fertile per la nascita di un nuovo tipo di criminalità che richiede altrettanta tecnologia per essere contrastata.

Il *cybercrime* è un aspetto con il quale chiunque deve confrontarsi: dal semplice cittadino che naviga su *internet* alla società multinazionale che utilizza sistemi informativi per gestire la propria attività. Il crimine informatico è un fenomeno che sfrutta le debolezze umane e informatiche e resta in agguato per scovare il momento più propizio per sferrare l'attacco. Il delicatissimo periodo storico che stiamo vivendo, caratterizzato dalla crisi sanitaria ed economica legata al Covid-19, ha registrato un drastico incremento del fenomeno che insiste prevalentemente su due fronti: attacchi a dispositivi personali e a strutture ospedaliere.

Per citare un esempio, la Polizia Postale ha comunicato che, durante il periodo dell'emergenza, caratterizzato dal crescente e diffuso ricorso allo *smartworking,* le truffe informatiche perpetrate sotto forma di *phising* sono aumentate del 600% a livello globale. Un particolare attacco *phising* ha visto protagonista anche l'Organizzazione mondiale della Sanità: una *e-mail* con la firma di una finta dottoressa dell'Oms invitava ad aprire un allegato contenente informazioni per prevenire e difendersi dall'infezione da Coronavirus ma che in realtà conteneva un *malware*. Gli attacchi, tuttavia, hanno riguardato anche altri temi cruciali delicati come disoccupazione e difficoltà economica. Un esempio di recente letteratura è un *malware* bancario, diffuso durante il periodo di parziale chiusura degli sportelli, che è stato diffuso in rete per mezzo di una *e-mail* contente un *curriculum* inviato da una persona alla ricerca di lavoro e che è emerso essere in grado di sottrarre le credenziali di accesso alle aree private dell'*home banking*. Anche l'*App* Immuni è stata al centro di un attacco di *cybercrime*: ad inizio giugno è stata diffusa una *e-mail* che indirizzava ad un sito fittizio che imitava quello della Federazione Ordini dei Farmacisti Italiani.

È evidente come le tecnologie attuali siano molto soggette a questo tipo di fenomeno che colpisce tutti i settori in cui i criminali intravedano la possibilità di profitto. Uno dei settori più colpiti, insieme a quello sanitario, è il settore finanziario.

Il presente lavoro di tesi mira ad introdurre il lettore al problema del *cybercrime* e ad analizzare ed indagare l'esposizione del settore finanziario a tale fenomeno utilizzando il *Value at Risk*, considerato una valida misura per comprendere l'incidenza degli attacchi informatici e la loro portata.

L'interesse per questo argomento è nato durante l'esperienza di tirocinio svolta presso la sede di Torino della società di consulenza internazionale KPMG S.p.A. dove ho avuto l'opportunità di lavorare nel *team* di *Information Risk Management.* Grazie a questa esperienza ho avuto occasione di approfondire il tema della sicurezza informatica e ho appreso l'importanza per le aziende di effettuare controlli su procedure gestionali ed infrastrutture fisiche. Questa esperienza diretta mi ha, inoltre, permesso di venire a conoscenza dei controlli che è necessario attuare al fine di mitigare il rischio di intrusioni indesiderate nel sistema informativo aziendale.

Il tirocinio svolto ha fatto nascere in me interesse per questa tematica e ho quindi deciso di approfondire il tema del rischio informatico, in particolare in ambito finanziario.

Nella prima parte dell'elaborato è stato brevemente introdotto il problema del *cybercrime*, argomento complesso che necessiterebbe un ampio approfondimento. Per continuare, sono state fornite alcune informazioni sui *trend* attuali e descritte le principali tipologie di attacchi informatici con un particolare *focus* sui *malware* ed infine, è stata descritta brevemente la mia esperienza di tirocinio e la sua attinenza al tema del *cybercrime*.

Nel secondo capitolo, dopo aver inquadrato i rischi che caratterizzano il mercato finanziario, l'attenzione è stata concentrata sul rischio operativo, il quale per molto tempo è stato ignorato e sottovalutato a causa della difficoltà di valutazione oggettiva e dell'assenza di una definizione chiara e precisa. Dopo aver introdotto i tre pilasti di Basilea, il capitolo si conclude con una descrizione dei metodi indicati dal comitato per il calcolo del requisito patrimoniale richiesto per far fronte al rischio operativo, con particolare attenzione al *Loss Distribution Approach* che è quello utilizzato per la valutazione del rischio nel presente elaborato.

Nel terzo capitolo è descritta la modalità con cui è stato costruito il *database* sul quale sono state effettuate le analisi, sono state chiarite le ipotesi e le assunzioni fatte, nonché le informazioni contenute. Il capitolo contiene poi analisi sui dati al fine di ottenere una visione d'insieme e di creare alcune statistiche atte a descriverli. Una sezione è stata poi dedicata al calcolo del costo degli attacchi.

Il quarto capitolo tratta i modelli statistici ed include le analisi svolte per indagare eventuali correlazioni nei dati. A tal fine è stato utilizzato il pacchetto *software* statistico STATA creato da *StataCorp*. In seguito, sono individuate le distribuzioni che meglio si adattano a descrivere la frequenza e la severità degli attacchi.

Nel quinto capitolo è dettagliata la simulazione Montecarlo effettuata che, grazie alla distribuzione cumulata fornita in *output*, ha permesso di calcolare il Valore a rischio per il settore finanziario. Infine, è presente un breve cenno *all'Expected Shortfall*, indicatore che permette di colmare le lacune del VaR.

Il Cybercrime

In un mondo in cui la parola d'ordine è "innovazione" e dove tutte le informazioni sono dematerializzate, l'uomo deve fare i conti con il veloce progredire della tecnologia e con le sue conseguenze, positive e negative. La crescita esponenziale di informazioni circolanti e la necessità di una loro gestione rapida ed efficiente ha portato allo sviluppo di strumenti informatici sempre più sofisticati, capaci di gestire la quantità e la complessità di dati e l'interconnessione tra sistemi. Nasce quindi l'era dei *Big Data* in cui alle informazioni personali, ma non solo, è associato un enorme valore economico su cui alcune società basano scelte di *business*. Lo sviluppo della tecnologia informatica ha inevitabilmente comportato lo sviluppo di aspetti "patologici": un valore crescente del mercato è stato accompagnato dalla comparsa di tentativi fraudolenti di impossessarsi di queste informazioni e alla nascita del cosiddetto *cybercrime*.

Nel capitolo è inizialmente introdotto il fenomeno del crimine informatico mediante una sua descrizione, la definizione degli attori coinvolti e la legislazione in vigore, nonché l'esposizione dei *trend* principali osservati nel mondo.

Sono, in seguito, descritte le principali tipologie di attacco ed è affrontato un tema centrale per il settore e nel quale si imbatte chiunque voglia fare un'analisi statistica riguardante il settore, ovvero l'asimmetria informativa che è rispecchiata nella difficoltà di trovare dati dettagliati del fenomeno.

Il capitolo prosegue con una descrizione degli elementi cardine della *cybersecurity* al fine di proteggersi da attacchi informatici e si conclude con una breve descrizione del lavoro di tirocinio svolto presso la società multinazionale KMPG S.p.A. e della sua forte connessione con l'argomento, nonché dell'importanza dei controlli GITC.

1.1 Definizione di Cybercrime

All'interno dell'enciclopedia Treccani, il *cybercrime* è definito come:

> "*Reato nel quale la condotta o l'oggetto materiale del crimine sono correlati a un sistema informatico o telematico, ovvero perpetrato utilizzando un tale sistema o colpendolo […]. Nel primo caso ci si riferisce anche a reati informatici impropri, ossia ai reati comuni previsti dal codice penale o dalla legislazione speciale, che solo incidentalmente vengono commessi mediante l'uso di un computer e della rete […]. Nel caso di un c. perpetrato per colpire un sistema informatico, si tratta invece di reati informatici propri […]. La categoria concettuale dei c. non ha, tuttavia, un significato tecnico preciso dal punto di vista giuridico, poiché, fatta eccezione per la presenza di un sistema informatico o telematico, vi rientrano una pluralità di condotte e beni giuridici protetti estremamente disomogenei."*[1]

Generalmente quando si parla di *cybercrime* ci si riferisce ad una attività criminosa caratterizzata dall'utilizzo abusivo di componenti tecnologiche informatiche, sia *hardware* che *software*.

Il crimine informatico può essere definito come un'attività illecita che coinvolga la struttura della tecnologia informatica e che comprenda:

- l'accesso non autorizzato ad informazioni riservate;
- l'intercettazione attraverso mezzi tecnici di trasmissioni non pubbliche di dati informatici, verso, da o all'interno di un sistema informatico;
- le interferenze di dati (danneggiamento, cancellazione, deterioramento, manipolazione o soppressione di dati informatici);
- i sistemi di interferenza (con il funzionamento di un sistema informatico);
- l'uso improprio di dispositivi;
- il furto di identità;
- le frodi elettroniche.

La grande quantità di condotte che sono racchiuse nella definizione di *cybercrime* rispecchia la complessità del fenomeno e le sue infinite declinazioni. I reati informatici

[1] "Cybercrime", Encicopedia Treccani.

sono un fenomeno molto diffuso ed in continua evoluzione che si può manifestare tramite fenomeni di spionaggio, sfruttamento, intrusione, furto, manomissione o sabotaggio e che può avere origine da molteplici fonti.

1.2 La legislazione

Agli esordi del fenomeno le condanne erano rare a causa della poca conoscenza delle potenzialità degli attacchi e delle possibili conseguenze. L'esigenza di punire questi reati è emersa verso fine degli anni Ottanta, a seguito della crescente migrazione sulle reti informatiche della maggior parte delle attività lavorative e sociali. Oggi attraverso *internet* sono scambiate, in ogni istante, un numero elevatissimo di informazioni con diverse finalità: acquisti *online*, pagamenti, ricerche di informazioni, *chat* con amici e molto altro. Da queste premesse nasce quindi l'esigenza di una tutela *ad hoc*.

Il primo passo concreto verso la legislazione dei reati informatici risale al 13 settembre 1989 quando il Consiglio d'Europa emanò la *"Raccomandazione sulla Criminalità Informatica"* No. R 89(9) all'interno della quale erano discusse le condotte informatiche abusive. I reati vennero divisi in due liste in base al grado di valutazione di questi come più o meno offensivi.

Alla prima lista, detta "*lista minima"*, appartenevano le condotte cui si raccomanda, da parte degli Stati, una persecuzione penale:

- la frode informatica attraverso cui è possibile alterare un procedimento di elaborazione di dati con lo scopo di procurarsi un ingiusto profitto;
- il falso in documenti informatici;
- il danneggiamento di dati e programmi;
- il sabotaggio informatico;
- l'accesso abusivo, ottenuto con la violazione delle misure di sicurezza del sistema;
- l'intercettazione non autorizzata;
- la riproduzione non autorizzata di programmi protetti.

Appartenevano invece alla seconda lista, detta "*lista facoltativa"*, condotte ritenute non eccessivamente offensive ma che richiedevano, allo stesso modo, un'azione giuridica, quali:

- l'alterazione di dati o programmi non autorizzata che non costituisca un danneggiamento;
- lo spionaggio informatico, inteso come la divulgazione di informazioni legate al segreto industriale o commerciale;
- l'utilizzo non autorizzato di un elaboratore o di una rete di elaboratori;
- l'utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto.

Successivamente, in occasione del XV Congresso dell'Associazione Internazionale di Diritto Penale del 1990, emerse la necessità di perseguire, con la stessa severità, i reati previsti da entrambe le liste in egual modo. Nel settembre 1994, le considerazioni effettuate dall'Associazione hanno quindi portato all'aggiornamento, da parte del Consiglio d'Europa, della precedente Raccomandazione con l'ampliamento delle condotte perseguibili penalmente e l'inserimento di due nuovi comportamenti ritenuti criminali: il commercio di codici d'accesso ottenuti illegalmente e la diffusione di *virus* e *malware*.

In Italia, la prima vera normativa contro il *cybercrime* è stata introdotta con la legge 547 del 23 dicembre 1993[2] che ha modificato ed integrato le norme del codice penale e del codice di procedura penale relative alla criminalità informatica.

Nonostante l'inserimento di nuove regole e di sanzioni sempre più severe, il *business* legato al crimine informatico non conosce crisi ed è, al contrario, in netto rialzo, come è evidente dall'aumento di codici maligni riscontrato nel *cyberspazio*. In passato il modo tradizionale di far circolare questi codici erano le *e-mail* ma il progresso tecnologico ha aumentato le modalità di diffusione. Con la diffusione dei *link* dinamici, secondo il Report 2011 sulla sicurezza del "*Web di Blue*", solamente i sistemi di difesa in tempo reale sono in grado di proteggere gli utenti da questo tipo di attacco, riuscendo immediatamente a rispondere dopo aver valutato i contenuti nuovi e sconosciuti e analizzato i *link* dinamici, i quali sono sempre più frequentemente parte degli attacchi *malware*.

[2] Legge 23 dicembre 1993 n. 547, "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

1.3 Cybercriminali e hacker

In gergo comune i due termini "*Cybercriminale*" e "*Hacker*" sono utilizzati come sinonimi per identificare una persona che commette un reato informatico. Esiste tuttavia una differenza tra queste due figure.

- ***Hacker:*** originariamente si intende colui che, grazie ad una buona conoscenza informatica, esplora i dettagli dei sistemi programmabili e sperimenta come ampliarne l'utilizzo. Un *hacker* è colui che utilizza le debolezze dei sistemi per modificarne alcuni aspetti ed estenderne alcune funzionalità per scopi personali o per ottenere notorietà. I sostenitori dell'*hacking* sono motivati da fini artistici e politici, ma spesso sono indifferenti all'utilizzo di mezzi illegali per raggiungerli.

- ***Cybercriminale***: è identificato come colui che attacca privati ed organizzazioni solamente a scopo di lucro, ovvero per ottenere informazioni a cui è associato un valore economico. Spesso il *cybercriminale*, inoltre, non lavora in solitudine bensì fa parte di organizzazioni criminali che agiscono per proprio o per conto di un mandante.

Entrambe queste due figure commettono reati sfruttando strumenti informatici ed individuando le debolezze del sistema; tuttavia la differenza principale tra queste due figure risiede nella motivazione per cui compiono il reato informatico: il primo agisce per notorietà, il secondo per denaro.

L'obiettivo del *cybercriminale* è quello di individuare debolezze nei sistemi informativi e sfruttarle per manomettere, cancellare, modificare o rubare informazioni che poi possono essere rivendute e che hanno un valore economico.

Tuttavia, è importante sottolineare come la figura del criminale informatico "tradizionale" stia evolvendo e acquisendo sempre più identità internazionale. Come riportato nel Rapporto Clusit 2019, gli attaccanti non sono più "*hackers*", o gruppetti (più o meno pericolosi) di "artigiani" del *cybercrime*: sono decine e decine di gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali dotate di mezzi illimitati, stati nazionali con relativi apparati di intelligence e gruppi *state-sponsored* che hanno come obiettivo e campo di battaglia infrastrutture, reti, *server, client*, *device mobili*, oggetti *IoT* e piattaforme *social* su scala globale, 365 giorni all'anno, 24 ore al giorno.

1.4 Le guerre cibernetiche o "Cyber War"

A partire dagli anni 2000 lo *United States Department of Defense* ha evidenziato come il crimine informatico abbia assunto forme che coinvolgono le strategie di politica globale. Oltre agli attacchi di massa finalizzati a sfruttare le vulnerabilità dei *software* comuni, è stato notato un sensibile aumento di attacchi contro le infrastrutture critiche degli Stati: si è dunque passati dal concetto di *cyber attack* a quello di *cyber war*.

Una definizione esaustiva del termine "*Cyber War*" è quella di Carlo Jean e dell'ex ministro Paolo Savona, presa dal loro libro *"Intelligence Economica"*:

> *"La cyberwar include tutte le forme di attacco e di difesa nel cyberspazio. È un'estensione della guerra elettronica nei suoi aspetti sia offensivi (contromisure, intercettazioni, ecc.) che difensivi (contro-contromisure, crittografia, firebreak, ossia sbarramenti per impedire l'accesso alle reti e alle banche dati) e va strettamente coordinata con essa. Può costituire una forma sia autonoma sia ausiliaria di lotta. Ha finalità sia politico-strategiche che economiche. In entrambi i settori, le reti informatiche agiscono come moltiplicatori – e anche come generatori – di potenza economica e militare. […] La cyberwar è estremamente dinamica, rapida e imprevedibile. Annulla il valore della distanza, del tempo e delle frontiere. Rende possibili sorprese strategiche, molto di più quanto esse siano possibili con gli strumenti hard. Può consentire a piccoli gruppi o ad individui singoli collegati in Rete di esprimere una grande potenza e di provocare danni disastrosi"*[3].

Dalla definizione risulta evidente come la digitalizzazione, nata come supporto per la gestione di dati ed informazioni, abbia profondamente modificato la società ed introdotto un nuovo concetto di guerra. In un'epoca in cui il valore delle informazioni è enorme ed in continua crescita appare evidente come il potere si concentri nelle mani di coloro che possiedono i mezzi per governarle. Da un concetto di guerra basato su capitale umano ed armi fisiche si approda ad un concetto molto più ampio, non legato a territori o mezzi di sterminio ma perpetrato con minacce invisibili in grado di attaccare la nuova ricchezza: i dati. Le guerre condotte con questi mezzi tuttavia, non hanno come unico scopo il furto di informazioni. Un attacco ad una infrastruttura nazionale può essere condotto con

[3] Jean, Carlo; Savona, Paolo; (2011), *Intelligence Economica*, Rubbettino, Soveria Mannelli.

l'intento di colpire ed arrecare danno, senza la finalità di carpire informazioni ma con il solo scopo di causare un "*blackout*" e dimostrare la vulnerabilità della vittima.

Il primo episodio di guerra informatica tra Nazioni a livello mondiale risale al 2007 quando la Repubblica d'Estonia è stata protagonista di un aspro confronto politico con la Russia, a seguito della decisione di rimuovere dal centro della capitale Tallinn un monumento al valore militare risalente all'epoca dell'occupazione sovietica. Il fatto, seppure seguito da alcune proteste, non ha determinato alcun evento riconducibile ad azioni belliche convenzionali da parte dell'ex madrepatria russa. Al contrario però il Governo estone è stato oggetto di una massiccia serie di attacchi informatici ad ampio raggio, veicolati mediante tecniche di *Distributed Denial of Service* (DDoS) e diretti verso i sistemi informatici delle istituzioni estoni. L'effetto è stato quello di compromettere quasi totalmente le attività ordinarie e straordinarie pubbliche e private, che consentono lo svolgimento della vita sociale ed economica dello Stato, nel quale le infrastrutture critiche ed i relativi servizi, risultano fortemente interconnessi sul piano delle tecnologie informatiche. Il volume di attacchi registrati e le peculiari modalità di esecuzione hanno rappresentato, per la prima volta, una chiara dimostrazione di come un *cyber* attacco possa trasformarsi improvvisamente in un problema di sicurezza nazionale.

1.5 Alcuni trend del cybercrime

L'adozione di tecnologie sofisticate volte a garantire la riservatezza dei dati e a proteggere i sistemi informativi avanza parallelamente alla ricerca di metodi sempre più raffinati per introdursi illegalmente in tali sistemi e di debolezze da utilizzare per abbattere le difese delle vittime. In questa corsa incessante non esiste una "vittoria" né un'arma che garantisca la sopraffazione dell'avversario: è un processo che richiede continua ricerca e la cui potenziale vittima deve essere in grado di individuare le proprie debolezze prima del nemico, il quale a sua volta, con tecniche nuove e sofisticate, utilizza doti camaleontiche al fine di introdursi nei sistemi informativi.

Il fenomeno della digitalizzazione, in vertiginosa crescita, e l'enorme valore associato alle informazioni custodite su sistemi informativi rende questa lotta sempre più agguerrita e il fenomeno del *cybercrime* in continua crescita.

1.5.1 Numero di attacchi

Ogni giorno, ad ogni ora, migliaia di attacchi informatici vengono perpetrati ai danni di vittime ignare. Nel mondo, in media, viene registrato un attacco grave ogni 5 ore, sebbene i tentativi siamo molto più numerosi. Il Rapporto 2020 sulla sicurezza ICT stilato da Clusit (Associazione Italiana per la Sicurezza Informatica) dipinge uno scenario preoccupante per quanto riguarda le tendenze del numero di crimini informatici.

Lo studio prende in considerazione tutti gli attacchi informatici che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non) avvenuti nel mondo. L'analisi si basa su un campione che al 31 dicembre 2019 è costituito da 10.087 attacchi noti di particolare gravità (di cui 7.284 dal 2014).

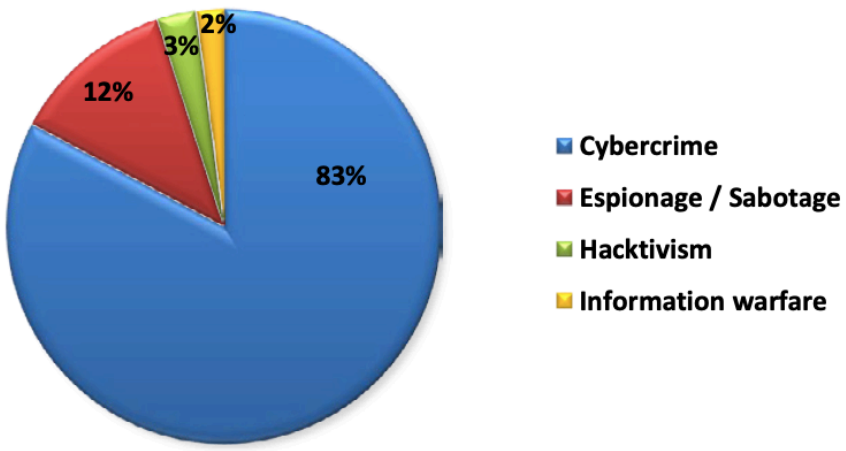
ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Cybercrime	526	684	751	857	1232	1383	12.3%	↑
Hacktivism	236	209	161	79	61	48	-21.3%	↓
Espionage / Sabotage	69	96	88	129	203	204	0.5%	→
Cyber Warfare	42	23	50	62	56	35	-37.5%	↓
Espionage / Sabotage + Cyber Warfare	111	119	138	191	259	239	-7.7%	→
TOTALE	**873**	**1012**	**1050**	**1127**	**1552**	**1670**	**+7,6%**	→

Tabella 1: Distribuzione della tipologia degli attaccanti negli anni considerati (Rapporto 2020 sulla Sicurezza ICT in Italia).

La tabella sopra riportata mostra come, nonostante il campione analizzato includa solamente gli attacchi resi noti pubblicamente (e che quindi rappresentano solo una frazione degli attacchi realmente avvenuti), il numero di reati sia in continua crescita.

Dal campione emerge che, mentre le attività riferibili ad attacchi della categoria "*Hacktivism*" diminuiscono notevolmente (-21,3%) rispetto al 2018, sono in continuo aumento gli attacchi gravi compiuti con finalità di "*Cybercrime*" (+12,3%). Sebbene per le categorie di spionaggio / sabotaggio e Guerre informatiche, considerate singolarmente, si registri rispettivamente un lieve aumento e una diminuzione di casi, si nota una diminuzione del 7,7% rispetto all'anno precedente per la categoria aggregata "*Espionage*

/ *Sabotage / Cyber Warfare*". Infatti, a differenza del passato, risulta oggi sempre più difficile effettuare una netta separazione tra queste tipologie di attacchi e pertanto un'analisi complessiva di questa categoria risulta più accurata. In Figura 1 è mostrata l'incidenza rispetto al totale delle varie tipologie di attacchi.



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

Figura 1. Tipologia e distribuzione degli attacchi nel 2019.

Il numero degli attacchi verificatisi nel 2019 conferma il trend crescente già riscontrato negli anni precedenti. Tuttavia, l'incremento assoluto di casi gravi riscontrati sembrerebbe minore rispetto alle aspettative. La Figura 2 mostra la crescita nel numero di attacchi informatici considerati gravi che sono stati rilevati dal 2014 al 2019 rispetto alla media degli attacchi per anno calcolata nello stesso intervallo di tempo (1214 attacchi di media).

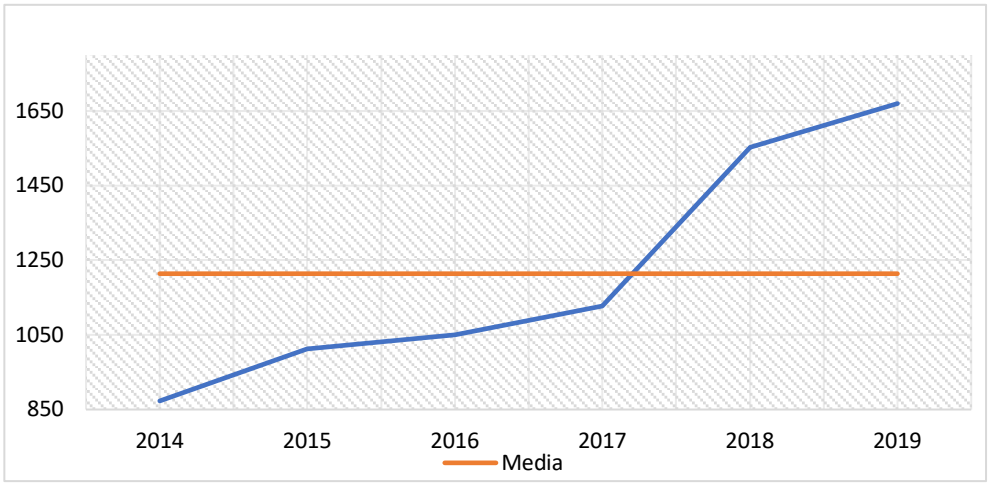


Figura 2. Andamento del numero di attacchi dal 2014 al 2019.

Dalle analisi effettuate dai ricercatori nel Rapporto Clusit emerge che nel corso del 2019 sono stati registrati, in media, 139 attacchi al mese (contro la media di 73 nel 2014) e che i mesi peggiori nel 2019 sono stati luglio ed ottobre con 153 attacchi. In Figura 3 è riportato il numero di attacchi totali, registrati, riportati per ogni mese dalle aziende.

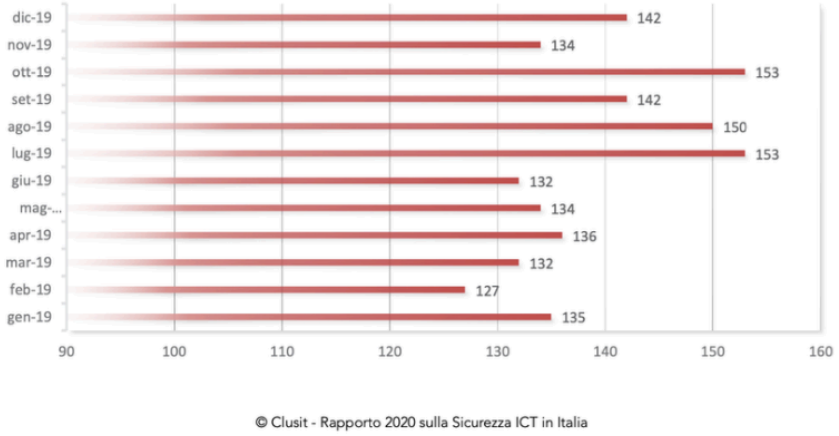


Figura 3. Numero di attacchi per mese nel 2019.

1.5.2 Tipologia e distribuzione delle vittime

Il fenomeno del *cybercrime* è una minaccia quindi molto diffusa e tutte le aziende, indipendentemente dal settore in cui operano, sono potenziali vittime e devono mettere in campo misure volte a prevenire gli attacchi o a ridurne l'impatto. Come emerge dal Rapporto Clusit, nel 2019 le categorie più colpite sono state *Multiple Targets* (con 395 attacchi, registrando un +29,9% rispetto al 2018), *Online Services* (con 247 attacchi, in crescita con +91,5%), *Government* (sebbene questo settore registri un -19,4%, nel 2019 sono stati condotti 203 attacchi contro questa categoria) ed *Healthcare* (186 attacchi, in crescita con un +17%). Il settore *Finance* e *Banking* registra una diminuzione -10,2% di casi. Questo potrebbe in apparenza essere interpretato come un segnale positivo per il settore ma è importante evidenziare come questa categoria può, talvolta, sovrapporsi a quello di "*Online Services*" ed è, in ogni caso, incluso nel settore "*Multiple Target*": per questi motivi la diminuzione di casi riscontrati in ambito *Finance* potrebbe essere "fittizia".

All'interno della categoria "*Multiple Target*" confluiscono i reati commessi contro più settori contemporaneamente ed è posizionata al primo posto per numero assoluto di attacchi a dimostrazione della crescente aggressività degli attaccanti che conducono

operazioni su scala sempre maggiore, con tecniche più raffinate e abbattendo le barriere territoriali.

Al secondo posto si posiziona il settore degli *Online services* / *Cloud* (15% circa), seguito dal settore Governativo (12% del numero totale) e da quello *Healthcare* (11%). Il settore *Fincance* / *Banking* è al quinto posto con il 8% dei casi registrati (Figura 4).

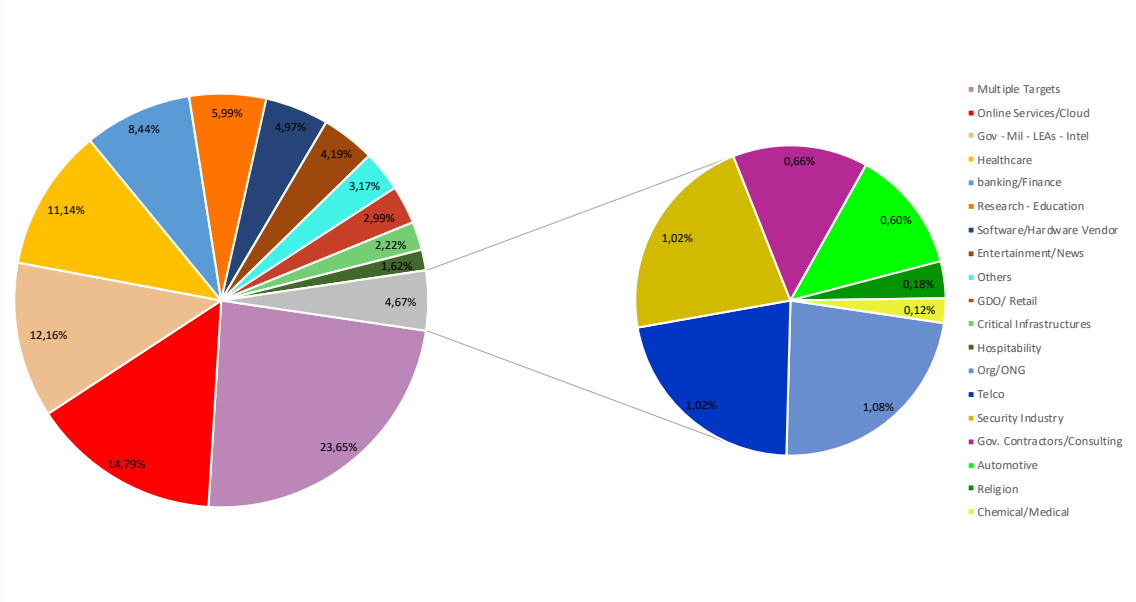


Figura 4. Tipologia e distribuzione delle vittime.

1.6 Data Breach

Un *data breach* rappresenta un incidente nella sicurezza durante il quale si assiste all'accesso, senza autorizzazione, ad informazioni riservate. Il GDPR definisce una violazione di dati personali come:

> *"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati."*[4]

La causa principale di questi eventi sono gli attacchi informatici ma possono anche essere anche conseguenza di errori umani. I *data breach* causati da attacchi *cyber* sono perpetrati al fine di sottrarre informazioni alle vittime e rendere pubbliche le credenziali di accesso

[4] Regolamento Generale sulla Protezione dei Dati, Articolo 4, Comma 12.

degli utenti. A volte può capitare che, in seguito a un attacco nei confronti di un fornitore di servizi, le informazioni personali degli utenti vengano rese note a malintenzionati. Altre volte, invece, un criminale può impossessarsi dei dati di un singolo utente tramite un attacco mirato: la conseguenza, in entrambi i casi, è che gli *account* protetti dalle *password* ormai rese pubbliche non siano più sicuri e che chiunque possa accedervi. Questo tipo di attacchi è solitamente perpetrato attraverso l'uso di *malware* che vengono inviati ai dispositivi della vittima.

