POLITECNICO
DI TORINO

Corso di Laurea Magistrale in Ingegneria Gestionale

Tesi di Laurea Magistrale

Modelli quantitativi per la cybersecurity negli intermediari finanziari

Relatore
prof. Franco Varetto

Candidato
Marco Lingua
matricola: 264603

Anno Accademico 2020/2021

Abstract

Per le istituzioni finanziarie, la cybersecurity rappresenta una nuova frontiera dei rischi operativi. In un settore con un tasso di digitalizzazione estremamente alto, la crescita delle cyber minacce ha raggiunto livelli inediti e gli attacchi informatici hanno raggiunto un grado di imprevedibilità, di impatto potenziale e di capacità diffusiva senza precedenti. Il processo di gestione dei cyber rischi risulta, pertanto, una pratica fondamentale per la sicurezza di un'organizzazione, indipendentemente dalle sue dimensioni e dalla sua collocazione geografica. In un contesto globale segnato dall'incertezza e in assenza di uno standard normativo univoco sono ancora troppe le infrastrutture con scarsa sensibilità e preparazione alle minacce provenienti dal cyber spazio, esponendosi ogni giorno ad un attacco invisibile e potenzialmente disastroso. Questa tesi nasce durante l'esperienza di tirocinio condotta dall'autore presso la società Augeos S.p.A. di Rivoli (TO) , operante nell'ambito dei servizi finanziari e della consulenza destinata agli intermediari finanziari, la quale ha proposto un percorso di conoscenza e approfondimento della cybersecurity volto alla creazione di uno modello prototipale per la gestione dei cyber rischi. Il lavoro è organizzato in sei capitoli: nel primo viene effettuata una breve panoramica attuale dello scenario globale e alcune definizioni introduttive necessarie alla comprensione della tematica affrontata. Nel secondo capitolo si pone un focus sulla cybersecurity negli istituti finanziari e nei settori ad essi connessi, riportando gli eventi recenti più significativi, oltre che un approfondimento sull'effetto della pandemia da COVID-19 sugli attacchi informatici e sulla potenziale evoluzione a livello sistemico dei cyber rischi. Nel terzo capitolo viene affrontata la tematica del *risk management* all'interno del settore finanziario, partendo da un punto di vista generale e focalizzandosi sulle normative vigenti in ambito della sicurezza informatica e delle criticità annesse. Nel quarto capitolo si descrive puntualmente il modello sviluppato per l'analisi di uno o più cyber rischi, con le ipotesi di base, le formule che permettono il suo funzionamento ed i risultati ottenuti. Nel quinto capitolo si propone un'estensione del modello descritto in precedenza basata sulla scomposizione dei rischi secondo la loro tipologia di impatto, riportando, come nel caso precedente, le assunzioni, le formule e gli output. Nel sesto capitolo, infine, si traccia un breve riassunto di quanto descritto in precedenza, riportando le conclusioni, i risultati raggiunti e i futuri sviluppi auspicabili.

Indice

Capitolo 1

Introduzione

1.1 Definizioni

Il termine "cybersecurity" risulta largamente utilizzato in svariati ambiti teorici e applicativi e le sue definizioni risultano altamente variabili, poiché includono considerazioni soggettive e spesso ambigue. Ad oggi non risulta ancora esserci una definizione univoca e totalmente accettata che catturi correttamente la sue molteplici accezioni, richiedendo, di fatto, l'esistenza di un termine di riferimento che includa tutte quelle discipline tecniche che concorrono nel risolvere problemi di sicurezza informatica. In letteratura è possibile ritrovare numerosi aspetti che possono essere direttamente collegati alla cybersecurity nelle più svariate discipline, dalle scienze politiche e sociali all'ingegneria, e alle scienze computazionali. Un primo passo verso la definizione di questo termine può essere effettuato analizzando attentamente i due termini che lo compongono:

- *Cyber*, un prefisso che si riferisce alla reti di comunicazioni elettroniche e alla realtà virtuale. Deriva a sua volta dal termine "cybernetica", ovvero «l'ambito delle scienze del controllo e della comunicazione» [1]. La parola "cyberspazio" è stata resa popolare dal romanzo *Neuromante*, scritto da William Gibson nel 1984, nel quale descrive uno spazio tridimensionale costituito puramente da dati e informazioni, generate e utilizzate dagli esseri umani. Public Safety Canada definisce il cyberspazio come "il mondo elettronico creato da reti di informazione interconnesse e dalle informazioni stesse, nel quale gli esseri umani sono connessi tra di loro condividendo idee e servizi" [2]. Secondo Deibert e Rohozinsky [3], il cyberspazio non rappresenta un'entità statica, bensì in costante evoluzione e racchiude dentro di sé un insieme di infrastrutture hardware e software, aspetti regolatori, idee, innovazioni e interazioni tra le persone che ne fanno parte.
- *Security*, ovvero la pratica condotta da un certo soggetto operante in una determinata struttura che mira a difendere un altro soggetto (nel senso più

globale del termine) da una certa minaccia, al fine di preservare tutte o parte delle sue caratteristiche.

Come detto in precedenza, il termine cybersecurity riguarda una moltitudine di aspetti pratici e concettuali e la ricerca di una sua definizione porta a numerose varianti, le quali differiscono tra loro sia per gli attori che esse includono che per l'ambito di destinazione. Di seguito si riportano le principali specificazioni rintracciabili in letteratura:

1. «La pratica di proteggere o difendere il cyberspazio da un cyber attacco oppure il processo di proteggere le informazioni attraverso la prevenzione, il rintracciamento e la risposta ad un attacco.» [4]

2. «La sicurezza informatica consiste in gran parte in metodi difensivi utilizzati per rilevare e contrastare potenziali intrusi.» [5]

3. «La sicurezza informatica implica la riduzione del rischio di attacchi dannosi a software, computer e reti. Ciò include strumenti utilizzati per rilevare intrusioni, bloccare i virus, bloccare l'accesso dannoso, applicare l'autenticazione, abilitare le comunicazioni crittografate e così via.» [6]

4. «Lo stato di protezione contro l'uso criminale o non autorizzato di dati elettronici o le misure adottate per raggiungere questo obiettivo. »[7]

5. «La sicurezza informatica implica la salvaguardia delle reti di computer e delle informazioni che contengono dalla penetrazione e da danni o interruzioni dolosi.» [8]

6. «L'attività o il processo, l'abilità o la capacità in base alla quale i sistemi di informazione e comunicazione e le informazioni in essi contenute sono protetti e/o difesi da danni, uso o modifica non autorizzati o sfruttamento.» [9]

7. «Rischi operativi per le risorse informatiche e tecnologiche che hanno conseguenze influenzanti la riservatezza, la disponibilità o l'integrità delle informazioni o dei sistemi informativi.» [10]

8. «L'arte di assicurare l'esistenza e la continuità della società dell'informazione di una nazione, garantendo e proteggendo, nel Cyberspazio, le sue informazioni, beni e infrastrutture critiche.» [11]

9. «La sicurezza informatica è la raccolta di strumenti, politiche, concetti di sicurezza, salvaguardie di sicurezza, linee guida, approcci di gestione del rischio, azioni, formazione, pratiche, garanzie e tecnologie che possono essere utilizzate per proteggere l'ambiente informatico, l'organizzazione e le risorse dell'utente.» [12]

10. «Il corpus di tecnologie, processi, pratiche e misure di risposta e mitigazione progettate per proteggere reti, computer, programmi e dati da attacchi, danni o accessi non autorizzati in modo da garantire riservatezza, integrità e disponibilità.» [13]

Analizzando tutte queste definizioni è possibile osservare come esse facciano in gran parte riferimento a concetti ed attività prevalentemente tecnici e pratici, tralasciando gli aspetti più morali e quelli che includono le iterazioni umane. In un già citato articolo, nel tentativo di coniare una definizione di cybersecurity che fosse quanto più esaustiva e oggettiva possibile, sono stati individuati cinque differenti ambiti che giocano un ruolo fondamentale: soluzioni tecnologiche, eventi, processi e metodi strategici, fattori umani e oggetti della sicurezza. Da tale lavoro è emersa la seguente definizione:

> «La sicurezza informatica è l'organizzazione e la raccolta di risorse, processi e strutture utilizzate per proteggere il cyberspazio e i sistemi abilitati per il cyberspazio da eventi che separano i diritti di proprietà *de jure* da quelli *de facto*.» [2]

Focalizzandosi per un attimo su questo enunciato è possibile notare come esso catturi tutti quegli aspetti menzionati in precedenza, includendo le interazioni tra umani e umani, tra sistemi e sistemi e tra umani e sistemi, considerando l'aspetto relativo alla protezione da determinate minacce, che siano di tipo intenzionale o accidentale. Infine, si fa riferimento alla separazione tra proprietà e controllo: un evento o una attività che disallinea i diritti di proprietà attuali (de facto) da quelli percepiti (de jure) è considerabile un incidente informatico. Nelle seguenti pagine verrà fatto uso di questa definizione riferendosi alla cybersecurity come a un aspetto del tutto rilevante nella gestione dei numerosi rischi che possono verificarsi all'interno di una qualunque infrastruttura che opera in ambito finanziario.

Come enunciato in precedenza, all'interno della sicurezza informatica ricadono sia quelle pratiche dannose scaturite da azioni non intenzionali sia i crimini eseguiti da un agente esterno malevolo. E' possibile suddividere questa categoria in due classi distinte, la cui distinzione è stata proposta dal Crown Prosecution Service: crimini *cyber-dipendenti* e *cyber-autorizzati*, come si evince dalla figura sottostante.

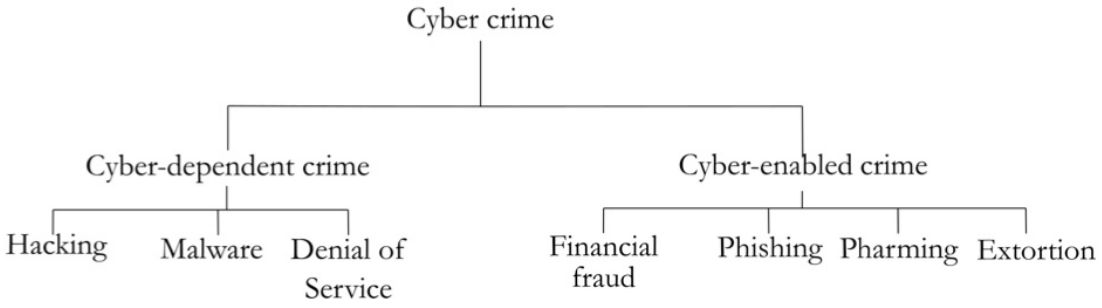

Figura 1.1: Famiglie di cyber crimini (fonte: [14])

Rientrano nel primo gruppo quegli atti che possono essere compiuti solamente utilizzando un computer, una rete di computer o altre tecnologie di comunicazione, mentre appartengono alla seconda categoria quei crimini tradizionali, il cui impatto può essere aumentato attraverso l'utilizzo di computer, di una una rete o tramite altri mezzi tecnologici.

1.2 Tassonomia dei cyber rischi

Secondo Cebula e Young è possibile definire un qualsiasi cyber-rischio come:

> «[...] un evento di natura operativa che si manifesta sugli asset informativi impattando la confidenzialità, la disponibilità e l'integrità dei dati o del sistema informativo stesso.» [10]

Questa tipologia di rischio può impattare sia sul target diretto dell'attacco, sia sulla sua controparte (ovvero le terze parti), provocando perdite economiche mediamente indipendenti tra di loro e dall'importo contenuto, nonostante sia possibile osservare rischi con bassa frequenza di accadimento ma impatto piuttosto elevato. Una particolarità del cyber rischio è il suo essere non necessariamente una conseguenza di un cyber attacco: rientrano infatti in questa categoria anche quei rischi provocati da attori non malevoli o da comportamenti non intenzionali, oppure ancora da processi operativi che non mirano a compiere un crimine (come un semplice aggiornamento software) oppure ancora disastri naturali il cui impatto si può ripercuotere direttamente sul business dell'organizzazione e sulla solidità delle informazioni in esso contenuta.

Un cyber attacco riguarda tipicamente i tre aspetti essenziali della sicurezza informatica: *confidenzialità*, quando informazioni private e sensibili risultano esposte a terze parti non autorizzate, *disponibilità*, quando i processi e le informazioni non risultano fruibili da chi ne necessita, provocando interruzioni del servizio, *integrità*,

ovvero la perdita totale o parziale di componenti dell'informazione. Qualsiasi tipologia di organizzazione pubblica o privata fa uso di processi IT per rendere migliore il proprio business e per veicolare i servizi offerti: un qualunque danneggiamento di questi asset (siano essi fisici o logici) lede la possibilità dell'impresa stessa di adempire alla sua *mission*. Vista l'importanza ricoperta da questi processi è di primaria importanza la fase di gestione del rischio per saper fronteggiare le tutte le potenziali minacce. A tal scopo, prima ancora di individuare un rischio, è necessario sapere a *cosa* ci si sta riferendo, ovvero, si rende opportuno disporre di un certo elenco di termini e definizioni che permettano di descrivere *in toto* il fenomeno in questione. Nelle pagine seguenti si fa riferimento alla tassonomia introdotta in [15] con lo scopo di identificare e organizzare le fonti dei rischi da cybersecurity in modo gerarchico, dividendo i cyber rischi in quattro *classi* distinte: 1) comportamenti umani 2) fallimenti tecnologici 3) fallimento dei processi interni 4) eventi esterni. Ciascuna di queste quattro classi è stata a sua volta divisa in *sottoclassi*. L'utilizzo di un framework di riferimento non è univoco, e può essere liberalmente integrato da altre definizioni o metodi che meglio rispettino l'operatività e il profilo di rischio dell'organizzazione che ne fa uso. Nelle righe seguenti si riportano dettagliatamente i singoli rischi contenuti nella tassonomia indicata.

1.2.1 Comportamenti umani

Questa classe incorpora tutti quei rischi derivanti da azioni intraprese intenzionalmente o non intenzionalmente da soggetti umani che si trovano all'interno o all'esterno della struttura aziendale. La prima sottoclasse in cui sono divisi è quella delle *azioni involontarie*, dove troviamo:

- *errori giustificati*: comportamenti tenuti da individui che conoscono le necessarie procedure corrette ma falliscono nel momento in cui le mettono in pratica

- *errori non giustificati*: comportamenti tenuti da individui che non conoscono le necessarie procedure corrette e falliscono nel momento in cui le mettono in pratica

- *omissione*: quando un operatore non intraprende un'azione corretta a causa dell'esecuzione affrettata di una certa procedura.

Nella seconda sottoclasse sono contenute le azioni cosiddette "deliberate", ovvero quelle intraprese intenzionalmente da alcuni soggetti interni o esterni che agiscono con l'intendo provocare un danno.

- *frode*: azione tenuta deliberatamente per ottenere un beneficio a spese di un altro individuo.

- *sabotaggio*: azione intrapresa con il fine di causare un fallimento all'interno di un asset o di un processo, tipicamente targetizzata verso asset chiave e facendo uso di conoscenza interna all'organizzazione.
- *furto*: appropriazione intenzionale e non autorizzata di un certo asset informativo.
- *vandalismo*: danneggiamento intenzionale di un certo bene tangibile o intangibile, spesso compiuta senza un vero e proprio obiettivo ma con il semplice intendo di provocare un danno.

La terza e ultima sottocalsse è denominata "inaction", e può essere intesa come l'incapacità di compiere certe azioni o di far fronte a determinate situazioni. All'interno possiamo trovare mancanze di:

- *skills*: la mancanza di abilità personali utili a fronteggiare un dato problema.
- *conoscenza*: l'ignoranza di un certo individuo, intesa come la non consapevolezza (giustificata o no) di un dato aspetto.
- *guida*: l'incapacità di prendere decisioni e di guidare se stessi o un gruppo di persone al compimento di un'azione.
- *disponibilità*: l'inesistenza delle risorse appropriate necessarie per fronteggiare una criticità

1.2.2 Fallimenti tecnologici

Questa classe è stata introdotta con l'obiettivo di includere tutte quelle problematiche derivanti da un funzionamento anormale o inatteso degli asset tecnologici. Nella prima sottoclasse si trovano le caratteristiche degli *hardware* che concorrono al verificarsi di un certo rischio:

- *capacità*: l'inabilità di sopportare un dato carico di lavoro o di gestire un certo numero di informazioni.
- *performance*: l'inabilità di completare determinate istruzioni e di svolgere incarichi rispettando certi parametri funzionali, come il consumo energetico, il surriscaldamento e la velocità.
- *manutenzione*: il mancato mantenimento degli aggiornamenti necessari o consigliati degli asset.
- *obsolescenza*: il prolungato utilizzo di un dispositivo oltre la sua vita utile.