1.7 Tipologie di attacchi informatici

Gli attacchi *cyber* sfruttano qualsiasi tipo di vulnerabilità, siano esse presenti nei *software* o nei dispositivi, oppure dipendenti dalla persona che li gestisce o utilizza. Con l'accrescersi della complessità dei siti *Web* e lo sviluppo più rapido delle applicazioni, aumenta anche il rischio di attacchi potenziali. Questi attacchi possono avvenire con diversi mezzi e con modalità che variano a seconda del fine con il quale vengono perpetrati.

Dos e DDos

Il termine DoS (*Denial of Service*) indica un'interruzione di servizio dovuto ad un attacco informatico in cui si colpiscono deliberatamente le risorse di un sistema informatico che fornisce un servizio ai *client*, ad esempio un *sito web* o un *web server*, fino a renderlo non più in grado di erogare il servizio ai *client* richiedenti.

Una versione più aggressiva è il DDoS: l'obiettivo è quello di colpire una risorsa mediante un sovraccarico di traffico proveniente, a differenza del più semplice DoS, da molteplici fonti. Questa tecnica è molto diffusa anche a causa della maggiore probabilità di successo: attacchi provenienti da un gran numero di fonti dislocate rendono questo tipo di attacco molto efficace e di difficile localizzazione. Colpiti infatti da un traffico troppo elevato, i server vengono spenti, con conseguente interruzione del servizio in questione.

Phishing

Con questo termine si indica una truffa realizzata a danno di un utente con l'obiettivo di impossessarsi delle credenziali di accesso ad account di servizi *online*. In particolare, i

malintenzionati sono interessati ad accedere ad *e-mail* personali e conti bancari. Il *phishing* è un'attività che sfrutta il fenomeno di ingegneria sociale e si basa interamente sull'ingenuità e sulla buona fede dell'utente: il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi a cui l'utente è iscritto (banche, *siti web*, *social media*, ecc…). Tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito, l'*username* o la *password* per accedere ad un determinato servizio o altre informazioni personali. Per la maggior parte la truffa è perpetrata attraverso messaggi di posta elettronica, ma sono utilizzati anche altri mezzi quali, ad esempio, i messaggi SMS. Il termine "*phishing*" rimanda al termine inglese "*fishing*", letteralmente "pescare", e richiama la modalità con cui l'utente viene adescato e persuaso a cliccare sul *link* malevolo.

Attacchi tramite cookie

I *cookie* sono dei piccoli file di testo inviati da un sito al computer dell'utente che lo visita. Si tratta di file innocui, che hanno come unico obiettivo quello di identificare l'utente e di eseguirne la profilazione. Questi possono essere impiegati da un *hacker* che può sfruttare alcune vulnerabilità dei siti per intercettare questi *cookie* e utilizzarli per impersonare l'utente: potrebbe così anche riuscire ad appropriarsi di *account* e credenziali di accesso, senza che né l'utente né il sito se ne accorgano.

SQL Injection

La tipologia di attacco informatico nota come *SQL injection* è una tecnica di *code injection*, usata per attaccare applicazioni di gestione dati e siti *Web*, con la quale vengono inserite delle stringhe di codice SQL malevole all'interno di campi di *input* in modo che queste ultime vengano poi eseguite automaticamente. In base al codice inserito, un *hacker* può avere accesso a diverse informazioni, tra le quali le credenziali di accesso degli utenti, o può permettere l'invio del contenuto del *database* all'attaccante all'insaputa della vittima.

Sniffing

Con questa tecnica, malintenzionati esperti possono essere in grado di inserirsi in una rete locale per catturarne il traffico. Questo attacco può essere perpetrato ai danni, ad esempio, di una rete *Wi-Fi* casalinga poco protetta: un *hacker* può collegarsi e utilizzare le debolezze di queste per avere accesso ai vari dispositivi connessi. Gli *sniffer* registrano tutto ciò che incontrano, inclusi i nomi utente e le *password* non criptate, pertanto possono essere sfruttati dai criminali per accedere a qualsiasi *account*.

Doxing e attacchi personali

Un sistema poco sofisticato ma comunque molto efficace per impossessarsi di informazioni personali è quello del *doxing* che consiste nel venire a conoscenza di dati sensibili con metodi non automatici, a volte anche semplicemente chiedendoli con l'inganno ai diretti interessati o effettuando ricerche incrociate su *Web*. Una volta ottenute queste informazioni, un malintenzionato può utilizzarle per impossessarsi degli *account* associati.

Malware

Tra gli strumenti utilizzati per perpetuare un attacco informatico, uno dei mezzi più utilizzati è indubbiamente l'utilizzo di un *malware* o "*Software* malevolo". Con questi termini si indica un programma che viene installato sul computer, solitamente all'insaputa dell'utente, con l'obiettivo di rendere il dispositivo vulnerabile ad altri attacchi. Invasivi e volutamente maligni, questi *software* cercano di invadere, danneggiare o disattivare computer, sistemi, reti e dispositivi mobili, spesso assumendo il controllo delle operazioni del dispositivo. Lo scopo dei *malware* è quello di agire illecitamente a spese degli utenti. Sebbene i *malware* non possano, solitamente, danneggiare gli *hardware* fisici di un sistema o le attrezzature di rete, possono, in ogni caso, rubare, criptare o eliminare i dati, danneggiare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione. I principali vettori di *malware* sono *internet* e le *e-mail*.

Esistono diverse tipologie di *malware*, a seconda della modalità con cui agiscono e dei danni che sono in grado di causare alla vittima. Di seguito sono esposte le tipologie più comuni.

- **Virus**

  Un *virus* è un programma malevolo che ha la capacità di infettare un computer. È un *malware* che necessita dell'interazione da parte dell'utente per essere eseguito ed è in grado di infettare solamente un singolo *host*; questa limitazione ha portato ad una diminuzione del numero di *virus* circolanti, a favore di altre tipologie. Comunemente con il termine *virus* ci si riferisce alla categoria di *malware*, tuttavia esso ne rappresenta una sottocategoria.

- **Ransomware**

  Con il termine *ransomware* è indicata una classe di *malware* che, una volta installati, rendono inaccessibili i dati dei computer infettati e chiedono il pagamento di un riscatto – dall'inglese *ransom* - per ripristinarli. Alcune forme di *ransomware* bloccano il sistema e intimano l'utente a pagare per poterlo sbloccare, altri invece cifrano i file dell'utente chiedendo una somma di denaro per riportare i file cifrati in chiaro (i *virus* di questo tipo sono detti Crypto). I vettori d'infezione più comuni utilizzati dai *ransomware* sono le *e-mail* di *phishing* - nel 75% dei casi - il cosiddetto "*driven-by-download*" (letteralmente "scaricamento ad insaputa") da siti nei quali sono stati introdotti *exploit kit* che sfruttano le vulnerabilità dei *browser*. Si presentano, ad esempio, come *banner* pubblicitari sui quali invitano l'utente a cliccare e attraverso i quali verrà scaricato sul dispositivo il *ransomware*: in questi casi si parla di "*Adware*", ovvero *malware* da pubblicità (dall'inglese "*Advertisement*").

- **Worm**

  A differenza di un *virus*, un *worm*, è un componente *software* dannoso autonomo che si replica per diffondersi in altri computer. Tipicamente un *worm* modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché il computer non viene spento o non si arresta il processo corrispondente. Il *worm* tenta di replicarsi sfruttando la rete *internet* in diverse maniere: spesso i mezzi di diffusione sono più di uno per uno stesso *worm*. Il mezzo più comune utilizzato per la diffusione è la posta elettronica: il programma maligno ricerca indirizzi *e-mail* memorizzati nel computer ospite ed invia una copia di sé stesso come file allegato a tutti (o parte) degli indirizzi che è riuscito a raccogliere. I messaggi contenenti il *worm* utilizzano spesso tecniche di *social engineering* per

indurre il destinatario ad aprire l'allegato. Alcuni *worm* sfruttano dei *bug* di *client* di posta molto diffusi per eseguirsi automaticamente al momento della visualizzazione del messaggio *e-mail*.

- **Logic Bomb**

  Utilizza un codice malevolo nascosto all'interno di un'applicazione ed è eseguita solo al verificarsi di un evento. Classico esempio solo le "*Time Bomb*" che attivano il *malware* solamente dopo un certo periodo di tempo al fine di restare silenti e potersi propagare in altri dispositivi prima di essere individuati.

- **Trojan Horse**

  Il *Trojan Horse* è un tipo di *malware* che si presenta come un *software* utile e apparentemente sicuro che l'utente esegue di sua spontanea volontà ma che in realtà contiene un codice dannoso che crea delle *backdoor* in un sistema, causando solitamente perdita o furto di dati. Questo tipo di *virus* non è quindi in grado di replicare sé stesso ma richiede un'azione diretta dell'aggressore per far giungere il *software* maligno alla vittima che deve eseguire il file malevolo. Spesso i veicoli utilizzati per iniettare ed installare i *Trojan Horse* sui sistemi sono i *Worm*. Gli attacchi APT (*Advanced Persistent Threat*) utilizzano un particolare *Trojan* (RAT) ad accesso remoto per avere un accesso illimitato all'*endpoint*.

- **Spyware**

  Uno *spyware* è un *software* che aiuta a raccogliere informazioni su una persona o un'organizzazione senza che questi se ne accorgano; può monitorare e registrare l'attività eseguita su un sistema di destinazione, ad esempio registrare le pressioni dei tasti (è il caso anche di *malware* detti *Keylogger)*, o raccogliere le informazioni su carte di credito e di altro tipo. Questo tipo di *virus* non gode della capacità di autoreplicarsi e può essere installato sul computer di un ignaro utente sfruttando le consuete tecniche di ingegneria sociale. Molti programmi *open source* su *internet* nascondono in realtà un *malware* di questo tipo: il *software* dunque non è gratuito, ma viene pagato attraverso un'invasione della *privacy* dell'utente, spesso inconsapevole. In alcuni casi, la stessa applicazione che promette di liberare dagli *spyware* ne ha in realtà installato uno o è essa stessa uno *spyware*.

La tipologia di *malware* utilizzata in un attacco informatico differisce quindi a seconda dell'obiettivo del criminale. Tuttavia, alcuni attacchi possono prevedere l'utilizzo di più *malware* contemporaneamente: è il caso di una *botnet*. Quest'ultima è una o rete di *bot* (detta anche armata zombi) composta da un gran numero di computer dirottati da *malware* al fine di raggiungere l'obiettivo prestabilito del criminale informatico che l'ha ideata. Assumendo il controllo di centinaia o perfino migliaia di computer, le *botnet* vengono generalmente utilizzate per inviare *spam* o *virus*, rubare i dati personali o lanciare attacchi DDoS. Sono considerate una delle principali minacce *online* odierne.

Da un'analisi riportata nel Rapporto Clusit 2020 sulla sicurezza ICT in Italia l'utilizzo di *malware* è una delle tecniche più diffuse. Dal grafico seguente si può osservare che tra i *malware* utilizzati negli attacchi informatici, quasi la metà (46%) sono *ransomware*. Di seguito si riporta il dettaglio relativo alle tipologie principali osservate nel campione di attacchi informatici presi in considerazione nel Rapporto Clusit (Figura 5).

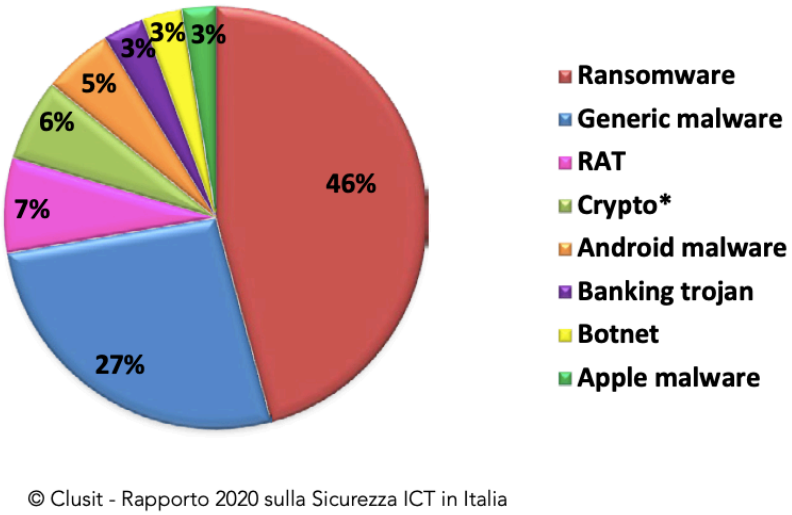


Figura 5. Tipologia e distribuzione malware nel 2019.

1.8 Distribuzione delle tecniche di attacco

Le tecniche di attacco fino a qui elencate possono essere utilizzate singolarmente o in modo aggregato e si diffondono in modi differenti a seconda della debolezza sfruttata (di sistema o umana).

TIPOLOGIA TECNICHE DI ATTACCO	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Malware	127	106	229	446	585	730	24.8%	↑
Unknown	199	232	338	277	408	317	-22.3%	↓
Known Vulnerabilities / Misconfig.	195	184	136	127	177	126	-28.8%	↓
Phishing / Social Engineering	4	6	76	102	160	291	81.9%	↑
Multiple Techniques / APT	60	104	59	63	98	65	-33.7%	↓
Account Cracking	86	91	46	52	56	86	53.6%	↑
DDoS	81	101	115	38	38	23	-39.5%	↓
0-day	8	3	13	12	20	30	50.0%	↑
Phone Hacking	3	1	3	3	9	1	-88.9%	↓
SQL Injection	110	184	35	7	1	1	0.0%	-
TOTALE	873	1012	1050	1127	1552	1670		

Tabella 2. Distribuzione delle tipologie di tecniche di attacco dal 2014 al 2019. (Rapporto 2020 sulla Sicurezza ICT in Italia).

La tabella sopra riportata evidenzia quali siano le tipologie di attacco maggiormente utilizzate dai criminali e, tramite un paragone con il 2018, indica il *trend* riscontrato per ciascuna di esse. Da questa analisi emerge che nel 2019 le tecniche sconosciute (categoria "*Unknown*") si confermano al secondo posto, diminuendo del 22,3% rispetto al 2018, superate dalla categoria "*Malware*", stabile al primo posto per il terzo anno consecutivo, che cresce ulteriormente del +24,8% e rappresenta ormai il 44% del totale.

Al terzo posto è presente la categoria "*Phishing/Social Engineering*" che cresce del +81,9% rispetto al 2018 e rappresenta il 17% del totale.

Le altre tipologie di tecniche di attacco sommate rappresentano nel 2019 solo il 12,3% del totale. Notevole l'incremento percentuale della categoria "*Account Cracking*" (+53,6%), mentre appaiono in diminuzione gli attacchi realizzati sfruttando vulnerabilità note (-28,8%), DDos (-39,5%) e tecniche multiple/APT (-33,7%). Di seguito sono riassunte le percentuali sul totale per le varie tipologie di attacco nel 2019 (Figura 6).

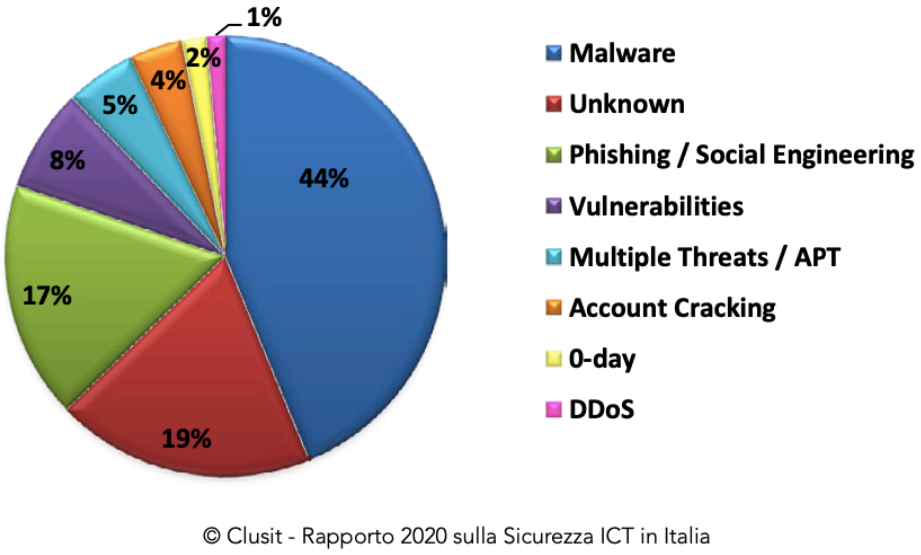


Figura 6. Tipologia e distribuzione delle tecniche di attacco nel 2019.

1.9 Asimmetrie informative

Le asimmetrie informative rappresentano un ostacolo imponente al miglioramento della sicurezza informatica. È molto difficile, infatti, avere un'idea chiara e precisa del panorama dei reati *cyber* che si verificano ogni giorno nel mondo. I dati di cui è possibile disporre sono spesso incompleti e inaffidabili, nonché, nella maggior parte dei casi, riferiti ad attacchi avvenuti molto tempo prima. Questa difficoltà nel reperire informazioni aggiornate è una conseguenza della diffidenza che le aziende hanno nel confessare pubblicamente di essere state colpite da attacco informatico. La capacità dei criminali di analizzare, individuare e sfruttare i punti deboli dei sistemi informativi, nonché la paura delle vittime di una perdita in reputazione, sono tra le principali cause del fenomeno di asimmetria informativa. Un'intrusione di *hacker* all'interno del proprio sistema informativo crea danni non solo fisici ed economici ma soprattutto reputazionali: riconoscere pubblicamente di aver subito un attacco, in particolar modo se questo è riuscito ad infiltrarsi nel sistema, comporta l'ammissione della presenza di una debolezza e quindi può portare ad una maggior diffidenza nei confronti dell'azienda con conseguente minor fiducia da parte dei clienti. Il danno alla reputazione è spesso la vera conseguenza temuta dalle imprese che, dunque, sono restie ad informare l'opinione pubblica e tendono a tenere nascosto l'attacco o a renderlo noto solamente anni dopo. Qualora un'azienda subisca un attacco, la reazione è quella di tentare di nascondere

l'avvenimento e, qualora questo non sia possibile a causa delle enormi dimensioni o di una fuga di notizie, di fornire poche informazioni pratiche sulle modalità con le quali i criminali si sono infiltrati nel sistema: un eccesso di dettaglio potrebbe esporre la società al rischio di nuovi attacchi di criminali che tentano di sfruttare le debolezze ammesse. Questi sono alcuni dei motivi che spingono le aziende a non diffondere informazioni qualora colpite o a diffonderle solamente anni dopo, quando i punti deboli sono stati rafforzati e il sistema reso più resiliente.

Guidati dalla California nel 2002, al fine di ridurre queste asimmetrie informative, 44 Stati americani hanno introdotto una legge sulla notifica delle violazioni della *privacy* secondo la quale gli enti, pubblici e privati, sono tenuti ad informare le persone interessate quando i dati personali sono stati acquisiti da una terza parte non autorizzata. Le leggi sulla divulgazione delle violazioni sono anche progettate per motivare le aziende a salvaguardare i dati personali e a renderle più consapevoli dei rischi derivanti da queste perdite con un conseguente aumento di investimenti in misure preventive. Nella sicurezza informatica infatti, le asimmetrie informative sono presenti anche tra le imprese stesse e non unicamente tra consumatori e imprese: le leggi introdotte negli Stati Uniti hanno come obiettivo la loro riduzione.

In Europa, con l'entrata in vigore nel secondo semestre del 2018 del Regolamento Generale sulla Protezione dei Dati, è stato introdotto, in caso di violazione di dati personali[5], l'obbligo di notifica da parte del titolare del trattamento all'autorità competente. Tale notifica deve contenere descrizione della natura della violazione dei dati personali compromessi, le categorie e il numero approssimativo di interessati coinvolti nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione. Qualora la violazione sia tale da compromettere i diritti e le libertà di persone fisiche, il Regolamento prevede l'obbligo di notifica anche all'interessato senza ingiustificato ritardo.

L'introduzione da parte della Comunità Europea e delle amministrazioni mondiali di norme volte alla divulgazione di casi di reati informativi evidenzia quindi l'interesse mondiale nel garantire trasparenza sia tra le imprese, sia nei confronti dei cittadini.

[5] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, Articoli 33-34.

1.10 Il processo di Digital Transformation

Nel panorama di business odierno i dati sono il nuovo *asset* su cui si fonda il valore di un'azienda. L'ascesa della *data driven economy* sta creando profondi cambiamenti nel tradizionale panorama economico. L'elemento fondamentale su cui si basa la prosperità di un'azienda è la capacità di saper sfruttare questi dati per estrarre il loro valore potenziale. I dati sono importanti poiché possiedono due caratteristiche fondamentali della trasformazione digitale: la velocità e la tracciabilità.

In termini di velocità, la digitalizzazione si diffonde a ritmi esponenziali e pervade sia la vita privata che quella lavorativa delle persone. La tracciabilità è, invece, una caratteristica esclusiva del mondo digitale ed è sicuramente l'aspetto di maggior valore legato ai dati. Questa fa riferimento alla capacità di analizzare i dati per trarne informazioni preziose e non è una caratteristica esclusiva delle aziende più giovani ma, al contrario, agevolerebbe le aziende cosiddette *incumbent* le quali, nel corso degli anni, hanno raccolto quantità infinite di dati e per questo motivo possiedono un grosso potenziale. Tuttavia, per acquistare valore, questi dati devono essere trasformati in informazioni in modo da poter essere utilizzati per compiere scelte strategiche: per questo diventa sempre più importante, per le aziende, saper sfruttare strumenti analitici adeguati.

1.10.1 Il valore dei dati

Alcuni reati informatici, come gli attacchi DDoS, hanno come scopo quello di creare disagio all'azienda e produrre un'interruzione nell'erogazione del servizio. La maggior parte degli attacchi ha però un altro obiettivo altrettanto grave e potenzialmente più pericoloso: il furto di dati. Le informazioni ricercate dai criminali sono quelle personali degli utenti come nome, cognome, *e-mail*, numeri di telefono, indirizzo e generalità. A seconda del settore in cui opera l'azienda poi, sono prese di mira altre tipologie di informazioni.

In attacchi a società finanziarie, ad esempio, sono rubate informazioni quali numeri di previdenza sociale, numeri di conto e informazioni bancarie, mentre per quelle che operano nel settore dei *social media* i dati che interessano sono quelli riguardanti le attitudini e gli interessi dei clienti. Il settore *healthcare* registra un modesto incremento nel numero di attacchi (+17% rispetto al 2018) e le informazioni alle quali sono interessati i criminali sono quelle riguardanti le condizioni di salute dei pazienti e le cartelle cliniche.

Le informazioni che sono state sottratte tramite, solitamente, *data breach* vengono messe in vendita sul mercato nero, il *dark web*, sul quale i venditori offrono "pacchetti" di dati tra cui gli acquirenti possono scegliere a seconda della tipologia. Secondo lo studio "*The Hidden Data Economy*" pubblicato da Intel Security Mcafee Lab il prezzo dei dati varia a seconda delle informazioni che contengono e a seconda del paese. Nella tabella seguente sono riassunti i valori indicati dallo studio.

Tipo di dati	USA	Gran Bretagna	canada	Australia	Unione Europea
Dati Software generated	5-8	20-25	20-25	21-25	25-30
Dati contenenti numero di conto corrente	15$	25$	25$	25$	30$
dati contenenti data di nascita	15$	30$	30$	30$	35$
Dati Fullsize	30$	35$	40$	40$	45$

Tabella 3.Valore in dollari delle informazioni personali sul dark web a seconda delle Nazioni.

In Europa, ad esempio, i prezzi possono oscillare tra i 25 dollari per dati "*software generated*" -contenenti numero identificativo di una carta di credito rubata, la data di scadenza e il codice CVV -e i 45 dollari per dati "*Fullzinfo*"- che includono informazioni su domicilio, numero di previdenza sociale, nome dei familiari ma anche il codice PIN e le credenziali di accesso per *banking online*.

Negli Stati Uniti, Gran Bretagna, Australia e Canada, invece, il prezzo è inferiore. L'acquisizione di dati "*software generated*" negli Usa oscilla tra i 5-8 dollari, contro i 20-25 dollari negli altri paesi mentre i dati "*Fullzinfo*" sono offerti negli USA ad un prezzo appena 30 dollari. Il prezzo aumenta per informazioni riguardanti la geo-localizzazione e disponibilità della carta di credito da un minimo di 110 dollari negli Stai Uniti ad un massimo di 190 dollari in Europa.

La vendita sul mercato nero tuttavia non è l'unico fine degli attacchi che mirano ad un *data breach*. Il valore che può essere estratto dai dati sanitari, ad esempio, potrebbe spingere le compagnie assicurative o farmaceutiche stesse a commissionare il furto. Per comprenderne il motivo è sufficiente pensare al potenziale economico che le informazioni riguardanti la salute dei pazienti potrebbero avere per tali agenzie, che avrebbero così a disposizione una base dati su cui effettuare studi per calcolare i prezzi delle assicurazioni o per lo sviluppo di nuovi farmaci.

1.11 Come proteggersi dagli attacchi informatici

La sicurezza informatica aziendale, o *cyber security*, può essere definita come l'insieme di prodotti, servizi, processi organizzativi e comportamenti individuali che proteggono i sistemi informatici di un'azienda. L'obiettivo è quello di difendere le risorse informatiche da accessi estranei in modo da garantire la sicurezza delle informazioni e dei dati sensibili.

1.11.1 Principi cardine della Cyber Security

La sicurezza informatica si basa su 3 elementi cardine che costituiscono la triade della sicurezza e sono conosciuti con l'acronimo CIA: *Confidentiality, Integrity* e *Availability*.

- ***Confidentiality*** (Confidenzialità): abilità di proteggere i dati da accessi non autorizzati. I metodi più utilizzati per mantenere la riservatezza dei dati sono la crittografia e l'introduzione di rigidi criteri per l'autenticazione come la complessità della *password* o l'impostazione di una data di scadenza minima.

- ***Integrity*** (Integrità): abilità di proteggere le informazioni da modifiche o cancellazioni indesiderate. Per impedire tali azioni senza consenso, nei sistemi informativi devono essere implementati vari livelli autorizzativi che presentino, a seconda della profilazione e del ruolo dell'utente, diverse autorizzazioni ad agire sui sistemi.

- ***Availability*** (Disponibilità): capacità di permettere un accesso sicuro ai dati nel momento del bisogno. Problemi di disponibilità possono essere causati da guasti, errori, *blackout* o cancellazione di dati a causa di attacchi DDoS. Sistemi di *backup* remoto, ridondanza di archivi, *firewall* e gruppi di continuità possono essere utili per mantenere un elevato grado di disponibilità delle informazioni.

Continua evoluzione come arma di prevenzione

Il progresso incessante delle tecnologie informatiche rende impossibile l'individuazione di una soluzione statica capace di evitare e contrastare gli attacchi informatici. Tuttavia, è possibile definire i pilastri su cui una buona strategia di prevenzione deve basarsi: ricerca, dinamismo e versatilità.

- ***Ricerca*** continua di soluzioni all'avanguardia e aggiornate. La base solida per una buona difesa è l'individuazione dei migliori prodotti di *hardware*, *software*, *antivirus*, e strumenti tecnologici e innovativi, senza i quali qualsiasi altro tentativo di protezione risulterebbe vano.

- ***Dinamismo*** e capacità di autoanalisi sono fondamentali per prevenire i possibili attacchi. La società deve essere in grado di individuare i "punti deboli" dei propri sistemi informativi studiando i processi, analizzando le minacce circolanti nel proprio settore e valutando il proprio grado di difesa nei confronti di queste.

- ***Versatilità*** nel pensare in modo innovativo. Fondamentale è la conoscenza del pericolo per potersi difendere. Questo è possibile solo tramite una approfondita analisi delle minacce e dei mezzi con cui si diffondono: pensare come il nemico può aiutare a contrastarlo.

1.12 KPMG e la gestione del rischio

A completamento del mio percorso di studi ho avuto modo di svolgere un'esperienza formativa di tirocinio presso la sede di Torino della nota società di consulenza internazionale KPMG SpA. Durante questo periodo sono stata inserita nel Team IRM – *Information Risk Management* – che si occupa di effettuare verifiche sull'adeguatezza dei controlli IT messi in atto dalle società per mitigare i rischi derivanti da una non adeguata gestione dei processi informativi e che possono avere una ripercussione sul bilancio aziendale. Per la maggior parte delle aziende di *auditing*, infatti, e in particolare per le "*Big Four*", il ruolo dell'IT è cruciale al raggiungimento degli obiettivi di *business*. Nelle aziende, l'utilizzo sempre crescente di sistemi gestionali integrati - noti come *Enterprise Resource Planning* (ERP) – ha come conseguenza il fatto che nell'attività di revisione contabile sia indispensabile avvalersi dell'*Information Technology* (IT). Come è stato evidenziato nel presente lavoro di tesi, infatti, tutte le organizzazioni, non solo finanziarie, sono esposte a minacce volte a minarne la funzionalità o la disponibilità di servizio, al fine di ottenere l'accesso a dati privati riguardanti i clienti o l'azienda stessa. Pertanto, avere risorse specialistiche per l'*Audit* in ambito IT risulta essere fondamentale per lo svolgimento di un'attività accurata di controllo, gestione e mitigazione del rischio.

Information Risk Management (IRM) è la linea di servizi di KPMG dedicata alla valutazione e gestione dei rischi connessi alle tecnologie che supportano i processi di business aziendali.

Il processo di IT *Audit* IRM è delineato mediante le seguenti attività:

- ***Understanding of IT***: prevede una chiara comprensione di come la società utilizzi i sistemi informativi per svolgere la propria attività e di come gestisca i rischi IT.

- ***IT Application Controls* (ITAC)**: attività di controllo che si riferiscono a transazioni e dati individuati essere critici per il rendiconto finanziario aziendale.

- ***General IT Controls* (GITC)**: controlli sui sistemi ERP per valutare l'efficacia operativa degli *IT Application Controls*.

Di seguito, in Figura 7, il processo di revisione individuato dal KAM (KPMG *Audit Methodology*):

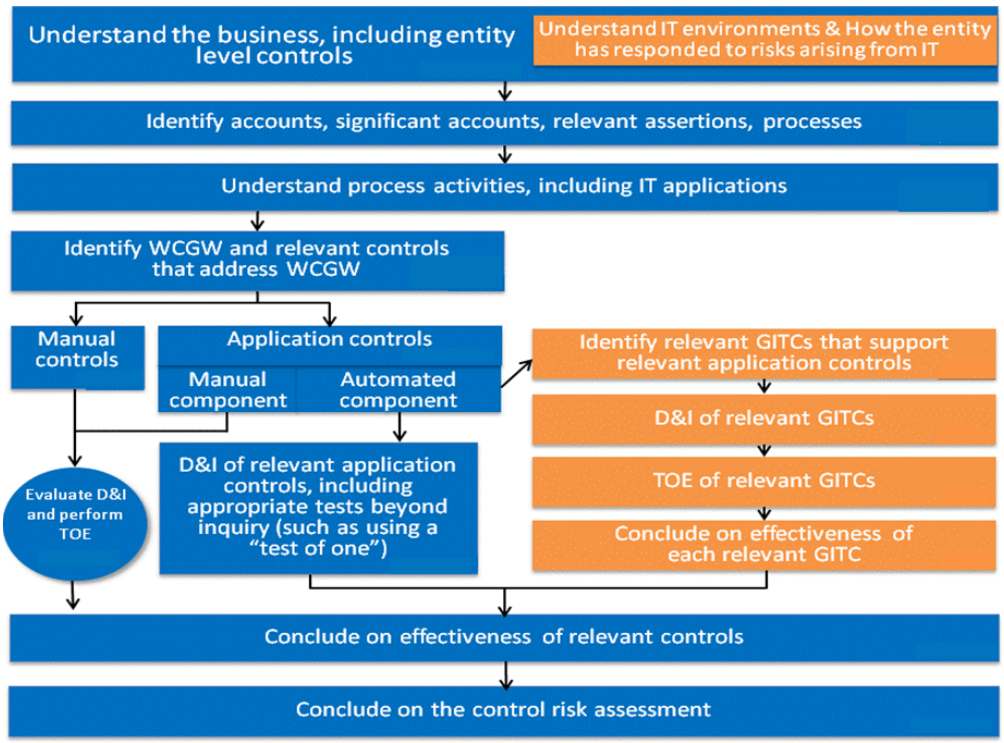


Figura 7. Processo di revisione di KPMG.

Patendo da una fase iniziale di "*Understanding of the business*", che include anche l'IT *Understanding*, in cui vengono identificati e analizzati tutti i processi e le attività rilevanti

per gli scopi della revisione, viene valutata una fase denominata WCGW (*What Could Go Wrong*). WCGW consiste nella revisione di tutti gli aspetti cruciali che potrebbero essere affetti da errore e comportare una esposizione a rischi. Questi rischi, per ogni processo e attività rilevante per il bilancio vengono identificati e analizzati. In base a questi ultimi, verranno svolti i controlli applicativi e i GITC per valutare l'efficacia dei controlli ITAC.

In seguito alla definizione di WCGW si procede con i controlli applicativi (ITAC). Gli ITAC vengono applicati a livello di processo di *business* ed hanno l'obiettivo di garantire l'integrità delle informazioni rilevate per la revisione del bilancio in termini di autorizzazione, completezza ed accuratezza. Successivamente vengono effettuati controlli GITC che tuttavia non forniscono un diretto parere sul bilancio, ma sono finalizzati a garantire che i controlli applicativi identificati funzionino correttamente durante tutto l'anno fiscale (con quindi impatto indiretto sul bilancio).

L'attività da me svolta si è focalizzata sui controlli GITC, ovvero sul controllo dei processi, automatici o manuali, sulla quale la società fa affidamento e che hanno un'influenza, spesso indiretta, sulla redazione del bilancio.

1.12.1 GITC e la gestione del rischio

I controlli generali IT hanno lo scopo di ridurre sia i rischi interni, derivanti da una minaccia interna e legati a comportamenti non idonei intrapresi dal personale aziendale, sia rischi esterni, legati invece alle minacce provenienti dall'ambiente esterno.

Le minacce interne sono rappresentate, ad esempio, da dipendenti scontenti nei confronti della società, che compiono volontariamente azioni contro l'interesse della stessa al fine di danneggiarla, o da negligenze e disattenzioni che quindi, pur essendo involontarie, possono compromettere la sicurezza delle informazioni custodite.

Le minacce esterne, invece, riguardano tutti gli eventi esterni che possono colpire il sistema informativo aziendale e che non possono essere controllati dalla società. Esempi di questo tipo di minacce sono *virus*, *malware*, interruzioni improvvise di corrente, danni alle infrastrutture tecnologiche, ovvero eventi che non dipendono strettamente dall'azienda e che nella maggior parte dei casi non possono essere evitati. Per questi eventi è necessario stabilire delle procedure volte a minimizzarne l'esposizione e l'entità dei danni derivanti.

1.12.2 Minacce interne

Una società stabilisce prassi da seguire per la gestione di processi considerati sensibili. Ad esempio, un controllo debole sull'assegnazione di poteri di amministratore su un applicativo potrebbe, a primo impatto, risultare poco significativo ai fini della mitigazione del rischio *cyber*. Tuttavia, un profilo con ampi poteri amministrativi comporta notevoli privilegi e illimitato accesso alle funzionalità del *software*: dalla creazione di utenze senza necessità di approvazione, alla libera gestione di modifiche applicative, alla modifica diretta di documenti di fatturazione o rendicontazione. Queste azioni, se effettuate da personale non competente o malintenzionato, possono esporre la società a enormi rischi che hanno influenza diretta o indiretta a bilancio. L'infiltrazione di personale non autorizzato può avere come conseguenza un furto di dati, un'interruzione di servizio o un attacco *malware* e possono rappresentare una minaccia interna di cui, senza controlli adeguati, la società può rimanere all'oscuro anche per lungo tempo.

Se si pensa ad un dipendente scontento che viene corrotto da un'azienda concorrente al fine di arrecare danno alla prima, è chiaro come l'assenza di controlli - o la presenza di controlli deboli – possa esporre ad enormi rischi: per il dipendente potrebbe essere facile infiltrarsi nel sistema, ottenere profili amministrativi e rubare o manomettere dati.

Per svolgere controlli GITC adeguati, è necessario analizzare alcuni elementi chiave che possono essere suddivisi in 4 macro-categorie:

1. ***Access to Progams and Data***: i controlli sugli accessi a dati e programmi riducono il rischio di accessi non autorizzati o inappropriati ai sistemi informativi rilevanti per il *financial reporting*. Lo scopo è quello di impedire agli utenti di effettuare o celare eventuali errori o irregolarità e di aver accesso a documenti privati della società.

2. ***Program Changes***: i controlli sono finalizzati ad assicurare che le modifiche ai sistemi e alle applicazioni esistenti siano autorizzate, testate, approvate, implementate e adeguatamente documentate. Lo scopo è quello di prevenire eventuali modifiche non autorizzate che possono comportare danni alla società.

3. ***Program Development***: i controlli hanno il fine di assicurare che i nuovi sistemi, applicazioni o *upgrade* di versioni ai sistemi esistenti sviluppati o acquisiti siano autorizzati, correttamente implementati, testati, approvati, e documentati.

4. ***Computer Operations***: controlli per garantire che le elaborazioni applicative siano appropriatamente autorizzate, pianificate e presidiate, in modo tale che eventuali anomalie nell'erogazione dei servizi siano identificate e risolte.

1.12.3 Minacce esterne

Ogni azienda che si affida ad un sistema informativo risulta esposta a questo tipo di minacce. I GITC permettono di effettuare controlli sull'adeguatezza delle misure messe in atto dalla società al fine di prevenire il verificarsi di attacchi e ridurne il rischio derivante. Le aziende, come abbiamo evidenziato nei capitoli precedenti, adottano procedure di prevenzione e predispongono piani da attuare qualora siano colpite da questi eventi.
Tra le procedure preventive adottate dalle società troviamo:

1. ***Penetration Test*** **(PT):** la società affida ad un'azienda terza specializzata - spesso aziende di consulenza - il compito di effettuare dei tentativi di intrusione nel sistema aziendale. Consiste in una sorta di "bombardamento" del sistema, una simulazione di un attacco informatico verso un determinato obiettivo valutato dalla società come critico o debole.

2. ***Vulnerability Assessment*** **(VA):** rappresenta uno *scanning* dei sistemi informativi effettuato al fine di individuare eventuali debolezze presenti nell'infrastruttura o nella rete IT.

3. **Procedura di aggiornamento *Antivirus*:** consiste in una schedulazione degli aggiornamenti da effettuare (annuali o mensili) da seguire per mantenere costantemente aggiornato il *firewall* a protezione dei sistemi IT.

4. **Procedura di *Backup***: al fine di prevenire perdite di dati che potrebbero essere causate da interruzioni improvvise di corrente o da eventi atmosferici (alluvioni, terremoti, incendi) che danneggiano fisicamente l'infrastruttura tecnologica, l'azienda si dota di una schedulazione (settimanale, giornaliera o oraria) di *backup*.

Il principale piano adottato dalla società per fronteggiare i danni derivanti da eventi esterni traviamo:

- **Piano di *Disaster recovery* (DR):** consiste nella stesura di una serie di azioni e misure da adottare qualora si realizzino eventi che danneggiano il sistema informativo della società o che minaccino la sua regolare funzionalità.

1.12.4 Test GITC

I passi fondamentali per lo svolgimento dei test sui GITC sono:

1. *Test of Design*
2. *Test of Implementation*
3. *Test of Operating Effectiveness*

Queste tre fasi di test consistono nella conferma dell'accuratezza del sistema ERP, con cui viene effettuato il rendiconto finanziario, che utilizza strumenti automatici o manuali con componente automatica e nella formalizzazione delle procedure in uno strumento aziendale *e-Audit* per documentare l'affidabilità e la correttezza delle valutazioni e dei test svolti.

1. Test of Design

Il primo test viene svolto attraverso *Inquiry*, seguito da una valutazione da parte dell'*auditor* sull'efficacia del *design* del controllo nel mitigare i rischi connessi. Per capire il funzionamento e per garantire l'efficacia del controllo è importante avere gli elementi necessari, capire la realtà aziendale ed effettuare delle valutazioni. Questa fase è particolarmente critica perchè un'errata comprensione del controllo o del suo funzionamento può rendere difficile trovare un test che possa verificarne l'efficacia.

2. Test of Implementation

Il test dell'implementazione ha come obiettivo principale una verifica indipendente sul fatto che il controllo, come è stato descritto, sia effettivamente operativo. Pertanto, non è possibile basarsi sull'*Inquiry*, ma sono necessarie altre procedure di *Audit* a supporto. Le procedure che garantiscono maggiore affidabilità sono l'ispezione dei documenti e un'esecuzione indipendente delle procedure o controlli interni della società.

L'obiettivo di questo test non è avere garanzia sull'efficacia durante tutto l'anno fiscale, ma assicurare che il controllo sia effettivamente implementato come descritto. Per questo motivo, si può esaminare un singolo caso per ogni attributo del controllo. Nel caso di controlli automatici, una corretta verifica di implementazione permette di attestare anche l'efficacia operativa.

3. Test of Operating Effectiveness

Il test di efficacia operativa ha come scopo quello di verificare che il controllo, esistente e funzionante, sia completo, accurato e costantemente efficace nel mitigare il rischio. I problemi di "incostanza" del controllo sono comuni soprattutto nei controlli manuali con componente automatica, dove è importante analizzare un campione delle occorrenze del controllo per dare un giudizio.

L'efficacia dei soli GITC fornisce poche o nessuna garanzia sulla correttezza del bilancio, ma hanno un impatto diretto sulla strategia utilizzata per la sua revisione.

È importante precisare che la verifica effettuata da KPMG consiste nel controllare che la politica stabilita in fase di *design* del Controllo della società corrisponda con quella effettivamente attuata, non la sua adeguatezza a prevenire gli eventi sfavorevoli.

1.13 L'importanza dei controlli GITC in società finanziarie

Le società che, per loro natura, sono più sensibili al tema del crimine informatico sono quelle che operano in ambito finanziario. Queste infatti dispongono di un'enorme quantità di dati che hanno un grande valore, sia per sensibilità delle informazioni, sia a causa del valore che andrebbe perso a causa della violazione della loro riservatezza. In un mondo

sempre più informatizzato in cui il valore dei dati è continuamente in crescita, le aziende non possono permettersi di subire un furto.

Durante il mio lavoro di tirocinio ho avuto modo di supportare il *Team* IRM nei controlli per una società in ambito finanziario. In particolare, i controlli hanno riguardato:

- Creazione utenze;
- Cancellazione utenze;
- Controllo di utenti con poteri amministrativi;
- Modifiche applicative;
- Pianificazione ed esecuzione di *backup*;
- Pianificazione ed esecuzione degli aggiornamenti di *Antivirus*;
- *Vulnerability Assessment*;
- *Penetration Test*.

Creazione utenze

I test sui processi autorizzativi seguiti per la creazione di nuove utenze sono di fondamentale importanza per un'impresa finanziaria: un'utenza creata in modo erroneo o con profili non adatti può avere accesso a informazioni riservate o che non sono di sua competenza. Questo può esporre l'azienda a enormi rischi che devono essere mitigati tramite processi autorizzativi ben definiti da seguire prima di poter creare una nuova utenza. È prassi consolidata, per le società finanziarie, effettuare una richiesta formale da parte delle risorse umane via *e-mail* per la creazione dell'utenza con indicazione dei dati del dipendente a cui l'utenza deve essere associata e con una precisazione della profilazione necessaria. In seguito, la richiesta - solitamente a seguito di apertura di *ticket*- deve essere sottoposta ad approvazione da parte dei responsabili e solo dopo è possibile procedere con la creazione. Questo meccanismo di richiesta formale e approvazione è necessario al fine di ridurre il rischio di creazione di utenze senza autorizzazione.

Il *Team* IRM procede, per un numero a campione di utenze create nell'anno, alla verifica della presenza della richiesta e del processo di approvazione, nonché al controllo della corrispondenza tra la profilazione richiesta e quella assegnata all'utenza.

Cancellazione utenze

Per le società è di fondamentale importanza che il personale dimesso non possa più avere accesso al sistema IT dopo che il rapporto lavorativo sia cessato. Se infatti un ex dipendente potesse accedere, avrebbe la facoltà di effettuare modifiche o intervenire sul sistema e questo potrebbe avere ripercussioni molto dannose.

Il *Team* di KPMG procede quindi alla verifica che le utenze appartenenti al personale dimesso siano state cancellate o disabilitate a sistema. Qualora un'utenza non sia stata eliminata o bloccata, la società potrebbe essere esposta a furti di dati, di informazioni o a modifiche non autorizzate.

Controllo di utenti con poteri amministrativi

All'interno di un sistema informativo esistono diversi livelli autorizzativi. Quelli più critici sono i cosiddetti "*Super Users*", ovvero coloro che hanno poteri amministrativi illimitati e possono, quindi, effettuare modifiche al sistema senza necessità di ottenere approvazione. Questi profili sono solitamente concessi al personale amministrativo e ai vertici di un'azienda i quali, rappresentando i massimi vertici nel consiglio di amministrazione, non necessitano di ottenere approvazione prima di effettuare interventi. È quindi fondamentale verificare che questi profili siano attribuiti solamente a personale autorizzato: il *Team* IRM verifica il personale che gode di questa autorizzazione e chiede alla società motivazione dell'attribuzione di tale ruolo.

Modifiche applicative

Un applicativo IT, nel corso del suo funzionamento, può subire interventi manutentivi o di modifica in seguito alla variazione di processi all'interno della società, alla necessità di correggere *bug* o alla richiesta di miglioramenti. Queste modifiche devono essere proposte e approvate prima di poter essere rese effettive. Come per la creazione di una nuova utenza, questo tipo di interventi deve seguire un processo articolato: la richiesta deve essere formalmente avanzata via *e-mail* o tramite apertura di un *ticket* e deve essere approvata e testata su un sistema di prova. Solo a seguito di evidenza del suo corretto funzionamento in ambiente di test, la modifica può essere approvata ed eseguita in quello di produzione.

Il *Team* IRM procede, per un numero a campione di modifiche applicative mandate in produzione durante l'anno, alla verifica della presenza di richiesta, test in ambiente di prova e autorizzazione al passaggio in produzione.

Pianificazione ed esecuzione di Backup

Non tutte le società stabiliscono un piano di *backup* complesso ed articolato: le piccole imprese, spesso, effettuano un *backup* settimanale e non attuano un vero e proprio controllo sull'effettivo svolgimento e sull'esito di quest'ultimo.

Le società finanziare però, attribuiscono a questa procedura una grande importanza: qualora si verifichi un evento che causi un *blackout* o un'interruzione di corrente con una conseguente perdita dei dati presenti sull'infrastruttura fisica IT, è fondamentale disporre di un *backup* recente e aggiornato da poter installare sulle macchine al fine di far ripartire il sistema il prima possibile e con i dati aggiornati. Si pensi, ad esempio, all'enorme quantità di dati che vengono registrati ogni secondo sui sistemi bancari: transazioni di denaro, pagamenti, calcoli di interessi. Queste informazioni risultano di vitale importanza e la loro perdita comporta un danno economico e reputazionale per la società: *backup* frequenti e completi riducono la probabilità di perdere dati e, qualora di verifichi l'evento dannoso, la quantità persa.

Se la società è molto grande, è possibile che per i diversi *server* esistano diverse strategie di *backup*, a seconda dell'importanza dei dati salvati su di esso. Il *Team* IRM richiede alla società l'elenco di macchine attive (solitamente per il *Fiscal Year* per il quale si sta facendo il lavoro di revisione) e procede ad un campionamento di *server* per i quali richiede documentazione della *policy* di *backup* definita e ne verifica la corretta implementazione. Il numero campionato varia a seconda della numerosità di macchine attive. Qualora la società preveda la generazione di *alert* automatici in caso di *backup* con esito negativo, è necessario ottenere l'elenco di questi e, a seguito di un campionamento, richiedere al cliente evidenze della presa in carico di questi *alert* e della loro risoluzione, tramite, a volte, esecuzione di *backup* manuale.

Pianificazione ed esecuzione degli aggiornamenti di Antivirus

Tutte le società sono consapevoli dei rischi derivanti da un *antivirus* debole o non aggiornato: non tutte, però, predispongono un controllo del suo aggiornamento. Per la

maggior parte delle aziende infatti, non è necessario un controllo vero e proprio con cadenza fissata in quanto, con ogni probabilità, disporranno di un unico sistema centrale con un unico *antivirus* per il quale è sufficiente un controllo annuale del suo aggiornamento. In questi casi il *Team* IRM si limiterà a richiedere evidenza del suo aggiornamento. Per le società più complesse invece, dove sono presenti *antivirus* diversi o dove le cadenze degli aggiornamenti sono diverse, è necessario effettuare un controllo. Il *Team* KPMG richiede il piano di aggiornamento e verifica la sua applicazione.

Vulnerability Assessment

Un'azione molto utile che può essere intrapresa per la riduzione dell'esposizione al rischio informatico è, come abbiamo in precedenza, l'analisi delle vulnerabilità interne all'azienda. Questa è effettuata tramite la redazione di *Vulnerability Assessment*. Le piccole società produttive effettuano di rado controlli sull'effettivo svolgimento dei VA (spesso non sono nemmeno previsti) a causa della loro minore complessità e del minore valore economico e reputazionale del danno che può conseguire ad una debolezza nel sistema. Per le grandi aziende invece, soprattutto in ambito finanziario, i VA sono di vitale importanza per la scoperta di eventuali vulnerabilità presenti nei sistemi e pertanto l'azienda adotta dei controlli interni per monitorarne lo svolgimento.

Il *Team* KPMG, dunque, prende inizialmente visione delle attività di *Vulnerability Assessment* pianificate per l'anno e richiede alla società, per alcuni di essi, documentazione ad evidenza del loro svolgimento. Grazie a questo controllo il *Team* può verificare che i VA pianificati siano stati correttamente eseguiti, rileva i ritardi nelle attività e chiede giustificazione alla società, la quale deve fornire una solida motivazione a supporto dell'eventuale ritardo. L'azienda, dopo aver preso coscienza delle debolezze presenti nei sistemi informativi provvederà a colmare le carenze e a predisporre dei piani per far fronte alle debolezze emerse durante il VA.

Penetration Test

Il secondo strumento utilizzato dalle aziende per testare la resistenza dei propri sistemi informativi è il *Penetration Test*. Anche questo strumento è usato prevalentemente dalle aziende più strutturate e che gestiscono una grande quantità di dati sensibili. La maggior parte delle società prevedono un piano di PT ma non un controllo: stilano un programma

temporale da seguire ma non monitorano che sia effettivamente rispettato. Il compito di KPMG è quello di verificare che i test siano stati effettuati in linea con la programmazione e che le criticità emerse dei sistemi informativi siano state evidenziate e riferite al personale addetto.

Il rischio operativo

La gestione del rischio è un elemento centrale nell'intermediazione finanziaria e ha come scopo quello di identificare, definire, valutare, quantificare e gestire il rischio. Il rischio è l'elemento su cui si fonda l'attività finanziaria e che ne giustifica l'importanza. Esistono diverse tipologie di rischi che spaziano da quelli più tradizionali, come il rischio di mercato e quello di credito, ad altri più recenti su cui il sistema finanziario si è focalizzato solo negli ultimi anni, come il rischio operativo. I primi due rischi sono considerati "propri" del sistema bancario, in quanto riguardanti caratteristiche intrinseche del settore, mentre il terzo può essere considerato un rischio "collaterale" dal momento che la banca non intende volontariamente assumerlo ma è costretta a causa della natura stessa della sua attività. Molte delle crisi che hanno colpito gli intermediari finanziari sono state originate da un rischio operativo gestito in modo inadeguato o, in alcuni casi, addirittura ignorato.

Nel presente capitolo è inizialmente definito il concetto di rischio e la suddivisione nelle tre tipologie di rischio che caratterizzano il sistema finanziario. In seguito, sono descritte le peculiarità del rischio operativo attraverso un breve cenno sulla sua regolamentazione e con un *focus* sulle cause. Infine, sono esposte le principali modalità di calcolo del requisito patrimoniale richiesto alle banche per fronteggiare tale esposizione al rischio.

2.1 Definizione di rischio

Le aziende sono esposte alla probabilità che si verifichino eventi che possono essere positivi, e quindi agevolare la produttività e aumentare i margini di guadagno, o dannosi, con conseguenti problemi anche notevoli. Questi eventi possono dipendere da numerose cause, sia naturali che artificiali, coinvolgendo beni, persone o infrastrutture. Al fine di prendere precauzioni, soprattutto per fronteggiare gli eventi dannosi, è nata la necessità di identificare, definire, valutare, quantificare e gestire tali eventi: questo ha portato alla nascita del *Risk Management*.

È stato quindi introdotto il concetto di rischio, inteso come l'eventualità di subire un danno connessa a circostanze più o meno prevedibili.

Nell'analisi del rischio, fenomeni complessi e aleatori si traducono in espressioni numeriche che non hanno un valore concreto e applicabile ma risultano utili per valutare la portata degli effetti derivanti. La formula comunemente usata per quantificare l'esposizione al rischio (*Risk Exposure*) è la seguente:

$$R = P * I$$

Dove:

R = *Risk Exposure,* considerato una quantificazione del rischio;

P = probabilità che possa concretizzarsi il rischio R sulla base degli elementi di rischio individuati;

I = effetto del danno (o opportunità) conseguente al concretizzarsi del rischio R.

Il *Risk Exposure* rappresenta un metodo quantitativo della valutazione del rischio e fornisce un valore indicativo (e non reale) utile ai fini del *ranking* dei rischi.

L'esposizione al rischio può anche essere calcolata in modo qualitativo applicando una scala di livelli sia per la probabilità (molto alta, alta, media, bassa, molto bassa) sia per l'impatto. Questo metodo permette di individuare una matrice grazie alla quale, indicando il livello di probabilità e di impatto di un evento, è possibile effettuare una valutazione dell'esposizione al rischio R. In Figura 8, la combinazione dei valori probabilità e impatto permette di suddividere i rischi assegnando loro un livello di bassa, media o alta priorità (BP, MP, AP).

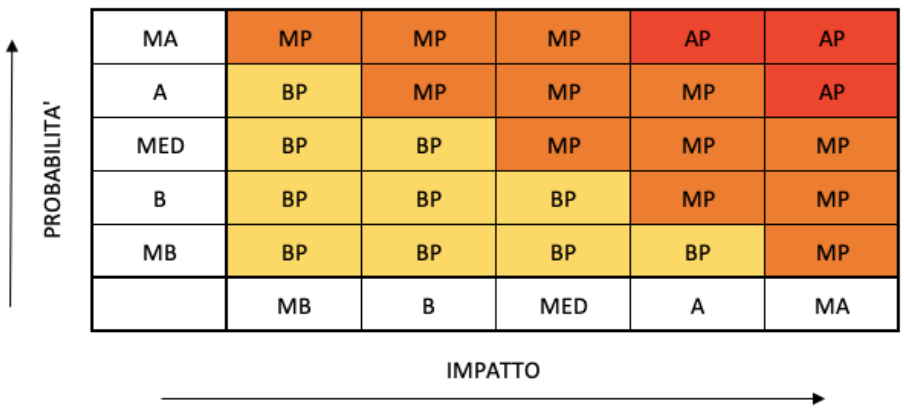


Figura 8. Matrice di valutazione qualitativa del rischio per i valori molto alto (MA), alto (A), medio (MED), basso(B), molto basso (MB).

Il rischio è correlato all'attività dell'azienda e al settore di appartenenza e può essere di diverso tipo:

- **Rischio strategico**, correlato al modo in cui l'organizzazione è gestita e alle scelte di indirizzo strategico (scelta di concorrenti, sviluppi di nuovi prodotti, ecc…);

- **Rischio finanziario**, che include il credito, l'esposizione sul mercato e la liquidità;

- **Rischio operativo**, che riguarda gli aspetti legati all'operatività di un'azienda.

Quest'ultimo si è rivelato di particolare importanza a seguito del rapido sviluppo dei sistemi informativi aziendali ed è quello su cui verrà concentrata l'attenzione nel presente elaborato.

2.2 Definizione di rischio operativo

La ricerca di un'adeguata definizione del concetto di rischio operativo rappresenta il punto di partenza per la sua comprensione. Non esiste, tuttavia, una definizione univoca e per molto tempo le banche hanno ignorato l'esistenza di questa tipologia di rischio o, qualora riconosciuto, hanno adottato definizioni proprie aziendali riportate nei bilanci. L'individuazione di una descrizione universalmente riconosciuta ha rappresentato un problema di difficile soluzione a causa della difficoltà nell'individuare le caratteristiche e i fattori da cui si origina questo particolare rischio.

Originariamente, nella classificazione dei rischi, la Banca d'Italia aveva incluso quelli operativi nella categoria "altri rischi" identificandone le cause in inefficienze nelle procedure, controlli inadeguati, errori umani e tecnici, eventi imprevisti, la cui natura - interna o esterna - non veniva specificata. Analogamente l'Associazione Bancaria Italiana aveva adottato una posizione "residuale" parlando di rischi operativi ma definendoli come rischi che non possono essere configurati come di credito e di mercato, con l'esclusione del rischio strategico e di *business*.

Le prime pubblicazioni della BIS (*Bank for International Settlements*) raggruppavano le definizioni di rischio operativo date dai vari Istituti bancari e lo definivano come[6]:

- qualsiasi rischio non classificato come rischio di mercato o di credito;
- il rischio di perdita derivante da vari tipi di errore umano o tecnico;
- rischio di regolamento e pagamento o interruzione di attività;
- rischi amministrativi e legali;
- rischio tecnologico.

La svolta nella definizione del rischio operativo si ebbe con la proposta della *British Bankers Association* (2001) che fu adottata dal Comitato di Basilea con la diffusione del *New Basel Capital Accord* (o semplicemente Basilea II) nel 2004 ed in seguito anche dalla Banca d'Italia. Con questa *regulation* il rischio operativo è definito non più in modo "residuale" ma in "positivo" come:

> *"Il rischio di subire perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni."*[7]

A differenza delle altre tipologie di rischi, che sono legate ad una particolare attività, il rischio operativo è insito in tutte le unità organizzative e rappresenta un aspetto trasversale all'interno del *business* di un'azienda. La peculiarità di questo rischio è quella di essere intrinseco alle attività stesse a causa della dipendenza da fattori che la società non può controllare direttamente ma sono conseguenza implicita e diretta delle procedure adottate. Questa caratteristica del rischio operativo che lo rende "invisibile" ad una prima analisi di *Risk Management* è la motivazione per cui per molto tempo gli Istituti finanziari non hanno tenuto conto del suo impatto. Tuttavia, a seguito di numerose perdite causate da eventi esterni non ricollegabili direttamente al rischio di mercato o di credito e della forte spinta del Comitato di Basilea è nata la consapevolezza dell'importanza dei rischi operativi nel settore finanziario, dando origine ad un sistema di implementazione di *Operational Risk Management*.

[6] Basel Committee on Banking Supervision, Operational Risk Management, Bank for International Settlements, Basel, September 1998, p. 3

[7] Basel Committee on Banking Supervision, Consultative Document: Operational Risk, Bank for International Settlements, Basel, January 2001, p. 120.

2.3 Caratteristiche del rischio operativo

Il rischio di credito e quello di mercato sono assunti volontariamente e consapevolmente dagli Istituti finanziari al fine di ottenere un ritorno economico e sono i pilasti su cui è fondata la loro attività. I mezzi usati per gestire questi rischi portano però inevitabilmente la banca a dover far fronte al rischio operativo che è una conseguenza naturale ed inevitabile delle organizzazioni.
Esistono due tipologie di rischio ai quali tutti vengono ricondotti: i rischi speculativi e i rischi puri.

- **Rischi speculativi**: sono così definiti i rischi che hanno la caratteristica di essere simmetrici, ovvero quelli che possono potenzialmente avere sia effetti positivi sia negativi per l'azienda e possono essere ridotti attraverso la diversificazione di portafoglio. I rischi di mercato e di credito appartengono a questa categoria.

- **Rischi puri**: sono rischi che colpiscono il patrimonio o la persona e non originano utili o perdite a seconda di come si manifesta il rischio ma solamente perdite. Il danno derivante da questa tipologia di rischio non può essere ridotto tramite diversificazione o trasferimento a terzi ma solamente con il ricorso a polizze assicurative. Il rischio operativo rientra in questa categoria.

Il rischio operativo, inoltre, possiede caratteristiche che lo rendono un rischio:

- **Idiosincratico:** le perdite derivanti sono riconducibili a fattori specifici riguardanti la singola banca e non fattori generali del mercato finanziario. Tutto il settore bancario è infatti esposto al rischio operativo ma il verificarsi di una perdita ad un attore finanziario denota una carenza nel suo particolare apparato difensivo e non in quello generale del settore.

- **Non sistemico:** i fattori specifici di rischio possono mettere a repentaglio la sopravvivenza della banca, ma non producono effetti di contagio con le altre componenti del sistema bancario. La perdita subita da un attore non "contagia" il settore nel suo complesso.

2.4 Il Comitato di Basilea e il rischio operativo

Il Comitato di Basilea per la Vigilanza Bancaria (CBVB) è un'organizzazione internazionale che opera sotto il patrocinio della Banca dei Regolamenti Internazionali (BRI), ovvero la più antica istituzione finanziaria internazionale. Istituito alla fine del 1874 dalle Banche Centrali dei dieci paesi più industrializzati (G10), riunisce oggi partecipanti da Belgio, Canada, Francia, Germania, Italia, Giappone, Lussemburgo, Paesi Bassi, Spagna, Svezia, Svizzera, Regno Unito e Stati Uniti e da altri 14 Stati del mondo. Il Comitato ricopre un ruolo fondamentale nel rafforzamento della sicurezza a della stabilità finanziaria delle banche attraverso la definizione di linee guida per le tecniche di valutazione e di gestione dei rischi a cui le banche sono soggette. Il CBVB non ha capacità di regolamentazione autonoma ma i paesi che vi aderiscono sono implicitamente vincolati agli accordi raggiunti.

Nonostante le prime pubblicazioni risalgano al 1988, solamente nel 1998 con l'accordo conosciuto come "Basilea II" emerge l'attenzione del Comitato per il Rischio Operativo. L'accordo, emanato in versione definitiva nel 2004, contiene i primi riferimenti espliciti ai requisiti di capitale necessari per fronteggiare il rischio operativo e impartisce istruzioni dettagliate sui metodi per calcolare la quota parte di capitale che gli istituti bancari devono destinare per fronteggiare il rischio operativo.

2.5 Fattori di rischio

Il Comitato di Basilea II ha inserito tra i suoi obiettivi l'introduzione di un requisito patrimoniale specifico per il rischio operativo. A tal fine è risultata utile l'ideazione di uno schema analitico per la misurazione e gestione del rischio stesso e l'analisi dei fattori da cui esso deriva. Il Comitato ha quindi individuato gli elementi ritenuti apportatori di perdite operative riconoscendoli, da un lato, negli errori interni alle aziende e, dall'altro, in eventi esterni non riconducibili propriamente alla banca.
Con riferimento alla classificazione del rischio operativo, sono stati individuati quattro fattori principali scatenanti:

- **Processi**
  Quest'area di rischio è strettamente legata ad una inadeguata formalizzazione di *policy* e procedure interne, a insufficienti controlli interni e ad una gestione poco

rigorosa dell'assegnazione di ruoli a personale aziendale. Controlli interni deboli possono causare errori nella gestione di strumenti finanziari e nell'allocazione di ruoli e responsabilità (*Settlement Error*) o carenze nei sistemi di *Risk Management* con conseguente stima poco precisa dei modelli di rischio ed errori nell'applicazione di metodologie (*Model Risk*). Altre conseguenze possono riguardare errori nelle procedure di calcolo, contabilizzazione e registrazione che possono generare *output* fuorvianti su cui sono basate decisioni del *management* (*Transaction Risk*).

- **Sistemi informativi**

  Questa categoria di rischio fa riferimento a problemi di natura tecnica connessi ai sistemi informativi come la mancata disponibilità, l'inefficienza o il malfunzionamento. Gli eventi rischiosi riguardano guasti di *hardware* e *software* (errori nelle procedure informatiche), accessi non autorizzati al sistema informativo interno, sia causati da *hackers* sia come conseguenza di errore umano e perdita di dati (*data breach*). Includono inoltre alterazioni di *database* o indisponibilità del sistema, dovuta ad attacchi informatici, a problemi di connessione o a seguito di interruzioni di energia elettrica ricollegabili alla società. Tipici di questa categoria sono anche errori nell'elaborazione di dati dovuti ai sistemi informativi carenti della banca o ad errori nella programmazione delle applicazioni.