Nella seconda sottoclasse sono indicati gli aspetti *software*, intesi come programmi, applicazioni e sistemi informativi. Qui si ritrovano i seguenti elementi:

- *compatibilità*: inabilità di due o più porzioni di software nel lavorare assieme correttamente.
- *gestione della configurazione*: applicazione impropria delle impostazioni e dei parametri necessari al funzionamento.
- *modifica dei controlli*: cambiamento nella configurazione dell'applicazione in mancanza di autorizzazione, rigore o conoscenza.
- *impostazioni di sicurezza*: errato procedimento di *setting* dei parametri di sicurezza del programma o dell'applicazione, rendendoli troppo restrittivi o troppo superficiali.
- *pratiche di programmazione*: errori nella stesura del codice, che includono la sintassi o l'organizzazione logica delle stringhe.
- *test*: pratica atipica o inadeguata nel test e nella configurazione dei programmi.

La sottoclasse successiva riguarda i *sistemi* e il loro fallimento nell'integrazione con altri e nel funzionamento finale. Questo comportamento è descritto dai seguenti elementi:

- *design*: inadeguata costruzione del sistema per l'utilizzo inteso.
- *specifiche*: impropria definizione delle specifiche necessarie o la mancata conformità agli standard richiesti al momento della costruzione del sistema.
- *integrazione*: malfunzionamento congiunto di più elementi una volta interfacciati.
- *complessità*: quando il sistema risulta poco intuitivo e troppo intricato rispetto al livello richiesto dell'organizzazione.

1.2.3 Fallimento dei processi interni

In questa classe sono riportate tutte le caratteristiche che provocano un rischio derivante dal fallimento dei processi interni e dal conseguente malfunzionamento; sono presenti tre distinte sottoclassi.

- *flusso di processo*: studio inadeguato del flusso di *outputs* vero i rispettivi destinatari.
- *documentazione dei processi*: documentazione non adeguata sugli outputs e sugli *stakeholders*.
- *ruoli e responsabilità*: insufficiente comprensione dei ruoli e delle responsabilità di ciascun attore coinvolto.

- *notifiche e avvisi*: processo inadeguato di segnalazione di potenziali criticità e pericoli.
- *flussi di informazione*: design scarno e non sufficiente relativo ai vari flussi di informazione e degli attori a cui sono destinati.
- *escalation dei problemi*: incapacità di ridurre problematiche inattese da parte del personale dedicato.
- *accordi di servizi legali*: mancanza di accordi legali tra i vari stakeholders riguardo alle aspettative di un certo servizio.
- *task hand-off*: trasferimento della responsabilità verso un certo problema da un operatore all'altro.

La seconda sottoclasse è riferita ai *controlli di processo* e descrive i fallimenti dei vari processi che possono intercorrere all'interno di un'organizzazione. Si descrivono i seguenti elementi:

- *monitoraggio degli status*: fallimento nel monitorare le varie *routines* informative relative ad un certo processo.
- *metriche*: fallimento nell'utilizzo di adeguati indicatori di performance temporali.
- *revisioni periodiche*: fallimento nelle necessarie revisioni dei processi *end-to-end* e nell'intraprendere le azioni correttive consigliate.
- *ownership dei processi*: inefficacia di un certo processo nel compiere i propri compiti a causa di responsabilità non correttamente definite e mancanza di una adeguata *governance*.

Nella terza e ultima sottoclasse si riportano i *processi di supporto* intesi come quelle azioni di sostegno ai processi operativi che non permettono il corretto veicolare delle risorse. All'interno si può trovare.

- *staffing*: inadeguata allocazione di risorse umane al supporto delle operazioni necessarie.
- *funding*: inadeguato apporto di risorse economiche al supporto dei processi e delle operazioni.
- *sviluppo e training*: fallimento nel mantenere le skills necessarie e nello sviluppo di nuove capacità operative.
- *procurement*: fallimento nella procura di beni e servizi necessari al supporto delle operazioni.

1.2.4 Eventi esterni

Questa classe di eventi racchiude dentro sé tutti quei rischi associati a criticità tipicamente al di fuori del controllo dell'azienda, le quali possono essere difficilmente previste o pianificate. Nella prima sottoclasse sono elencati i cosiddetti *hazards*, ovvero i rischi di origine naturale o umana che non sono sotto il controllo dell'organizzazione:

- *eventi atmosferici*: condizioni meteorologiche avverse come pioggia, neve, uragani e tornadi.
- *fuoco*: danneggiamento totale o parziale di asset fisici a causa di incendio.
- *alluvioni*: danneggiamento totale o parziale di asset fisici a causa di alluvioni o allagamenti.
- *terremoti*: interruzione e danneggiamento dell'operatività dell'organizzazione a causa di terremoti.
- *proteste*: interruzione e danneggiamento dell'operatività dell'organizzazione a causa di disordini civili, proteste o attacchi terroristici..
- *pandemic*: interruzione dei processi aziendali a causa della diffusione su scala globale di malattie.

Nella seconda sottoclasse si descrivono le *criticità legali*, nella quale si trovano:

- *compliance regolatoria*: incompatibilità tra le nuove disposizioni governative con quelle già esistenti.
- *legislazione*: impatti negativi di nuove legislazioni sull'organizzazione.
- *dispute legali*: tensioni tra operatori interni e altri stakeholders nei confronti dell'organizzazione.

La terza sottoclasse di rischi comprende al suo interno le *criticità del business*, ovvero quelle problematiche emergenti dall'ambiente (inteso in senso figurato) in cui opera l'azienda. Gli elementi descritti sono:

- *fallimento degli approvvigionamenti*: mancanza di adeguate forniture di beni e servizi essenziali come energia elettrica, risorse idriche e servizi di telecomunicazione.
- *condizioni di mercato*: ridotta capacità dell'organizzazione nel far fronte a condizioni di mercato avverse.
- *condizioni economiche*: incapacità dell'azienda nell'ottenere i necessari approvvigionamenti finanziari.

Nell'ultima sottoclasse sono poi riportati i rischi derivanti dai *servizi esterni*, ovvero quando le minacce provengono da comportamenti (intenzionali e non) di una o più controparti esterne all'azienda, come:

- *utenze*: fallimento nella fornitura di beni e servizi essenziali, come utenze elettriche.
- *servizi di emergenza*: apporto non adeguato dei servizi pubblici come assistenza medica, antincendio e servizi di polizia.
- *carburanti*: insufficiente fornitura di liquidi carburanti utili a sopperire alla mancanza di servizi essenziali (si pensi ad un generatore alimentato a combustibile fossile utilizzato in assenza di corrente elettrica).
- *trasporti*: fallimenti nei trasporti di beni e servizi (inclusi i dipendenti) che possono in qualche modo impattare sull'operatività giornaliera dell'azienda.

Tutti questi rischi elencati seguono la tassonomia proposta dagli autori e descrivono esaustivamente tutti o quasi i rischi da cybersecurity riscontrabili all'interno di una organizzazione. Nella fase di gestione del rischio è infatti fondamentale il saper riconoscere e classificare un certo rischio e le criticità ad esso associate; nei capitoli successivi verranno descritte le altre fasi del *risk management* applicato alla sicurezza informatica.

1.3 Principali attori all'interno del cyber-crimine

Una volta definiti i concetti di cybersecurity e le altre definizioni ad esso correlate è possibile soffermarsi sugli *attori*, ovvero su chi siano le persone che conducono un cyber-rischio e quali siano le motivazioni che muovono queste persone. Secondo il Canadian Centre for Cybersecurity è possibile definire questi CTA (dall'inglese "Cyber Threat Actors", ovvero i protagonisti delle cyber-minacce) come:

> «[...] Singole persone o individui che compiono azioni malevole e ostili nei confronti di un altro soggetto mediante l'utilizzo di computer, strumentazione elettronica, sistemi informatici e reti.» [16]

E' possibile suddividere i CTA in base alla loro motivazione e all'organizzazione alla quale si riconoscono o sono affiliate:

1. *Cybercriminali*, ovvero gruppi di singole persone guidate che agiscono per scopo di lucro e rappresentano una minaccia nel lungo periodo, difficilmente eradicabile e strutturalmente organizzata. Il loro obiettivo principale sono dati e informazioni sensibili che poi rivendono o ne chiedono il riscatto, oppure agiscono per motivi personali e per ledere alla reputazione della vittima.

2. *Insiders*, trattasi di impiegati o stretti collaboratori dell'azienda che hanno quindi accesso ai suoi sistemi, reti o alle sue informazioni. Questi individui fanno uso volontario della loro posizione per intraprendere azioni dannose contro l'organizzazione, a differenza di altri che, ad esempio, provocano una minaccia non intenzionalmente. La loro motivazione è prettamente economica o per rivalsa personale.

3. *Nation-State*, quei soggetti che conducono azioni tipicamente aggressive nei confronti di istituzioni pubbliche o private, con l'intento di compromettere, rubare o distruggere informazioni. La loro peculiarità risiede nel fatto che fanno parte di apparati statali o sono alle direttive di una certa nazione, dalla quale ne ricevono il supporto economico e tecnologico. Essi sono mossi da motivazioni di spionaggio oppure politiche, economiche, militari, strategiche e geopolitiche.

4. *Hacktivisti*, ovvero hacker criminali mossi da ideologie o da motivazioni sociali e ideologiche ma che agiscono anche per fini economici o per motivi propagandistici. Tipicamente sono affiliati a gruppi criminali più grandi, organizzazioni criminali o agiscono sotto le direttive di una certa etnia o nazione.

5. *Organizzazioni terrorisitiche*, costituiti da quei gruppi di hacker o esperti del settore che utilizzano il cyberspazio principalmente per la comunicazione di stampo terroristico o per il reclutamento di nuove forze alleate. Anch'essi agiscono spinti da diverse motivazioni, da ideologie politiche fino a motivi propagandistici ed economici, oltre che dall'intento di operare ai danni della popolazione civile.

6. *Thrill-seekers*, racchiude tutti quei criminali che agiscono per semplice soddisfazione personale poiché traggono giovamento nel compiere determinate azioni illegali. A questa categoria si può ricondurre lo stereotipo di "hacker", inteso come un singolo isolato che attacca un certo obiettivo esclusivamente per divertimento.

Tutti questi attori differiscono tra loro sia per capacità e conoscenza, ma anche per le risorse a cui possono appoggiarsi. Queste informazioni possono essere utili nello stabilire l'obiettivo dei loro attacchi, così come il danno che ne può scaturire. Tipicamente, gli individui appartenenti alla terza categoria sono maggiormente sofisticati proprio perché supportati da solide istituzioni statali mentre gli hacktivisti, i gruppi terroristici e i thrill-seekers dispongono di mezzi inferiori che non necessitano di particolari conoscenze o skills per essere sfruttati. Infine, gli insiders rappresentano una seri minaccia per una certa organizzazione, poiché essi partono da una posizione di assoluto vantaggio rispetto a tutti gli altri attori, essendo direttamente (o quasi) a contatto con i processi e le informazioni aziendali.

Capitolo 2

La cybersecurity nel settore finanziario

> «[...] Gli intermediari finanziari hanno una probabilità 300 volte maggiore rispetto ad altre società di essere prese di mira da un attacco informatico: affrontare tali attacchi e le loro conseguenze comporta un costo maggiore per le banche e i gestori patrimoniali rispetto a qualsiasi altro settore.» [17]

Il settore finanziario rappresenta storicamente il principale target di attacchi informatici per via della natura delle informazioni che esso manovra e per il contenuto altamente sensibili dei dati in esse contenuti. Inoltre, la crescente digitalizzazione dei processi ha portato ad una riduzione dei costi e a nuove opportunità di business, rendendo però il mondo finanziario estremamente esposto ai cyber rischi e vulnerabile ad attacchi massivi, oltre che oggetto di frodi e attacchi mirati da parte di gruppi criminali. Qualunque tipologia di intermediario finanziario, dalla più piccola banca regionale fino ai grandi colossi della finanza mondiale basa le sue operazioni sul trasferimento di denaro facendo uso di un sistema costituito da asset hardware e software altamente esposto alle minacce, che possono provocare una semplice interruzione del servizio fino a danni economici dall'impatto significativo. La reputazione di cui essi godono nei confronti dei loro clienti e sulla fiducia che ne consegue è un aspetto di vitale importanza, pertanto devono dimostrarsi attenti e dediti a mantenere integre tutte le peculiarità dei propri servizi, al fine di restituire un'immagine di solidità e autorevolezza alla vista di chi li osserva. Il danno reputazionale può, pertanto, essere considerato un aspetto di pari importanza rispetto alle perdite "tradizionali", poiché esso si traduce sia in una perdita di profitti ma anche, in seconda battuta, in una perdita di autorità ben più difficile da risanare. Nel corso degli ultimi decenni il settore finanziario ha sperimentato e adottato un processo di digitalizzazione tramite l'adozione di numerosi asset, rendendo le operazioni ivi condotte estremamente vulnerabili alle cyber minacce. Questo aspetto è

dovuto principalmente all'infrastruttura globale che collega tra di loro i vari servizi finanziari, dai mercati ai sistemi bancari: ad esempio, oggi è possibile compiere un vasto numero di operazioni in maniera digitale, partendo dai pagamenti e dalla consulenza bancaria fino alla compravendita di strumenti finanziari (*trading*), liberamente accessibili ai singoli cittadini. Tutti questi servizi si basano su sistemi IT e altri mezzi di comunicazione elettronica, ampliando enormemente l'impatto che ciascun cyber rischio potrebbe generare qualora si verificasse.

2.1 La digitalizzazione e il settore FinTech

Per le aziende operanti nel settore finanziario la digitalizzazione non rappresenta più una scelta ma un vero e proprio imperativo. Condurre una strategia di trasformazione digitale non ricopre più un ruolo di differenziazione ma è una caratteristica di vitale importanza per la corretta conduzione del proprio business. Le nuove innovazioni stanno, di fatto, rimodellando il profilo dell'intero settore: l'intelligenza artificiale ed il *machine learning* permettono di migliorare alcuni aspetti chiave come le sottoscrizioni, gestire i reclami, la contabilità e le funzioni attuariali. Allo stesso tempo, nuovi modelli di business e nuove tecnologie distruttive come la blockchain permettono alle organizzazioni che le adottano di capitalizzare le nuove opportunità create.[1] Il primo aspetto fondamentale alla base di questo trend riguarda la volontà di migliorare la *customer experience*, ovvero la modalità con cui i propri clienti utilizzano i servizi erogati dall'azienda. Alla base di questo vi è, ancora, la fedeltà dei consumatori e la fiducia che essi ripongono nell'infrastruttura: semplicità d'uso, velocità e sicurezza sono i primi aspetti fondamentali richiesti. Investire in tecnologie digitali che migliorino l'esperienza è un aspetto critico per trattenere i propri clienti ed attrarne di nuovi. Un altro fattore chiave della digitalizzazione riguarda il miglioramento dell'efficienza operativa attraverso l'utilizzo di intelligenza artificiale e di processi di gestione automatica del business. Questo permette di ridurre i costi, di accelerare le operazioni e di migliorare la qualità del servizi specie per quelle pratiche ad alta frequenza e ad elevato tasso di standardizzazione, come, ad esempio, il processamento delle transazioni. Altri aspetti automatizzabili sono quelli inerenti alla compliance normativa, come la gestione dei registri elettronici, l'identificazione dei clienti e il monitoraggio di attività sospette e potenzialmente dannose. L'adozione di queste pratiche permette, infatti, sia di ridurre la percentuale di errori umani, sia di migliorare l'efficienza lavorativa dei dipendenti e, infine, di incrementare ulteriormente l'esperienza d'uso delle proprie

[1]Una blockchain è un registro digitale in grado di memorizzare dati e "transazioni" in modo sicuro, verificabile e permanente. E' stata introdotta per la prima volta dal misterioso personaggio Satoshi Nakamoto con l'obiettivo di raccogliere tutte le transazioni del Bitcoin, la più famosa valuta digitale che in quel momento stava per originarsi.

piattaforme. Altre tecnologie che incentivano la digitalizzazione possono essere, ad esempio:

- *Cloud Computing*, permette di spostare l'accesso e l'archiviazione di dati e servizi online.
- *Analitiche Avanzate*, permettono di analizzare i dati storici e fornire previsioni in tempo reale.
- *Robotic Process Automation*, con i quali si possono automatizzare i task più ripetitivi.
- *Machine Learning*, che dona agli algoritmi la capacità di imparare dai propri errori senza l'intervento umano.
- *Stampa 3D*, detta anche "additive manifacturing" che permette di ottenere oggetti fisici a partire da modelli virtuali.
- *Realtà virtuale, estesa ed aumentata* che conducono l'essere umano in un mondo parzialmente o totalmente creato da processi digitali.