- **Fattori umani**

  Eventi connessi a questa categoria possono generare perdite riconducibili ad incompetenza, negligenza o mancanza di esperienza del personale addetto, ovvero a frodi, collusioni, violazioni di leggi e normative internazionali, regolamenti interni e standard etici o ad altre attività criminali.

- **Eventi esogeni**

  A questa categoria sono ricondotti i danni derivanti da situazioni non sotto controllo diretto della società quali le calamità naturali (terremoti, incendi, inondazioni, ecc…), modifiche alla regolamentazione, furti, vandalismi, interruzione di corrente ad opera del fornitore o qualsiasi evento che impatti sull'azienda per cause esterne.

L'assetto regolamentare di Basilea II ha introdotto una classificazione degli eventi che generano perdite operative al fine di facilitare la raccolta dei dati e la gestione del rischio. Il comitato ha quindi stilato un elenco di 7 classi di eventi (*Event Types*) che risultano essere causa di una perdita operativa.

- **Frode interna *(Internal fraud)***: perdite dovute ad attività non autorizzate, frodi, violazione di leggi, regolamenti o direttive aziendali in cui sia coinvolto personale interno alla società (*insider*);

- **Frode esterna *(External fraud)*:** perdite dovute a frodi o violazione di leggi da parte di soggetti esterni alla società (*outsider*);

- **Rapporto di impiego e sicurezza sul lavoro *(Employment practices & workplace safety)***: perdite derivanti da atti non conformi agli accordi in materia di impiego, salute e sicurezza sul lavoro, da episodi di discriminazione o di mancata applicazione di condizioni paritarie tra il personale dipendente;

- **Clientela, prodotti e prassi operative *(Clients, products & business pratics)***: perdite derivanti da inadempienze di obblighi nei confronti di clienti o non conformità del prodotto o servizio fornito;

- **Danni ad attività materiali *(Damage to physical assets)***: perdite derivanti da eventi esterni non sotto il controllo diretto della società, quali catastrofi naturali, terrorismo, atti vandalici o eventi esogeni;

- **Interruzioni dell'operatività e disfunzioni dei sistemi informatici *(Business disruption & system failures)*:** perdite dovute ad interruzioni dell'operatività che causano blocchi alla produzione o all'erogazione di servizi;

- **Esecuzione, consegna e gestione dei processi *(Execution, delivery & process management)***: perdite dovute a gestione dei processi non conforme o a relazioni commerciali con fornitori e clienti non adeguata.

In Tabella 4 è riportato l'elenco degli *Event Types* con le relative descrizioni ed alcuni esempi di attività rientranti in ciascun gruppo, così come proposto dall'autorità regolamentare nel 2003.

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.	Unauthorised Activity	Transactions not reported (intentional) Trans type unauthorised (w/monetary loss) Mismarking of position (intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account take-over / impersonation / etc. Tax non-compliance / evasion (wilful) Bribes / kickbacks Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery Check kiting
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee Relations	Compensation, benefit, termination issues Organised labour activity
		Safe Environment	General liability (slip and fall, etc.) Employee health & safety rules events Workers compensation
		Diversity & Discrimination	All discrimination types
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etc.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender Liability
		Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
		Product Flaws	Product defects (unauthorised, etc.) Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activities	Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage / disruptions
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model / system misoperation Accounting error / entity attribution error Other task misperformance Delivery failure Collateral management failure Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing Legal documents missing / incomplete
		Customer / Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty misperformance Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing Vendor disputes

Tabella 4. Classificazione degli Event Types. (Basel Committee on Banking Supervision, The New Basel Capital Accord, Bank for International Settlements, Basel, April 2003, p 203)

All’interno delle tipologie di evento, le perdite sono poi attribuite alle aree operative da cui hanno origine gli eventi che generano perdite. Le aree interessate da possibili perdite operative sono:

- *Corporate Finance;*
- *Negoziazioni e vendite (Trading & sales);*
- *Retail Banking;*
- *Commercial Banking;*
- *Pagamenti e regolamenti (Payment &Settlement);*
- *Gestioni fiduciarie (Agency Services);*
- *Asset Management;*
- *Intermediazione al dettaglio (Retail Brokerage).*

La Tabella 5 riporta l’elenco delle *Business Line* e i gruppi di attività in ognuna di esse ricompresi, così come proposto dall’autorità regolamentare nel 2003.

Level 1	Level 2	Activity Groups
Corporate Finance	Corporate Finance	Mergers and Acquisitions, Underwriting, Privatisations, Securitisation, Research, Debt (Government, High Yield), Equity, Syndications, IPO, Secondary Private Placements
	Municipal/Government Finance	
	Merchant Banking	
	Advisory Services	
Trading & Sales	Sales	Fixed Income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage
	Market Making	
	Proprietary Positions	
	Treasury	
Retail Banking	Retail Banking	Retail lending and deposits, banking services, trust and estates
	Private Banking	Private lending and deposits, banking services, trust and estates, investment advice
	Card Services	Merchant/Commercial/Corporate cards, private labels and retail
Commercial Banking	Commercial Banking	Project finance, real estate, export finance, trade finance, factoring, leasing, lends, guarantees, bills of exchange
Payment and Settlement[154]	External Clients	Payments and collections, funds transfer, clearing and settlement
Agency Services	Custody	Escrow, Depository Receipts, Securities lending (Customers) Corporate actions
	Corporate Agency	Issuer and paying agents
	Corporate Trust	
Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
	Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open
Retail Brokerage	Retail Brokerage	Execution and full service

Tabella 5. Classificazione delle Business Line. (Basel Committee on Banking Supervision, The New Basel Capital Accord, Bank for International Settlements, Basel, April 2003, p 199)

Il Comitato di Basilea ha effettuato un'analisi utilizzando le osservazioni raccolte per le principali banche, partecipanti su base volontaria, al fine di individuare le linee operative maggiormente colpite.

	Internal Fraud	External Fraud	Employment Practices & Workplace Safety	Clients, Products & Business Practices	Damage to Physical Assets	Business Disruption & System Failures	Execution, Delivery & Process Management	All	Business Line Loss Amount as Percent of Total
Corporate Finance	6.6	3.2	16.2	2,565.1	0.1	0.6	146.7	2,738.5	28.0%
	0.2%	0.1%	0.6%	93.7%	0.0%	0.0%	5.4%		
Trading & Sales	145.8	4.5	30.3	384.7	2.7	23.8	732.6	1,324.4	13.6%
	11.0%	0.3%	2.3%	29.0%	0.2%	1.8%	55.3%		
Retail Banking	198.5	607.9	305.6	1,263.6	34.0	48.0	670.6	3,128.0	32.0%
	6.3%	19.4%	9.8%	40.4%	1.1%	1.5%	21.4%		
Commercial Banking	84.7	112.8	23.1	262.4	3.3	12.7	241.2	740.2	7.6%
	11.4%	15.2%	3.1%	35.5%	0.4%	1.7%	32.6%		
Payment & Settlement	7.1	18.1	2.3	18.7	8.0	5.8	194.4	254.4	2.6%
	2.8%	7.1%	0.9%	7.3%	3.2%	2.3%	76.4%		
Agency Services	2.5	8.1	1.7	92.3	46.7	15.4	89.8	256.5	2.6%
	1.0%	3.2%	0.7%	36.0%	18.2%	6.0%	35.0%		
Asset Management	27.0	2.3	6.1	74.9	0.6	3.6	128.3	242.9	2.5%
	11.1%	1.0%	2.5%	30.8%	0.3%	1.5%	52.8%		
Retail Brokerage	89.8	6.7	31.1	294.6	0.4	1.0	71.5	495.1	5.1%
	18.1%	1.4%	6.3%	59.5%	0.1%	0.2%	14.4%		
Unallocated	38.5	16.3	167.1	166.8	38.3	7.6	154.0	588.5	6.0%
	6.5%	2.8%	28.4%	28.3%	6.5%	1.3%	26.2%		
All	600.5	780.0	583.4	5,123.1	134.0	118.4	2,429.2	9,768.5	100.0%
	6.1%	8.0%	6.0%	52.4%	1.4%	1.2%	24.9%		

Note 1. Losses of € 20,000 or more in the stable dataset.
Note 2. First row for each business line: Sum of annualised loss amounts.
Note 3. Second row for each business line: Distribution of loss amounts across event types.

Tabella 6. Somma e distribuzione delle perdite annuali (Milioni di euro) per Event Type e Business Line. (Basel Committee on Banking Supervision, Results from the 2008 Loss Data Collection Exercise for Operational Risk, Bank for International Settlements, Basel, Luglio 2009, p 7)

La Tabella 6 raccoglie, per *Event Type* e *Business Line*, le distribuzioni degli eventi nel 2009. Come si può notare la *Business Line* che risulta maggiormente colpita da perdite operative risulta essere quella del *Retail Banking,* seguita *Corporate Finance*.

2.5 I tre "pilastri dell'accordo di Basilea II"

Il secondo accordo di Basilea pone tra gli obiettivi quello di indicare i metodi di valutazione della quota parte di capitare da destinare alla gestione del rischio operativo. La mutevolezza dello scenario informatico richiede però l'introduzione di metodologie che permettano di gestire la dinamicità del settore e monitorarne gli sviluppi. Per questo motivo si è rivelato fondamentale il dialogo con gli attori del settore finanziario al fine di comprendere le novità e prendere provvedimenti adeguati. Il documento emanato dal Comitato si base su tre "pilastri":

- **Primo Pilastro - Requisiti patrimoniali minimi:** fa riferimento ai requisiti patrimoniali minimi richiesti per fronteggiare il rischio di mercato, di credito e operativo. Il calcolo si basa sulla definizione di patrimonio di vigilanza e di attività ponderate per il rischio.

- **Secondo Pilastro - Processo di controllo prudenziale:** stabilisce i principi fondamentali del controllo prudenziale, le linee guida per la gestione del rischio e gli *standard* di riferimento del controllo di vigilanza da parte degli Istituti preposti. L'accordo prevede che le aziende possano in autonomia definire le strategie di *business* e gestione del rischio ma conferisce alle Banche Centrali la discrezionalità di valutare l'adeguatezza patrimoniale delle banche e il potere di imporre una copertura superiore ai requisiti minimi qualora non siano adeguatamente considerate le particolari caratteristiche dei mercati in cui rientrano.

- **Terzo Pilastro - Disciplina di Mercato:** sezione contenente le disposizioni per i requisiti minimi in materia di trasparenza informativa tra le banche. Lo scopo del terzo pilastro è quello di integrare i requisiti patrimoniali minimi (primo pilastro) e il processo di controllo prudenziale (secondo pilastro).

2.6 Il requisito patrimoniale per il rischio operativo

Come detto in precedenza, Basilea II ha introdotto per la prima volta il calcolo del requisito patrimoniale anche per il rischio operativo. Il Comitato ha proposto tre differenti metodologie di calcolo dei requisiti richiesti:

1. Metodo Base – BIA (*Basic Indicator Approach*)
2. Metodo Standardizzato – SIA (*Standardised Indicator Approach*)
3. Metodi Avanzati di Misurazione – AMA (*Advanced Measurement Approches*)

I tre modelli si differenziano per la complessità richiesta nel calcolo e per la quantità di dati storici richiesta per l'applicazione della metodologia. La Figura 7 riporta alcune delle caratteristiche di tali metodi.

Figura 9. Caratteristiche dei metodi per il calcolo dei requisiti minimi.

Il metodo Base ed il metodo Standardizzato seguono un approccio *Top-Down,* ovvero quantificano il rischio senza considerare gli eventi scatenanti e l'entità delle perdite. Il vantaggio di questi approcci consiste nella loro facilità di misurazione e nel fatto che non richiedono serie storiche di dati per il calcolo. Queste metodologie tuttavia sono poco raffinate e portano, spesso, ad una sovrastima del capitale allocato.

I metodi Avanzati, al contrario, seguono un approccio *Bottom-Up* ovvero quantificano il rischio a partire dagli eventi interni scatenanti e richiedono, per questo motivo, una grande quantità di dati. La loro maggiore complessità rappresenta un ostacolo nel calcolo ma permette una quantificazione più precisa della quota di capitale da attribuire al rischio operativo. L'elevata raffinatezza di questi metodi avanzati permette alle banche di determinare il capitale da allocare in modo preciso e sulla base delle caratteristiche interne proprie dell'azienda.

La scelta del modello da utilizzare è lasciata alle singole banche ma, tuttavia, è soggetta ad autorizzazione da parte delle autorità di vigilanza nazionali, le quali accordano il consenso sulla base del possesso di requisiti tecnico-organizzativi e della esposizione al rischio della società. In particolare, gli attori attivi a livello internazionale e con una notevole esposizione al rischio operativo sono tenuti ad utilizzare metodologie più complesse al fine di ottenere stime più precise di tale requisito.

2.7 Basic Indicator Approach

La metodologia BIA è la più semplice tra quelle proposte dal Comitato e può essere utilizzata da tutte le banche in quanto non presenta requisiti minimi da soddisfare per la sua applicazione. La semplicità di tale approccio deriva infatti dal fatto che i parametri di

calcolo sono definiti a livello di sistema aziendale e non richiede serie storiche di dati per il calcolo.

Tale metodo prevede l'utilizzo del Margine di Intermediazione (MID) della banca per il calcolo del requisito patrimoniale. Il MID misura i ricavi operativi lordi di una banca ed è considerato una misura assimilabile al fatturato delle imprese industriali e dunque idonea alla valutazione del grado di esposizione al rischio operativo di una banca. Seguendo le linee guida fornite, la frazione di capitale che le banche devono riservare per fronteggiare il rischio operativo è pari alla media dei valori positivi del MID riferiti ai tre anni precedenti moltiplicata per una percentuale fissa (α). Il valore del coefficiente α è fisso ed è stabilito dal Comitato pari al 15% e indica, per il settore nel suo complesso, la percentuale minima di capitale di vigilanza richiesto rispetto al MDI dei tre esercizi precedenti.

La porzione di capitale richiesta viene quindi espressa come segue:

$$K_{BIA} = \alpha * \frac{\sum_{i=1}^{3} MDI_i}{3}$$

Dove:

K_{BIA} = requisito patrimoniale richiesto, determinato secondo il metodo BIA;

MDI_i = Margine di Contribuzione, se positivo, riferito all'i-esimo anno;

α = coefficiente di rischio.

La semplicità della metodologia rappresenta sia un pregio, che si riflette nella facilità di calcolo, sia un difetto, poiché ha come conseguenza, in alcuni casi, la sovrastima della quota di capitale richiesta per fronteggiare il rischio operativo.

2.8 Standardised Indicator Approach

Il secondo approccio, denominato *Standardised Approach*, rappresenta un'evoluzione della logica utilizzata nel *Basic Indicator Approach*, e consiste in un modello maggiormente articolato in relazione alle diverse aree di operatività della banca.

Questo metodo prevede la suddivisione delle aree di attività della banca in otto linee di *business* all'interno delle quali il Margine di Intermediazione rappresenta un indicatore della loro grandezza e della loro esposizione al rischio operativo.

Il metodo SIA prevede quindi, innanzitutto, di individuare gli indicatori dell'esposizione al rischio per ciascuna *Business Line*. Tali indicatori sono ottenuti moltiplicando il valore del MDI per un parametro β, caratteristico della linea di *business* corrispondente. Il parametro β è considerato un valore rappresentativo della relazione esistente a livello di settore tra le perdite per rischi operativi storicamente rilevate in una determinata linea di *business* e il valore aggregato del margine MDI per quella stessa linea (considerato adatto a descrivere il volume di operatività all'interno delle linee di *business*). In un dato esercizio i requisiti patrimoniali negativi (risultanti da un MDI negativo) per una determinata linea di *business* possono compensare senza alcuna limitazione i requisiti positivi riferiti ad altre linee. Tuttavia, nel caso in cui il requisito patrimoniale aggregato per tutte le linee di *business* con riferimento a un dato esercizio fosse negativo, l'*input* del numeratore per quell'anno dovrà essere posto pari a zero.

Di seguito sono riportati in Tabella 7 i valori del coefficiente β per le 8 Linee di *Business*.

Business Lines	**Beta Factors**
Corporate finance (β_1)	18%
Trading and sales (β_2)	18%
Retail banking (β_3)	12%
Commercial banking (β_4)	15%
Payment and settlement (β_5)	18%
Agency services (β_6)	15%
Asset management (β_7)	12%
Retail brokerage (β_8)	12%

Tabella 7. Valori dei coefficienti β. (Basel Committee on Banking Supervision, International Convergence of Capital Measurement and Capital Standards, Bank for International Settlements, Basel, June 2006, p 147)

Il requisito patrimoniale totale viene quindi calcolato come la media aritmetica, dei tre anni precedenti, della sommatoria dei requisiti patrimoniali di ciascuna *Business Line*. La formula utilizzata per calcolare l'indicatore aggregato è dunque la seguente:

$$K_{SIA} = \frac{\sum_{i=1}^{3}\left[\sum_{j=1}^{8}\left(MDI_j * \beta_j\right); 0\right]}{3}$$

Dove:

K_{SIA} = requisito patrimoniale richiesto, determinato secondo il metodo SIA;

MDI_j = Margine di Contribuzione per la j-esima *Business Line*;

β_j = coefficiente di rischio fissato per la j-esima *Business Line*.

Sebbene la suddivisione nelle 8 linee di *business* rappresenti un lato positivo del metodo standardizzato, l'assunzione di correlazione perfetta sottostante questo metodo può rappresentare un elemento criticabile in quanto è sottointesa una contestuale manifestazione delle perdite per tutte le aree di *business* e quindi la necessità della banca di riservare una quota di capitale sufficiente per fronteggiare le perdite congiunte.

2.8.1 Alternative Standardized Approach

Da giugno 2004, le banche, dietro autorizzazione particolare da parte delle autorità nazionali di vigilanza, hanno ottenuto autorizzazione ad adottare una versione leggermente modificata del Metodo Standardizzato, detto "Metodo Standardizzato Alternativo" (ASA). La metodologia di calcolo del requisito patrimoniale nell'approccio ASA è la stessa prevista per il metodo standardizzato tradizionale, ad eccezione per due linee di *business*: *retail banking* e *commercial banking*. In queste ultime due, infatti, l'indicatore di esposizione non è più rappresentato dal margine di intermediazione, ma dall'ammontare del valore di prestiti ed anticipazioni moltiplicati per un fattore fisso "m". Il valore del coefficiente "m" è stabilito dal Comitato pari a 0,0035. I valori di β per il *Retail Banking* ed il *Commercial Banking* restano invece immutati.

La formula utilizzata per calcolare l'indicatore aggregato è dunque la seguente:

$$K_{ASA} = \sum_{j=1}^{2} MDI_j * \beta_j + \sum_{j=3}^{4} LA * \beta_j * m + \sum_{j=5}^{8} MDI_j * \beta_j$$

Dove:

K_{ASA} = requisito patrimoniale richiesto, determinato secondo il metodo ASA;

MDI_j = Margine di Contribuzione per la j-esima *Business Line;*

β_j = coefficiente di rischio fissato per la j-esima *Business Line*;

m = coefficiente di rischio fissato per le *business line Retail Banking* e *Commercial Banking;*

LA = media, calcolata per i precedenti tre esercizi, del totale dei prestiti e delle anticipazioni in essere delle linee operative *Retail Banking* e *Commercial Banking* (linee 3 e 4).

2.9 Advanced Measurement Approches

Il Comitato di Basilea ha concesso, inoltre, l'utilizzo di modelli per la misurazione e gestione del rischio operativo più complessi, detti "*Advanced Measurement Approaches*". Tali modelli non si configurano con una formulazione analitica, ma sono metodi che le banche possono utilizzare per mettere a punto un modello sulla base della propria particolare esposizione al rischio. I requisiti patrimoniali calcolati con questi approcci includono quindi aspetti qualitativi e quantitativi propri del sistema di valutazione interno alla banca stessa.

La decisione del Comitato di Basilea di proporre questa tipologia di modelli si pone come fine quello di concedere alle banche un ampio grado di flessibilità nell'individuazione della metodologia utilizzata per il calcolo del requisito patrimoniale, al fine di renderla aderente alle diverse operatività e a permettere all'indicatore di rappresentare a pieno la specifica banca.

I modelli AMA offrono, pertanto, il vantaggio di una più puntuale misurazione dell'esposizione al rischio operativo, in quanto costruiti *ad hoc* per la singola banca.

Gli approcci avanzati sono caratterizzati dal ricorso a metodologie con un elevato rigore statistico e sensibilità verso il rischio, basate sulla stima delle perdite operative attraverso l'analisi di serie storiche. Questa caratteristica evidenzia come solamente le grosse società possono ottenere autorizzazione all'utilizzo di tali metodologie in quanto la necessità di avere a disposizione un elevato numero di serie storiche di dati è una prerogativa di grossi

gruppi, che hanno a disposizione tecnologie in grado di raccogliere tale mole di informazioni.

Il Comitato di Basilea non fornisce linee guida per la scelta degli approcci utilizzabili per il calcolo del requisito patrimoniale, ma tuttavia subordina il loro effettivo utilizzo al rispetto di criteri qualitativi e quantitativi. I tre approcci avanzati menzionati dal Comitato sono i seguenti:

- *Internal Measurement Approach* (IMA);
- *Loss DistributionApproach* (LDA);
- *Scorecard Approach (*SA*)*.

2.9.1 Internal Measurement Approach - IMA

L'approccio *Internal Measurement Approach* prevede che il capitale da allocare a ciascuna linea operativa derivi dalla somma delle perdite attese e delle perdite inattese. In particolare, è ipotizzata una relazione lineare tra perdita attesa e inattesa. L'approccio fa riferimento alle 8 linee operative già presentate; per ognuna di queste l'autorità di vigilanza definisce le tipologie di eventi di perdita da considerare.

Per ciascuna combinazione linea operativa/tipologia di evento, l'organo di vigilanza associa l'indicatore EI (*Exposure Indicator*) che rappresenta un'approssimazione dell'esposizione di ciascuna linea operativa ad una determinata tipologia di evento di perdita. Le banche misurano inoltre, per ciascuna combinazione linea operativa/ tipologia di evento, la probabilità PE (*Probability of Loss Event*) che si verifichi un evento di perdita e l'entità della perdita potenziale che potrebbe fare seguito all'evento, indicata con LGE (*Loss Given that Event*). La combinazione di questi tre valori permette di individuare la perdita attesa EL (*Expected Loss*) definita come:

$$EL = \text{EI} * \text{PE} * \text{LGE}$$

In seguito, le banche indicano, per ciascuna combinazione di linea operativa/tipologia di evento, un fattore γ che è sottoposto ad accettazione da parte delle autorità di vigilanza. Tale fattore gamma traduce la stima della perdita attesa EL nel requisito patrimoniale

richiesto per fronteggiare il rischio e deve tener conto delle perdite inattese, le quali sono ipotizzate correlate stabilmente con quelle attese.

Il requisito patrimoniale per ciascuna combinazione di linea operativa/tipologia di evento di perdita è uguale al prodotto di gamma per la perdita attesa. Il requisito richiesto alla banca è, infine, calcolato come la somma aritmetica di tutti i prodotti risultanti ed è riassunto con la formula di seguito esposta:

$$K_{IMA} = \sum_{i}^{n} \sum_{j}^{m} [\gamma(i,j) * EI(i,j) * PE(i,j) * LGE(i,j)]$$

Dove:

K_{IMA} = requisito patrimoniale richiesto, determinato secondo il metodo IMA;

γ = percentuale fissa, concordata da banche e autorità di vigilanza, indicativa della perdita attesa per ciascuna combinazione linea operativa / tipologia di evento;

EI (i,j) = indicatore di esposizione relativo alla i-esima linea operativa e al j-esimo tipo di evento;

PE (i,j) = indicatore della probabilità che si verifichi un evento di perdita sulla i-esima linea operativa e della j-esima tipologia;

LGE (i,j) = entità della perdita, causata da un evento, sulla i-esima linea operativa e della j-esima tipologia.

2.9.2 Loss Distribution Approach – LDA

Il metodo LDA si differenzia dal precedente in quanto permette di calcolare in modo diretto la stima delle perdite attese e inattese, e non mediante la stima del fattore di correlazione γ come per la metodologia IMA. Pertanto, il metodo *Loss Distribution* è in grado di riflettere in maniera più accurata il rischio a cui sono sottoposte le banche.

Per ciascuna combinazione linea operativa/tipologia di evento, la banca deve stimare due diverse distribuzioni di probabilità che sono considerate indipendenti tra loro:

- Una distribuzione che modellizzi la frequenza dell'evento di perdita (PE) dato un certo intervallo temporale;

- Una distribuzione che descriva l'entità delle perdite che si verificano a seguito degli eventi (LGE).

La combinazione delle due distribuzioni permette di individuare la distribuzione delle perdite complessive. L'approccio più flessibile per combinare le due distribuzioni è la simulazione Montecarlo. La distribuzione così individuata permette poi di calcolare il valore a rischio (VAR – *Value At Risk*) di ciascuna combinazione linea operativa/tipo di evento e, tramite la somma di tutti i valori ottenuti, è possibile calcolare il requisito patrimoniale richiesto con tale metodologia.

Il VAR è calcolato come differenza tra la perdita corrispondente al percentile considerato (solitamente il 99° percentile) e la perdita attesa ed indica la perdita potenziale in un certo arco di tempo considerato. Di seguito è esposta la formula per il calcolo del valore a rischio:

$$VAR = perdita\ al\ percentile - EL$$

La somma complessiva del *Value At Risk* per una banca, sotto ipotesi di indipendenza tra le combinazioni linea operativa/tipologia di evento può essere calcolata con la formula riportata di seguito:

$$VAR = \sqrt{\sum_{i}^{n}\sum_{j}^{m}[VAR^2(i,j)]}$$

Dove:

VAR (i,j) = valore del *Value At Risk* per la i-esima linea operativa e il j-esimo tipo di evento.

2.9.3 Scorecard Approach – SA

L'approccio *Scorecard* si basa sull'esperienza e le opinioni di esperti interni all'azienda, i quali emettono pareri che possono essere sintetizzati e modellati al fine di ottenere una misura dell'esposizione ai diversi rischi ed un elenco prioritario di interventi necessari. La società effettua quindi un'autovalutazione e sulla base di questa predispone un piano

di esposizione al rischio. Le perdite percepite e prospettate contenute nel questionario di autovalutazione possono essere rappresentate graficamente (tramite strumenti come istogrammi, grafici, tabelle). I modelli *Scorecard* sono particolarmente utili per stabilire la priorità degli interventi necessari al fine di ridurre efficacemente l'impatto dei rischi *ex ante* e non a posteriori. Queste valutazioni hanno come fine l'identificazione di indicatori in grado di esprimere particolari tipologie di rischio all'interno delle singole linee operative. Gli *Scorecard* sono tabelle che permettono di monitorare la situazione ed avere una visione d'insieme del rischio affrontato dalle linee operative al fine di contribuire all'individuazione del giusto ammontare di capitale destinato alla gestione del rischio operativo.

La banca, dunque, con l'utilizzo di questo metodo, traduce i giudizi qualitativi che sono raccolti tramite il processo di *scoring* in stime quantitative previsionali basati su indicatori di rischio che sono approvati dalle autorità di vigilanza.

Il database

Il presente lavoro di tesi si pone l'obiettivo di effettuare un'analisi del panorama di crimini informatici perpetrati nei confronti delle società finanziarie. La presenza di asimmetrie informative che caratterizza questo settore, tuttavia, non ha permesso di utilizzare un database precostruito. In Europa, l'obbligo di notifica a seguito di violazioni informatiche, introdotto dal GDPR nel secondo semestre del 2018 e nel corso del 2019, non ha ancora ottenuto l'effetto desiderato poiché le aziende rimangono restie a divulgare informazioni circa tali eventi. Il numero di crimini comunicati è cresciuto ma non in misura considerevole. Questo evidenzia come le società europee oppongano resistenza alla normativa e facciano prevalere l'interesse personale, di mantenere le informazioni riservate, a quello collettivo, di ridurre le asimmetrie informative e creare un *database* comune tra le aziende.

Negli Stati Uniti d'America, l'introduzione dell'obbligo di notifica è stata meno ostacolata dalle società le quali, già in precedenza, si dimostravano meno restie a comunicare i dettagli dei crimini informatici subiti. Tale fenomeno può essere ricondotto alla maggiore rigidità delle normative USA.

Grazie alle norme introdotte tuttavia, alcune aziende hanno iniziato a comunicare i casi di reati subiti e queste informazioni hanno portato alla creazione di *database* che, però, rimangono riservati agli organi di vigilanza e non sono accessibili al pubblico. Lo scopo delle normative è, infatti, quello di diminuire le asimmetrie tra aziende e pertanto solamente attori del settore hanno la facoltà di accedere a queste informazioni riservate.

Per questi motivi, per il presente lavoro non è stato possibile fare riferimento ad una base di dati precostruita e, pertanto, l'analisi è stata svolta su un *database* costruito appositamente, raccogliendo informazioni di pubblico dominio.

Il capitolo descrive le modalità di raccolta dei dati del campione, le caratteristiche delle società incluse e le informazioni di cui è stata tenuta traccia. In seguito, sono state esposte alcune assunzioni fatte per quanto riguarda la determinazione delle variabili principali necessarie all'analisi. Il terzo paragrafo contiene un'analisi delle aziende e degli attacchi al fine di ottenere una visione d'insieme dei dati inclusi nel campione. Infine, particolare

attenzione è stata posta nella determinazione del costo degli attacchi informatici e nel calcolo della severità, un indicatore chiave per l'analisi della gravità dei reati.

3.1 Raccolta dei dati

I dati utilizzati per l'analisi sono stati raccolti mediante un'approfondita ricerca sul *web,* effettuata allo scopo di ottenere informazioni sui crimini informatici perpetrati nei confronti di aziende attive in ambito finanziario. La ricerca è stata impostata selezionando un bacino temporale e geografico ben definito ed effettuando alcune assunzioni che saranno chiarite meglio in seguito.

- **Bacino geografico**. Al fine di restringere l'area geografica degli attacchi sono stati presi in considerazione esclusivamente gli attacchi perpetrati nei confronti di società finanziarie con sede principale negli Stati Uniti o in Europa. Non sono stati quindi considerati i reati contro banche che non appartengano a questi paesi.

- **Bacino temporale.** L'arco di tempo considerato copre gli ultimi 15 anni, dal primo quadrimestre del 2005 al primo quadrimestre del 2020. Tale scelta temporale è stata effettuata considerando che le fonti risalenti ad un periodo anteriore abbiano poca affidabilità a causa della poca sensibilità all'argomento e della mancanza quasi totale di norme che obbligassero le aziende ad informare gli organi competenti in caso di reati informatici. Con l'introduzione, nel 2004, di una definizione univoca di rischio operativo infatti, è ragionevole ritenere che questo periodo possa essere considerato come spartiacque tra un periodo di carenza di informazione e uno di sensibilizzazione nei confronti di tali eventi.

Al fine di ottenere un elenco di partenza, è stata stilata una lista delle principali società finanziarie americane ed europee per capitalizzazione di mercato. Per ciascuna sono state così riportate le seguenti informazioni:

- Nome della società;
- Breve descrizione;
- Stato che ospita la sede principale;
- *Total Asset* (TA) in milioni di dollari;

- Anno di valutazione del *Total Asset* riportato.

L'informazione circa il *Total Asset* delle società considerate è stata ritenuta utile per avere una stima della grandezza della società. La valuta utilizzata per esprimere tale valore è il dollaro statunitense ed il tasso di cambio utilizzato è il seguente:

1 Euro (€) ⟷ 1,10 Dollari Statunitensi ($)

Questa scelta è stata effettuata al fine di adottare un'unità di misura unica e poter quindi confrontare tra loro le società per dimensione.

Il valore di *Total Asset* riportato è quello relativo all'informazione più recente reperita sul *web*. Qualora la società abbia subito una notevole mutazione di fatturato (a causa ad esempio di acquisizione da parte di altre società), è stato preso come riferimento il valore di *Total Asset* relativo all'anno in cui è stato perpetrato l'attacco (qualora tale società ne abbia subito uno).