Tutte queste attività comportano, però, la necessità da parte di chi le compie di modernizzare i propri asset IT e di renderli omogenei tra di loro, evitando quei tipici fallimenti dei processi che si verificano quando le tecnologie non sono coerenti, come la riduzione del flusso di informazione e l'impoverimento delle capacità informative dei processi. Modernizzare il proprio *core* informativo è anche necessario per la istituzioni finanziarie tradizionali al fine di fronteggiare la concorrenza condotta dalle aziende (che nascono spesso come start-up) operanti nel settore della *tecnofinanza*. Con questo termine ci si riferisce a quella tipologia di business che mira a competere con i metodi tradizionali della finanza, proponendo soluzioni e servizi basati sulle tecnologie dell'informazione più recenti e facendo dell'innovazione la loro peculiarità. Ad oggi non è presente una definizione universalmente condivisa in ambito accademico e operativo, nonostante possa essere definite come una «industria finanziaria che utilizza l'innovazione tecnologica per migliorare le proprie attività.» [18] Le aziende operanti in questo settore offrono servizi molto eterogenei tra di loro, tra i quali: pagamenti elettronici, analisi dati, mercati di capitali, immobiliare e finanza personale. Negli ultimi anni si è potuto osservare un forte incremento su scala mondiale numero di queste aziende, che hanno contribuito ad una vera e propria rivoluzione dei mercati finanziari tradizionali attraverso l'utilizzo massimo della tecnologia d'avanguardia. Questo fenomeno si è riversato sul consumatore finale, consentendo ai singoli clienti di compiere gran parte di quelle operazioni da remoto e in totale autonomia.

Parallelamente, è possibile notare come il cyber crimine si sia evoluto a partire dal 2017 come portata degli attacchi e come frequenza, sviluppando una vera e propria specializzazione verso le diverse attività presenti nel settore, molte volte con

Tabella 2.1: Segmenti per maggiore valore delle transazioni, in milioni di dollari (fonte: Statista)

Pagamenti digitali	*Finanza personale*	*Prestiti alternativi*	*Finanza alternativa*
6.699.201	2.695.361	390.583	20.000

un tasso di crescita nettamente superiore rispetto a quello dei sistemi di sicurezza [19]. Questo ha portato ad una massiva riformulazione della *regulation* finanziaria, oltre che una maggiore presa di consapevolezza verso i numerosi aspetti delle tecnologie internet e della loro sicurezza, una maggiore collaborazione tra le aziende che compongono il sistema finanziario mondiale e altre specializzate in cybersecurity. Vi è dunque una criticità strutturale insita nel *fintech* e nei settori ad elevata digitalizzazione che è riscontrabile nell'alto tasso di innovazione, il quale porta, inevitabilmente, ad uno sviluppo concorrenziale delle minacce informatiche che si riflettono sul consumatore finale. L'innovazione deve, pertanto, essere coadiuvata da appropriate misure di regolamentazione e sicurezza, promuovendo l'utilizzo di framework condivisi e standardizzati.

2.2 Timeline dei principali cyber eventi nel 2020

Come detto in precedenza, il tema della cybersecurity rappresenta l'ultima frontiera del risk management nel settore finanziario e la sua importanza è destinata ad accrescersi ulteriormente. Il sito Carnegie fornisce una timeline dei principali incidenti in ambito cybersecurity su scala mondiale avvenuti dal 2007 ad oggi, per la cui costruzione sono stati utilizzati i dati forniti dalla *Cyber Threat Intelligence* di BAE Systems. Di seguito si riportano alcuni eventi meritevoli di attenzione che si sono verificati nel 2020 presso istituti finanziari di tutto il mondo, in ordine cronologico [20].

- *2 gennaio - Attacco presso le principali banche dell'Africa sub-sahariana.* Nella prima settimana dell'anno si sono verificati numerosi attacchi mediante *malware* con scopo il furto di dati sensibili presso le principali banche dell'africa centro-meridionale. Alcuni esperti hanno attribuito la responsabilità al gruppo criminale "Silence", già autore di altri attacchi informatici. Gli aggressori hanno avviato una campagna di *phishing* (furto di credenziali) entrando in possesso delle specifiche degli utenti e compiendo prelievi massivi presso gli ATM diffusi nelle città.

- *21 febbraio - Hacker attaccano PayPal.* Un gruppo di criminali, di matrice ignota, ha compiuto un attacco con metodi sconosciuti verso il colosso mondiale PayPal, sfruttando una falla nell'integrazione con Google Pay. I soggetti sono riusciti ad autorizzare da remoto alcuni pagamenti presso diversi negozi degli Stati Uniti, per un furto di decine di migliaia di dollari.

- *6 marzo - furto di credenziali per pagamenti elettronici.* Sono state rubate oltre 200.000 informazioni relative a carte di credito emesse dalle principali banche asiatiche (Singapore, Vietnam, Indonesia) e pubblicate online. Ad oggi non si conosce ancora il responsabile né il metodo utilizzato.

- *30 marzo - furto di credenziali presso Monte dei Paschi.* La banca, di proprietà dello stato italiano, ha subito un furto di mail e credenziali dei dipendenti usate per contattare alcuni clienti e ottenere informazioni sensibili, come credenziali dei clienti affiliati.

- *9 aprile - furto e condivisione di dati di pagamento.* Oltre 400.000 *records* appartenenti a diverse banche sudcoreane e americane sono stati rubati e pubblicati su di un noto sito di e-commerce, includendo il numero identificativo della banca (codice BIN), il numero del conto, la data di scadenza e il CVV (ovvero il codice a tre cifre situato sul retro di ogni carta). Questo evento ha rappresentato la più grande fuga di dati all'interno avvenuta nel sistema finanziario della Corea del Sud ne corso del 2020.

- *11 maggio - attacco ransomware ad azienda costruttrice di ATM.* La ditta americana Diebold Nixdorf ha dichiarato di essere stata oggetto di un attacco ransomware che ha causato un interruzione limitata dei sistemi IT. Non sono stati dichiarati dettagli aggiuntivi sulla vicenda.

- *21 giugno - il più grande DDOS mai registrato.* Una grande e non meglio identificata banca europea è stata vittima di un denial of service distribuito che ha causato una notevole interruzione dei servizi emessi dalla banca. L'attacco è stato compiuto inviando 809 milioni di richieste al secondo al sito web interessato, causandone il collasso: per questo motivo è stato dichiarato come il più grande mai registrato.

- *15 luglio - furto di identità famose su Twitter.* Diversi account Twitter degni di nota tra cui Joe Biden ed Elon Musk sono stati hackerati per pubblicare un indirizzo Bitcoin che garantiva di raddoppiare eventuali contributi donati all'indirizzo specificato. In tutto, gli hacker hanno guadagnato più di 113.500 dollari americani. Il 31 luglio, un sospetto di 17 anni legato a questa vicenda è stato arrestato in Florida.

- *26 agosto - New Zealand Stock Exchange DDoS.* Il provider di rete della Borsa della Nuova Zelanda ha subito un attacco DDoS esteso che è durato diversi

giorni e ha causato l'arresto delle operazioni della Borsa. Anche il sito web NZX e la piattaforma di annunci di mercato sono stati influenzati. Secondo quanto riferito, il governo australiano e altri stati hanno aiutato l'istituzione nel processo di risposta e recupero.

- *23 settembre - Ransomware in alcune banche della Russia.* Il 23 settembre 2020, Group-IB ha riferito che una banda di criminali informatici soprannominata "OldGremlin" aveva preso di mira banche e altre aziende in Russia con ransomware dall'inizio di marzo 2020. OldGremlin utilizza e-mail di phishing per accedere alle reti e quindi crittografa i dati, richiedendo in cambio un riscatto di circa 50.000 dollari americani.

- *1 ottobre - glitch tecnico nella borsa giapponese.* Un problema tecnico ha interrotto le negoziazioni sulle borse valori giapponesi, incluso il Nikkei 225. L'interruzione si è verificata quando un sistema di backup non è riuscito a entrare in azione dopo un malfunzionamento dell'hardware, secondo il Japan Exchange Group. L'arresto non era collegato a un attacco informatico. Le negoziazioni sono state sospese presso la borsa valori principale di Tokyo insieme alle borse collegate a Nagoya, Fukuoka e Sapporo.

2.2.1 Effetto del COVID-19 sugli attacchi informatici

La pandemia da COVID-19 e i *lockdown* messi in atto per arginare la diffusione del virus hanno radicalmente modificato le abitudini e la vita della popolazione mondiale, privando noi cittadini di abitudini che mai avremmo pensato di dover abbandonare. Anche le imprese e le organizzazioni, di qualunque dimensione e tipologia, hanno dovuto velocemente riorganizzarsi per cercare di proseguire il proprio lavoro da remoto e di limitare di danni - inevitabili e talvolta incalcolabili - al loro interno. La grande maggior parte dei lavoratori si è trovata quindi a dover lavorare da remoto tramite lo *smartworking* e ciò ha portato ad una transazione forzata che non sempre è stata condotta nel modo corretto, sia per mancanza di una adeguata conoscenza ma sopratutto per la modalità con la quale è stata impiegata, visto il diffuso stato di assoluta emergenza. Strumenti digitali che prima erano utilizzati solo in minima parte sono divenuti il principale mezzo su cui lavorare mediante nuove modalità operative e proprio questi sono stati i target primari dei cybercriminali. La pandemia ha permesso agli aggressori di rafforzare le loro tecniche di attacco tradizionale mediante l'introduzione di tematiche strettamente legate al virus, facendo leva sulla paura delle persone e sulla loro sensibilità all'argomento. Questa evoluzione malevola non è stata accompagnata da una rapida presa di coscienza da parte delle aziende, che spesso non si sono dimostrate rapide nell'adottare sistemi di tutela delle informazioni. Basti pensare all'adozione da parte di numerose realtà aziendali sull'adozione dei RDP (Remote Desktop Protocol) che

contente ai dipendenti di accedere ai sistemi da remoto e che in numerose occasioni ha portato direttamente all'esposizione delle informazioni e dei dati aziendali a potenziali minacce. Ne è conseguito che durante i primi mesi della pandemia si sia registrato un picco di attacchi, sopratutto ransomware, veicolati tramite RDP. A tal proposito, il rapporto CLUSIT (nella sua edizione di ottobre 2020) riporta un'interessante studio condotto su un gruppo di 850 attacchi certificati durante il primo semestre 2020, dove il 14% è stato collegato direttamente alla tematica COVID-19. La ricerca ha inoltre mostrato come le tecniche utilizzate dagli aggressori siano state piuttosto variegate, con una netta predominanza di phishing (61% del totale), seguita dai malware (21%), minacce multiple (8%), vulnerabilità (5%), cracking di account (3%), mezzi sconosciuti (1%) e DDOS (1%). Di tutti questi attacchi, il 61% hanno avuto un impatto "medio", 26% "alto" e 13% "critico" [21]. Alla luce di quanto osservato si può affermare che, poiché la pandemia risulti ancora in corso, non accennando ad arrestarsi, sia quantomai necessaria una maggiore attenzione alla cybersecurity, partendo dalla sensibilizzazione dei singoli utenti verso tematiche spesso prese in scarsa considerazione.

Per quanto concerne gli intermediari finanziari, il 2020 è stato un anno di assoluto sviluppo di tutto il cybercrime finanziario, dove si sono osservate vere e proprie organizzazione internazionali di criminali, dotate di una definita struttura e organizzazione. Le metodologie di attacco hanno subito una ulteriore evoluzione: per quelle destinate a banche o aventi come movente il furto di denaro si sono utilizzate spesso tematiche strettamente legate alla pandemia, approfittando dell'elevata sensibilità del pubblico a queste tematiche. Malware e phishing sono stati i principali metodi utilizzati per ottenere credenziali dei clienti e permettere l'accesso ai sistemi bancari. Esempio di quanto successo sono state le numerose campagne di spamming con oggetto (finte) comunicazioni riguardo all'erogazione di aiuti economici da parte di Agenzie dell'Entrate e altri enti della pubblica amministrazione, le quali inducevano gli utenti ad eseguire un documento Office® con macro "contraffatte" che consentono l'infezione del virus. Durante la pandemia si sono osservate, inoltre, numerose azioni di phising con target varie istituzioni finanziarie, veicolate per lo più tramite mail o SMS e con obiettivo quello di rubare credenziali dei clienti e altre informazioni utili a compiere con successo un furto di denaro. Nello specifico, si sono registrate in media 1,6 nuove campagne giornaliere, tutte basate sulla replicazione visiva dell'interfaccia utente originale della banca. Nel mese di marzo 2021 è stato diffuso il nuovo rapporto CLUSIT dove si indica la frode bancaria o finanziaria al primo posto tra le minacce nel panorama europeo durante il 2020[2]. Questa consiste, nella maggior parte dei casi, attraverso il furto delle credenziali d'accesso dei clienti ai circuiti bancari e nel loro riutilizzo per transazioni fraudolente all'insaputa di questo ultimo. L'analisi mostra che la frode avviene prevalentemente

[2]Per maggiori informazioni sulle minacce avvenute durante il periodo della pandemia si rimanda al già citato rapporto CLUSIT (ottobre 2020) e all'ultima edizione del 2021.

attraverso i seguenti vettori: malware per il furto di credenziali o intercettazione di una transazione, hacking del dispositivo mobile, phishing per il furto di credenziali di accesso e autenticazione forte. Il primo e l'ultimo si sono ripartiti il compito in maniera abbastanza equa sulle vittime retail (i consumatori finali), mentre per il mercato *corporate* c'è stata invece una prevalenza di schemi di attacco tramite malware [22]. All'interno della timeline fornita da Carnegie, è possibile osservare diversi cyber-incidenti presso istituzioni finanziarie che hanno sfruttato tematiche o mezzi direttamente collegate al COVID per veicolare le proprie minacce, ad esempio:

- *13 aprile - banche spagnole vittime di un trojan proveniente dal Brasile.* I ricercatori dell'IBM hanno riferito che le banche spagnole sono state prese di mira da un trojan bancario brasiliano, "Grandoreiro", mediante una campagna durata mesi. In particolare, sono state sfruttate l'epidemia di Coronavirus, utilizzando video a tema sulla pandemia che convincono gli utenti a eseguire un eseguibile nascosto. Grandoreiro è un trojan bancario con *overlay* remoto che, quando un utente accede al proprio banking online, può visualizzare immagini per impersonare detta banca. Ciò consente agli attacchi di trasferire quindi denaro dagli account delle vittime. Il malware viene eseguito all'accesso a un elenco di entità codificate, per lo più banche locali.

- *22 giugno - un nuovo malware utilizza come attrattivo tematiche del virus.* Alcuni ricercatori hanno notato l'esistenza di una nuova versione del trojan "IcedID", destinato ad essere utilizzato verso le banche, che sfrutta messaggi di allerta con tema la pandemia per indurre la vittima ad eseguirlo.

- *15 agosto - il Governo del Canada denuncia furto di fondi per la ripresa da pandemia.* Oggetto dell'attacco è stato il sistema informativo dell'autorità statale dal quale sono state rubate oltre 11.000 credenziali, al fine di appropriarsi di fondi destinati a cittadini o piccole imprese gravemente danneggiate dagli effetti collaterali della pandemia.

La crisi da COVID-19 ha ulteriormente evidenziato come le risorse digitali siano fondamentali all'interno di un mondo senza interazioni umane. Sarebbe un errore considerare questo *shift* come momentaneo: già da alcuni anni i consumatori preferiscono l'utilizzo del mobile ed online banking, dell'assistenza virtuale e automatizzata e dei servizi di assicurazione digitale. Il trend pare essere ormai irreversibile e, per certi versi, la pandemia non ha fatto altro che anticipare i tempi.

2.3 La cybersecurity come rischio sistemico

Per *rischio sistemico* si intende il rischio che un intero sistema finanziario, di scala nazionale o internazionale, giunga al collasso a causa di eventi e condizioni idiosincratiche, propagandosi a cascata in tutte le istituzioni collegate e causando

il crollo dell'intero sistema. Secondo l'ESRB (European Systemic Risk Board) un cyber rischio può, sotto determinate circostanze, mutare rapidamente in un rischio sistemico causando una crisi di liquidità globale, dalla quale potrebbe scaturire una crisi sistemica e quindi conseguenze gravissime per l'economia reale [23]. Questo sarebbe reso possibile dall'alterazione di dati sensibili e dei processi fondamentali su cui si basa l'intero sistema finanziario globale, impedendo il corretto svolgimento di alcune funzioni chiave, provocando perdite economiche e pregiudicando irreversibilmente la fiducia della popolazione nei confronti del sistema finanziario.

Tabella 2.2: Funzioni economiche chiave del sistema finanziario (fonte: ESRB)

Depositi e risparmi	Conti correnti al dettaglio CC medie e piccole imprese Risparmi al dettaglio Risparmi medie e piccole imprese Depositi aziendali
Prestiti e servizi di credito	Mutui al dettaglio Prestiti al dettaglio Carte di credito al dettaglio Prestiti a piccole e medie imprese Prestiti corporate Mercati finanziari Prestiti di infrastrutture Carte di credito e servizi commerciali
Mercato di capitali e investimenti	Derivati Trading Asset management Assicurazioni generali Assicurazioni sulla vita e pensioni
Finanziamenti all'ingrosso	Finanziamento titoli Prestito titoli
Pagamenti e compensazioni	Servizi di pagamento Servizi di regolamenti Servizi cash Servizi di custodia Servizio operazionali a terze parti

Nel 2017 l'ESRB ha dato vita all'European Systemic Cyber Group, con il fine di focalizzarsi maggiormente sulle minacce provenienti dal cyberspazio e sui loro impatti all'interno dell'Unione Europea tramite la creazione di un framework analitico,

permettendo di capire come un cyber rischio possa divenire sistemico e minacciare la stabilità finanziaria, con conseguenze catastrofiche sull'economia reale. Tale effetto è catalizzato direttamente sia dall'entità delle perdite in termini monetarie che, indirettamente, dalla perdita di fiducia e dall'incertezza nei confronti del sistema finanziario, le quali provocano una radicale modifica del comportamento (spesso irrazionale) tenuto dai principali attori del sistema. Le crisi finanziarie passate hanno dimostrato come influiscano sia la magnitudine dello shock iniziale sia la sua distribuzione, ma anche il grado di trasparenza delle istituzioni nel comunicare le perdite subite, senza la quali si assume una visione distorta riguardo la capacità degli altri di sopportare tali perdite e di assorbirle, creando ulteriore incertezza economica. Il modello sviluppato dal ESCG (contenuto nel report appena citato) permette l'analisi di un cyber rischio potenzialmente sistemico suddividendolo in quattro aspetti principali:

1. *Contesto*, ovvero le circostanze attorno alle quali il rischio si concretizza, includendo tutti i concetti fondamentali ad esso associato come asset, vulnerabilità, minacce e controlli. Questi possono essere considerati come i macroelementi di un cyber rischio e sono largamente utilizzati nella maggior parte dei frameworks e negli standard internazionali.

2. *Fase di shock*, ovvero l'impatto che scaturisce nel momento in cui il rischio prende vita, ponendo la distinzione tra impatti tecnici e conseguenze sul business dell'azienda.

3. *Fase di propagazione*, nella quale ci si focalizza sull'interazione tra le istituzioni finanziarie infettate e i sistemi da esse utilizzate, considerando i fattori che amplificano la probabilità o l'impatto e quelli che promuovono il contagio all'interno dei sistemi.

4. *Fase di evento sistemico*, dove si esamina il momento in cui il rischio ha compiuto la sua metamorfosi a livello sistemico e non si è più in grado di assorbire lo shock generato. Per consentire questo passaggio sono definiti dei "limiti di tolleranza" che evidenziano la capacità di assorbimento dell'impatto e il punto in cui essa viene a mancare.

Non tutti i cyber rischi rappresentano una concreta minaccia alla stabilità finanziaria, poiché solo una minima parte di essi potrebbe, per le motivazioni appena descritte, tramutarsi in un evento sistemico. Tuttavia, esiste una concreta possibilità che un evento di questo rischio di verifichi, come un cyber incidente su larga scala che comprometterebbe l'intero sistema, ripercuotendosi sulle singole economie nazionali e, in ultima battuta, sulla popolazione civile.

Capitolo 3

Il processo di gestione del rischio informatico

Per una banca o, più in generale, per un qualsiasi intermediario finanziario, la cybersecurity rappresenta l'ultima frontiera dei rischi *operativi* (la cui definizione verrà data nelle pagine seguenti) e come tale necessita di un delicato processo di gestione del rischio, che sia conforme, prima di tutto, alle norme vigenti e personalizzato in base alle proprie esigenze. L'attuale situazione mondiale, in cui una pandemia continua e imperversare e, giorno dopo giorno, ledere le certezze dei cittadini, obbliga tutte le imprese ad una presa di coscienza tempestiva e all'adozione di protocolli interni che aiutino la comprensione del problema, partendo dalle semplici operazioni quotidiane. Proteggere i propri server aziendali non è più sufficiente, poiché, ogni giorno, con il lavoro da remoto, l'archiviazione sta subendo una transazione progressiva verso il cloud: ciascun dispositivo in rete, che sia un PC o uno smartphone, racchiude dentro sé delle vulnerabilità e rappresenta quindi una fonte di rischio da prendere in considerazione. La sicurezza informatica rappresenta oggi un'aspetto talmente fondamentale da indicare una fonte di differenziazione tre le imprese stesse e, sopratutto, di vantaggio competitivo. Ogni singola azienda può raggiungere una posizione di superiorità grazie alla propria resilienza e alla capacità di adattarsi ad una minaccia così mutabile nel tempo, dimostrando sia la propria *compliance* alle varie normative sia la modalità con cui esse vengono implementate

3.1 Classificazione dei rischi negli intermediari finanziari

Ciascuna istituzione finanziaria è direttamente esposta ad una certa tipologia di rischi dovuti alla natura dell'attività che essa svolge e che impattano direttamente sulla redditività dell'impresa. La principale criticità dell'intermediazione finanziaria

risiede nell'impossibilità sul medio e lungo termine che i ricavi coprano i costi, impedendo la remunerazione degli azionisti e i flussi di casa necessari al sostegno dell'operatività. I rischi specifici di questa tipologia di attività possono essere inclusi in cinque differenti macro categorie, che verranno descritte nei paragrafi successivi.

3.1.1 Rischio di credito

Con questo termine si indica la possibilità che la controparte contrattuale non adempia totalmente o parzialmente alla restituzione degli interessi e del capitale. Questo rischio si manifesta quando si presenta una variazione non attesa del merito creditizio della controparte, verso la quale l'organizzazione ha una certa esposizione (ci si riferisce ad una variazione "inattesa" poiché, nel caso questa fosse prevedibile, essa sarebbe già incorporata nelle condizioni contrattuali con le quali la banca concede il finanziamento alla controparte). Nello specifico, il rischio di credito include alcune tipologie principali di rischio, tra le quali:

1. *Rischio di insolvenza* ovvero l'incapacità della controparte di ottemperare ai propri obblighi contrattuali poiché divenuta insolvente. Questa è la peggiore condizione per il creditore, in quanto sarà sottoposto ad una perdita più che modesta, data dalla differenza tra il valore del credito e l'ammontare che si è recuperato.

2. *Rischio di migrazione*, a cui corrisponde il deterioramento del merito di credito della controparte, che si ripercuote sulla qualità del credito, aumentando la probabilità di default e, infine, il rischio ad essa associata. Operativamente questo si traduce in una variazione negativa del *rating* associato al debitore, a un conseguente innalzamento della probabilità di default e del rendimento richiesto.

3. *Rischio di recupero*, consiste nel caso in cui, qualora il debitore risulti insolvente, la banca non riesca a compiere una stima accurata del *recovery rate*, ovvero dell'ammontare che verrebbe effettivamente recuperato durante il contenzioso con la controparte.

4. *Rischio di esposizione*, che si verifica quando l'intermediario ha un'esposizione (in questo caso, ad esempio, un credito) di dimensioni inaspettatamente troppo elevate poco prima che si determini l'insolvenza della controparte.

5. *Rischio di spread* rappresenta quel caso in cui il premio al rischio (lo spread) aumenti contestualmente ad una parità di rating, ovvero ad una corrispondenza del merito di credito. Questo può verificarsi in alcune situazioni particolari nelle quali i mercati siano investiti da una crisi di liquidità o gli investitori risultino maggiormente avversi al rischio.

Per una banca l'attività creditizia è la principale fonte di guadagno, nonché il suo *core business*, pertanto, il rischio di credito è stato oggetto nel corso degli anni di grande attualità in seguito alla regulation di Basilea, nella quale sono state dettate le disposizioni cui gli istituti devono far riferimento.[1]

3.1.2 Rischio di mercato

Questa categoria di rischi sottende l'eventualità che una determinata posizione o un portafoglio di esse subisca una variazione inattesa del proprio rendimento, dovuta a variazioni non previste di alcune variabili di mercato:

1. *Tassi di interesse*: nel caso, ad esempio, di un detentore di obbligazioni a tasso fisso, un aumento dei tassi provoca un deprezzamento del titolo stesso con una conseguente perdita da parte di chi lo detiene, che sarà pertanto esposta ad un *rischio di interesse*. In generale, questo rischio si verifica nel caso in cui esista uno squilibrio tra le scadenze delle attività e delle passività detenute da un intermediario, creando una variazione non voluta sul margine di interesse (dato dalla differenza tra interessi attivi, proventi finanziari ed interessi passivi).

2. *Tassi di cambio*: nel caso in cui variazioni del rapporto tra due valute portino ad un degradamento del potere di acquisto e una perdita conseguente, oppure quando una banca possiede una qualche passività finanziaria in una valuta diversa rispetto a quella con cui l'emittente formalizza la propria attività. Queste situazioni portano tutte all'insorgere di un *rischio di cambio*.

3. *Prezzo*: nel caso in cui le quotazioni dei valori mobiliari o di attività finanziarie subiscano delle variazioni e portino alla creazione di guadagni o perdite, fino al caso estremo in cui un intermediario subisca un deprezzamento tale delle sue attività da poter registrare difficoltà nella raccolta di ulteriori fondi o nell'impossibilità di ottenere prestiti a condizioni migliori o uguali a quelle antecedenti tale perdita.

Questa tipologia di rischio è strettamente connessa alla presa di posizione dell'intermediario, intesa come l'atto di compiere un certo investimento sotto determinate condizioni, esponendosi all'evenienza che il risultato ottenuto non sia quello desiderato.

[1] Il "Nuovo accordo di Basilea" o "Basilea II" è il termine con cui si fa riferimento al documento "Nuovo Accordo sui requisiti minimi di capitale", firmato nell'omonima città svizzera nel 2004 e in vigore dal gennaio 2007.

3.1.3 Rischio di liquidità

Esso intende la possibilità che la banca non riesca a far fronte nell'immediato ai propri obblighi di pagamento, non riuscendo a rispettare le tempistiche stipulate in fase di contrattazione. Questo è tipicamente dovuto ad un *lag temporale* tra le attività e le passività della banca stessa, nel caso in cui essa debba affrontare uscite o entrate inattese e sia costretta alla vendita massiva delle proprie attività, in modo da procurarsi la liquidità necessaria. L'intermediario deve pertanto coordinare in ogni istante la corrispondenza tra i flussi in entrata e quelli in uscita, in modo da assicurare la propria solvibilità, pur essendo consapevole che la detenzione di eccessiva liquidità possa essere onerosa per la propria redditività, ma allo stesso tempo essa si rende necessaria nel momento in cui si debba far fronte ai propri obblighi previsti. Il rischio di liquidità contiene al suo interno due differenti categorie, strettamente collegate tra loro:

1. *Funding liquidity risk*, ovvero quel rischio per cui la banca non sia completamente in grado di ottemperare alle proprie promesse in maniera efficiente, senza che questo intacchi la sua operatività.

2. *Market liquidity risk*, ovvero quel rischio che si ripercuote su tutto il mercato il quale, privo dell'adeguata liquidità, influenza negativamente il valore delle attività su di esso negoziate, portando ad una perdita verso chi le detiene.

Tipicamente una banca misura maggiormente la prima categoria di rischio, nonostante essa sia strettamente correlata alla seconda. Si pensi, ad esempio, alla necessità di un individuo di vendere una propria attività per far fronte ad un certo obbligo di pagamento contrattuale: nel caso in cui il mercato rispondesse in maniera poco efficiente si provocherebbe una perdita sul valore dell'attività stessa, comportando il rischio di non riuscire a raccogliere un ammontare adeguato. Il rischio di liquidità è una conseguenza logica dell'operatività della banca stessa, tuttavia esistono alcuni fattori che concorrono alla sua formazione o all'aumento della sua criticità, come, ad esempio, una cattiva reputazione dell'intermediario di fronte al pubblico oppure eventi di natura sistemica esterni all'organizzazione stessa, come crisi finanziarie, disastri naturali ed attacchi terroristici [24].

3.1.4 Rischio operativo

Appartengono a questa categoria quei rischi strettamente connessi con il quotidiano funzionamento della banca, a cui possono essere ricondotti tutti quegli eventi che provocano un danno economico e una perdita di redditività non direttamente collegata alle condizioni creditizie o ai fattori di mercato. Secondo Basilea II, appartengono a questa classificazione differenti rischi che derivano da fattori interni ed esterni all'organizzazione. Una prima categoria include i comportamenti

umani (intenzionali e non), come semplici errori non voluti, frodi da parte di dipendenti ed eventi derivanti dalla mancata osservanza di regolamenti interni o di normative. La seconda categoria proposta comprende i fallimenti che possono intercorrere nei sistemi informativi aziendali, come guasti alle componenti hardware o software, accessi non autorizzati e degradamento delle informazioni contenute nei processi operativi. Nella terza categoria sono incluse le svariate procedure di controllo dell'attività, in cui rientrano anche la cattiva gestione dei rischi e l'utilizzo di modelli non adeguati per la loro quantificazione; nella quarta e ultima categoria si fa riferimento agli eventi esterni che non sono sotto il controllo della banca, come emergenze sanitarie ed eventi atmosferici.

Il rischio di credito, di mercato e di liquidità sono rischi tradizionalmente *revenue-driven*, che riflettono la propensione di un'azienda al rischio stesso, secondo la basilare relazione inversa che intercorre tra rischio e rendimento. I rischi operativi, invece, includono al loro interno una componente non eradicabile, poiché provengono da comportamenti insiti nella natura umana o nell'ambiente circostante. Secondo un recente articolo [25], i cyber rischi sono sì eventi di natura operativa, ma differiscono dai tradizionali rischi operativi in due aspetti:

- *Velocità di propagazione*: un evento di natura informatica è in grado di infettare e di propagarsi all'interno dei sistemi informativi di una banca in maniera drasticamente più rapida rispetto alle altre tipologie di rischio.[2]. Questo aspetto è dovuto essenzialmente alla natura del sistema informativo stesso e alla sua interconnessione con gli altri.

- *Scala di propagazione*: un cyber incidente rappresenta, non solo a livello potenziale, una minaccia di proporzioni continentali, se non globali. Questo perché, se ben progettato, un attacco informatico può espandersi facilmente all'interno di tutti i sistemi che risultano oggi globalmente comunicanti, includendo anche quelle strutture che non sono obiettivo diretto dell'attacco. Proprio l'elevata velocità di comunicazione e l'assenza di confini geografici per il transito dei dati rappresentano da un lato un punto di forza per la qualità del servizio, ma, inevitabilmente, una vulnerabilitàà dai connotati catastrofici.

- *Possibili intenti*: Come descritto nel capitolo 1, molti attori compiono attacchi deliberatamente con l'obiettivo di compiere un danno economico il più elevato possibile, in contrasto con le perdite causate da piccoli eventi non intenzionali che caratterizzano gran parte dei rischi operativi.

Come affermato in precedenza, in un mondo in cui la digitalizzazione prosegue incessantemente e di pari passo le minacce ad essa associata, è necessario che le

[2]Uno dei maggiori cyber incidenti che si siano mai verificati fu l'attacco del malware "NotPetya" contro il sistema finanziario ucraino, infettando quasi completamente il sistema in meno di un minuto

imprese sviluppino una strategia di resilienza operativa. A partire dal 2014, il comitato di Basilea ha incluso i cyber-rischi come uno dei molteplici scenari che possono intercorrere all'interno dei rischi operativi:

> «[...] alcune banche hanno sviluppato scenari relativi a terremoti e altri eventi catastrofici, come un attacco informatico, per valutare non solo l'esposizione al rischio operativo (ad es. costi di continuità operativa, perdite per frode, azioni legali, ecc.) ma anche altri rischi come il rischio di credito (ad es. svalutazioni delle garanzie), rischio di mercato e condizioni economiche generali (ovvero minori entrate).» [26]

L'economia reale richiede, per poter funzionare efficientemente, di operare in sinergia con il sistema finanziario globale e i servizi ad esso associati, come i pagamenti, prelievi e depositi di denaro e la compravendita di strumenti finanziari. Questi sistemi si basano per la loro interezza su infrastrutture di comunicazione, e il mantenimento dell'integrità, della disponibilità e della riservatezza risulta di cruciale importanza per il corretto funzionamento di tutti questi sistemi. Ne consegue che questa caratteristica strutturale rende l'intero ecosistema altamente sensibile ai cyber incidenti e, pertanto, comprendere i loro impatti rappresenta la base per migliorare la propria resilienza nei confronti di questi rischi.