A partire dalla lista così individuata, per ciascuna società è stata effettuata una approfondita ricerca sul *web* al fine di prendere nota di eventuali casi di reati informatici subiti dalla stessa.

A causa dell'elevato numero di informazioni talvolta discordanti, sono state selezionate esclusivamente notizie provenienti da fonti valutate come affidabili. Sono infatti stati consultate le fonti *online* di quotidiani attivi a livello nazionale o internazionale ma anche siti specifici dedicati al mondo del *cybercrime*, nonché rapporti tecnici provenienti da fonti ufficiali.

Qualora per una società non siano stati rilevati casi di attacchi, è stata riportata tale informazione. D'altra parte, per le società che sono state riconosciute come vittime di *cybercrime*, sono stati raccolti tutti i dettagli dell'attacco disponibili. In particolare, per ciascun attacco informatico sono state individuate informazioni relative a:

- Data dell'attacco;
- Tipologia di attacco;
- Conseguenze dell'attacco;
- Eventuali note relative.

In figura 10 è riportato un estratto del database costruito.

Nome	Descrizione	Nazione	Attacco	Giorno/mese	Anno	Tipo	Conseguenze	TOTAL ASSET (in milioni di $	Anno di valutazione total asset	Numero attacchi per società
ABN AMRO	banca	Olanda	SI	gennaio	2018	DDos	6 ore di disservizio	414,270	2018	2
	banca	Olanda	SI	maggio	2018	DDos	una giornata, 24 ore	414,270	2018	
Allied Irish Banks	Banca	Irlanda						102,020	2018	0
Ally Financial	holding bancaria	USA						178,869	2018	0
American Express	società che opera nei servizi finanziari e di viaggio	USA	SI	aprile	2013	DDos	2 ore	188,602	2018	1
Banco BPM	banca	Italia						174,340	2018	0
Banco Sabadell	banca	Spagna						242,070	2019	0
Banco Santander	banca	Spagna	SI	agosto	2008	DataBreach	3000 carte di credito dei clienti sono state bloccate	1,650,000	2019	1
Bank of America	banca	USA	SI	18-set	2012	DDos	1 giornata ad intermittenza	2,355,000	2018	2
	banca	USA	SI	28-gen	2014	DDos	4 ore	2,355,000	2018	
Bank of Ireland	banca	Irlanda						138,190	2018	0
Bank of New York Mellon	società multinazionale del settore bancario e dei s	USA	SI	maggio	2008	DataBreach	12,5 milioni di clienti	362,870	2018	1
Bank of Scotland	banca	Gran Bretagna	SI	gennaio	2017	DDos	2 giorni di disservizio	880,910	2018	1
Bank of Spain	banca	Spagna	SI	agosto	2018	DDos	intermittenza, un giorno	289,000	2018	2
	banca	Spagna	SI	maggio	2018	DDos	intermittenza, un giorno	289,000	2018	
Bankia	banca	Spagna						194,580	2017	0
Bankinter	banca	Spagna						83,120	2018	0
Barclays PLC	banca	Gran Bretagna	SI	febbraio	2014	DataBreach	27 mila clienti. I dati riguardano dettagli personali, guadagni dei clienti, dettagli di mutui, polizze assicurative, numero di passaporto e assicurazione nazionale	2,230,000	2008	1
BB&T Corp	holding bancaria	USA	SI	17-ott	2012	DDos	intermittente, 24 ore	463,700	2018	1
BBVA	banca	Spagna	SI	ottobre	2010	DDos	6 ore di disservizio	734,440	2018	2
	banca	Spagna	SI	dicembre	2012	DDos	5 ore	734,440	2018	
BCE	banca centrale	Europa	SI	luglio	2014	DataBreach	20 mila indirizzi email di persone che hanno partecipato a conferenze ed eventi organizzati dall'Eurotower e si erano registrate elettronicamente	447,083	2018	2
	banca centrale	Europa	SI	dicembre	2018	DataBreach	481 utenti esposti: nomi, indirizzi e email	447,083	2018	
Belfius Bank	banca	Belgio						182,950	2018	0
Black Rock	Società di investimento	USA						159,60	2018	0
BNG Bank	banca	Olanda						153,250	2018	0
Bnl	gruppo bancario	Italia						85,790	2017	0
BNP Paribas	banca	Francia	SI	giugno	2017	Ddos	18 ore	2,220,000	2018	1
BOK Financial Corp	holding bancaria	USA						38,020	2018	0
BPER Banca	banca	Italia						76,380	2017	0
Capital One	holding bancaria	USA	SI	settembre	2012	DDos	1 giornata ad intermittenza, 24 ore	372,500	2018	4
	holding bancaria	USA	SI	09-ott	2012	DDos	1 giornata ad intermittenza, 24 ore	372,500	2018	
	holding bancaria	USA	SI	luglio	2019	DataBreach	106 millioni di clienti, numeri di sicurezza sociale e altri dettagli di account bancari	372,500	2018	
	holding bancaria	USA	SI	22-23marzo	2019	DataBreach	100 milioni di utenti negli stati Uniti e 6 in Canada	372,500	2018	
Cassa Depositi e Prestiti	istituzione finanziaria	Italia	SI	ottobre	2013	DDos	12 ore	473,640	2018	1
Charles Schwab	banca americana e società di intermediazione azi	USA	SI	23-24aprile	2013	DDos	2 ore il 23 e a tratti il 24	296,480	2018	2
	banca	USA	SI	04-mag	2016	DataBreach	975 clienti:rubati username e password	296,480	2018	
Checkfree Corp	Fornitore di servizi elettronici finanziari	USA	SI	gennaio	2009	DataBreach	5 milioni di clienti	1,738,263	2006	1
CIT Group Inc	società di partecipazione finanziaria	USA						48,540	2018	0

Figura 10. Estratto del database di partenza costruito.

3.1.1 Data dell'attacco

Per ogni reato informatico individuato è stata riportata la data relativa con indicazione di anno, mese e, se disponibile, giorno dell'evento. È stata inoltre posta particolare attenzione nel discernere la data di avvenimento dell'attacco. Nella maggior parte dei casi, infatti, le società comunicano di aver subito un attacco informatico solamente in data posteriore (anche parecchi anni) rispetto all'evento. Questo può accadere non solamente per volere della banca ma, in alcuni casi, in modo involontario. Talvolta, infatti, i criminali informatici riescono ad infiltrarsi silenziosamente nel sistema e a nascondere le proprie tracce, rimanendo nascosti per anni senza che la società noti anomalie nei sistemi. In questi casi quindi la banca si può accorgere anche dopo molto tempo di aver subito un furto di informazioni e rende noto il fatto solamente a posteriori.

Per questo motivo è stata posta particolare cura nella ricerca e nella selezione della data in cui l'evento si è verificato e non di quella in cui è stata comunicata la notizia.

3.1.2 Tipologia di attacco

Per quanto concerne le tipologie di attacco su cui si è focalizzato lo studio, è stato scelto di includere nel *database* solamente gli eventi che rispettassero determinate condizioni. In particolare, sono stati presi in considerazione esclusivamente gli attacchi dovuti a minacce esterne e pertanto sono stati esclusi quelli relativi a errori interni del personale (sia volontari, sia involontari). Gli eventi individuati sono stati suddivisi in due caterogie: DDoS e *Data Breach*.

La prima categoria include gli attacchi DoS o DDoS che hanno avuto come causa un sovraccarico del sistema e che hanno portato ad un suo rallentamento o ad un *blackout* temporaneo.

La seconda classe, invece, comprende tutti gli attacchi che hanno causato una perdita informativa e tramite i quali i criminali hanno ottenuto accesso ad informazioni riservate della società. Tali eventi sono stati classificati come *data breach* indipendentemente dallo strumento utilizzato per introdursi nel sistema delle vittime, dalla tipologia di *malware* impiegato o dalla debolezza di sistema sfruttata. La scelta di non effettuare una distinzione tra le varie metodologie di attacco è stata dettata dalla mancanza di informazioni sul *web* e dalla loro poca attendibilità; spesso infatti, le aziende non comunicano il metodo

attraverso il quale i criminali si sono infiltrati nel sistema o, in alcuni casi, non ne sono a conoscenza. Pertanto, è stato scelto di non effettuare tale distinzione.

Sono stati esclusi, inoltre, gli attacchi condotti da parte di organi statali a danni di altri, ovvero il *cybercrime* condotto a fini politici.

3.1.3 Conseguenze dell'attacco

Per ciascun attacco rilevato sono state riportate informazioni circa i danni che l'evento ha causato per la società. In particolare, a seconda della tipologia di attacco, sono stati riportati diversi dati.

Per gli eventi di tipo DoS o DDoS (in seguito faremo riferimento ad attacchi DoS per semplicità ma sono inclusi anche attacchi DDoS), è stato ricercato il dettaglio del tempo di *blackout* che hanno causato. L'effetto registrato può essere stato un'interruzione del servizio ad intermittenza oppure un *blackout* totale, con conseguente indisponibilità del sistema per molte ore. È stata quindi riportata l'informazione del tempo in cui il sistema ha risentito degli effetti dell'attacco. Questa è stata poi convertita in ore al fine di rendere omogenea la valutazione dell'impatto ed indicare un'unità di misura uguale per tutti gli eventi.

Per gli attacchi che hanno causato *data breach,* invece, quale dato rilevante è stato considerato il numero di *record* di *database* sottratti dai criminali o esposti ad una possibile divulgazione. Pertanto, è stata ricercato questo dettaglio con indicazione della tipologia di informazioni che è stata sottratta che può includere nomi, indirizzi *e-mail*, informazioni personali, numeri di carta di credito o altri dati personali.

3.2 Assunzioni sui dati

I dati raccolti presentano alcune limitazioni di cui è necessario prendere atto. I casi di reati informatici raccolti ed utilizzati per le analisi, infatti:

- Rappresentano una piccola percentuale dei casi realmente avvenuti nel mondo: a causa dell'introduzione solo recente di norme atte alla riduzione delle asimmetrie informative, molti casi di reati informatici avvenuti prima dell'entrata in vigore di queste leggi, sono rimasti nascosti al pubblico. Inoltre, le società, in particolare

quelle piccole, sono soggette a numerosi attacchi che possono causare danni anche trascurabili e che non sono comunicati ufficialmente. Infine, come già detto, la riluttanza delle società di comunicare casi di *cybercrime* non permette di avere una visione completa del fenomeno;

- Rappresentano solamente eventi che si sono dimostrati particolarmente significativi da essere resi noti pubblicamente: i reati resi noti sul *web* sono quelli che hanno una portata tale da non poter essere nascosti. In caso di reati che producono danni irrilevanti, è possibile che le società comunichino la notizia agli organi competenti senza che una fuga di notizie esponga l'azienda pubblicamente. È inoltre importante considerare che non è possibile avere informazione degli attacchi che avvengono giornalmente ma che sono bloccati dalle difese aziendali e che dovrebbero rientrare formalmente nel conteggio ma non producono danni alle società.

- Le informazioni circa le conseguenze dei reati sono da considerarsi indicative in quanto non è possibile avere indicazioni precise. Le società forniscono infatti indicazioni generali riguardo agli effetti che un attacco ha avuto su un sistema ma è probabile che le stime siano considerate "al ribasso" al fine di limitare agli occhi del pubblico la gravità dell'evento. La tendenza a comunicare solo le informazioni necessarie e il principio di prudenza adottato dalle aziende può causare una distorsione delle conseguenze degli attacchi riportati nel *database* che potrebbe quindi risultare sottostimato.

- Per i casi di *data breach* è stato rilevato il dato relativo al numero di *record* esposti. Ogni *record* è stato considerato come l'insieme di informazioni relative ad una persona. Ad esempio, qualora in un attacco siano stati implicati 100 mila *record*, è stato considerato un pari numero di clienti coinvolti.

3.3 Il campione

Le aziende incluse nel *database* e i casi di reati informatici riportati sono stati accuratamente selezionati al fine di utilizzare solamente informazioni attendibili e sono state escluse le notizie per le quali i dati riportati sono risultati poco credibili. La lista

stilata include 128 società con sede principale negli Stati Uniti o in Europa. Sulla base dei dati raccolti possono essere quindi effettuate alcune considerazioni.

3.3.1 Distribuzione geografica delle società

I dati raccolti sono stati inseriti all'interno di un unico *database* costituito da 155 *record.* La lista comprende 128 società di cui 62 americane e 66 appartenenti all'area europea. Nella tabella sono elencati gli stati europei con indicazione del numero di società per ciascuna nazione.

Nazione	Numero società
Italia	12
Spagna	7
Gran Bretagna	5
Svezia	3
Francia	5
Germania	10
Austria	2
Belgio	3
Danimarca	2
Europa	2
Finlandia	2
Grecia	1
Irlanda	2
Norvegia	3
Olanda	4
Russia	2
Svizzera	1
TOTALE	66

Tabella 8. Stati di provenienza delle società europee.

In Figura 10 è mostrato un grafico a torta contenente un dettaglio delle Nazioni Europee da cui provengono le società incluse nel *database*.

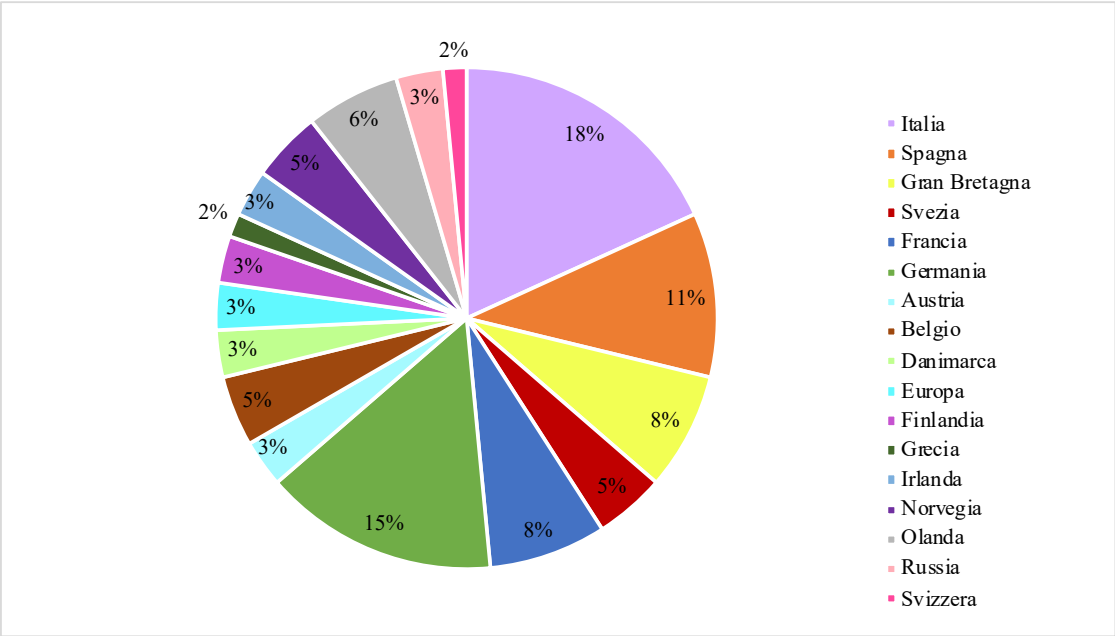


Figura 11. Grafico a torta per nazione di provenienza delle società europee considerate.

A partire dall'elenco così stilato, è stata effettuata una ricerca sul *web* al fine di individuare casi di attacchi informatici ai danni di queste aziende. È emerso che 65 aziende non hanno subito attacchi (di cui 27 americane e 38 europee), mentre 63 hanno subito almeno un attacco informatico (di cui 35 americane e 28 europee). Di queste 63, inoltre, 43 hanno subito solamente un attacco mentre 20 società ne hanno subito più di uno. In Figura 11 un dettaglio del numero di aziende considerate e il numero di attacchi subiti.

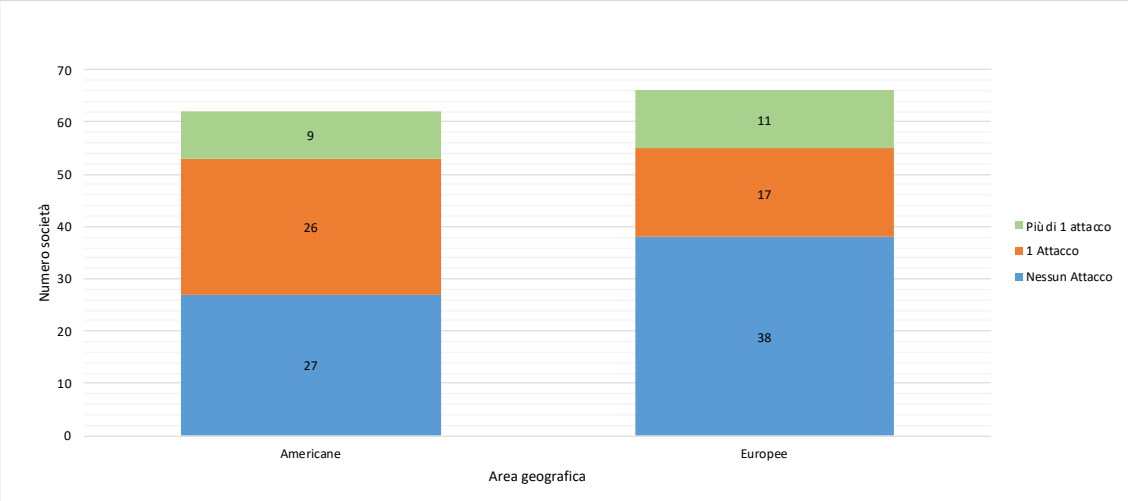


Figura 12. Numero di attacchi perpetrati ai danni delle società a seconda della localizzazione.

3.3.2 Dimensione delle società

Le aziende riportate nell'elenco variano notevolmente per la loro dimensione. Al fine di tenere traccia della caratteristica dimensionale è stato individuato ed utilizzato il valore del *Total Asset*. Tutte le società incluse nell'elenco possono ritenersi di grandi dimensioni in quanto, secondo le norme comunitarie, il loro totale di bilancio è superiore a 50 milioni di € (55 milioni di $). È stata, tuttavia, effettuata una sotto-categorizzazione. La suddivisione prevede di considerare un'azienda grande, media o piccola, come indicato in tabella, a seconda del valore di TA indicato a bilancio dalla stessa. Di seguito il riepilogo dei valori di riferimento, scelti in modo arbitrario.

Categoria	Valore TA in milioni di dollari (M$)
Piccola	≤ 300
Media	> 300 & ≤ 900
Grande	> 900

Tabella 9. Categorizzazione società per Total Asset.

Questa classificazione permette di fare alcune osservazioni riguardo alla grandezza delle società incluse nella lista precedentemente stilata.

Nella tabella seguente è indicato il numero di società per ciascuna categoria.

Categoria	Numero società
Piccola	85
Media	29
Grande	14
TOTALE	128

Tabella 10. Numero di società per categoria.

Emerge che le imprese piccole costituiscono il 66% del totale (85 società), quelle medie il 23% (29 società), mentre quelle grandi rappresentano solo l'11% della lista (14 società). In Figura 12 è presente un grafico a torta che rappresenta la suddivisione in percentuale delle categorie.

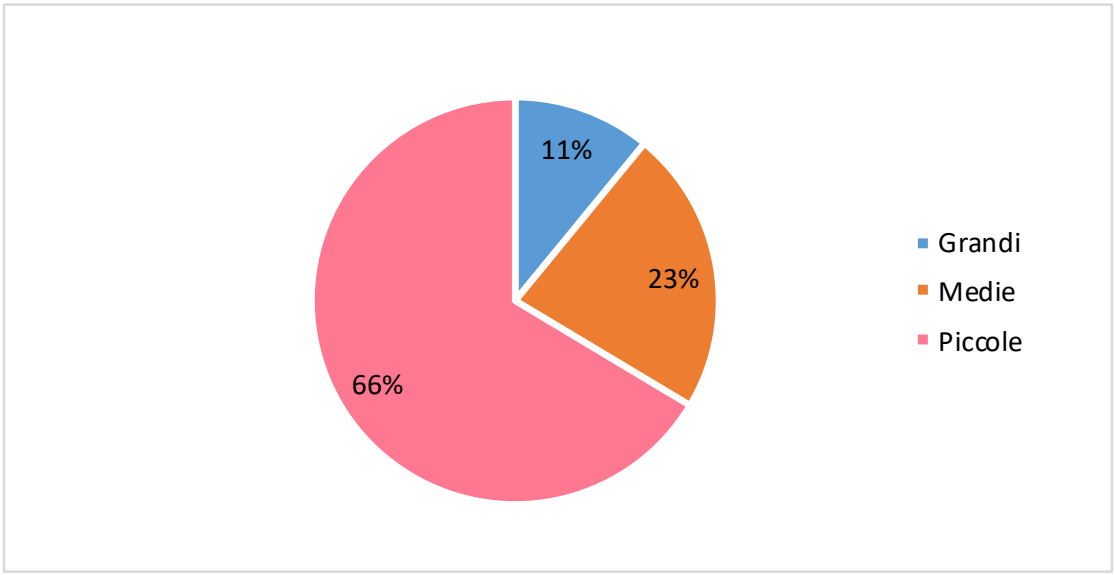


Figura 13. Grafico a torta rappresentante il numero di società per categoria.

Da un'ulteriore analisi emerge che le aziende maggiormente colpite risultano essere quelle classificate come grandi con una percentuale del 64% di società che hanno subito almeno un attacco informatico. La categoria delle piccole aziende risulta invece essere quella meno colpita ed è l'unica dove "solo" il 43% di società è stata soggetta a crimini informatici. In figura il dettaglio del numero di società colpite per ciascuna categoria.

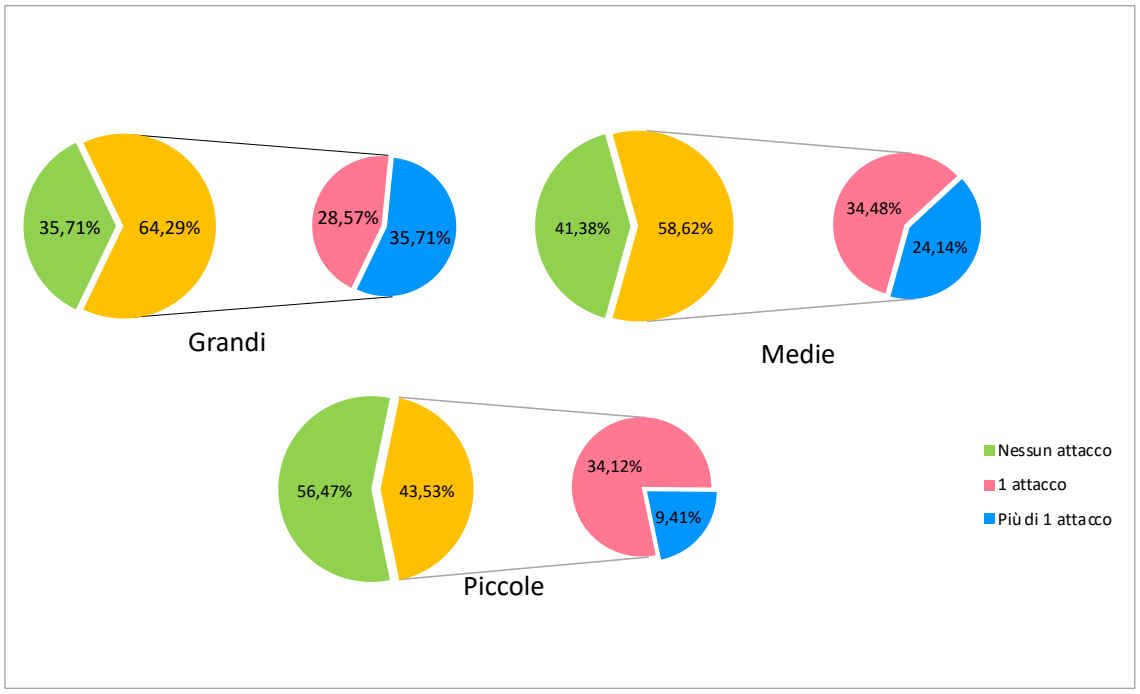


Figura 14. Percentuale di società attaccate suddivise per dimensione.

In Figura 14 il dettaglio del numero di società, suddivise per dimensione, che hanno subito relativamente nessuno, uno o più attacchi.

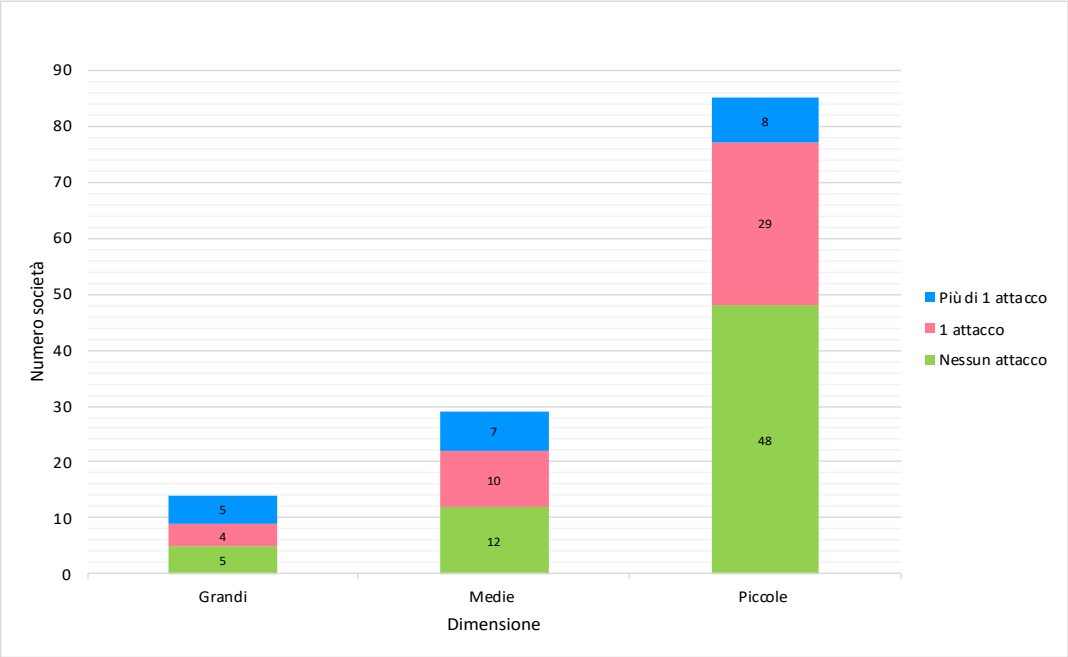


Figura 15. Numero di società attaccate suddivise per dimensione.

3.3.3 Tipologia di attacchi

La tipologia di crimini riportati all'interno del *dataset* riguarda solamente attacchi di tipo DoS (o DDoS) o eventi esterni che hanno portato a *data breach*. Sono stati individuati 89 casi di attacchi informatici così suddivisi:

Tipologia attacco	Numero attacchi
DoS (DDoS)	53
Data Breach	36

Tabella 11. Numero di società attaccate suddivise per dimensione.

Nel dettaglio, le società con sede in USA risultano colpite in egual misura da eventi di tipo DoS e *data breach* (rispettivamente nel 49% e nel 51% dei casi) mentre emerge che quelle con sede in territorio europeo sono vittime, nel 71% dei casi, di attacchi di tipo *Denial of Service* e solo per il 29% di *data breach*, con rispettivamente 30 e 12 casi (Figura 15).

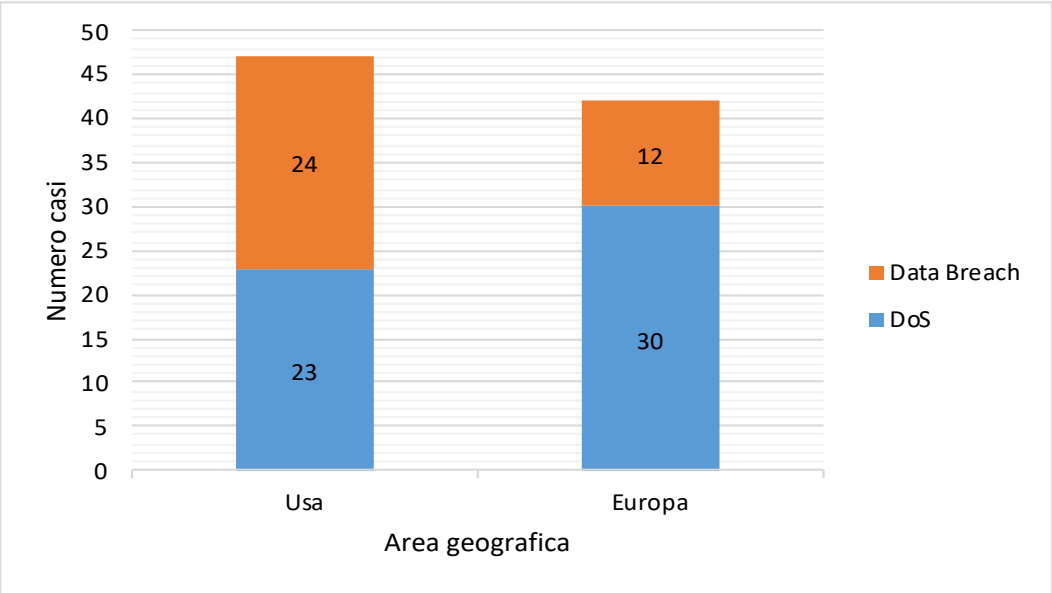


Figura 16. Tipologia di attacchi per area geografica.

3.3.4 Distribuzione temporale degli attacchi

I dati raccolti riguardo ai crimini informatici permettono di effettuare un'analisi temporale. Per ottenere una visione di insieme della distribuzione temporale degli attacchi e della loro frequenza, l'arco di tempo è stato suddiviso in trimestri. Tale scelta è stata effettuata in quanto si ritiene che la finestra temporale di 3 mesi sia sufficiente a garantire una visione generale del fenomeno e, nel contempo, presenti una granularità tale da non alterare le analisi sul campione. È stata dunque effettuata una suddivisione degli attacchi per tipologia ed è stato proiettato graficamente il numero di eventi di tipo DoS e *data breach* che si sono verificati in ciascun trimestre. In figura emerge che è registrato un notevole aumento di casi di *cybercrime* a partire dall'ultimo trimestre del 2012. In particolare, si nota un picco di attacchi DoS tra il terzo trimestre del 2012 ed il primo del 2013. Questa concentrazione è dovuta ad una serie di attacchi *denial of service* perpetrati ai danni delle banche, americane principalmente, da parte di un gruppo attivista musulmano auto-identificato con il nome "*Izz ad-Din al Qassam Cyber Fighters*". L'enorme rilevanza di attacchi DoS in questo arco temporale ha quindi un'origine "straordinaria" che non è riscontrata negli anni precedenti. Tuttavia, il 2012 può essere considerato come un anno di rivoluzione per il mondo del *cybercrime*: negli anni successivi si nota infatti un sensibile aumento di attacchi informatici.

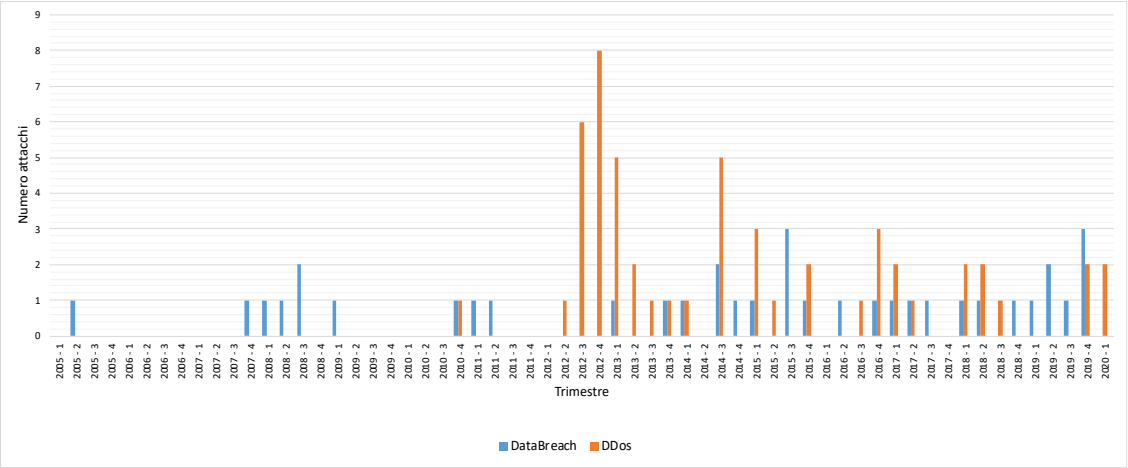


Figura 17. Distribuzione su base trimestrale degli attacchi informatici, suddivisi tra DDoS e Data Breach.