3.2 Misure di rischio finanziario

Nella definizione analitica del concetto di rischio è bene, per prima cosa, discernere tra due aspetti fondamentali che, nel linguaggio comune, vengono spesso usati come sinonimi ma, nell'ambito della gestione del rischio, indicano due concetti ben differenti, ovvero i termini *incertezza* e *rischio*. Al primo ci si riferisce quando si intende un'azione (come un investimento) il cui esito non risulta prevedibile, mentre la seconda indica la non prevedibilità che si verifichi un certo effetto negativo o non gradito (come un investimento con rendimento negativo). In ambito finanziario un primo indicatore di rischio può essere inteso come la *varianza* (o la *volatilità*) dei rendimenti di un investimento o di un portafoglio di asset finanziari, riferendosi al fatto che tali rendimenti siano eccessivamente dispersi e volatili e implicando una variabilità eccessiva del risultato atteso. L'utilizzo della varianza come indicatore di rischio, tuttavia, non risulta sempre efficace poiché essa incorpora anche i movimenti "verso l'alto" di un rendimento, cosa che, nella pratica, assume connotazioni certamente positive. Alcuni studiosi hanno provveduto a fornire una definizione operativa di rischio finanziario come "la minima somma certa" che, se aggiunta ad un portafoglio, rende accettabile la loro combinazione [27]. In termini matematici:

$$\rho(X) = \inf\{a : X + a \in G\} \tag{3.1}$$

dove ρ(X) indica tale somma, X un dato portafoglio, a la somma certa e G l'insieme dei portafogli considerati accettabili. Una misura di rischio finanziario, per poter

essere definita "coerente", deve rispettare alcuni assiomi fondamentali. La prima condizione rappresenta l'*invarianza per traslazione*, per la quale:

$$\rho(X + a) = \rho(X) - a \; \forall a \in R \tag{3.2}$$

Questa equazione implica che l'aggiunta di un capitale certo ad un portafoglio diminuisce, per propria definizione, il rischio associato allo stesso portafoglio. Il secondo assioma della coerenza è indicato dalla proprietà di *monotonia*:

$$X \geq Y \Rightarrow \rho(X) \leq \rho(Y) \tag{3.3}$$

Dove R è l'insieme dei numeri reali e Y un secondo portafoglio: se un portafoglio è "migliore" dell'altro, allora lo è anche la sua misura di rischio finanziario (mrf). Un'altra proprietà fondamentale (detta anche "terzo assioma della coerenza") delle mrf risulta essere la *subadditività*, che si esprime come:

$$\rho(X + Y) \leq \rho(X) + \rho(Y) \tag{3.4}$$

Questa condizione implica che un un portafoglio composto da X e Y, per il principio fondamentale della diversificazione, comporta un rischio inferiore rispetto alla somma dei rischi dei due portafogli distinti. Infine, il quarto e ultimo assioma definisce l'*omogeneità positiva*, per cui:

$$\rho(\lambda X) = \lambda\rho(X) \tag{3.5}$$

λ è definito come un parametro scalare maggiore o uguale a zero. All'interno delle misure di rischio finanziario è possibile definire il "valore a rischio a livello di confidenza c" come quella mfr tale per cui:

$$VaR_c(X) = \inf\{a : P[X + a < 0] \leq 0\} \tag{3.6}$$

Con opportuni passaggi è possibile dimostrare che:

$$P[(X + VaR(X)) \geq 0] = 1 - c \tag{3.7}$$

L'equazione (3.6) indica il Value at Risk come quella somma che, se aggiunta ad un portafoglio garantisce, con una certa probabilità $1-c$, che questo non assuma valori negativi. In altri termini, è possibile esprime il VaR come la massima perdita che si potrebbe registrare in riferimento ad un dato orizzonte temporale e ad un livello di confidenza c. Il concetto di VaR è stato reso noto al pubblico da J.P. Morgan nel 1994, che contribuì a rivoluzionare sostanzialmente le metodologie della gestione dei rischi, introducendo una loro misura espressa in termini di ammontare di capitale. Semplificando ulteriormente, è possibile affermare che:

$$P[Perdita \geq VaR] = 1 - c \iff P[Perdita < VaR] = c \tag{3.8}$$

Questo indicatore ha riscontrato un notevole consenso poiché restituisce, in termini puntuali e in modo diretto, una sintesi dei vari rischi che possono intercorrere all'interno di un intermediario finanziario. Una tecnica per verificare la bontà della stima compiuta dal VaR consiste nel *backtesting*, ovvero confrontando "a ritroso" sulle serie storiche i valori stimati dal modello con quelli che effettivamente si sono verificati. Per la stima del VaR si possono utilizzare tre differenti tipologie:

1. *Approccio parametrico o di varianza-covarianza*, rappresenta l'approccio più immediato da utilizzare e si basa tipicamente sull'ipotesi di normalità della variabile casuale in questione (profitti e perdite), permettendo di stimare i parametri di questa v.c. direttamente dalla sua distribuzione.

2. *Simulazione storica*, consiste in un approccio non parametrico in cui non si fanno assunzioni sulla distribuzione della variabile di interesse ma ci si limita all'osservazione dei valori da essa assunta lungo il periodo considerato.

3. *Simulazione Monte Carlo*, consta anch'esso in un metodo non parametrico e si basa sulla generazione casuale di numerosi scenari di rischio, nei quali la variabile di controllo assume valori casuali appartenenti ad una certa distribuzione selezionata. I risultati ottenuti da tale simulazione rappresentano il punto di partenza per l'ottenimento dei parametri della distribuzione delle perdite. Questo metodo risulta essere il più preciso perché si basa su di un numero molto elevato di "osservazioni fittizie", ma richiede maggiore potenza computazionale per poterle generare.

Ad oggi, tutte le metodologie utilizzate nell'ambito del risk management sono derivate dal VaR e questo rende l'idea sull'importanza che esso ha rappresentato in questo ambito: permette infatti di conoscere, in ogni istante, l'ammontare di capitale che è necessario mantenere per coprirsi dall'eventuale perdita. L'utilizzo di questo indicatore può essere fatto nell'ambito di tutte le categorie di rischio, utilizzando una piuttosto che l'altra tecnica di calcolo illustrata. Volendo aggregare più VaR in un unico indicatore è necessario conoscere i coefficienti di correlazione tra le singole componenti (intese come singole fonti di rischio, ad esempio strumenti finanziari). In generale, tale coefficiente (noto anche come coefficiente di correlazione lineare di Pearson) viene calcolato come:

$$\rho_{xy} = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \tag{3.9}$$

dove σ_{xy} è la covarianza tra le due variabili x e y e σ_x e σ_y sono le loro deviazioni standard. Il coefficiente di correlazione assume valori compresi tra -1 e 1, e può essere qualitativamente interpretato come il legame percentuale tra le variazioni che intercorrono tra due variabili. Nell'ipotesi più generale di considerare n variabili di rischio a cui sono associati n VaR, si può calcolare il VaR complessivo nel seguente

modo. Per prima cosa, si considera il vettore colonna dei VaR:

$$VaR = \begin{bmatrix} VaR_1 \\ VaR_2 \\ \vdots \\ VaR_n \end{bmatrix}$$

e mediante trasposizione si ottiene il suo vettore trasposto

$$VaR^T = \begin{bmatrix} VaR_1 & VaR_2 & \dots & VaR_n \end{bmatrix}$$

Considerando poi la matrice n x n dei coefficienti di correlazione

$$\rho = \begin{bmatrix} 1 & \rho_{1,2} & \dots & \rho_{1,n} \\ \rho_{2,1} & 1 & \dots & \rho_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{n,1} & \rho_{n,2} & \dots & 1 \end{bmatrix}$$

si ottiene il VaR complessivo con la seguente equazione in forma matriciale:

$$VaR_{tot} = \sqrt{VaR \times \rho \times VaR^T} \tag{3.10}$$

Nel caso dei rischi operativi si assume spesso assenza di correlazione tra i singoli VaR, nonostante questa sia un'approssimazione talvolta grossolana, poiché i singoli rischi sono tra loro correlati in qualche maniera, sebbene la stima del coefficiente sia alquanto complessa, vista la natura dei fenomeni operativi (si pensi ad un cyber rischio che causa una interruzione dei servizi erogati da una banca, una volta che il guasto sia stato riparato può accadere che si verifichino errori umani dettati dall'agitazione o dalla fretta di ripristinare a più presto le comunicazioni). In questo modo è possibile esprimere un VaR "operativo" come:

$$VaR_{tot} = \sqrt{\sum_{i=1}^{N} VaR_i^2} \tag{3.11}$$

In questa sede non verrà trattato l'utilizzo delle numerose varianti del VaR che nel corso degli anni sono state proposte, tuttavia, se ne riportano alcune a titolo informativo:

- *Modified VaR*, detto anche *Corn-Fisher VaR* dal nome dei matematici che lo introdussero per la prima volta. Questo metodo permette, sostanzialmente, di rilassare l'ipotesi di normalità dei rendimenti (la fonte di rischio), "aggiustando" la distribuzione con l'introduzione del momento terzo e quarto, ovvero, rispettivamente, l'indice di simmetria e di curtosi.[3]

[3]Per "asimmetria" si intende la non simmetria di una distribuzione rispetto ad un suo particolare valore delle ascisse, mentre per "curtosi" si indica quando una distribuzione risulta "allugata" e dotata di code insolitamente "grasse".

- *Relative VaR*, ovvero il calcolo del valore a rischio in relazione ad un certo benchmark, ad un certo orizzonte temporale e con un dato livello di confidenza, esprimendo in tali termini il "peggiore" valore assunto da un certo portafoglio rispetto ad un valore di riferimento.
- *Marginal VaR*, che permette di comprendere in che modo i singoli elementi apportino un rischio all'interno di un certo portafoglio, ovvero al comportamento del VaR complessivo rispetto ad una variazione delle singole componenti. In termini matematici può essere calcolato semplicemente come la derivata parziale del VaR totale rispetto alla variazione del singolo peso.
- *Component VaR*, può essere inteso come una misura parziale del VaR e permette di assegnare alle singole componenti di un portafoglio o ad ogni asset il corrispettivo ammontare di VaR. In questo approccio la somma dei singoli VaR deve essere pari a quello complessivo del portafoglio, consentendo anche il calcolo dell'impatto percentuale di una singola fonte di rischio all'interno del portafoglio.
- *VaR Incrementale*, che consente di modellare le variazioni del Valore a Rischio dovute all'aggiunta o alla rimozione di un certo strumento da un portafoglio. Questa misura si fonda sulla comparazione tra il VaR del portafoglio "modificato" rispetto a quello di partenza, permettendo di quantificare la variazione globale del VaR.

Come detto in precedenza, il Value at Risk è una misura omogenea di rischio che permette di esprimere sinteticamente e in termini di capitale il grado di rischio che una qualsiasi banca o istituzione incontrano durante la loro operatività. Tuttavia, a questo metodo sono state mosse nel corso degli anni diverse critiche che hanno portato all'adozione di nuove misure coerenti per il rischio, permettendo, in qualche modo, di superare i limiti insiti in questo approccio.

3.2.1 Le limitazioni del VaR, l'Expected Shortfall

Le principali critiche che sono state mosse all'utilizzo del Value at Risk possono essere riassunte sinteticamente in due aspetti. Per prima cosa, esso viola l'assioma di subadditività, proprietà definita dall'equazione (3.4), collidendo con il principio elementare per cui la diversificazione di portafoglio, condotta mediante l'aggiunta di un titolo negativamente correlato a quello già presente, possa compensare variazioni sfavorevoli di quest'ultimo. Secondo il primo teorema dell'Integrated Risk Management, il Value at Risk rispetta l'assioma di subadditività solamente sotto l'ipotesi che i rendimenti di portafoglio appartengano alla classe delle distribuzioni ellittiche (tra le quali possiamo trovare la normale multivariata, la t di Student e altre). In tali circostanze vale quindi la condizione per cui:

$$VaR(X+Y) \leq VaR(X) + VaR(Y) \tag{3.12}$$

In questo caso l'aggiunta di un titolo si comporta coerentemente con il principio della diversificazione, per cui il Valore a Rischio del portafoglio è minore o uguale alla somma dei VaR delle singole posizioni. Nel momento in cui suddette ipotesi non siano più rispettate, ad esempio quando si opera con distribuzioni asimmetriche, l'utilizzo di questo indicatore non è più coerente con il principio per cui "a merger does not create extra risk", ovvero che l'aggiunta di un opportuno titolo al portafoglio non contribuisca ad aumentarne la rischiosità. In questo caso sarà quindi vero che:

$$VaR(X+Y) > VaR(X) + VaR(Y) \tag{3.13}$$

Pertanto, i tutti quei casi reali dove non si opera con distribuzioni ellittiche, non valgono più i risultati fondamentali del primo teorema dell'IRM, rendendo necessaria l'adozione di un metodo coerente che sopperisca a tale criticità. Un primo strumento introdotto fu l'Expected Shortfall, creato proprio per porre rimedio alla violazione dell'assioma di subadditività del VaR e dalla sua incapacità di tener conto della dimensione delle perdite. Questa misura può essere interpretata come il valore atteso delle perdite presenti nella coda della distribuzione oltre alla soglia critica del VaR, e può essere espresso dalla seguente formula:

$$ExpectedShortfall = E[Perdite|Perdite > VaR] \tag{3.14}$$

L'ES corrisponde quindi ad una una media delle perdite, condizionate al fatto che l'ammontare di ciascun di queste sia superiore al VaR e permette di ottenere un valore medio dell'impatto che potrebbe avvenire per quelle probabilità sfavorevoli non contemplate dal VaR.

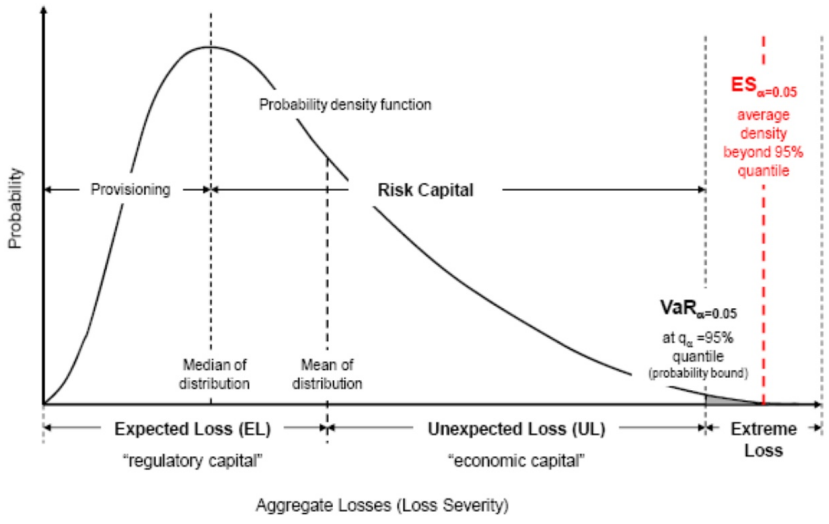

Figura 3.1: Rappresentazione grafica di VaR ed ES (fonte: [28])

Acerbi e Tasche hanno dato ampia dimostrazione della coerenza di questa misura dimostrandone la conformità ai quattro assiomi definiti in precedenza [29] [30]. E' comunque necessario far notare come l'ES non sia una misura sostitutiva del VaR, ma deve essere utilizzata in modo complementare per analizzare quegli scenari di rischio poco probabili, ma comunque non impossibili, che sono contenuti nella coda di destra della distribuzione delle perdite considerata.

3.3 La cybersecurity regulation nel settore finanziario

I rischi provenienti dal cyberspazio sono tipicamente inclusi nella categoria dei rischi operativi, nonostante essi riguardino fenomeni differenti sia per modalità di impatto che per tipologia di diffusione. Nel corso degli anni la regulation sui rischi finanziari ha compiuto numerosi passi in avanti, stabilendo delle normative univoche da rispettarsi ed implementarsi in ciascun intermediario finanziario. Lo stesso non può essere affermato riguardo alle normative in materia di cybersecurity, nonostante questo problema abbia ricevuto, nel corso del tempo, un'attenzione via via maggiore dagli enti regolatori. Numerose organizzazioni, come il Comitato di Basilea per la Supervisione Bancaria (BCBS), il Comitato per Pagamenti ed infrastrutture di mercato (CPMI), il Consiglio per la Stabilità Finanziaria (FSB), il Gruppo dei Sette (G7) e il Fondo Monetario Internazionale (FMI) hanno, recentemente, posto l'attenzione sulla criticità della sicurezza informatica, con una serie di regolamenti e raccomandazioni adottate da svariate istituzioni. Tuttavia, ancora oggi è possibile osservare l'assenza di un approccio internazionale globalmente condiviso e adottato da tutti i paesi: le regole da adottare variano infatti a seconda della giurisdizione e il loro utilizzo risulta spesso frammentato e fortemente discrezionale.

Tradizionalmente, il risk management è inteso come quel processo di gestione del rischio che si basa essenzialmente su diverse fasi: *identificazione*, *analisi e valutazione*, *mitigazione* e *monitoraggio*. Tuttavia, come riportato in un articolo [31], nella gestione di un cyber rischio, data la sua natura, si utilizza un approccio basato prevalentemente sulla fase di risposta al rischio, sotto l'ipotesi (più che realistica) che questo rischio si verifichi quasi sicuramente, vista l'impossibilità di costruire sistemi completamente impenetrabili. Inoltre, aspetti come la crescente digitalizzazione, la complessità delle connessioni presenti nell'ecosistema finanziario mondiale, lo storico degli attacchi passati (che hanno già colpito numerose banche centrali sparse in tutto il mondo) e il costo ad essi associato rendono quantomeno necessario un ulteriore focus sulla materia da parte degli istituti di regolazione, al fine di creare una serie di regolamenti e strumenti univoci che possano migliorare la fase di gestione dei cyber rischi.