3.4 Costo dell'attacco

I criminali informatici possono colpire un sistema *target* con modalità differenti a seconda dell'obiettivo con il quale l'attacco è perpetrato. Un criminale può introdursi in un sistema informativo sfruttando vulnerabilità di un *software* o in modo legittimo attraverso la brutale forzatura della *password* associata ad un utente (questo metodo è considerato legittimo in quanto è "apparentemente" un ingresso non invasivo). L'accesso al sistema può essere effettuato tramite informazioni ottenute con *phishing* o tramite l'invio di *malware* al sistema ma può anche non prevedere un "ingresso" nel SI ma esclusivamente un suo rallentamento, come nel caso degli attacchi DoS. Le conseguenze che la vittima deve fronteggiare variano quindi a seconda della tipologia di attacco che subisce ed è molto difficile valutare economicamente le perdite a causa dei vari fattori che concorrono. Un attacco può portare ad un danneggiamento fisico del sistema o ad una perdita di informazioni ma la conseguenza più grave associata ad un attacco è il danno reputazionale che la società subisce a seguito di un attacco *cyber* ed è la più temuta dalle aziende.

In particolare, si ritiene che le principali conseguenze generate da un attacco DoS siano:

- perdita dovuta ad indisponibilità del sistema per un certo periodo di tempo;
- costo sostenuto per il ripristino tecnico del sistema;
- costo di *disruption*;
- costo associato ad un fermo della produttività;
- costo per danni associati all'infrastruttura di rete.

Le conseguenze di un attacco che porta ad un *data breach* invece, riguardano principalmente il costo associato alla perdita stessa dei dati. Questo non è, solitamente, un costo effettivo sostenuto dall'azienda ma può essere considerato come il valore economico associato a questo tipo di attacchi.

Comune ad entrambe le tipologie di reati informatici considerati è il danno derivante dalla perdita di reputazione che le società subiscono a seguito dell'attacco.

3.4.1 Quantificazione del costo di un attacco informatico

La valutazione del costo di un attacco informatico è un'operazione molto complessa. Nel calcolo infatti rientrano molti fattori che possono variare a seconda del settore, della dimensione e delle caratteristiche proprie della società. Al fine di dare una valutazione economica dei casi di crimini informatici raccolti nel database sono state effettuate alcune semplificazioni.

Attacco DoS

Per valutare il costo di questi attacchi è stata utilizzata la stima del costo di un attacco DoS effettuata da esperti di *cyber security* e proposta dall'operatore Fastweb che ripartiscono il costo di un attacco di questo tipo nelle seguenti componenti di perdita:

- **Indisponibilità del sistema**: è definita come il rapporto tra il tempo in cui un sistema è *offline* rispetto al tempo totale. Questo fattore rappresenta una perdita per la società poiché indica il numero di ore (ma anche giorni, minuti, secondi, ecc…) in cui l'utente non può avere accesso al sistema ed è l'unità di misura con cui il cliente valuta l'entità del danno subito. È fondamentale per le aziende lavorare al fine di ripristinare il servizio nel minore tempo possibile.

- **Supporto tecnico**: è legato alla necessità di effettuare manutenzione di tipo tecnico e tecnologico per ripristinare il sistema che risulta danneggiato a seguito dell'attacco. Questo rappresenta un costo effettivo che la società deve sostenere.

- **Interruzione della continuità operativa di un sistema**: la cosiddetta *disruption* può causare numerosi problemi alle aziende quali una diminuzione dei ricavi, una

maggiore esposizione al rischio, una perdita di clienti e può avere molte altre spiacevoli conseguenze. Consiste nell'interruzione della continuità di servizio e dimostra poca capacità di reazione da parte della società.

- **Fermo di produttività**: per le società produttive questo può riflettersi in un minore fatturato a causa di mancate vendite mentre in ambito finanziario è la sospensione delle transazioni che può arrecare danno.

- **Danni all'infrastruttura di rete**: sono legati a problemi fisici che si verificano a causa del sovraccarico della rete e generano costi che la società sostiene per il lavoro di tecnici chiamati a ripristinare la parte *hardware* del sistema.

Ai costi individuati è stato associato un valore economico che l'azienda sostiene. Nella tabella seguente sono indicati i costi associati a ciascuna componente, così come indicato nel rapporto Fastweb:

Fattore	Costo fisso (k$)	Costo orario (k$)
Perdita per indisponibilità (PI)	-	38,55555556
Supporto tecnico (ST)	350	
Interruzione continuità (disruption) (D)	230	
Produttività ferma (P)	170	
Danni all'infrastruttura di rete (IR)	160	

Tabella 12. Costi associati ad un attacco DoS.

Il costo associato alla perdita per indisponibilità è stato calcolato come segue:

$$Costo\ orario\ PI = \frac{Costo\ medio\ attacco}{Durata\ media\ attacco}$$

Dove:

costo medio attacco = costo medio causato da perdita di indisponibilità associato ad un attacco, stimato pari a 347 mila dollari (valore indicato nel rapporto *Fastweb*);

durata media attacco = valore medio della durata di un attacco di tipo DoS, stimato pari a 9 ore (valore indicato nel rapporto *Fastweb*).

Sostituendo i valori numerici nella formula sopra indicata si ottiene quindi:

$$Costo\ orario\ PI = \frac{347}{9} = 38{,}555 \quad \left[\frac{\$}{h}\right]$$

Per ogni evento di attacco DoS individuato nel *database*, il costo è stato poi calcolato sommando i costi di ciascun fattore sopra riportato:

$$Costo\ attacco\ DoS = PI + ST + D + P + IR$$

È importante evidenziare che, nel calcolo del costo degli attacchi, un'interruzione di servizio ad intermittenza è stata considerata alla stregua di un'interruzione totale. Per i casi nei quali si siano verificati periodi di interruzione ad altri di funzionamento (a pieno o ridotto regime), l'arco di tempo per il quale è stato calcolato il costo è quello dal momento dell'inizio del verificarsi dell'interruzione a quello di ripristino completo delle funzionalità.

Data Breach

Il costo di un attacco di tipo *data breach* risiede principalmente nel danno derivante dalla perdita di informazioni riservate. Non è tuttavia semplice associare un valore economico a tale perdita di dati. In alcuni casi, questa fuoriuscita di informazioni è associata ad un reale esborso economico per l'azienda. Si pensi, ad esempio, ai casi di criminali che utilizzano *malware* che cifrano i dati dell'azienda e chiedono un riscatto in cripto valute per fornire la chiave di decriptazione. La società deve quindi effettuare un pagamento ed in questi casi esiste un costo reale associato al *data breach,* costo che tuttavia rimane un'informazione riservata dell'azienda. Al contrario, nella maggior parte dei casi, i criminali sottraggono i dati al fine di vendere queste informazioni a terze parti.

Il costo di attacchi di questo tipo è stato calcolato valorizzando le informazioni sottratte alla società sulla base del valore che potenzialmente possono assumere sul mercato nero. I prezzi di tali informazioni variano a seconda della localizzazione geografica e della tipologia di dato trattato. Si riporta di seguito la tabella, utilizzata per valorizzare le informazioni, contenente l'indicazione del prezzo a cui sono vendute le informazioni

personali, sottratte illegalmente, sul *dark web,* a seconda della tipologia di informazione e della regione geografica.

Tipologia di dati	Prezzo USA	Prezzo Europa
Software Generated	8 $	25$
Contenenti informazioni di conto corrente	15$	35$
Fullsize	30$	40$

Tabella 13. Prezzo dei dati personali sul dark web con distinzione geografica secondo lo studio "The Hidden Data Economy" pubblicato da Intel Security Mcafee Lab.

Per ciascun attacco è stato quindi associato il relativo costo calcolato moltiplicando il numero di *record* sottratti per il relativo prezzo, considerato in base alla natura delle informazioni rubate. Tale metodologia è riassumibile con la formula:

$$Costo\ attacco = P * n$$

Dove:

P = prezzo relativo alla tipologia di informazioni sottratte;

n = numero di *record* interessati dall'attacco.

Per entrambe le tipologie di attacco, non è stato considerato il danno subito dalla società associato alla perdita di reputazione a seguito dell'incidente. La quantificazione di questa variabile, infatti, richiede informazioni molto dettagliate riguardo all'attacco e alla società che non sono pubblicamente note sul *web*.

È possibile, tuttavia, proporre alcune variabili con cui può essere valutato questo costo, quali:

- **Danno emergente**, interpretato come la spesa necessaria per ripristinare lo stato di reputazione originaria;

- **Lucro cessante**, ovvero il mancato guadagno dovuto alla perdita della clientela posseduta dalla società e che, alla notizia, potrebbero decidere di recedere il contratto;

- **Perdita di nuovi clienti**, riferito alla perdita dei potenziali nuovi clienti che avrebbero potuto avvicinarsi all'azienda.

3.5 Severità degli attacchi

Il costo correlato ad un attacco informatico può essere considerato un indicatore della sua portata in quanto permette di valutare quanto gravi siano state le conseguenze. Questa indicazione non permette, tuttavia, di comprendere l'entità di un attacco. Per un'azienda con un *total asset* di 900 bilioni di dollari, un attacco del valore economico di 150 milioni di dollari rappresenta un evento di dimensione ridotta mentre qualora lo stesso evento colpisca una società il cui *total asset* è di 1 bilione di dollari, l'evento assume importanza maggiore.

Per sopperire a questa soggettività, è stato introdotto il concetto di "severità". Tale grandezza è misurata come il rapporto tra il costo, calcolato come descritto precedentemente, e il *Total Asset* della società. La formula è riassunta come segue:

$$Severità = \frac{Costo\ dell'attacco}{Total\ asset}$$

Questa misura permette di comparare tra loro gli attacchi e di osservare il fenomeno relativamente alla dimensione della società colpita. In questo modo è stata ottenuta una serie di valori i cui parametri principali sono riassunti in tabella.

Parametro	Valore
Valore massimo	1,2687052700065100000
Valore minimo	0,0000000013761972916
Media	0,0294019900401461000
Varianza	0,0266377345515234000
Mediana	0,0000049635436830559

Tabella 14. Parametri della distribuzione dei valori di severità.

Data la grande dispersione dei dati, una rappresentazione grafica dei valori risulterebbe poco significativa pertanto, al fine di ottenere una rappresentazione della distribuzione della severità degli eventi, è stata introdotta una classificazione come riportato in tabella.

Classe	Valore Severità (incidenza del danno rispetto al TA)
Extraordinary	> 10%
Mega	1% - 10%
Big	0,1% - 1%
Tolerable	0,01% - 0,1%
Small	0,0001% - 0,01%
Micro	< 0,0001%

Tabella 15. Classificazione eventi sulla base del valore di severità.

Analizzando i valori di severità ottenuti è emerso che la maggior parte degli eventi presenta una severità compresa tra 0,0001% e 0,01%, ovvero la valutazione del danno economico incide tra lo 0,0001 e lo 0,01 sul valore del *total asset*. Gli eventi più frequenti risultano essere infatti quelli classificati come "*Small*", seguiti da quelli "*Micro*" mentre gli eventi più rari risultano essere quelli molto grandi e di dimensioni straordinarie: sul campione, solamente 4 eventi hanno avuto una dimensione tale da incidere per un valore superiore all'1% del TA. In figura una rappresentazione grafica della distribuzione degli eventi suddivisi in classi.

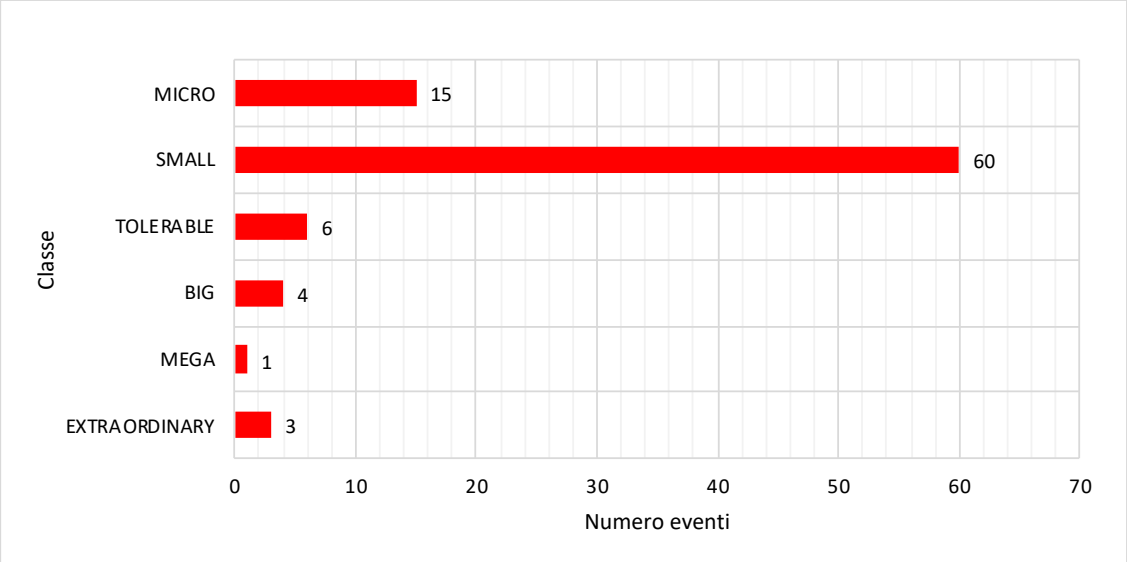


Figura 18. Numero di eventi per classe di severità.

Modelli statistici

Il *database* raccolto secondo le modalità descritte nel capitolo precedente è stato sottoposto ad alcune analisi statistiche per indagare la presenza di correlazione tra i dati.

Sono state inizialmente eseguite due regressioni multiple. La prima è stata effettuata al fine di individuare una eventuale dipendenza della frequenza degli attacchi dalla localizzazione della società, nonché dalla sua dimensione.

Successivamente sono stati indagati gli effetti di localizzazione e dimensione della società sulla severità degli attacchi.

In seguito, lo studio si è concentrato sulla costruzione di due modelli statistici per la distribuzione della frequenza e della severità degli attacchi raccolti del *database*.

4.1 Il modello di regressione

In prima analisi sono state effettuate due regressioni multiple. La frequenza e il costo degli attacchi sono, infatti, caratteristiche fondamentali per l'analisi svolta in questo elaborato; è pertanto importante indagare l'esistenza di correlazione tra queste e le altre variabili, nonché analizzare la natura della correlazione qualora emerga una dipendenza. Il modello seguito per le regressioni è del tipo:

$$y_i = \beta_0 + \beta_1 x_{1i} + \beta_2 x_{2i} + \varepsilon_i \qquad \text{con i} = 1, \ldots, \text{n}$$

Dove:

- y_i = variabile dipendente, ossia la risposta ai valori delle variabili indipendenti;
- β_0 = intercetta, ovvero il valore di y_i quando le variabili indipendenti sono tutte uguali a 0;
- x_1, x_2 = variabili indipendenti del modello, dette regressori;
- β_1 = coefficiente di x_1 (la prima caratteristica presa in considerazione), ovvero effetto su y di una variazione di x_1, tenendo costante x_2;

β_2 = coefficiente di x_2 (la seconda caratteristica presa in considerazione), ovvero effetto su y di una variazione di x_2, tenendo costante x_1;

ε_i = errore di regressione dovuto a fattori omessi.

Le ipotesi sottoposte a test con la regressione multipla sono l'ipotesi nulla H_0 di assenza di correlazione tra le due variabili indipendenti e quella dipendente contro l'ipotesi alternativa H_1 di presenza di correlazione (cioè che i coefficienti siano diversi da 0). Le ipotesi sono riassumibili come segue:

$$H_0\colon\ \beta_1\ \&\ \beta_2\ = 0$$
$$(H_0\colon\ \beta_1 =\ \beta_2\ = 0)$$

$$\text{Vs} \qquad H_1\colon\ \ o\ \ \beta_1 \neq 0\ o\ \beta_2\ \neq 0\ o\ enrambi$$

L'ipotesi sottoposta ad analisi è dunque quella di assenza di correlazione che si ha nel caso in cui, al variare del valore di una caratteristica, non cambia il valore della variabile dipendente considerata.

4.2 Frequenza degli attacchi

La frequenza degli attacchi può variare notevolmente nel tempo e può dipendere da diverse variabili quali la dimensione delle aziende e la loro localizzazione geografica, che a loro volta possono essere ricollegate alla propensione particolare delle società di dotarsi di tecnologie avanzate a difesa dei sistemi informativi o alla legislazione presente nei diversi paesi. A causa della difficoltà a stimare adeguatamente il livello tecnologico dei sistemi adottati e la dipendenza dalla legislazione in vigore nel paese in cui la società opera, sono state prese in considerazione le due variabili ritenute più rilevanti e oggettive: dimensione e posizionamento geografico.

È stata quindi eseguita una regressione multipla al fine di analizzare la correlazione tra la frequenza degli attacchi, come variabile dipendente, con la dimensione delle società e la localizzazione, come variabili indipendenti. Il modello adottato per la regressione è quindi il seguente:

$$Frequenza_i = \beta_0 + \beta_1 localizzazione_i + \beta_2 dimensione_i + \varepsilon_i$$

Al fine di svolgere la regressione è stato utilizzato il *software* statistico STATA, che permette agevolmente di inserire i dati, identificare le variabili di interesse ed effettuare l'analisi desiderata.

In tabella sono descritte e valorizzate le variabili utilizzate per la regressione:

Nome variabile	Tipo	Valore	Descrizione
ATTACCO_B	booleana	0 se non avvenuto attacco 1 altrimenti	Indica l'eventuale attacco ad una banca e permette di monitorare la frequenza
NAZIONE_B	booleana	0 se società europea 1 se società americana	Indica la localizzazione geografica della società
TA_milioni_dollari	intero	numerico	Riporta il *total tsset* della società espresso in milioni di dollari

Tabella 16. Descrizione a valorizzazione delle variabili utilizzate per la regressione con variabile dipendente la frequenza.

La regressione così impostata evidenzia che non è possibile rifiutare l'ipotesi nulla di assenza di correlazione con un livello di confidenza del 98% (con α pari al 2%). Il valore della statistica "t" per entrambe le variabili indipendenti è infatti minore, in modulo, al valore limite accettazione/rifiuto dell'ipotesi nulla corrispondente al livello di confidenza considerato e pari a 2,33. È possibile ottenere conferma anche osservando il valore del *p-value* ottenuto per entrambe le variabili indipendenti.

In figura 18 è mostrato *l'output* STATA ottenuto.

```
. reg ATTACCO_B NAZIONE_booleana TA_milioni_dollari, robust level(98)

Linear regression                               Number of obs =     154
                                                F(  2,   151) =    2.69
                                                Prob > F      =  0.0715
                                                R-squared     =  0.0219
                                                Root MSE      =  .49427

------------------------------------------------------------------------------
             |               Robust
   ATTACCO_B |      Coef.   Std. Err.      t    P>|t|     [98% Conf. Interval]
-------------+----------------------------------------------------------------
NAZIONE_boo~a |   .0801873   .0814406     0.98   0.326    -.1113037    .2716782
TA_milioni_~i |   8.54e-08   4.81e-08     1.78   0.078    -2.77e-08    1.99e-07
        _cons |   .5091334   .0572342     8.90   0.000     .3745589    .6437079
------------------------------------------------------------------------------
```

Figura 19. Output STATA ottenuto per la regressione con la frequenza come variabile dipendente.

Dall'analisi dell'*output* sopra riportato, si può quindi affermare che la frequenza degli attacchi è indipendente dalla nazione in cui ha sede principale la società e dalla grandezza della stessa.

4.3 Costo degli attacchi

Come per la frequenza, anche per il costo degli attacchi informatici è interessante indagare la natura della eventuale correlazione tra l'ammontare del danno subito, qualora si verifichi un attacco, e la dimensione della società, nonché la sua localizzazione geografica.

La regressione multipla è stata impostata identificando il costo degli attacchi, come variabile dipendente, e la dimensione delle società e la localizzazione come regressori. Il modello utilizzato per la regressione è quindi il seguente:

$$Costo\ attacco_i = \beta_0 + \beta_1 localizzazione_i + \beta_2 dimenzione_i + \varepsilon_i$$

In tabella sono descritte e valorizzate le variabili utilizzate per la regressione:

Nome variabile	Tipo	Valore	Descrizione
Costo_milioni_dollari	intero	numerico	Rappresenta il costo dell'attacco informatico
NAZIONE_B	booleana	0 se società europea 1 se società americana	Indica la localizzazione geografica della società
TA_milioni_dollari	intero	numerico	Riporta il *total asset* della società espresso in milioni di dollari

Tabella 17. Descrizione a valorizzazione delle variabili utilizzate per la regressione con variabile dipendente il costo.

Per quanto concerne la dimensione della società, dalla regressione si osserva che non è possibile rifiutare l'ipotesi nulla di assenza di correlazione con un livello di confidenza del 98%. Osservando i risultati ottenuti per la localizzazione della società invece, emerge che il valore della statistica "t" è leggermente maggiore del limite di accettazione previsto con il livello di confidenza preso in considerazione. Tuttavia, considerando un livello di confidenza del 99%, a cui è associato un valore della statistica t pari a 2,58, si osserva che non è possibile rifiutare l'H_0; pertanto è possibile concludere che anche questa variabile non influisce sul costo degli attacchi.

In figura 19 è mostrato *l'output* STATA ottenuto.

```
. reg Costo_milioni_dollari Nazione_B T_A_milioni_dollari, robust level(98)

Linear regression                               Number of obs =      89
                                                F(  2,    86) =    3.42
                                                Prob > F      =  0.0373
                                                R-squared     =  0.0561
                                                Root MSE      =  974.41

------------------------------------------------------------------------------
                             |               Robust
Costo_milioni_dol~i |      Coef.   Std. Err.      t    P>|t|     [98% Conf. Interval]
--------------------+---------------------------------------------------------
         Nazione_B |   464.9115   198.1938     2.35   0.021    -4.905624    934.7286
T_A_milioni_dollari |   .0000282    .000166     0.17   0.865    -.0003652    .0004216
              _cons |  -11.05001   91.4962    -0.12   0.904    -227.9411    205.8411
------------------------------------------------------------------------------
```

Figura 20. Output STATA ottenuto per la regressione con il costo come variabile dipendente.

Dall'analisi dell'*output* è quindi possibile affermare che il costo degli attacchi è indipendente dalla nazione in cui ha sede principale la società e dalla grandezza della stessa.

4.4 Modelli statistici

La frequenza degli attacchi è stata dimostrata essere indipendente dalla localizzazione geografica della società e dalla sua dimensione. La stessa conclusione è stata raggiunta per la severità degli attacchi. A seguito di queste considerazioni è necessario identificare dei modelli statistici che descrivano il comportamento di queste variabili. Per procedere nell'operazione sono stati identificati alcuni passaggi chiave che hanno portato alla scelta dei modelli che meglio rappresentano la frequenza e la severità degli attacchi individuati nel *database*. Sono state dunque seguite quattro fasi fondamentali:

1. Raffigurazione grafica dei dati ed individuazione delle distribuzioni che visivamente sembrerebbero rappresentare le osservazioni;

2. Misura della bontà di adattamento dei modelli teorici ipotizzati alle osservazioni;

3. Confronto grafico tra modelli;

4. Scelta del modello più adeguato.

4.5 Modello della distribuzione degli attacchi

La rappresentazione grafica dei dati sperimentali ha permesso di circoscrivere il numero di distribuzioni teoriche da analizzare, selezionando quelle che, graficamente, a prima vista si adattano meglio alle osservazioni. Sono stati quindi riportatiti i dati di frequenza degli attacchi informatici sotto forma di istogramma. Per fare ciò, è stata presa in considerazione la frequenza ottenuta sia a seguito di una suddivisione dell'arco temporale in trimestri, sia in quadrimestri. Gli istogrammi ottenuti sono riportati, rispettivamente, in figura 20 e 21.

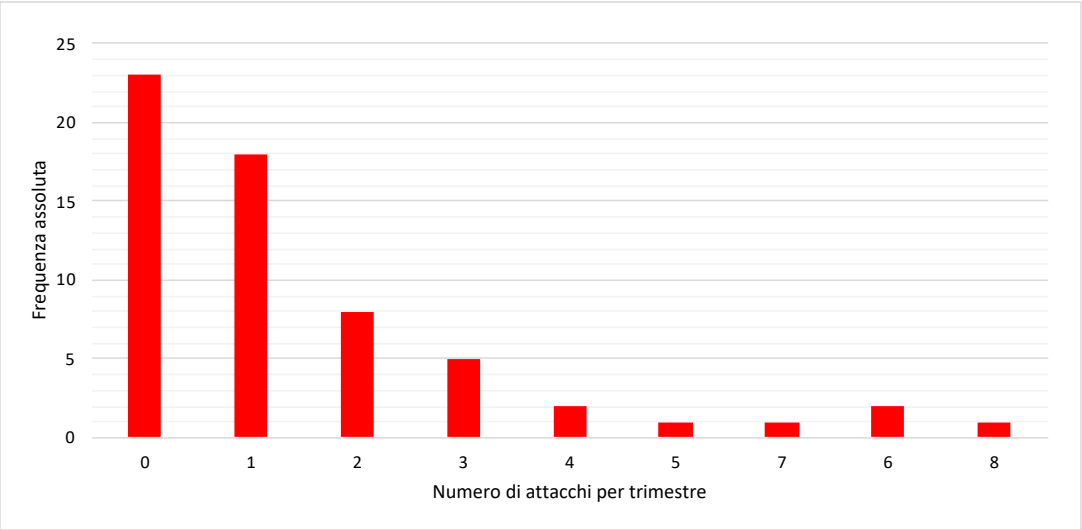


Figura 21. Frequenza degli attacchi su base trimestrale.

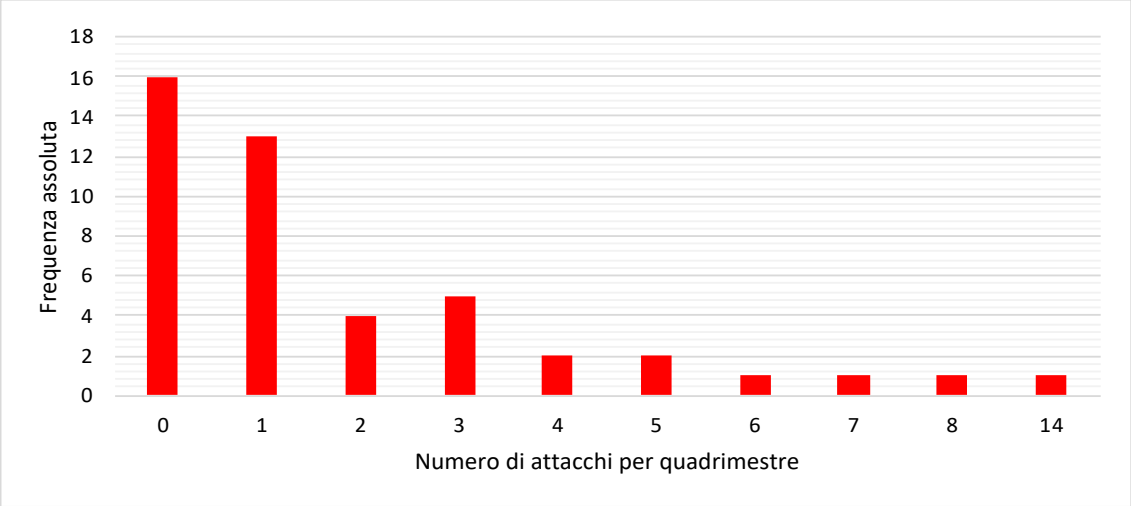


Figura 22. Frequenza degli attacchi su base quadrimestrale.

Dall'osservazione dei grafici sono state così ipotizzate 3 distribuzioni teoriche discrete che graficamente richiamano le osservazioni:

a) Distribuzione binomiale negativa;

b) Distribuzione di Poisson;

c) Distribuzione geometrica.

4.5.1 Metodo per la misura della bontà di adattamento

La misura della bontà di adattamento di distribuzioni teoriche alle osservazioni può essere effettuata in diversi modi. Nel presente elaborato è stato utilizzato il metodo di *Akaike*.

Il criterio *Akaike* (*Akaike's Information Criterion*, indicato come AIC), è un metodo per la valutazione e il confronto tra modelli statistici sviluppato dal matematico giapponese Hirotsugu Akaike. Il metodo fornisce una misura della qualità della stima di un modello statistico tenendo conto sia della bontà di adattamento sia della complessità del modello e rappresenta un metodo per la selezione dello stesso.

Lo stimatore deve dunque essere calcolato per ciascuno dei modelli teorici ipotizzati ed il metodo di scelta prevede di preferire il modello con il valore di AIC più basso.

Lo stimatore è definito come:

$$AIC = 2 * k - 2 * \ln(Lik)$$

Dove:

k = numero di parametri del modello statistico;

Lik = valore massimo della funzione di massima verosimiglianza del modello stimato.

Il calcolo dello stimatore AIC è stato effettuato tramite l'utilizzo del *software* R studio. All'interno di questo strumento, la funzione per il calcolo dell'AIC utilizza come *input* i dati ed un oggetto R che necessita di una funzione *log-likelihood* implementata al suo interno.
Per questo motivo è stata costruita separatamente la funzione di *Likelihood*. In particolare, è stata calcolata come il prodotto delle densità di probabilità di ogni elemento del vettore dei dati osservati. La densità di probabilità è stata calcolata utilizzando in *input* i dati e il valore dei parametri, stimati con il metodo della massima verosimiglianza, per la distribuzione di cui si sta calcolando la *Likelihood*. Nel dettaglio, la formula utilizzata su R studio è la seguente:

$$Lik = prod(ddistr(x, n))$$

Dove:

ddistr = densità di probabilità per ogni elemento del vettore, secondo la distribuzione indicata. Ad esempio, se si calcola l'AIC della distribuzione di Poisson, dovrà essere inserito il comando "dpoisson".

x = vettore dei dati osservati;

n = valore dei parametri della distribuzione. Ad esempio, per la distribuzione di Poisson è dato come *input* il valore stimato di lambda.

Il valore di *Lik* così calcolato può essere quindi inserito nella formula al fine di calcolare il valore di AIC corrispondente per la distribuzione.

4.5.2 Misura della bontà di adattamento per i modelli ipotizzati

Per ciascuna delle distribuzioni teoriche, ipotizzate per modellare la frequenza degli attacchi informatici, è stata effettuata una stima dei parametri con il metodo della massima verosimiglianza. Tale metodo prevede che i parametri siano valorizzati tramite la massimizzazione della funzione di verosimiglianza definita come:

$$L = \prod_{i=1}^{N} f(x_i|\Lambda)$$

Dove:

$f(x_i)$ = distribuzione di probabilità di osservare una particolare realizzazione delle X_i;

$\Lambda = \{ \lambda_{1;\ ...;}\ \lambda_m \}$, rappresenta l'insieme degli m parametri da cui dipende la funzione f_i.

Per semplificare i calcoli è consuetudine utilizzare il logaritmo della funzione sopra descritta, ovvero:

$$\mathcal{L} = \ln L = \ln \prod_{i=1}^{N} f(x_i|\Lambda) = \sum_{i=1}^{N} f(x_i|\Lambda)$$

Il metodo prevede che i valori preferiti dei parametri di una funzione di verosimiglianza siano quelli che rendono massima la probabilità di ottenere i dati osservati, ovvero i valori ottenuti dalla soluzione del sistema:

$$\begin{cases} \frac{\delta \mathcal{L}}{\delta \lambda_1} = 0 \\ \frac{\delta \mathcal{L}}{\delta \lambda_2} = 0 \\ \dots \\ \frac{\delta \mathcal{L}}{\delta \lambda_m} = 0 \end{cases}$$

La stima dei parametri così ottenuti è detta stima di massima verosimiglianza dei parametri.

Per le distribuzioni più semplici, la stima dei parametri di massima verosimiglianza è stata effettuata tramite il metodo sopra descritto. Per quelle più complesse, invece, per le quali risulta più difficile la soluzione del sistema, si è fatto ricorso all'ausilio del *software* R Studio. Tale *software* permette infatti, tramite la funzione "*fitdistr*" di stimare i parametri con il metodo della massima verosimiglianza. Di seguito sono riassunti i valori stimati dei parametri per ciascuna distribuzione presa in considerazione per la frequenza, per entrambe le suddivisioni temporali analizzate.

Distribuzione	Stima parametri	
	Trimestrale	Quadrimestrale
Binomiale negativa	p = 0, 6592593	p = 0, 59333
Poisson	λ = 1,9347826	λ = 1,4590164
Geometrica	p = 0,34074074	p = 0,40666667

Tabella 18. Parametri stimati per le distribuzioni di riferimento.

È importante precisare che alla distribuzione geometrica sono associate due distribuzioni di densità. Quella utilizzata in questo elaborato è la funzione che esprime la probabilità di avere k fallimenti prima di ottenere un primo successo e la sua funzione di densità è riportata di seguito:

$$f(X = k) = p * (1 - p)^k \qquad \text{con k = 1, 2, …, n}$$

Dove:

k = numero di fallimenti prima di ottenere un successo.

È stato quindi calcolato, tramite il *software* citato, il valore di AIC per ciascuna distribuzione e per entrambe le suddivisioni temporali considerate. Di seguito i valori ottenuti.

Distribuzione	AIC	
	Trimestrale	Quadrimestrale
Binomiale negativa	225,8414	231,9715
Poisson	228,63	219,6463
Geometrica	204,6867	175,2119

Tabella 19. Valori di AIC calcolati.

Un valore minore di AIC indica un miglior adattamento del modello ai dati sperimentali. Pertanto, è possibile affermare che la distribuzione geometrica è quella che meglio approssima i dati sperimentali osservati per la frequenza, sia considerando una suddivisione temporale in trimestri, sia in quadrimestri.

Come è stato detto, l'AIC indica quale tra le distribuzioni proposte si adatta meglio al modello ma non il grado di bontà di adattamento. Non è possibile inoltre fare confronti tra AIC diversi calcolati a partire da dati differenti, ovvero non è possibile confrontare i valori dell'indicatore calcolati su base trimestrale con quelli calcolati su base quadrimestrale.

Per osservare graficamente le distribuzioni ed avere un'indicazione visiva del loro adattamento, sono stati rappresentati graficamente i dati. Utilizzando il *software* R sono stati generati, per ciascuna delle distribuzioni proposte (con i relativi parametri) e per entrambi gli archi temporali considerati, 1000 numeri casuali. Con i numeri così generati è stato costruito un grafico al fine di osservare quale curva si adattasse meglio ai dati sperimentali. In figura 22 e 23 sono stati riportati i grafici di confronto tra i dati osservati e le curve delle distribuzioni prese in considerazione, rispettivamente per l'arco di tempo trimestrale e quadrimestrale.

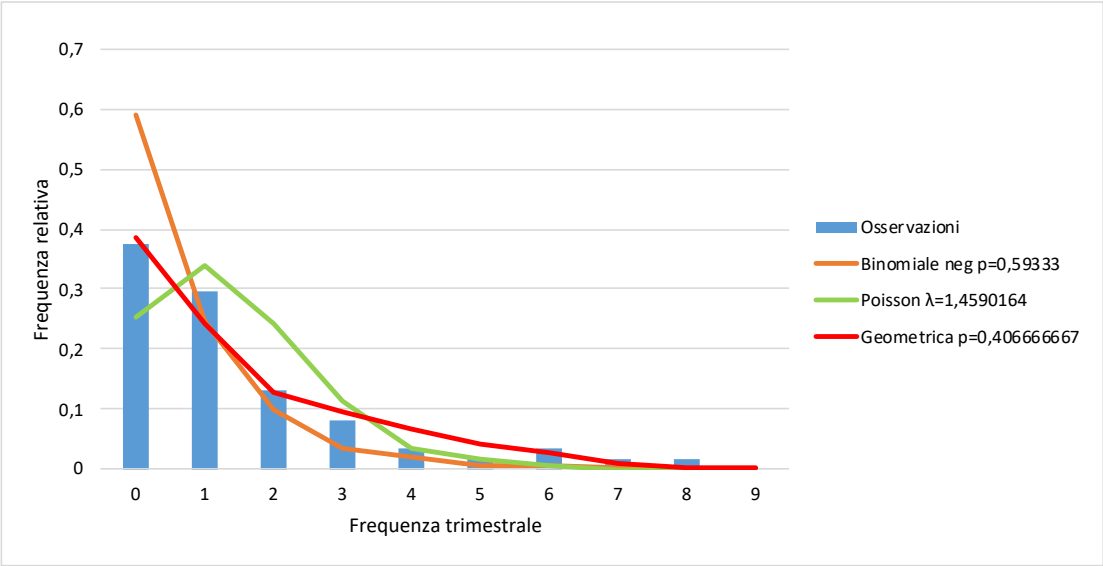


Figura 23. Confronto tra distribuzioni e dati sull'arco di tempo trimestrale.

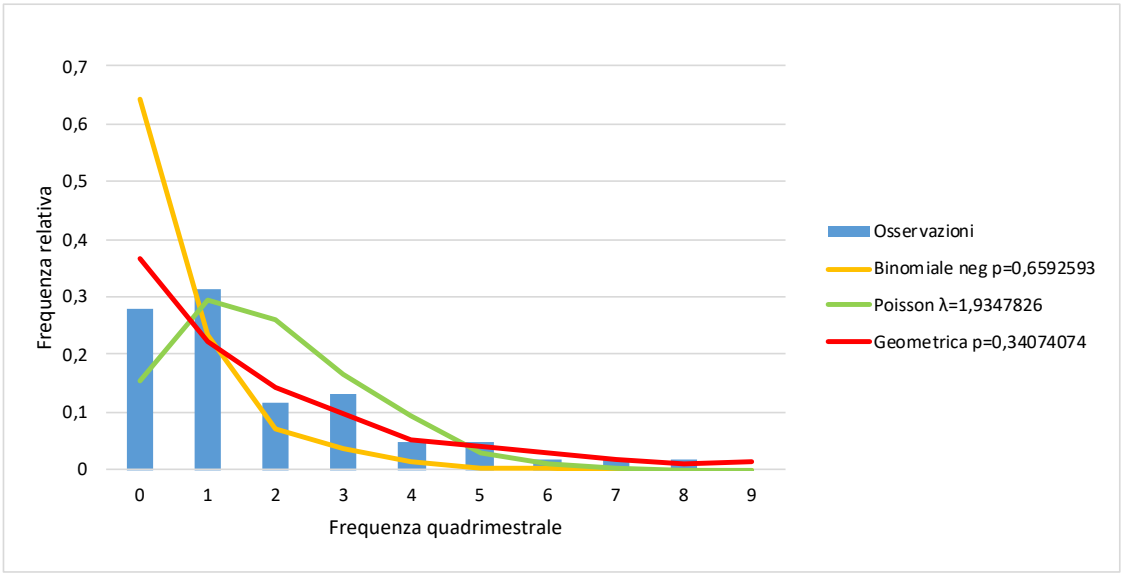


Figura 24. Confronto tra distribuzioni e dati sull'arco di tempo quadrimestrale.

I grafici sopra riportati confermano che la distribuzione geometrica è quella che meglio rappresenta i dati osservati e permettono anche di notare come questa approssimi meglio le osservazioni con un arco temporale suddiviso in trimestri.

In conclusione, è possibile affermare che la frequenza degli attacchi informatici, espressa su base trimestrale, è bene approssimata da una distribuzione geometrica con parametro p pari a 0,40666667.

4.6 Modello statistico per la severità degli attacchi

Come esposto nel capitolo precedente, per descrivere l'entità di un attacco informatico è stata utilizzata la severità. Tuttavia, l'ampia varianza riscontrata nei valori di severità degli attacchi all'interno del *database* ha reso difficile l'analisi dei valori di tale variabile. Per superare l'ostacolo, è stata quindi effettuata una trasformazione logaritmica dei valori della variabile. In precedenza, il valore della severità è stato calcolato come valore relativo e in alcuni casi si sono riscontrati valori molto prossimi allo 0. Pertanto, per poter lavorare con valori maggiori di 1 e poter così procedere con la trasformazione, i valori di severità sono stati moltiplicati per un multiplo di 10 e, solo in seguito, è stato calcolato il logaritmo di tali dati. Di seguito è riassunto il calcolo effettuato.

$$Severità\ in\ LN = LN(Severità * 10^9)$$

Dove:

Severità in LN = valore della severità espresso in logaritmo;

Severità = valore della severità relativa.

Sono stati quindi riportatiti i dati di severità degli attacchi informatici sotto forma di istogramma (Figura 24).

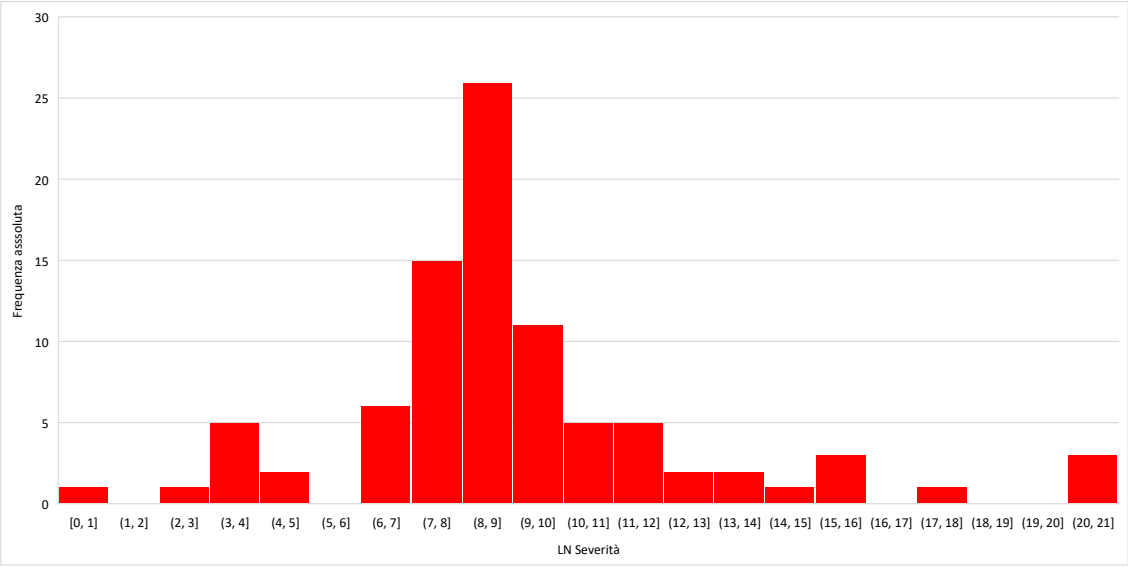


Figura 25. Frequenza dei valori di severità (espressa in logaritmi).

Dall'osservazione del grafico sono state così ipotizzate 3 distribuzioni teoriche continue che graficamente richiamano le osservazioni:

a) Distribuzione normale;
b) Distribuzione Weibull;
c) Distribuzione Gamma.

4.6.1 Misura della bontà di adattamento per i modelli ipotizzati

Il secondo passo per la scelta del modello statistico è la misura della bontà di adattamento. Come è stato fatto per la frequenza, per ciascuna delle distribuzioni teoriche ipotizzate per modellare la severità degli attacchi, è stata effettuata una stima dei parametri con il metodo della massima verosimiglianza.
Sebbene i parametri della distribuzione normale siano semplici da stimare, è stato utilizzato il *software* R studio con il metodo descritto per la frequenza. Di seguito sono riassunti i valori stimati dei parametri per ciascuna distribuzione presa in considerazione.

Distribuzione	Stima parametri
Normale	μ = 9,0998767 σ = 3,5429240
Weibull	λ = 10,1771871 k = 2,6110398
Gamma	λ = 5,41517554 r = 0,59508238

Tabella 20. Parametri stimati per le distribuzioni di riferimento.

È stato quindi calcolato il valore di AIC per ciascuna distribuzione considerata. Di seguito i valori ottenuti.

Distribuzione	AIC
Normale	481,7326
Weibull	483,5271
Gamma	487,8297

Tabella 21. Valori di AIC calcolati.

I valori dell'indicatore AIC per le distribuzioni considerate sono molto vicini tra loro. Questo significa che tutte si adattano quasi in egual misura ai dati di severità stimati. Tuttavia, la distribuzione normale è quella a cui è associato un valore di AIC minore, pertanto può essere ritenuta quella che meglio approssima i dati.

Per avere un'ulteriore conferma, è possibile rappresentare graficamente le distribuzioni ed avere un'indicazione visiva del loro adattamento.

Come in precedenza, utilizzando il *software* R sono stati generati, per ciascuna delle distribuzioni proposte (con i relativi parametri) 1000 numeri casuali. Con i numeri così ottenuti è stato costruito un grafico per osservare l'adattamento dei modelli teorici ipotizzati ai dati raccolti. In figura 25 è stato riportato il grafico di confronto tra i dati e le curve delle distribuzioni prese in considerazione.

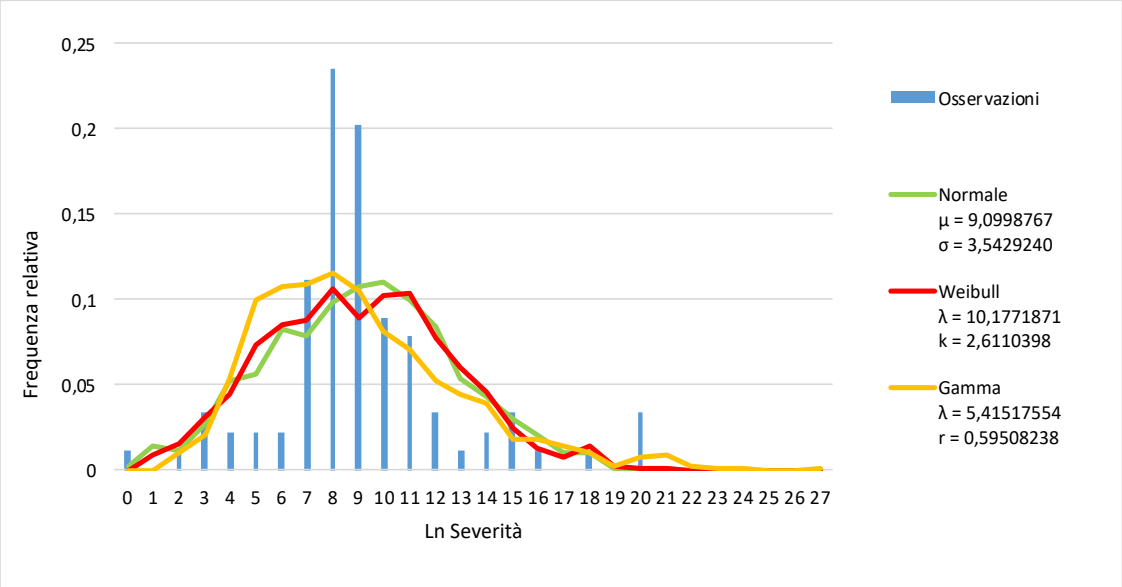


Figura 26. Confronto tra distribuzioni per la severità.

I grafici sopra riportati confermano che tutte le distribuzioni si adattano bene alle osservazioni, tuttavia, la distribuzione normale è quella che presenta un valore di AIC minore e pertanto è quella selezionata per il modello.

In conclusione, è possibile affermare che la severità degli attacchi informatici è bene approssimata da una distribuzione normale con parametri μ pari a 9,0998767 e σ pari a 3,5429240.

Stima del VaR con Metodo Montecarlo

Nel presente capitolo sono affrontati la simulazione Montecarlo e la stima del valore a rischio per il settore finanziario. La prima è stata effettuata a partire dalle distribuzioni di frequenza e severità individuate in precedenza ed è stata impostata a seguito di alcune considerazioni e dopo aver generato, con due diversi metodi, i valori casuali necessari.
In seguito, sono state effettuate alcune trasformazioni sui dati in *output* alla simulazione al fine di calcolare il *Value at Risk*.

Infine, è stato brevemente descritto un indicatore utilizzato per sopperire alla limitatezza di informazioni fornite dal VaR. L'*Expected Shorfall* infatti, è un valore che permette di ottenere una stima delle perdite che si possono verificare nella percentuale di casi non presi in considerazione dal VaR.

5.1 Il metodo Montecarlo

Il metodo Montecarlo è una tecnica molto antica e le sue origini storiche sembrano risalire al '700, molto prima quindi dell'avvento dei calcolatori. Nel '900 il metodo fu ampiamente utilizzato in studi per la ricerca nucleare e il suo utilizzo fu sostenuto poi a partire dagli anni '40 dalla nascente tecnologia dei calcolatori elettronici.

Oggi il metodo Montecarlo trova applicazione in vari ambiti scientifici. La prima applicazione alla valutazione degli investimenti è probabilmente dovuta a David Hertz il quale, nel suo articolo "*Risk analysis in capital investment*" del 1964, propone il metodo per valutare un progetto di espansione di un impianto chimico.

Con il tempo, la simulazione è stata applicata sempre più frequentemente ed oggi è ormai diffusamente utilizzata come tecnica di analisi del rischio nella valutazione degli investimenti nei manuali di economia applicata all'ingegneria.

Nella pratica, la simulazione Montecarlo è un metodo numerico basato su procedimenti probabilistici ed è usato in statistica per la risoluzione di problemi di varia natura, che presentano difficoltà analitiche difficili da superare con altri metodi. La simulazione

consiste nello studio del comportamento di un sistema (considerato nell'accezione generale del termine) mediante la sua riproduzione in un contesto controllabile. Nella simulazione si costruisce un modello matematico formato da equazioni che descrivono le relazioni tra le componenti del sistema oggetto di studio e il loro legame con il suo comportamento, al fine di effettuare esperimenti "virtuali" sul modello matematico. I risultati di tali esperimenti sono considerati essere una "riproduzione" sufficientemente accurata del comportamento che avrebbe il sistema "in natura".

In ambito aziendale, ma anche in fisica, matematica e sociologia, la simulazione Montecarlo è una delle più diffuse modalità di risoluzione dei problemi che hanno per oggetto la stima di variabili aleatorie e consiste in una stima quantitativa dei rischi.

L'utilizzo della simulazione permette inoltre di testare facilmente, e con elevato grado di dettaglio, gli effetti di variazioni nelle variabili di ingresso (ad esempio del modello o di sue variabili) sulla funzione di *output*.

5.2 Elementi della simulazione

La simulazione consiste nella creazione di scenari che sono combinazione dei dati in *input* forniti. Possono quindi essere definiti alcuni elementi essenziali necessari per lo scopo:

- **Parametri***: input* specificati dall'analista e quindi controllabili come, ad esempio, il numero di ripetizioni N;

- **Variabili di *input* esogene***:* variabili in ingresso che dipendono da eventi che non sono sotto il controllo del decisore, il cui andamento è però descrivibile per mezzo di modelli probabilistici;

- **Variabili di *output****:* i risultati della simulazione;

- **Modello***:* equazioni matematiche che descrivono le relazioni tra le componenti del sistema e definiscono il legame degli *output* con i parametri e le variabili fornite in *input*.

In figura 26 è riportato un grafico che riassume gli elementi in *input* e in *output* della simulazione.

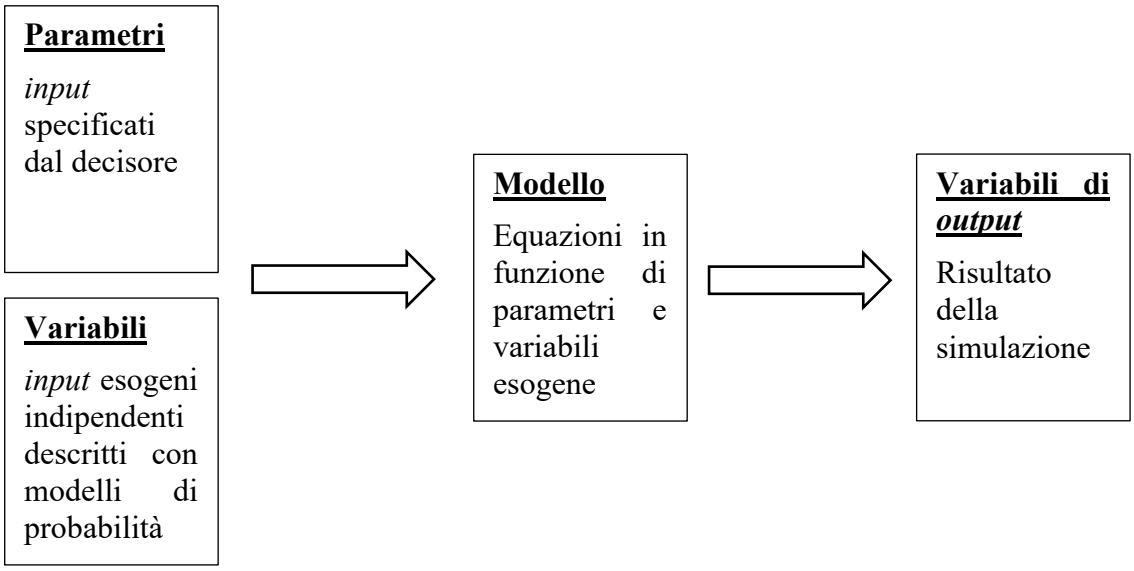


Figura 27. Schema rappresentante gli elementi della simulazione Montecarlo.

Il metodo Montecarlo si basa sulla constatazione che, per alcune tipologie di problemi, una soluzione analitica diretta, che espliciti direttamente il legame tra i dati di *input* e di *output*, risulterebbe troppo complessa. Il problema è quindi risolto in maniera numerica, generando un numero N sufficientemente alto di possibili combinazioni tra i valori che le variabili in ingresso possono assumere e calcolando il relativo *output* sulla base del modello assunto. Per ciascuna delle N combinazioni, viene generato casualmente un valore per ognuna delle variabili di *input*, in base al particolare modello statistico associato ad essa. Ripetendo per le N combinazioni questo procedimento, si ottengono così N valori indipendenti delle variabili di *output* che costituiscono un campione che può essere analizzato con tecniche statistiche al fine di stimarne i parametri descrittivi, generare istogrammi delle frequenze, ricavare numericamente gli andamenti delle funzioni di distribuzione *dell'output* e, come in questo caso, di stimare il valore a rischio.

I passi da seguire per impostare la simulazione possono essere riassunti come segue.

a) **Identificazione delle variabili esogene e dei parametri.**
   Inizialmente è fondamentale individuare i dati di interesse, ovvero gli elementi critici dai quali dipende il progetto; è infatti da ricercare un *trade-off* tra accuratezza e semplicità di implementazione del modello ed è quindi opportuno selezionare solo le variabili davvero rilevanti per l'analisi.

b) Definizione del modello.

È necessario esplicitare le relazioni matematiche che consentono di determinare il risultato desiderato, in funzione delle variabili di *input* e dei parametri, e considerare esplicitamente le correlazioni tra le variabili.

c) Attribuzione delle distribuzioni di probabilità.

In seguito, la simulazione prevede di esplicitare le distribuzioni di probabilità di ogni variabile di *input*. La distribuzione può essere assegnata sulla base di dati quantitativi o in modo soggettivo dal decisore, eventualmente supportato dal parere di esperti che godono di un'approfondita conoscenza del settore.

d) Impostazione della simulazione.

A questo punto si può procedere alla definizione del piano degli esperimenti, fissando il numero N di scenari da generare, stabilendo il modo adeguato a riprodurre numericamente nel calcolatore le funzioni statistiche delle variabili di *input* ed implementando gli algoritmi di generazione dei numeri pseudocasuali.

Dopo aver fissato i valori in *input* e generato i valori necessari al modello, è quindi possibile effettuare al calcolatore la simulazione pianificata e ottenere il campione dei valori assunti dalle variabili di *output*. Al termine delle simulazioni possono essere seguite alcune verifiche al fine di valutare eventuali problemi con il procedimento implementato ed analizzare i risultati ottenuti dalla simulazione.

Identificazione delle variabili esogene e dei parametri

La simulazione Montecarlo effettuata nel presente elaborato ha come obiettivo la stima del VaR del rischio informatico a cui sono sottoposte le aziende. A questo scopo, le variabili di interesse per il calcolo sono:

- frequenza degli attacchi informatici;

- conseguenze e costo degli attacchi, valorizzate con la severità, indicatore descritto e calcolato nei capitoli precedenti.

In questa fase è inoltre importante stabilire i valori dei parametri. Come detto in precedenza, la simulazione Montecarlo si basa sulla generazione di un certo numero di scenari con lo scopo di ottenere un campione di valori la cui frequenza permette di ricavare un'indicazione approssimata della distribuzione della variabile di *output*. A tal fine è necessario stabilire un certo numero N di scenari da generare. È statisticamente dimostrato (con riferimento al Teorema del Limite Centrale) che aumentando il numero di simulazioni si ottiene un campione più grande e, di conseguenza, una maggior precisione e accuratezza. In breve, all'aumentare del numero di iterazioni si ha una convergenza dell'*output* verso i valori che sarebbero analiticamente "esatti".
Nel presente elaborato, sono stati generati 10.000 scenari. Tale numero è stato ritenuto sufficientemente grande da rappresentare un campione che permetta di trarre conclusioni con un buon grado di affidabilità.

Definizione del modello

Per quanto concerne la frequenza, sono stati presi in considerazione sia i casi di banche che hanno subito attacchi, sia i casi di quelle che non sono state colpite.

Per la severità degli eventi invece, lo studio è partito da un'analisi delle conseguenze di ciascun attacco, se avvenuto. In seguito, alle conseguenze è stato associato valore numerico ed un costo e, solamente dopo aver calcolato i danni economici, è stato individuato un valore di severità.

Nei primi capitoli è stata indagata, tramite l'impostazione di regressioni multiple, la presenza di correlazione tra alcune variabili del modello. In particolare, è stata analizzata l'influenza della localizzazione della società e della sua dimensione su frequenza e costo degli attacchi. Le analisi hanno permesso di concludere che queste ultime due sono indipendenti dalle due precedenti. Pertanto, essendo il costo e la frequenza entrambi indipendenti dalle due variabili ritenute più caratterizzanti (dimensione e localizzazione della società), è ragionevole assumere che siano anche indipendenti tra loro. Inoltre, essendo il costo indipendente dalla dimensione dell'azienda, la severità, calcolata come costo rispetto al *total asset*, può essere a sua volta considerata indipendente dalla frequenza degli attacchi.

Le due variabili selezionate per la simulazione, frequenza e severità, possono pertanto essere considerate non correlate tra loro come conseguenza della loro indipendenza da variabili comuni ad entrambe.

In conclusione, è possibile confermare che la correlazione tra le variabili prese in considerazione nel modello Montecarlo è nulla.

Attribuzione delle distribuzioni di probabilità

Alle variabili indentificate è stato associato un modello statistico. Dalla distribuzione temporale degli eventi e dalla severità di questi sono state individuate, sia per via grafica sia con metodi analitici, le distribuzioni statistiche che meglio rappresentano i dati. In particolare, è stato riscontrato che la frequenza degli attacchi segue una distribuzione geometrica con parametro p pari a 0,40666667 mentre la severità è rappresentata da una distribuzione normale con parametri μ pari a 9,0998767 e σ pari a 3,5429240.

Impostazione della simulazione

Questa fase di impostazione della simulazione comprende un elemento chiave per il metodo Montecarlo: la selezione di un metodo per la generazione di numeri casuali adeguato all'esperimento.

Per poter effettuare N scenari di simulazione è necessario generare casualmente un certo numero di valori che seguano le rispettive funzioni di probabilità e le eventuali correlazioni. I valori possono essere generati utilizzando tre diversi algoritmi e, a seconda di quello selezionato, si ottengono diverse tipologie di numeri:

- **numeri "propriamente" casuali:** derivano da misure di fenomeni fisici intrinsecamente aleatori (come, ad esempio, la misura delle variazioni delle emissioni di un determinato componente). È possibile anche ricorrere a serie di numeri pubblicate su manuali specializzati che possono essere utilizzate per predisporre tabelle all'interno delle quali un apposito programma interno al calcolatore può pescare;

- **numeri pseudocasuali***:* sono serie generate direttamente dal calcolatore secondo un determinato algoritmo. Questa è, solitamente, la modalità più diffusa;

- **numeri “quasi” casuali**: sono anch’essi prodotti da un algoritmo, con l’obiettivo di rappresentare una serie di numeri disposti in maniera uniforme e non, come nel caso precedente, una vera sequenza casuale.

Di norma, i calcolatori utilizzano una funzione predefinita di generazione di numeri pseudocasuali che riproduce una distribuzione uniforme. Qualora sia necessario generare sequenze che riproducono distribuzioni non uniformi è possibile ricorrere a differenti metodi, quali, ad esempio, il metodo della funzione di ripartizione inversa.

È evidente come in realtà creare numeri casuali con un algoritmo deterministico sia complesso e, in pratica, impossibile. Tuttavia, i numeri casuali ottenuti da un calcolatore sono normalmente ritenuti tali nella misura in cui essi soddisfano i requisiti statistici (in termini di frequenze di estrazione) di cui godono i numeri veramente casuali.

Nel presente elaborato, al fine di generare numeri casuali sono stati utilizzati due diversi metodi. Si è infatti fatto ricorso, in alcuni passaggi, all’apposita funzione in *Excel* che permette di generare numeri casuali selezionando la distribuzione, i parametri e il numero di valori da generare e, in altri momenti, al metodo della funzione inversa. In tal modo sono stati generati i valori casuali necessari alla simulazione.

5.3 Avvio della simulazione

Dopo aver determinato tutte le variabili in *input* al modello, è stata affrontata la simulazione. Sono stati generati 10.000 scenari. Ogni scenario è rappresentativo del numero e della severità degli eventi che si possono verificare nell’arco di un trimestre.

Per prima cosa è stato generato un numero casuale che rappresentasse il numero di eventi che avvengono in questo arco temporale, ovvero la frequenza. In particolare:

1. È stato estratto, da una distribuzione uniforme tra 0 e 1, un numero casuale che è interpretato come probabilità cumulata del numero di eventi nel trimestre;

2. Dato il valore di probabilità cumulata, tramite il metodo della funzione inversa si è risalito al numero di eventi compatibile con la funzione geometrica con parametro p pari a 0,40666667.

Il metodo della funzione inversa prevede di partire dall'individuazione della funzione di ripartizione della distribuzione in oggetto. Nel caso in esame quindi, della distribuzione geometrica è definita come:

$$f(x) = 1 - (1 - p)^x$$

Essendo questa una funzione iniettiva e suriettiva, è possibile calcolare la funzione inversa definita come segue:

$$f^{-1}(x) = \frac{\log(1 - x)}{\log(1 - p)}$$

Sostituendo la variabile *x* con il valore casuale estratto in precedenza dalla distribuzione uniforme e il parametro p con il valore indicato (0,40666667) si ottiene così un numero che è interpretato come numero di eventi nell'arco del trimestre. Tuttavia, essendo quello risultante un valore decimale, è stata necessaria un'approssimazione del valore per ottenere una stima del numero di eventi da considerare.

In seguito, per calcolare la severità di ciascun evento, la cui frequenza è stata già stimata, è stato utilizzata una metodologia analoga:

1. Per ciascuno scenario e per ciascun evento, è stato estratto, da una distribuzione uniforme tra 0 e 1, un numero casuale che è interpretato come probabilità cumulata di una distribuzione normale;

2. Dato il valore di probabilità cumulata, tramite il metodo della funzione inversa si è risalito al numero di eventi compatibile con la funzione normale con parametri μ pari a 9,0998767 e σ pari a 3,5429240.

Data la difficoltà di calcolare la funzione inversa della funzione di ripartizione di una distribuzione normale, è stata utilizzata per lo scopo l'apposita funzione di *Excel*:

$$INV.NORM.N(p, \mu, \sigma)$$

Dove:

p = probabilità corrispondente alla distribuzione normale. Nel caso in esame il valore di probabilità estratto dalla distribuzione uniforme;

μ = valore di media, pari a 9,0998767;

σ = valore di deviazione standard, pari a 3,5429240.

A ciascun evento è stato così associato un valore di severità. Qualora la funzione abbia restituito un valore di severità negativo, questo è stato sostituito dal valore 0.