3.3.1 L'evoluzione della regulation nell'Unione Europea

A livello europeo è possibile osservare una prima intenzione di *cybersecurity regulation* nel 2013, con la pubblicazione della "Cybersecurity Strategy", un documento in cui si dava una visione generale della tematica a livello continentale, definendo ruoli e responsabilità per conseguire l'ambizioso obiettivo di «rendere l'Unione Europea il più sicuro ambiente online del mondo» [32]. Successivamente, nel 2017, è stata proposto un sostanziale miglioramento al regolamento precedente, con lo scopo di: 1) costruire una resilienza europea ai cyber attacchi, 2) creare una cyber deterreza, 3) rafforzare la cooperazione internazionale a livello di cybersecurity. [33] Questo ha portato alla dichiarazione dell'European Network and Information Security Agency (ENISA) come un'ente indipendente destinato allo studio della cybersecurity e ad un contestuale framework di riferimento. Nel 2018 la Banca Centrale Europea (ECB) ha diffuso, per i paesi membri, un framework noto come "TIBER-EU", che permette la simulazione di un attacco informatico e l'impatto di questo sui vari aspetti organizzativi dell'azienda.[4] Questo è stato il primo caso in cui si sia effettivamente definito un metodo globale e indipendente dalla giurisdizione cui chi lo applica appartiene, nonostante la sua implementazione non sia obbligatoria e la sua efficacia sia strettamente legata alla modalità con cui viene impiegato. Nel corso degli anni sono state introdotte anche altre regolamentazioni non strettamente dedicate al settore finanziario, ma destinate a quelle organizzazioni che operano in settori *data-intensive*, come nel 2016 con la General Data Protection Regulation (GDPR) che tratta dettagliatamente il processamento dei dati personali, la sicurezza delle informazioni, e l'obbligo di notificare alle autorità competenti di aver osservato una perdita di dati malevola e l'oggetto di tali informazioni [34]. In ambito finanziario è possibile individuare almeno otto differenti "settori" della cybersecurity, destinati ad altrettante tipologie di attività che vengono svolte dall'organizzazione. Nello specifico:

1. Gli intermediari creditizi e le società di investimento sono soggette a specifiche richieste in materia di rischi operativi, includendo i requisiti patrimoniali [35], l'adozione di processi per la valutazione e gestione di suddetti rischi e la creazione di piani di continuità e di emergenza, nel caso si verificasse un'interruzione severa del proprio business [36]. Inoltre, a partire da luglio 2017, le banche sottostanti alla supervisione della ECB sono tenute alla dichiarazione di quei cyber eventi che si sono verificati presso la loro infrastruttura [37].

2. Le aziende eroganti servizi di pagamento sono soggette alle "Payment Services Directive" (PSD2), nelle quali si stabilisce un framework focalizzato sulla fase

[4]Questo strumento fu inizialmente inteso come "sector neutral", ovvero dedicato ad una qualunque azienda, a prescindere dal settore in cui essa opera. Tuttavia, è possibile osservare come questo sia stato appositamente disegnato per essere applicato al settore finanziario.

di mitigazione dei cyber rischi e di quelli operativi, oltre che all'obbligo di riportare l'accadimento di questi rischi, nel caso si siano dimostrati di maggiore entità [38]. L'ECB ha adottato la regolamentazione SIPS, che riguarda i cosiddetti "Sistemi di Pagamento Sistematicamente Importanti", nei quali si richiede all'operatore di stabilire un framework per l'identificazione, il monitoraggio e la gestione dei rischi operativi, includendo anche i cyber rischi e suggerendo un focus su di essi [39]. I sistemi di pagamento retail sono invece soggetti al "Revised Oversight Framework for Retail Payment Systems", in cui i cyber rischi vengono trattati alla strenua dei semplici rischi operativi [40]. Nel 2018 l'ECB ha pubblicato il CROE (Cyber Resilience Oversight Expectations for Financial Market Infrastructures), dedicato all'implementazione di metodi e strumenti utili a migliorare la resilienza alle cyber minacce [41].

3. I reperitori di dati sulle negoziazioni (meglio noti come "trade repositories") sottostanti alle direttive sui rischi operativi dell'EMIR (European Market Infrastructure Regulation) sono tenuti ad utilizzare sistemi informativi "affidabili e sicuri", oltre che dei piani di continuità e recupero [42].

4. Per quanto concerne le compagnie di riassicurazione, esse sono soggette alla direttiva "Solvency II" (creata appositamente per estendere i dettami di Basilea II al settore assicurativo), nel quale è specificata la necessità di possedere piani di risposta e di recupero ai rischi operativi, assieme ai requisiti minimi di capitale [43].

5. Alle agenzie di rating creditizio è richiesto di implementare gli adeguati controlli e di possedere procedure di controllo congruenti all'interno dei propri processi informativi [44].

6. I Depositi Centrali Titoli devono rispettare diverse direttive, tra le quali: 1) il mantenimento di strumenti IT ad alto grado di sicurezza, 2) possedere piani di "business continuity" e di recupero, come la creazione di un sito di processamento secondario, 3) organizzare programmi di test e di verifica dei controlli, 4) gestire i rischi provenienti dall'esterno che possano intaccare l'operatività dell'istituzione [45].

7. Infine, per le parti implicate nel trading di strumenti finanziari sui mercati regolamentati come società di investimento, società di borsa e *providers* di dati, si applicano del direttive MiFID II [46] e MiFIR [47], nelle quali si richiede l'utilizzo di sistemi di sicurezza per le risorse IT, di minimizzare il rischio di alterazione delle informazioni e di prevenire gli accessi non autorizzati per ridurre le perdite di dati. Ulteriori richieste valgono per le società correlate al trading algoritmico, come l'obbligo di implementare gli standard necessari per evitare che la suddetta attività sia condotta contro le regole del mercato, oltre

che l'obbligo di condurre test di penetrazione annuali e simulazioni di cyber attacchi [48].

8. Infine, per quanto concerne le aziende del settore FinTech, la necessità di una maggiore consapevolezza e di una migliore implementazione della cybersecurity è stata oggetto, nel 2018, nel "FinTech Action Plan" della Commissione Europea, dove si è suggerita esplicitamente maggiore resilienza in merito alle cyber minacce, al fine di garantire un servizio il più efficiente e sicuro possibile, oltre che al mantenimento della fiducia dei consumatori e dei mercati [49].

Tutte queste disposizioni permettono di apprezzare come il *trend* recente riguardi una maggiore presa di coscienza sui cyber rischi, oltre che ad una maggiore prevenzione e sensibilizzazione sulla materia. Tuttavia, è immediato notare come le disposizioni siano altamente variegate a seconda dell'ambito di impiego dell'azienda, producendo spesso incongruenze, sovrapposizioni delle stesse e conflitti legali, in assenza di una normativa unica e ampiamente condivisa da tutti segmenti del settore finanziario.

3.3.2 L'incertezza normativa

Ad oggi, i cyber-rischi sono largamente considerati come dei semplici rischi informatici o di natura operativa, come riportato anche dal Comitato di Basilea [50]. A livello puramente teorico è certamente possibile affermare che questi rischi siano di natura operativa, ma, in merito alle loro caratteristiche e al loro potenziale impatto, occorre porre una maggiore distinzione. Questo non sempre accade, poiché si utilizza spesso un approccio *one-size-fits-all*: ad esempio, le richieste di capitale per i rischi operativi non pongono una distinzione sui cyber rischi [51]. Un'altra incongruenza la si ritrova anche quando la cybersecurity e i rischi operativi risultino separati ma unicamente a livello testuale, come nel caso dell'Articolo 95 del PSD2, in cui ci si riferisce a "operational and security risks" senza porre alcuna distinzione concreta tra le due classi di rischio [52]. Anche nel caso in cui si menzioni direttamente la cybersecurity, le normative definiscono un approccio superficiale ed astratto, suggerendo le azioni che sarebbe meglio compiere senza imporre una procedura solida, univoca e verificata. Questa mancanza, tuttavia, è da imputarsi anche alla natura della tematica in questione e all'estrema variegatura del settore finanziario, oltre che alla sua estrema criticità. Infatti, la presenza di normative troppo specifiche potrebbero in qualche modo fornire a dei potenziali criminali informazioni utili per scovare vulnerabilità all'interno dei sistemi. Inoltre, le aziende regolate sono altamente differenziate sia a livello di dimensione che di ambito operativo, richiedendo una certa flessibilità della regulation certamente difficile da stabilire e da implementare. A questi aspetti si aggiunge l'inarrestabile digitalizzazione del settore finanziario, che implica una maggiore complessità

delle architetture hardware e software e un conseguente inasprimento delle misure preventive da adottare.

3.3.3 Standard emergenti e aspettative future

Se, da un lato, il panorama della regulation appare piuttosto frammentato e privo di una vera e propria linea guida, gli enti regolatori hanno fatto uso di standard e framework già esistenti da utilizzarsi come punto di partenza per una normativa unica. Tra questi possiamo ritrovare:

- Gli standard tecnici della cybersecurity sono stati sviluppati dall'Organizzazione Internazionale per la Normazione (ISO) in collaborazione con l'ISACA (Information Systems Audit and Control Association), dando vita alla normativa ISO 27001 [53]. Qui vengono sancite le basi del sistema di sicurezza delle informazioni che devono essere implementate all'interno dell'organizzazione tramite l'adozione del'ISMS (Information Security Management System), un framework di gestione del rischio che aiuta a identificare, analizzare e affrontare i rischi e a proteggersi da minacce informatiche e violazioni dei dati, simili nella progettazione ai sistemi di gestione per la garanzia della qualità (ISO 9000) e protezione ambientale (ISO 14000). Successivamente è stata introdotta la norma ISO 27002, il cui obiettivo principale è la definizione dei controlli nell'ambito del processo di implementazione di un sistema di gestione della sicurezza delle informazioni basato sulla 27001, fondandosi su 14 "clausole" di controllo di sicurezza, in 35 categorie principali di sicurezza e 144 controlli [54].

- Il NIST (National Institute of Standards and Technology) ha sviluppato quello che, ad oggi, è il framework di riferimento per l'implementazione della cybersecurity a livello internazionale, creato con lo scopo di aiutare le organizzazioni ad una migliore comprensione e gestione delle cyber minacce. Il Framework si concentra sull'utilizzo di drivers di business per guidare le attività di cybersecurity, considerando i rischi di sicurezza informatica parte dei processi di gestione del rischio dell'azienda, includendo al suo interno 98 tipologie di controlli (portati a 256 nel NIST 800-53) utili a definire un livello di maturità raggiunto della propria sicurezza. Il framework è diviso in 3 "tiers" essenziali, ovvero tre step differenti utili a definire un profilo di rischio dell'organizzazione. La prima parte, detta "Framework Core" è un insieme di procedure di sicurezza, risultati e riferimenti comuni a tutte le infrastrutture critiche. Il Core contiene gli standard, le linee guida e le pratiche del settore in modo da consentire la comunicazione delle attività e dei risultati di sicurezza informatica in tutta l'organizzazione, dal livello esecutivo a quello operazionale. Questa prima parte è costituita da cinque differenti funzioni: *identificazione*, *protezione*, *rilevamento*, *risposta* e *ripristino*. Se considerate insieme, forniscono

una visione strategica della gestione del rischio per la sicurezza informatica, identificando le categorie chiave e le sottocategorie inferiori, confrontando per ciascuna gli standard gli esistenti, le linee guida e le pratiche riscontrabili. La seconda parte, denominata "livelli di implementazione del framework" fornisce un contesto su come ciascuna azienda percepisca il rischio di sicurezza informatica ed i corrispettivi processi di gestione. Ciascun livello descrive il grado con cui le pratiche di gestione del rischio mostrano le caratteristiche definite nel Framework (ad esempio, "Consapevole del rischio e delle minacce"), e caratterizzano le pratiche di un'organizzazione in diverse classi, da "Parziale" (Livello 1) ad "Adattivo" (Livello 4). Questi livelli sottendono un progressivo miglioramento della gestione del rischio, da risposte informali a reattive ed agili. Durante il processo di selezione dei livelli, un'organizzazione dovrebbe considerare le sue attuali pratiche di gestione del rischio, il contesto delle minacce, i requisiti legali e normativi, la mission aziendale e i vincoli organizzativi. Infine, la terza parte (detta "Profilo"), rappresenta i risultati in base alle esigenze che si sono indicate negli step precedenti. Il risultato può essere interpretato come il grado di allineamento degli standard, delle linee guida e delle pratiche utilizzate. I differenti profili risultanti possono essere utilizzati per identificare i possibili miglioramenti della propria sicurezza informatica, confrontando il profilo attuale con un profilo target. Per poter sviluppare un profilo occorre rivedere le categorie e le sottocategorie e determinare quali siano le più importanti. Il profilo attuale può quindi essere utilizzato per la definizione delle priorità e la quantificazione dei progressi verso il profilo obiettivo, tenendo conto di altre esigenze aziendali, tra cui l'efficacia in termini di costi. Ciascun esito può essere utilizzato per condurre autovalutazioni e per comunicare, sia all'interno della propria organizzazione che all'estero di essa [55].

- Nell'ambito delle procedure di mitigazione, il CIS (Center for Internet Security) ha diramato una serie di "Controlli critici di sicurezza" (CSC) in cui sono contenute 20 azioni fondamentali e 171 "sotto-controlli" utili diminuire il tasso di incidenza delle minacce informatiche. Ciascun controllo è caratterizzato da una sigla identificativa, un nome, l'asset a cui ci si riferisce, la funzione e la sua descrizione. La suddivisione dei controlli per ordine di importanza (Basici, Fondamentali e a livello organizzativo) è stata implementata proprio per suggerire alle alle organizzazioni un numero limitato di controlli prioritari che dovrebbero essere implementati per ottenere risultati immediati [56].

- Il Federal Financial Institutions Examination Council (FFIEC) ha introdotto uno strumento di *self-assesment* dedicato agli istituti finanziari, con lo scopo di aiutare tali soggetti all'identificazione dei rischi (con l'ottenimento di un "Inherent Risk Profile") e ad avere una prospettiva sul livello di maturità delle procedure di cybersecurity correntemente implementate all'interno della

propria organizzazione ("Cybersecurity Maturity"). Il metodo è coerente con il framweork NIST e con altri standard di sicurezza accettati dall'industria [57].

Un esempio di questa armonizzazione degli standard è il già citato CROE, sviluppato dalla ECB in riferimento al framework NIST, alla ISO 27002, al tool dell'FFIEC e ad altri standard internazionali di riferimento. Questo atto rappresenta, però, un evento isolato: ad oggi non si osserva ancora la presenza di una *baseline* normativa per la cybersecurity che rispecchi realisticamente le variegate realtà organizzative presenti (non solo) nel settore finanziario. Il design di tali strumenti deve, inoltre, superare la superficialità di molte normative esistenti, indicando i requisiti sostanziali e suggerendo azioni concrete ed analizzabili, considerando anche quei settori trasversali al mondo finanziario, mirando quindi ad una standardizzazione sia verticale che orizzontale. Vista la centralità del sistema in questione, sono innumerevoli i settori ad esso strettamente connessi, rendendo necessario il focus sui servizi di terze parti che comunicano direttamente con gli intermediari, in quanto essi possono essere oggetto di minacce e contribuire alla diffusione di queste. In ogni caso, la crescente complessità delle infrastrutture IT renderà necessario un costante aggiornamento, oltre che alla revisione degli standard introdotti, al fine di allineare i cyber rischi con i loro metodi di gestione e di colmare un gap che, fino ad oggi, risulta ancora troppo elevato per la criticità degli effetti possibili.

Capitolo 4

Modello quantitativo per l'analisi di un cyber rischio

4.1 Origine e obiettivi del modello

I modelli che verranno illustrati nelle pagine seguenti sono stati sviluppati durante l'esperienza di tirocinio dell'autore condotta tra settembre e dicembre 2020 presso la società Augeos S.p.A. di Rivoli (TO), la quale da diversi anni opera nel settore dei servizi finanziari e della consulenza dedicata principalmente a banche e altri intermediari di medie-piccole dimensioni, sparsi su tutto il territorio nazionale (tra le altre, Banca Intesa San Paolo, Banca Popolare di Puglia e Basilicata, Banca del Piemonte). Questi studi sono stati condotti come analisi preliminare per lo sviluppo di un modulo integrativo del prodotto GRC®, una piattaforma altamente personalizzabile nella quale il cliente dispone di numerosi strumenti per l'analisi dei rischi (operativi, informatici, di conformità alle normative vigenti). La volontà dell'azienda è stata quella di introdurre un metodo quantitativo per la stima delle perdite in seguito a eventi di sicurezza informatica, per dotare i propri clienti di uno strumento di supporto alla gestione dei propri rischi.