5.4 Esiti della simulazione

La simulazione impostata con gli *input* definiti in precedenza è quindi stata avviata. In figura 27 sono riportati i primi 20 scenari generati: la simulazione completa contiene un numero maggiore di colonne a causa di alcuni scenari per i quali è stato stimato un numero maggiore di eventi nel trimestre.

La prima colonna presenta indicazione del numero di scenario di riferimento: ad ognuno è associato, nella seconda colonna, un numero decimale che è poi riportato in forma approssimata (per difetto) nella terza e che rappresenta la somma degli eventi nell'arco del trimestre. Le restanti colonne indicano, per ciascuno degli eventi indicati nella terza colonna, la relativa severità, il cui valore cumulato è indicato nell'ultima colonna di destra.

Costruzione ammontare della severità degli eventi per scenario											
			Valore della severità per evento								
Scenario	numero eventi	numero intero di eventi	1	2	3	4	5	6	7	8	TOTALE
1	4,007425111	4	9,514808606	1,383784302	4,311226028	15,84461236	0	0	0	0	31,0544313
2	0,154353099	0	0	0	0	0	0	0	0	0	0
3	0,114203258	0	0	0	0	0	0	0	0	0	0
4	2,023596148	2	6,426964468	5,930605684	0	0	0	0	0	0	12,35757015
5	1,855781012	1	4,09062657	0	0	0	0	0	0	0	4,09062657
6	1,58824711	1	11,3837747	0	0	0	0	0	0	0	11,3837747
7	1,150851608	1	4,193755132	0	0	0	0	0	0	0	4,193755132
8	7,182779566	7	11,71521532	12,98447454	7,558504648	8,61181253	4,328085842	13,33405919	12,11546857	0	70,64762064
9	1,332862169	1	11,69395022	0	0	0	0	0	0	0	11,69395022
10	0,87409983	0	0	0	0	0	0	0	0	0	0
11	1,195919113	1	7,314401218	0	0	0	0	0	0	0	7,314401218
12	0,624176047	0	0	0	0	0	0	0	0	0	0
13	1,06683714	1	4,45951757	0	0	0	0	0	0	0	4,45951757
14	2,77489325	2	5,849727727	10,26645793	0	0	0	0	0	0	16,11618566
15	1,877832804	1	10,42855862	0	0	0	0	0	0	0	10,42855862
16	1,644992974	1	6,248740911	0	0	0	0	0	0	0	6,248740911
17	1,543773644	1	6,869959748	0	0	0	0	0	0	0	6,869959748
18	0,343138994	0	0	0	0	0	0	0	0	0	0
19	0,497900406	0	0	0	0	0	0	0	0	0	0
20	2,213731634	2	11,37292591	6,002014497	0	0	0	0	0	0	17,37494041

Figura 28. Simulazione Montecarlo per i primi 20 scenari.

La simulazione permette di ottenere una distribuzione della severità complessiva. I valori totali indicati nell'ultima colonna possono essere rappresentati mediante un istogramma, come riportato in figura 28. Emerge che, nella maggior parte dei casi, nell'arco di un trimestre, si verificano eventi i cui indicatori di severità spaziano in un intervallo molto ampio ma si concentrano principalmente, in media, nel *range* tra 5 e 16.

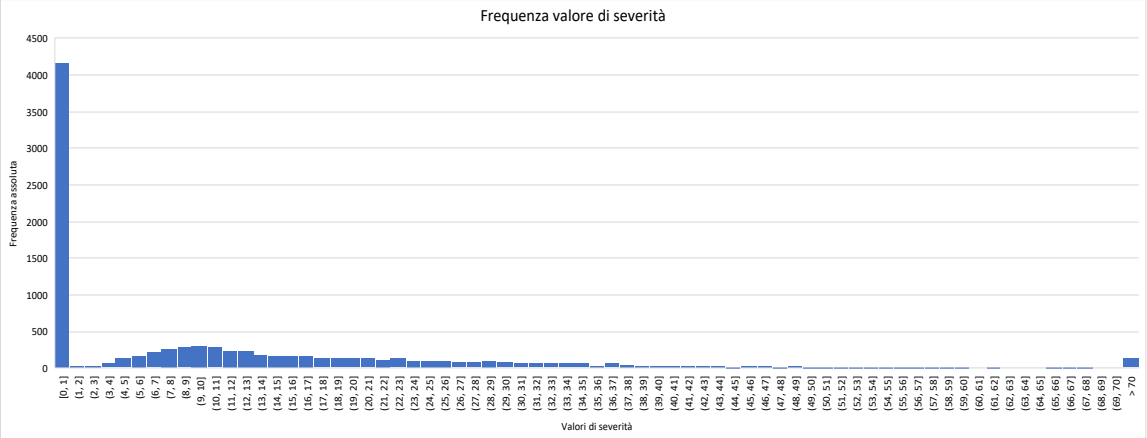


Figura 29. Istogramma della funzione della severità complessiva.

La distribuzione della frequenza della severità complessiva ottenuta in *output* alla simulazione è derivata dalla combinazione delle distribuzioni della frequenza degli eventi e delle severità individuali, assumendo che le due distribuzioni siano tra loro indipendenti. Osservando le due distribuzioni in *input* e quella complessiva in *output* è possibile riscontrare che quest'ultima deriva dalla combinazione delle prime due (Figura 29).

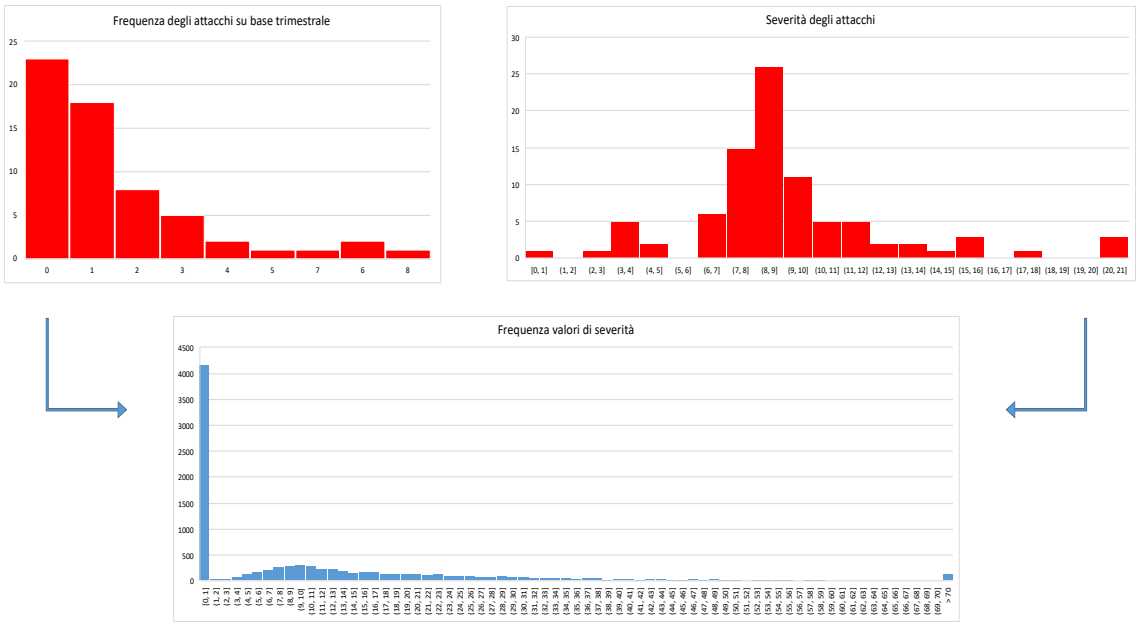


Figura 30. Confronto tra distribuzioni delle variabili in input e output alla simulazione.

5.5 Valore a Rischio

Il *Value at Risk* (Valore a rischio) è comunemente definito come la massima perdita potenziale derivante dalla detenzione di una particolare attività, relativamente ad un determinato livello di confidenza e ad un orizzonte temporale futuro stabilito. In altre parole, il VaR rappresenta la potenziale perdita massima che una società, un'attività o un portafoglio può sopportare, in un predefinito arco di tempo, con una certa probabilità.

Il VaR è una misura di rischio di tipo probabilistico, il cui valore dipende dalla grandezza di due caratteristiche:

- *Intervallo di confidenza scelto*: all'aumentare dell'intervallo di confidenza, aumenta il valore di VaR. Ad un intervallo del 99% sarà quindi associato un valore a rischio maggiore di quello relativo ad un intervallo del 95%;

- *Ampiezza dell'arco temporale:* maggiore è l'arco temporale, maggiore sarà il valore stimato di VaR. Questo implica che qualora si consideri un intervallo di 1 anno o di 1 giorno, il primo presenterà un valore a rischio maggiore del secondo intervallo temporale.

Il metodo di calcolo del VaR differisce a seconda della quantità e della natura dei dati a disposizione, della disponibilità di calcolatori, del tempo a disposizione e della qualità della stima che si vuole ottenere. È possibile calcolare il VaR utilizzando 3 diversi metodi:

1. **Approccio varianza-covarianza (o approccio parametrico)**
   Questo metodo è caratterizzato dall'utilizzo di un modello statistico di riferimento tramite un'assunzione a priori di una determinata distribuzione di probabilità, solitamente identificata con una distribuzione normale. È l'approccio più semplice poiché l'assunzione di normalità facilita notevolmente il calcolo dei parametri di portafoglio.

2. **Simulazione storica**
   È un approccio non parametrico che non richiede ipotesi di alcun tipo poiché la distribuzione viene calcolata sulla base di dati storici raccolti. Questo metodo richiede quindi la presenza di una serie storica di dati sufficientemente lunga per poter operare efficacemente. La grande quantità di informazioni richieste rende questo secondo metodo poco utilizzato.

3. **Simulazione Montecarlo**
   È un approccio non parametrico e consiste nella generazione di un numero sufficientemente alto di scenari al fine di ricavare una distribuzione di possibili esiti di perdite e profitti i cui parametri possono essere utilizzati nel calcolo del VaR. Questo metodo è il più complesso ma permette di ottenere una stima del valore a rischio più precisa rispetto alle altre metodologie.

5.5.1 Considerazioni sui dati

I dati ottenuti in *output* dalla simulazione Montecarlo possono essere utilizzati per calcolare il *Value at Risk* per i rischi informatici nel mondo finanziario. I valori stimati tuttavia, necessitano di alcune considerazioni.

A causa della elevata dispersione dei valori di severità calcolati inizialmente e al fine di individuare una distribuzione che rappresentasse i dati, è stata effettuata una trasformazione logaritmica, come descritto dettagliatamente nei capitoli precedenti. I valori generati dalla simulazione, pertanto, sono espressi in scala logaritmica. Questi però

non hanno un significato economico e quindi il calcolo del valore a rischio effettuato su tali dati non avrebbe un significato economico.
È necessario, per questo motivo, effettuare la trasformazione inversa a quella fatta inizialmente per poter ottenere i valori di severità nuovamente espressi in forma relativa. Data la trasformazione effettuata inizialmente sui dati:

$$f(x_i) = LN(x_i * 10^9)$$

È stata calcolata la funzione inversa come segue:

$$f^{-1}(x_i) = \frac{e^{x_i}}{10^9}$$

Ovvero:

$$Severità = \frac{e^{Sevrità\ in\ LN_i}}{10^9}$$

Pertanto, dopo aver effettuato la simulazione utilizzando la distribuzione individuata per i valori espressi in logaritmi, per ciascun valore di severità generato per ciascuno scenario, è stato effettuato il calcolo sopra indicato.

A titolo esemplificativo, in figura 30 sono riportati i valori ottenuti dopo la trasformazione per i primi 20 scenari generati.

Ad esempio, il valore in scala logaritmica, generato nella simulazione per il primo evento dello scenario 1, pari a 9,514808606 (figura 27) è stato convertito nel valore 0,000013559038 utilizzando la formula descritta sopra. Lo stesso procedimento è stato utilizzato per tutti gli altri valori.

Costruzione ammontare della severità degli eventi per scenario											
			Valore della severità per evento								
Scenario	numero eventi	numero intero di eventi	1	2	3	4	5	6	7	8	TOTALE
1	4,007425111	4	0,000013559038	0,000000003990	0,000000074532	0,007607250507	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,007620888066
2	0,154353099	0	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000
3	0,114203258	0	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000
4	2,023596148	2	0,000000618294	0,000000376382	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000994677
5	1,855781012	1	0,000000059777	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000059777
6	1,58824711	1	0,000087884146	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000087884146
7	1,150851608	1	0,000000066271	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000066271
8	7,182779566	7	0,000122420280	0,000435597765	0,000001916977	0,000005496202	0,000000075799	0,000617885964	0,000182675853	0,000000000000	0,001366068838
9	1,332862169	1	0,000119844484	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000119844484
10	0,87409983	0	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000
11	1,195919113	1	0,000001501772	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000001501772
12	0,624176047	0	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000
13	1,06683714	1	0,000000086446	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000086446
14	2,77489325	2	0,000000347140	0,000028751866	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000029099005
15	1,877832804	1	0,000033811580	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000033811580
16	1,644992974	1	0,000000517361	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000517361
17	1,543773644	1	0,000000962910	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000962910
18	0,343138994	0	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000
19	0,497900406	0	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000
20	2,213731634	2	0,000086935862	0,000000404242	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000000000000	0,000087340105

Figura 31. Simulazione Montecarlo per i primi 20 scenari dopo la trasformazione.

Dopo aver effettuato questa trasformazione per tutti i valori generati dalla simulazione, è possibile calcolare il VaR.

Essendo i valori nuovamente espressi in scala decimale, l'ampia dispersione dei dati non permette una rappresentazione grafica della distribuzione di severità complessiva.

È possibile, tuttavia, utilizzare la suddivisione in classi di severità individuata nei capitoli precedenti per avere una visione generale dei valori ottenuti. Nella tabella seguente sono ricapitolati, per comodità, i valori di severità delle classi, con l'aggiunta della categoria "Nulla" nella quale confluiscono gli scenari per i quali è stata calcolata una frequenza di eventi pari a 0.

Classe	Valore Severità	Numero di eventi della distribuzione cumulata per categoria
Extraordinary	> 10%	46
Mega	1% - 10%	277
Big	0,1% - 1%	850
Tolerable	0,01% - 0,1%	2461
Small	0,0001% - 0,01%	1424
Micro	< 0,0001%	804
Nullo	= 0	4138

Tabella 22. Numero di scenari per ciascuna classe di severità.

La figura 31 riporta un grafico con indicazione del numero di scenari per i quali è stato individuato un certo tipo di severità cumulata. Dal grafico è possibile osservare come la distribuzione della severità cumulata ottenuta per i valori espressi in percentuale rispecchi molto per forma quella in figura 28 per i dati espressi in scala logaritmica: si riscontra un

picco per eventi con severità nulla e si nota un andamento normale al crescere della severità, con una concentrazione di eventi "*Tolerable*".

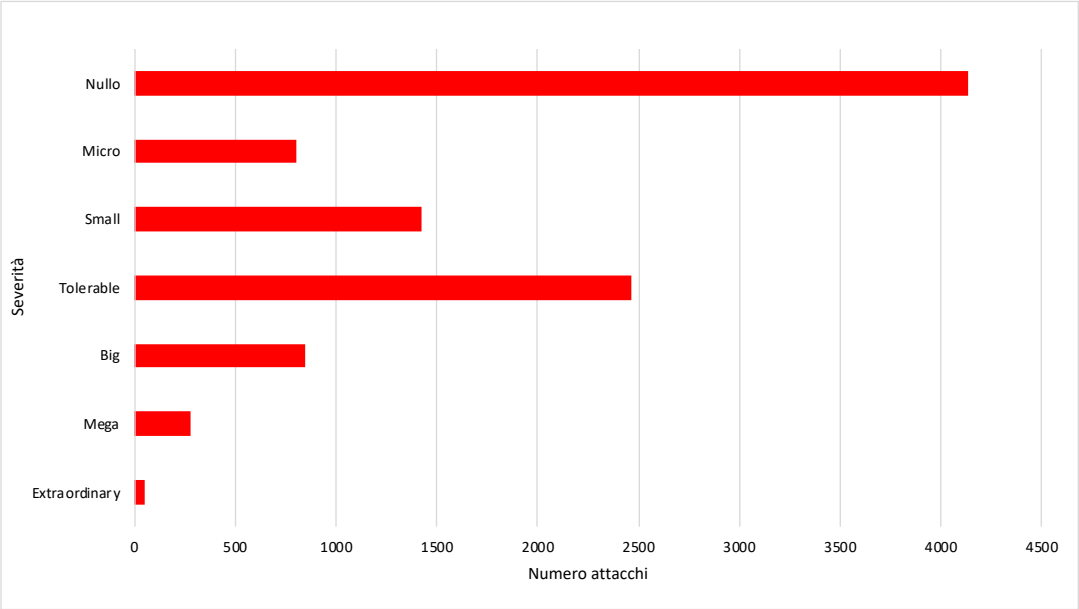


Figura 32. Distribuzione degli eventi per classe di severità.

5.5.2 Calcolo del VaR

Il calcolo del valore a rischio con la simulazione Montecarlo è effettuato utilizzando la seguente formula:

$$VaR = perdita\ al\ percentile - EL$$

Dove:

perdita al percentile = perdita al percentile di riferimento selezionato. Di norma sono utilizzati il 99°, 98° o 95° percentile;

EL = *Expected Loss*, perdita attesa (media).

Tramite la funzione di *Excel* apposita, sono stati calcolati, per i valori di severità cumulata ottenuta, i valori dei percentili di riferimento:

Percentile	Perdita
99°	0,042407044
98°	0,01965326
95°	0,005024669

Tabella 23. Valori dei percentili di riferimento.

Sono state, in seguito, calcolate alcune delle principali statistiche della distribuzione di severità cumulata:

Statistica	Valore
Media	0,003002868
Deviazione standard	0,051476566
Varianza	0,002649837
Mediana	0,000001223

Tabella 24. Principali statistiche della distribuzione di severità cumulata.

È stato quindi possibile calcolare il valore del VaR corrispondente a ciascun percentile.

Percentile	Valore VaR
99°	0,039404175
98°	0,016650391
95°	0,002021800

Tabella 25. Valori di VaR corrispondenti a ciascun percentile.

I valori di VaR così calcolati fanno riferimento a valori di severità cumulati, calcolati sulla base di tutte le aziende, nell'arco di un trimestre.

Prendendo come riferimento il valore del VaR al 99° percentile, è pertanto possibile affermare che con il 99% di probabilità, nell'arco di un trimestre, i crimini informatici colpiranno il mercato finanziario nel suo complesso per un valore non superiore al 3,9% del valore totale delle attività del settore nel suo complesso. Questo valore rappresenta quindi il grado di esposizione del settore finanziario al fenomeno del *cybercrime*.

5.6 Expected Shortfall

L'*Expected Shortfall* (ES) è una misura di rischio che può essere interpretato come il valore atteso delle perdite che si può verificare qualora il danno ecceda il *Value at Risk*. L'ES rappresenta quindi un valore condizionato al superamento del VaR ed è descrivibile con la seguente formula:

$$ES = E[Perdite|Perdite > VaR]$$

Graficamente, l'ES rappresenta la media delle perdite registrate nella parte di coda di una distribuzione non compresa nel VaR (figura 32).

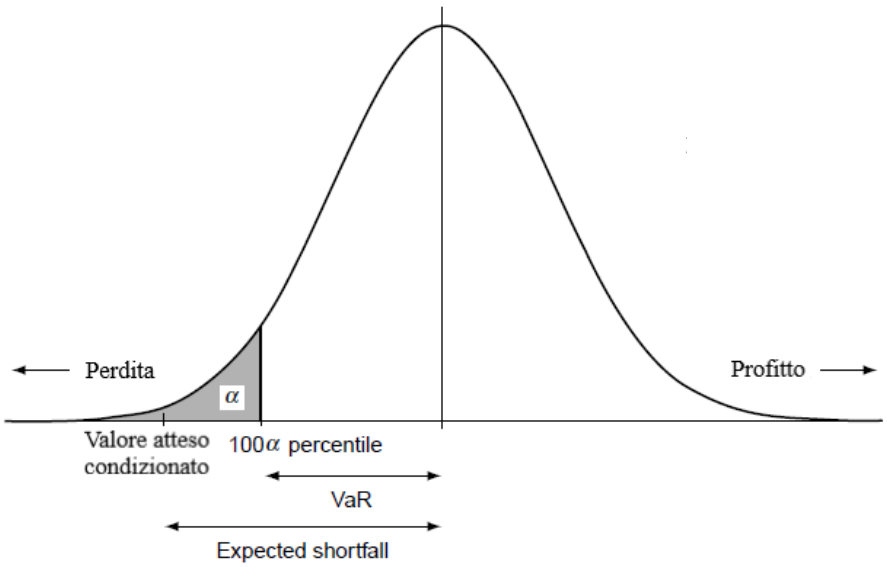


Figura 33. Rappresentazione grafica di VaR e ES.

Al fine di ottenere una stima del valore dell'*Expected Shortfall* è quindi necessario calcolare il valore atteso delle perdite tali che esse siano superiori al VaR.

Effettuando il calcolo per i dati raccolti di ottiene un valore di ES pari a 0,220724295. Trasformando tale valore in percentuale, è possibile affermare che, qualora nell'arco del trimestre i danni subiti dal mercato finanziario impattino sulla ricchezza totale per un valore superiore al 3,9%, è ragionevole ritenere che le perdite avranno un'entità, in media, tale da rappresentare il 22,07% della ricchezza totale del settore.

VI Conclusioni

Nel presente elaborato è stato analizzato il fenomeno del *cybercrime* nel mondo finanziario. Sulla base dei dati raccolti e delle analisi effettuate è possibile affermare che le società finanziarie risultano molto esposte a questo pericolo, indipendentemente dalla loro dimensione e dalla localizzazione geografica. I criminali informatici, infatti, attaccano indistintamente le aziende e il *target* può variare in base agli interessi personali di chi commette il reato o alla volontà di chi lo commissiona. L'analisi svolta sul *database* raccolto ha evidenziato, inoltre, che non esiste correlazione tra la frequenza con cui il le aziende sono attaccate e la severità dell'attacco. Società di grosse dimensioni possono subire danni ridotti grazie alla capacità di difesa del proprio *asset* di risorse o danni importanti, conseguenza della grande scala su cui è condotto l'attacco. Al contrario, aziende piccole possono subire conseguenze marginali grazie al minore interesse degli *hacker* a colpire piccole realtà, o danni enormi a causa dell'insufficiente sistema di difesa.

L'obiettivo dello studio di dare un'indicazione dell'impatto dei crimini informatici sul settore finanziario è stato approcciato effettuando una simulazione Montecarlo a seguito della quale è stato calcolato un *Value at Risk* al 99-esimo percentile pari a 0,039404175. Questo risultato permette di affermare che nel 99% dei casi, nell'arco di un trimestre, il settore finanziario nel suo complesso subirà un danno non superiore al 3,9% del valore totale delle attività. Il valore ottenuto evidenzia come i crimini informatici rappresentino una minaccia reale per il settore, il quale è colpito giornalmente da attacchi di questo tipo. Il 3,9% del valore delle attività è infatti un valore importante sia in termini relativi per il settore stesso che risulta colpito sia in termini di valore economico assoluto.

Il valore stimato è stato ottenuto a seguito di una serie di assunzioni e pertanto è da considerare indicativo. È stato calcolato prendendo in considerazione, come valori significativi, frequenza e severità degli attacchi, a loro volta considerati in relazione a dimensione e localizzazione della società.

L'assenza di fonti pubbliche alle quali poter attingere come base dati è sicuramente uno dei principali limiti del presente elaborato. La stima è stata effettuata utilizzando le informazioni contenute in un *database* costruito *ad hoc* e in cui sono stati riportati i casi di attacchi informatici dei quali sono state diffuse informazioni *online*. La ricerca è stata effettuata con cura al fine di includere solamente dati provenienti da fonti affidabili ma sarebbe necessario avere a disposizione una base dati più sostanziosa per effettuare calcoli

più accurati. È inoltre necessario tenere presente che la stima del VaR effettuata potrebbe risultare una sovrastima del valore reale in quanto è ragionevole ritenere che i casi di reati che hanno avuto conseguenze trascurabili o lievi siano più facili da tenere nascosti all'opinione pubblica rispetto invece a quelli che hanno comportato conseguenze importanti e che le società sono state obbligate a dichiarare.

Comunemente, il valore a rischio è espresso relativamente ad una singola azienda per la quale è calcolato il valore massimo delle perdite in cui può incorrere, con una certa probabilità, nell'arco di tempo considerato. Nel presente elaborato, a causa della impossibilità di reperire informazioni dettagliate per una singola società, è stato considerato il mercato nel suo complesso e pertanto è stato calcolato non un costo ma un valore percentuale, indicato come incidenza del fenomeno sul settore nel suo complesso.

Un'evoluzione futura dello studio potrebbe includere analisi più dettagliate sulle variabili che, oltre a dimensione e localizzazione, possono impattare su frequenza e severità degli attacchi. Qualora ci fosse disponibilità di un *database* più ampio potrebbe essere interessante anche restringere il campo di applicazione, considerando separatamente un valore di VaR per le società piccole, medie e grandi. Infine, un'azienda che disponga di un servizio di monitoraggio e tenga traccia di tutti gli attacchi informatici subiti, sia che questi abbiano recato danno effettivo, sia che siano stati fermati dal sistema informativo o prevenuti grazie ad un'organizzazione efficacie, potrebbe effettuare l'analisi fatta nel presente elaborato, applicandola al caso specifico e individuando un valore di VaR specifico per l'azienda.

In conclusione, l'analisi effettuata in questo lavoro di tesi presenta alcuni limiti ma rappresenta uno studio volto ad analizzare il danno che il settore nel suo complesso di trova ad affrontare.

VII Sitografia

- Treccani (http://www.treccani.it)
- The Times (https://www.thetimes.co.uk/)
- The Wall Street Journal (https://www.wsj.com/)
- The New York Times (https://www.nytimes.com/)
- Banca Centrale Europea (https://www.ecb.europa.eu/ecb/html/index.it.html)
- Da meno di 10 a 1000 dollari, ecco quanto costano i nostri dati nel dark web, Repubblica (https://www.repubblica.it/tecnologia/sicurezza/2015/10/19/news/da_meno_di_10_a_1000_dollari_ecco_quanto_costano_i_nostri_dati_nel_dark_web-125429639/#gallery-slider=125429824)
- Furto di identità: ecco quali informazioni e (dati) tenere protetti, Il sole 24 Ore (https://www.ilsole24ore.com/art/furto-identita-ecco-quali-informazioni-e-dati-tenere-protetti-AEpxNZ9G)
- Il valore dei dati è un asset chiave nella digital trasformation, Il Sole 24 Ore (https://www.ilsole24ore.com/art/il-valore-dati-e-asset-chiave-digital-trasformation-AEzwdclD)
- BASILEA II, Standard per la gestione del credito delle banche, Borsa Italiana (https://www.borsaitaliana.it/notizie/sotto-la-lente/basileaii.htm)
- Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, Inter Lex (http://www.interlex.it)
- Recepimento della nuova regolamentazione prudenziale internazionale (nuovo accordo sul capitale di Basilea e nuova direttiva C.E. sui requisiti di capitale delle banche e delle imprese di investimento), rischi operativi (Metodi Base e Standardizzato), Banca d'Italia (https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Doc_Cons_Rischi_operativi.pdf)
- The advanced measurement approach for banks, Bank of International Settlements (https://www.bis.org/ifc/publ/ifcb33p.pdf)
- BIS Working Papers, The drivers of cyber risk, No 865, Bank of International Settlements (https://www.bis.org/publ/work865.pdf)

- Cos'è il Cybercrime e come possono combatterlo le aziende in Italia, Osservatori.net, Digital Innovation (https://blog.osservatori.net/it_it/cybercrime-definizione-italia)
- Pirateria informatica, cos'è e dove si nasconde, Associazione PMI (http://www.associazionepmi.it/news/sicurezza/cybercrimine-pirateria-informatica.html)
- Attacchi di cyber war: quali sono, come funzionano, Agenda Digitale (https://www.agendadigitale.eu/sicurezza/attacchi-di-cyber-war-quali-sono-come-funzionano/)
- Dal concetto di cyber attack al cyberwarfare: l'uso della forza in ambito cyber, Cybersecurity 360 (https://www.cybersecurity360.it/nuove-minacce/dal-concetto-di-cyber-attack-al-cyberwarfare-luso-della-forza-in-ambito-cyber/)
- California Legislative Information, Civil Code – civ, Division 3. Obligations [1427 - 3273], Part 4. Obligations arising from particular transactions [1738 - 3273], title 1.81. Customer records [1798.80 - 1798.84] (https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82)
- Regolamento Generale sulla Protezione dei dati, Garante per la Protezione dei Dati Personali, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018.pdf/1bd9bde0-d074-4ca8-b37d-82a3478fd5d3?version=1.9)
- Operational Risk Management, Basle Committee on Banking Supervision, Basle September 1998; Bank of International Settlements (https://www.bis.org/publ/bcbs42.pdf)
- The New Basel Capital Accord, Issued for comment by 31 May 2001, January 2001, Bank of International Settlements (https://www.bis.org/publ/bcbsca02.pdf)
- Internal Measurement Approach to operational Risk Capital Charge, Bank of Japan (https://www.boj.or.jp/en/research/wps_rev/wps_2001/data/fwp01e02.pdf)
- A Critique of the Advanced Measurement Approach to Regulatory Capital Against Operational Risk

(http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.474.9427&rep=rep1&type=pdf)

- Scorecard Models for Operational Risk Management (http://old.sis-statistica.org/files/pdf/atti/SIS%202007%20Venezia%20intermedio_63-69.pdf)
- La simulazione Monte Carlo (http://static.gest.unipd.it/labtesi/eb-didattica/EAI/montecarlo)
- https://ycharts.com/companies/BAC/assets

VIII Bibliografia

- Varetto Franco, Economia degli Intermediari Finanziari, Rischio Operativo
- Rapporto CLUSIT 2020 sulla sicurezza ICT in Italia
- Rapporto CLUSIT 2019 sulla sicurezza ICT in Italia
- Rapporto CLUSIT 2018 sulla sicurezza ICT in Italia

IX Ringraziamenti

A conclusione dell'elaborato desidererei ringraziare alcune persone che mi hanno accompagnata durante il percorso universitario e mi sono state di supporto durante la stesura della presente tesi.

Un primo ringraziamento al mio relatore, il professore Franco Varetto, che da una mia prima proposta generale ha saputo fornirmi consigli concreti, idee e supporto per la stesura della tesi. Lo ringrazio per la disponibilità dimostrata nei miei confronti e per il suo sostegno.

Vorrei ringraziare in particolar modo mia mamma Anna, la quale mi ha sostenuta durante tutta la mia carriera scolastica, dal periodo delle elementari, quando tutto era facile, fino all'università, dove ho incontrato qualche difficoltà in più. Il suo essere sempre presente, con parole di sprone ed incoraggiamento ma anche di critica, è stato per me fondamentale. La ringrazio inoltre per avermi dato la possibilità, durante tutti questi anni, di dedicarmi interamente allo studio senza preoccupazioni. A lei vanno tutta la gratitudine e la riconoscenza di cui sono capace. I suoi famosi "no" mi hanno resa ciò che oggi sono e mi hanno insegnato molto, anche se ho ancora tanto da imparare.

Desidero poi ringraziare la mia famiglia che mi è sempre stata vicina e mio nonno, che sta aspettando la mia festa di laurea con impazienza.

Proseguo ringraziando la mia amica di lunga data Malvina la quale, nonostante la distanza, è sempre presente nella mia vita e con la quale avrò in comune, d'ora in poi, anche il giorno di laurea. Unitamente devo ringraziare la mia amica Micol, consulente medica personale nel momento del bisogno e le mie amiche con le quali aspetto in coda al ristorante tutti i sabati sera. Vorrei anche ringraziare Edoardo che mi ha fornito spunti utili per questa tesi.

Ultimo ma non meno importante un ringraziamento al mio ragazzo Enrico, il quale ha saputo darmi consigli utili e pratici che mi hanno permesso di arrivare fino a qui, mi ha incoraggiata sempre e "rimproverata" quando, ammetto, me lo meritavo. Tra giri in moto e bagni in acque verdi mi ha insegnato a rendere facili le cose difficili.

Infine, un particolare ringraziamento a Bruno, Lina e Attilio, angeli custodi il cui pensiero mi sostiene ogni giorno della vita.