In generale, un cyber rischio può essere inteso come il concatenarsi di tre oggetti fondamentali: *asset*, *minacce* e *vulnerabilità*. Appartengono alla prima categoria sia gli elementi tangibili presenti nell'azienda (PC, server, ATM ecc.) sia quelli intangibili, intesi come i processi logici potenzialmente intaccabili da una minaccia (si pensi, ad esempio, al processo di erogazione di denaro presso uno sportello ATM). Ciascuno di questi asset è caratterizzato, per sua stessa natura, da una o più vulnerabilità, ovvero delle falle hardware o software che, potenzialmente, ne compromettono il funzionamento totale o parziale. Infine, la minaccia rappresenta quella condizione (ipotetica o no) per cui un certo agente interno o esterno sfrutta una certa vulnerabilità per colpire un dato asset. L'intersezione di queste tre caratteristiche costituisce il concetto di *rischio*, ovvero il manifestarsi di una certa

minaccia, in relazione ad un asset ed alle sue vulnerabilità. L'effetto di ciascun rischio, sia in termini di probabilità che di impatto finale può essere mitigato mediante l'adozione di opportuni *controlli*. I controlli di sicurezza informatica sono le contromisure implementate per gestire le minacce verso i sistemi e le reti; essi non sono statici e perpetui, ma cambiano in continuazione per adattarsi a un scenario informatico in costante evoluzione. L'adozione di determinate contromisure implica l'adesione a standard internazionali, il rispetto delle normative e l'implementazione di strategie difensive. Nella piattaforma GRC® ciascun cliente rileva i propri rischi mediante strumenti di self-assesment, nei quali si censiscono gli asset, le minacce e le vulnerabilità e si ottengono differenti scenari di rischio, considerando anche i rispettivi controlli CSC associati. Il risultato finale è una panoramica globale sui propri scenari di rischio dove, in base ai punteggi di criticità associati a ciascun elemento, si ottiene uno score globale del rischio in termini di importanza. I modelli proposti si collocano, idealmente, a valle di questo processo: una volta individuati le singole componenti di un rischio e i relativi controlli si offre la possibilità di compiere un'analisi probabilistica riferita all'orizzonte temporale di un anno, e di ottenere risultati quantitativi sulla base dei dati inseriti. Questo studio è stato implementato con l'obiettivo di:

- Compiere un'analisi statistica delle probabilità di accadimento di ciascun rischio.
- Condurre un'analisi statistica dell'impatto di uno o più rischi aggregati.
- Ottenere una distribuzione finale delle perdite mediante il metodo Monte Carlo.
- Quantificare il proprio livello di tolleranza al rischio in termini di perdita monetaria accettabile.
- Supportare il processo di *decision making* mediante il calcolo delle curve di rischio.
- Confrontare il profilo di rischio corrente dell'organizzazione con altri profili benchmark.
- Condurre un'analisi *what-if* in merito all?efficacia dei controlli nella mitigazione dei rischi.
- Ottenere una scomposizione dei rischi in base alla loro tipologia.

Nello specifico, sono stati proposti tre differenti modelli, tutti basati sullo stesso funzionamento, i quali permettono di analizzare singolarmente un rischio, molteplici rischi aggregati e di ottenere una loro scomposizione a seconda del processo che essi intaccano. Per i calcoli sono stati presi in considerazione quattro cyber

rischi ("Data breach", "Denial of service", "Abuse of personal data" e "Loss of sensitive information") ed i dati numerici inseriti sono frutto di osservazioni reali o di stime soggettive. I dati di output non sono da intendersi, pertanto, come valori che rispecchino effettivamente una certa realtà ma permettono di capire il funzionamento del modello e la sua coerenza nel fornire i risultati. Il software è da intendersi ancora nelle prima fasi dello sviluppo e, ad oggi, costituisce essenzialmente uno "studio di fattibilità". Nei seguenti paragrafi verrà esaustivamente descritto il metodo utilizzato per i calcoli, con le ipotesi di partenza e i principali dati di input e output, oltre che ad alcune porzioni di codice MATLAB® utili a farne comprendere il funzionamento.

4.2 Determinazione della probabilità di accadimento

Uno degli ostacoli principali nella quantificazione di un rischio risiede nella disponibilità dei dati provenienti da osservazioni reali, specie nel caso in cui l'evento in questione sia piuttosto raro o poco frequente, come, in questo caso, una perdita di dati significativa ("Data breach"). Nel caso particolare dei cyber rischi, inoltre, risulta talvolta difficile accedere ad informazioni dettagliate sul numero di eventi che si sono verificati e nei confronti di quale istituzione, per via della scarsa propensione delle vittime a diffondere certe informazioni, vista la perdita di reputazione e al danno economico che ne conseguirebbe. Per questo motivo, la determinazione della probabilità di accadimento per un singolo rischio può essere effettuata mediante svariati metodi, tra i quali:

1. Si stima in maniera soggettiva con che probabilità si possa verificare un certo rischio. Questo metodo può essere visto come un punto di partenza ed è tipicamente il meno preciso, poiché affetto da svariati *bias* cognitivi e spesso supportato da insufficienti dati a favore.

2. Si utilizzano processi logici tipici della teoria della probabilità, coinvolgendo stime soggettive con l'ausilio di metodi analitici più rigorosi.

3. Si ricorre all'uso delle distribuzioni di probabilità (Beta, binomiale, esponenziale ecc.) più idonee a rappresentare una certa percentuale di un campione e si utilizzano come dati di input per la loro costruzione osservazioni reali o stime soggettive nel caso queste non siano presenti.

Di seguito verranno descritti il secondo e terzo metodo, fornendo un'analisi della metodologia seguita e i principali risultati ottenuti dal modello.

4.2.1 Approccio Bayesiano alla stima delle probabilità

Un metodo per determinare con quale probabilità è possibile che si verifichi un evento può essere condotto utilizzando la logica di Bayes, costituita da una serie di enunciati largamente utilizzati nel campo della probabilità e della statistica. Uno dei principali aspetti positivi dell'adozione di questo metodo in ambito cybersecurity risiede nel fatto che permette di sfruttare correttamente le informazioni già possedute riguardo al rischio considerato, più alcune considerazioni soggettive richieste ad esperti del settore. In riferimento al calcolo della probabilità di una perdita copiosa di dati (in seguito ad un attacco informatico), è necessario introdurre alcune notazioni essenziali che saranno utilizzate in seguito per il computo degli output:

Notazione	Significato
P(Data breach)	Prob. che si verifichi una perdita di dati.
P(Vuln)	Prob. che esista una vulnerabilità sfruttabile da un agente esterno.
P(PTP)	Prob. che il risultato di un test di penetrazione dia esito positivo.
P($\sim$ Data breach)	Prob. che non si verifichi una perdita di dati.
P($\sim$ Vuln)	Prob. che non esista una vulnerabilità sfruttabile.
P($\sim$ PTP)	Prob. che il risultato di un test di penetrazione dia esito negativo.

Si noti come le probabilità negative non sono altro che il complemento a uno delle loro coniugate.

A questo punto è possibile richiamare il concetto di probabilità condizionata all'accadimento o meno di un evento, ovvero quella possibilità che, nel caso in esame, una perdita di dati si verifichi, noto che esista una vulnerabilità potenzialmente sfruttabile all'interno di un asset:

$$P(Data\,breach|Vuln) = \frac{P(Data\,breach, Vuln)}{P(Vuln)} \tag{4.1}$$

Dove al numeratore troviamo la probabilità congiunta dei due eventi, ovvero quando si verificano contemporaneamente una perdita di dati ed esiste una vulnerabilità. Riflettendo brevemente, è possibile che un data breach accada sia in seguito ad un test di penetrazione positivo, sia ad uno negativo, questo perché tali test non garantiscono l'adeguatezza assoluta contro un attacco informatico. Alla luce di questa considerazione, è possibile quindi scrivere la probabilità che questo evento si verifichi in relazione al duplice possibile esito del test:

$$P(Data\,breach) = P(Data\,breach|PTP)P(PTP)+P(Data\,breach|\sim PTP)P(\sim PTP) \tag{4.2}$$

Ora, secondo il Teorema di Bayes, si può affermare che:

$$P(Data\,breach|Vuln) = \frac{P(Vuln|Data\,breach)P(Data\,breach)}{P(Vuln)} \tag{4.3}$$

Secondo la medesima logica dell'equazione (4.2), è possibile riscrivere il numeratore come:

$$P(Vuln) = P(Vuln|Data\,breach)P(Data\,breach)+P(Vuln|\sim Data\,breach)P(\sim Data\,breach) \tag{4.4}$$

Infine, sostituendo nell'equazione (4.3), si ottiene:

$$P(Data\,breach|Vuln) = \frac{P(Data\,breach|Vuln)P(Data\,breach)}{P(Vuln|Data\,breach)P(Data\,breach) + P(Vuln|\sim Data\,breach)P(\sim Data\,breach)} \tag{4.5}$$

Questa formula ci permette quindi di conoscere il legame tra la probabilità di perdita di dati condizionata alla presenza di una vulnerabilità con la probabilità che ci sia una vulnerabilità, condizionata al fatto che si sia osservata una perdita di dati malevola. Tale formulazione è estendibile a tutte le combinazioni logiche tra i diversi scenari di rischio, a patto che si dispongano degli input necessari, ottenibili da stime soggettive, questionari rivolti ad esperti o dati di settore. Di seguito si riportano alcuni risultati:

Tabella 4.1: Riepilogo delle principali probabilità elementari e condizionate

Input	*Risultati*
$P(DB\|Vuln.) = 25\%$	$P(Vuln.\|DB) = 26\%$
$P(DB\|\sim Vuln.) = 3\%$	$P(Vuln.\|\sim DB) = 3{,}1\%$
$P(Vuln.\|PTP) = 97\%$	$P(\sim DB\|Vuln.) = 75\%$
$P(Vuln.\|\sim PTP) = 0{,}1\%$	$P(Vuln.\|DB) = 3{,}9\%$
$P(PTP) = 4\%$	$P(Vuln.) = 4\%$
	$P(DB\|PTP) = 24{,}34\%$
	$P(DB\|\sim PTP) = 3{,}02\%$

Come già detto, gli input utilizzati provengono da stime soggettive o da risultati di assesment sulle probabilità: è possibile definire questi parametri come delle "informative priors", poiché informano a priori riguardo ad una condizione che si

vuole esaminare. Analogamente, è possibile parlare di "uninformative priors", il cui concetto verrà descritto nel paragrafo successivo. Nel modello non è stato inserito direttamente questo metodo visto l'ampio numero di parametri richiesti per il calcolo che potrebbero rendere poco intuitivo l'utilizzo a chi non conosce gli aspetti teorici della logica bayesiana. Tuttavia, qualora si volessero approfondire il ruolo dei singoli fattori è possibile utilizzare questo approccio per una analisi più dettagliata. Per il calcolo delle probabilità è stato implementato un secondo approccio basato sulla distribuzione Beta, la quale permette di ottenere una stima del tasso di accadimento di un certo rischio partendo da alcune osservazioni compiute, in un certo intervallo temporale, all'interno di un dato campione di banche che si ritiene possano essere significativi, per importanza e dimensioni, rispetto alla propria organizzazione.

4.2.2 Note generali sulla distribuzione Beta

Nella teoria della probabilità e in statistica, la distribuzione Beta appartiene alla classe delle distribuzioni di probabilità continue ed è definita da due parametri, entrambi positivi, noti come α e β. Considerando un variabile aleatoria x che segue questa distribuzione, è possibile definire tali parametri dal valore atteso e dalla varianza di x secondo le seguenti formule:

$$\alpha = E[x](\frac{E[x](1-E[x])}{Var[x]} - 1) \tag{4.6}$$

$$\beta = (1-E[x])(\frac{E[x](1-E[x])}{Var[x]} - 1) \tag{4.7}$$

$E[x]$ e $Var[x]$ sono rispettivamente il valore atteso e la varianza della variabile casuale e sono legati ai fattori di forma della distribuzione secondo le relazioni sottostanti.

$$E[x] = \frac{\alpha}{\alpha+\beta} \tag{4.8}$$

$$Var[x] = \frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \tag{4.9}$$

Da un punto di vista meramente interpretativo, la Beta rappresenta una distribuzione di probabilità riferita, a sua volta, a delle probabilità, ovvero, permette di modellare la verosimiglianza di un certo evento (in questo caso una determinato cyber rischio), in base al suo tasso di accadimento. Questo è vero anche per altre distribuzioni, come la binomiale, con la differenza che questa riguarda il numero

di successi di un processo di Bernoulli[1] mentre nella prima la variabile aleatoria x rappresenta la probabilità che si verifichi un certo esito. Le due distribuzioni possono quindi essere considerate come complementari: con la beta si stima una certa proporzione di una popolazione dati un certo numero di osservazioni sul campione, mentre con la binomiale la probabilità di un certo numero di successi, data una certa proporzione della popolazione. Qualitativamente, la forma e l'orientamento di questa distribuzione sono governati dai due parametri α e β, come si può osservare nell'immagine 4.1.

La particolarità della distribuzione beta risiede nell'essere una "prior coniugata" delle distribuzioni binomiali, di Bernoulli, negative binomiali e geometriche quando si tratta di inferenza bayesiana, ovvero quel processo di inferenza statistica in cui si aggiornano le probabilità di un certo evento con l'aumentare delle osservazioni compiute e delle informazioni da esse raccolte. L'approccio utilizzato prende il nome di "hits and misses", il quale trova un largo utilizzo in svariate applicazioni reali, non solo in ambito finanziario.

4.2.3 Hits and misses

Il fondamento logico di tale metodo consiste nell'interpretare i due parametri di forma della distribuzione come il numero di successi e fallimenti, ovvero:

1. α il numero di individui di un campione (con dimensioni note) estratto da una popolazione, che, per un dato intervallo temporale di osservazioni, hanno riscontrato il verificarsi di tale evento in questione ("hits").

2. β, analogo ad alfa, ma rappresentante il numero di individui appartenente al campione osservato che non hanno subito l'evento ("misses").

Per il computo di tali valori si fa riferimento a delle uninformative priors, ovvero delle stime a priori riguardanti la probabilità di successo o di fallimento: esse contengono essenzialmente un'informazione preliminare riguardo al numero di successi (un attacco informatico con furto di dati) e di insuccessi che ci si può aspettare senza che nessuno di questi si sia ancora effettivamente verificato. Una caratteristica essenziale di questi parametri risiede nel fatto che sia rispettate la seguente condizione:

$$prior_\alpha = prior_\beta \iff prior_\alpha \leq 1 \land prior_\beta \leq 1 \tag{4.10}$$

[1]Un processo di Bernoulli è un processo aleatorio discreto in cui la variabile di riferimento può assumere due e soltanto due valori distinti fra loro: 1 in caso di successo, 0 in caso di fallimento. Il più tipico dei processi di Bernoulli è il lancio di una moneta, dove i possibili esiti discreti sono distintamente due: testa o croce.

Nel seguente modello si pongono entrambe la priors uguali a uno, ovvero ci si attende a priori un successo e un fallimento di un attacco informatico con perdita di dati, in riferimento ad un campione di individui (intermediari finanziari) con dimensione nota. Una delle potenzialità della distribuzione Beta risiede nel fatto che, aggiornando i suoi valori per il calcolo di α e β, essa restituisce un'interpretazione migliore man mano che si compiono delle osservazioni rispetto a quelle precedenti. Per comprendere tale concetto, è utile fare un esempio. Si immagini di voler conoscere quale sia la probabilità che al primo lancio di una moneta esca testa. Non avendo altre informazioni a riguardo, né sapendo se la moneta sia perfettamente bilanciata, l'unica cosa che possiamo aspettarci è una identica probabilità (50%) di ottenere testa oppure croce. Ripetendo il lancio e aggiornando i valori di α e β, la funzione modifica la propria forma, passando da una linea perfettamente orizzontale (una distribuzione uniforme) ad una con picco in prossimità del valore medio della probabilità di ottenere testa, date le osservazioni precedenti. Ad ogni iterazione, la distribuzione converge sempre più rapidamente verso quel valore medio che meglio riflette la realtà.

Tabella 4.2: Alcune osservazioni per 100 lanci di una moneta

Lancio	*Testa oss.*	*Croce oss.*	*Prob. testa*
1	1	0	100%
2	2	0	100%
3	2	1	40%
4	2	2	50%
5	3	2	60%
...	...	...	...
20	11	9	55%
...	...	...	...
30	14	16	47%
...	...	...	...
40	21	19	53%
...	...	...	...
50	22	28	44%
...	...	...	...
60	28	32	46%
...	...	...	...
80	36	44	45%
...	...	...	...
90	44	35	49%
...	...	...	...
100	54	46	54%

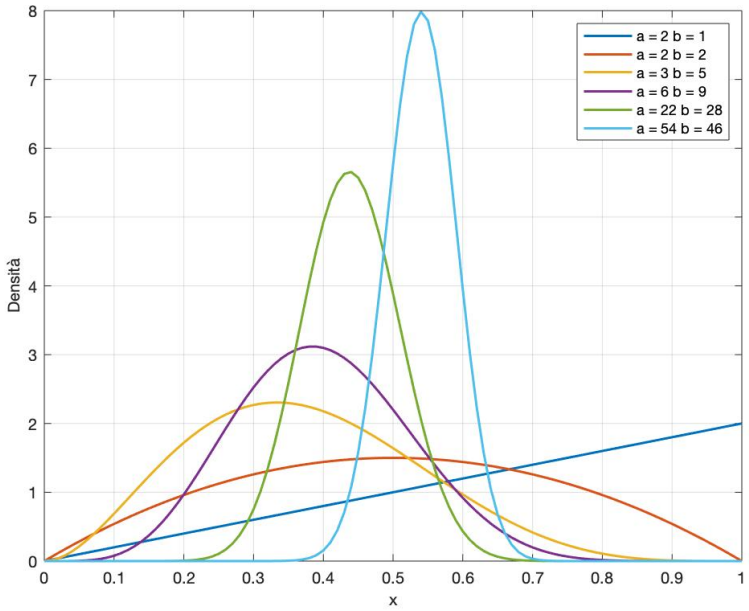

Figura 4.1: Distribuzioni di probabilità per i lanci in tabella 4.2

4.2.4 Dati di input ed esempi di calcolo

Tornando alla perdita di dati sensibili, si procede in maniera analoga al caso appena descritto: partendo dalle priors, si aggiornano i valori ottenuti in seguito alle osservazioni effettuate e si rileva la probabilità media dell'evento in questione. Ai fini del calcolo si utilizzano le seguenti formule:

$$\alpha = Numero\,di\,successi - prior_{\alpha} \tag{4.11}$$

$$\beta = n_c[y_e - y_s] - Numero\,di\,successi + prior_{\beta} \tag{4.12}$$

n_c è la numerosità del campione, mentre y_e e y_s sono rispettivamente l'anno di fine e di inizio osservazioni. Di seguito si riportano i dati di input e output utilizzati nel modello: il numero di successi e la popolazione del campione sono stati rilevati dal DBIR.[2]

[2]Il Data Breach Investigation Report è un documento annuale creato da Verizon, azienda di fama internazionale operante nel campo della sicurezza informatica. Esso costituisce lo stato dell'arte a livello mondiale sulle perdite malevole di dati che si verificano durante l'anno solare di riferimento [58].

Tabella 4.3: Dati di input e output per il calcolo della probabilità di "Data breach"

y_s	y_e	n_c	$Succ.$	p_α	p_β	α	β	$Prob.\,med.$
2019	2020	4209	185	1	1	186	4025	4,4170%

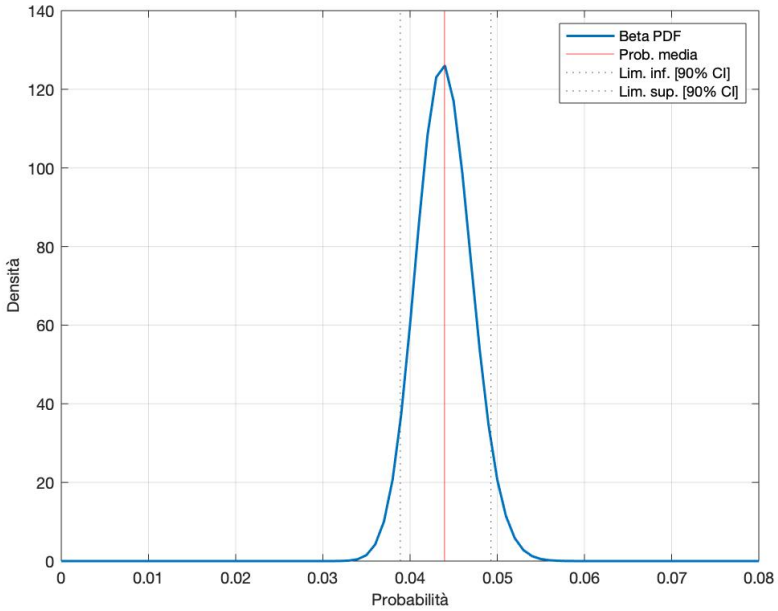

Figura 4.2: Distribuzione di probabilità media per il rischio "Data breach"

La probabilità media viene poi utilizzata come il riferimento per determinare se l'evento sia accaduto o no durante la simulazione. Per agire in maniera più conservativa, sarebbe anche possibile utilizzare come tale soglia il valore corrispondente al limite superiore dell'intervallo di confidenza al 90%.

4.3 Determinazione della distribuzione delle perdite

Una volta stabilita con quale probabilità si possa verificare un certo rischio nell'intervallo temporale considerato, è necessario determinare l'entità e la tipologia degli impatti, ovvero come si distribuiscono le perdite nel caso in cui la minaccia si manifesti. I dati di input del modello sono basati su valutazioni effettuate dal cliente (idealmente un responsabile della sicurezza informatica di una certa banca) al quale viene richiesto di indicare, per ciascun rischio, un range di valori (stabilendo

un minimo e un massimo) che rappresentino la perdita associata a tale evento. In questo modello si assume che le perdite si distribuiscano secondo una lognormale, per via della forma propria di questa distribuzione: la sua asimmetria pone una verosimiglianza massima verso valori modesti delle perdite, ma non esclude perdite di proporzioni molto significative grazie alla sua coda di destra piuttosto allungata, a differenza del caso in cui si assumesse una normalità delle perdite in questione.

Sarebbe comunque possibile utilizzare altre tipologie di distribuzioni, come la Triangolare[3] e la Legge di potenza[4](troncata e non), nonostante la loro costruzione sia meno intuitiva per via della stima necessaria dei parametri.

4.3.1 Note generali sulla distribuzione lognormale

Nella teoria della probabilità e in statistica la distribuzione lognormale appartiene alla classe delle distribuzioni di probabilità continue, in cui il logaritmo naturale della variabile aleatoria x è distribuito come una normale. In termini matematici:

$$x \sim Lognorm(\mu, \sigma^2) \iff logX \sim N(\mu, \sigma^2) \tag{4.13}$$

La lognormale ha funzione di densità di probabilità descritta come:

$$f(x) = \frac{e^{-\frac{(lnx-\mu)^2}{2\sigma^2}}}{\sqrt{2\pi}\sigma x} \tag{4.14}$$

Dove μ e σ sono rispettivamente la media e la deviazione standard della variabile casuale x. Il valore atteso e la varianza di questa v.c. si ottiengono dalle seguenti formule:

$$E[x] = e^{\mu+\frac{\sigma^2}{2}} \tag{4.15}$$

$$Var[x] = e^{2\mu+\sigma^2}(e^{\sigma^2} - 1) \tag{4.16}$$

Nella figura riportata di seguito è possibile avere un punto di vista qualitativo su come si modifica la funzione di densità di probabilità lognormale al variare di alcuni parametri.

---

[3]Nella costruzione della Triangolare occorre prestare attenzione che essa non ammette perdite al di fuori dei propri limiti superiori e inferiori, i quali rappresentano gli estremi dell'intervallo di confidenza al 100%. Può essere utile in situazioni nelle quali si vuole porre dei limiti assoluti alla variabile in esame.

[4]La Legge di potenza una distribuzione utile quando occorre modellare eventi con impatti di enormi proporzioni (epidemie, disastri naturali, eventi textitblack swan, per via della sua caratteristica coda "spessa". I parametri necessari sono α (fattore di forma) e θ (fattore di posizione). La sua variante "troncata" differisce solamente per la presenza di un limite massimo della coda, che esclude di fatto i valori della variabile ad esso maggiori.

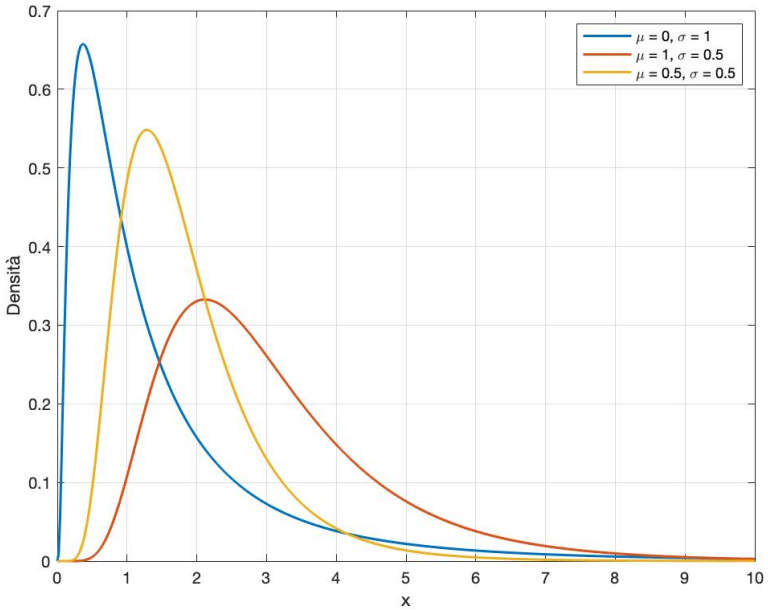

Figura 4.3: Distribuzioni lognormali al variare dei parametri μ e σ

4.3.2 Metodo di costruzione delle distribuzioni ed esempi di calcolo

Il primo passo per determinare la struttura delle perdite risiede nell'individuare i valori dei limiti inferiori e superiori, facendo riferimento ad un livello di confidenza $1-\alpha$: nel modello è stato assunto il 90%, valore non troppo elevato ma adeguato nel caso in cui vengano richieste delle stime soggettive, vista anche la variabilità con cui ciascun individuo quantifica personalmente l'ampiezza di tale intervallo. Esistono due approcci differenti con cui l'essere umano interpreta il concetto di probabilità:

1. *Approccio frequentista*, ovvero quello che applica il concetto di probabilità solo ad eventi tipicamente casuali o a bassa ripetibilità e con infiniti esiti possibili, rendendo di fatto l'uso della probabilità quasi impossibile da utilizzare in un contesto reale. Questo metodo è applicabile in ambiti ed esperimenti casuali infinitamente ripetibili sotto le medesime condizioni, in cui i singoli esiti non sono considerati equiprobabili.

2. *Approccio soggettivista*, in cui si associa al concetto logico di probabilità una componente interpretativa, un "grado di conoscenza" che ogni individuo stabilisce nel determinare l'incertezza di una certa situazione. Chi segue questo metodo utilizza la probabilità per descrivere ciò che egli ritiene di sapere riguardo ad un evento.

E' possibile affermare che il modello descritto in queste pagine richieda il secondo approccio: esso infatti intende l'utilizzo della probabilità (in questo caso espressa in termini di un intervallo di confidenza) come un livello di (in)certezza riferita all'impatto che si potrebbe registrare, una volta appurato che il rischio si sia verificato. Fatta questa premessa, per la stima dei limiti inferiori e superiori dell'intervallo, ci si chiede quei valori che racchiudano al loro interno il 90% dei casi osservabili, incluso il valore medio. Più semplicemente, ci si pone la seguente domanda:

> «Quali sono le perdite minime e massime che si potrebbero osservare, a seguito del verificarsi di una certa minaccia, nel 90% dei casi, in riferimento all'orizzonte temporale di un anno?»

Una volta determinati gli estremi dell'intervallo di confidenza, è possibile derivare la media e la deviazione standard della distribuzione, utilizzando le seguenti formule:

$$\mu = \frac{log(limite\,inferiore) + log(limite\,superiore)}{2} \tag{4.17}$$

$$\sigma = \frac{log(limite\,inferiore) - log(limite\,superiore)}{2 * \phi^{-1}[0{,}5\alpha]} \tag{4.18}$$

Dove ϕ^{-1} è la funzione normale inversa che restituisce il quantile del suo argomento ed $\alpha = 1 - CI$ è l'errore di prima specie (in questo caso pari a 10% per un livello di confidenza del 90%).

Tabella 4.4: Media e deviazione standard delle perdite da Data breach

$Limite\,inferiore$	$Limite\,superiore$	μ	σ
5.000.000	100.000.000	16,9228	0,9106

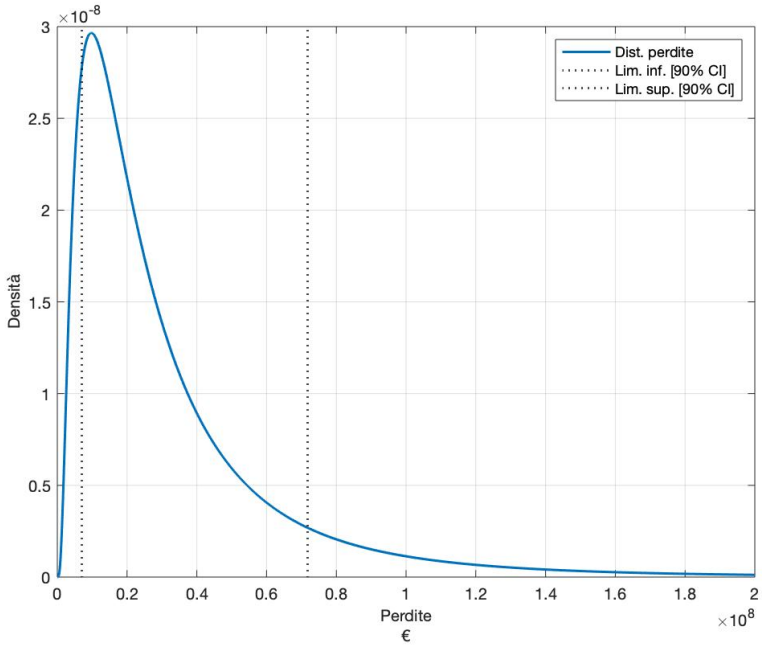

Figura 4.4: Distribuzione di densità di probabilità per le perdite causate dal rischio "Data breach"

4.4 Quantificazione degli impatti

Una volta determinata la probabilità con cui si può manifestare una perdita di dati causata da un attacco esterno malevolo e il danno da essa provocato, ovvero le perdite monetarie che ne conseguono, è possibile procedere al computo di alcuni valori fondamentali degli impatti che tengono conto sia della distribuzione di probabilità dell'evento, sia di quella delle perdite generate. I dati riportati nelle tabelle seguenti sono da intendersi, dove non specificato, espressi in euro.

4.4.1 Calcolo dei valori attesi e simulati delle perdite con il metodo Monte Carlo

Il modello prende in esame due tipologie di impatto associate al rischio: le perdite attese, ovvero il valore atteso della distribuzione delle perdite e quelle simulate, ottenute mediante l'impiego del noto algoritmo computazionale Monte Carlo. Per entrambe le categorie ci si riferisce sia al caso in cui non si mettono in pratica i controlli utili a mitigare il rischio (perdite), sia al caso in cui sono messi in pratica (perdite residue). Ai fini del calcolo delle perdite attese si sono utilizzate le seguenti equazioni:

$$Perdita = p_r[e^{\mu+\frac{\sigma^2}{2}}] \tag{4.19}$$

$$Perdita\,residua = p_r(1 - C_e)[e^{\mu + \frac{\sigma^2}{2}}] \tag{4.20}$$

Dove p_r è la probabilità media di accadimento determinata con la distribuzione Beta nei paragrafi precedenti, C_e è il coefficiente di efficacia dei controlli, espresso su una scala da 0 a 1 (può essere inserito mediante valutazioni interne, ad esempio analizzando report su test di penetrazione o seguendo altre procedure[5]). Il contributo di questo parametro si manifesta abbassando di una certa percentuale la probabilità dell'evento, e di conseguenza riducendone l'impatto totale, coerentemente a quanto si osserva nella realtà.

Tabella 4.5: Output per i valori attesi delle perdite

μ	σ	p_r	C_e	$Perdita$	$Perdita\,residua$
16,9228	0,9106	4,4170%	0,35	1.487.817,4457	967.081,3397

A questo punto il modello procede con il calcolo delle perdite simulate verificando iterativamente 100.000 scenari di rischio attraverso il metodo Monte Carlo. La genesi di questo approccio risiede negli anni '40 del secolo scorso, durante lo svolgimento del Progetto Manhattan [6]. e prende il nome dalla nota cittadina francese famosa per il gioco d'azzardo, vista l'aleatorietà su cui è basato il suo procedimento. Lo scopo di questo algoritmo risiede nell'analisi di un generico sistema, le cui leggi non sono facilmente risolvibili in forma chiusa mediante i metodi tradizionali, e nella possibilità di compiere numerosi esperimenti virtuali. Con questo approccio è possibile indagare quei problemi in cui sono coinvolte numerose variabili, anche di natura aleatoria, testando con facilità l'effetto degli input del problema e il comportamento del sistema in seguito ad una loro variazione. Tale metodo risulta estremamente flessibile e ben si adatta ai più svariati ambiti di applicazione: finanza, metodi numerici, scienze comportamentali, fisica e numerosi altri contesti. La simulazione Monte Carlo trae il suo fondamento sulla generazione di numeri casuali e permette l'analisi del comportamento di quelle variabili su cui non si hanno sufficienti dati a disposizione per determinarne il carattere. Nel modello si ricorre a questo tipo di simulazione per ottenere una stima della distribuzione finale delle

[5]Non esiste un metodo univoco e standardizzato per la quantificazione dell'efficacia dei controlli. Ciascuna azienda fornitrice di servizi di sicurezza propone un proprio approccio, il quale è tipicamente basato su tre fattori cardini: raccolta di dati sperimentali, analisi e benchmarking delle prestazioni, verifica della conformità alle normative.

[6]Il progetto Manhattan fu l'insieme di una fitta rete di attività di ricerca e sviluppo volto allo studio e alla realizzazione della bomba atomica, al quale parteciparono i migliori scienziati dell'epoca, per volere degli Stati Uniti d'America

perdite generate dal rischio in questione. Di seguito si riporta la porzione di codice utilizzata:

```
n_scenari = 100000; %numero di simulazioni effettuate

res = zeros(n_scenari,1);

for k = 1:n_scenari

   if    rand < prob_media %verifica se evento è accaduto

       sim_loss = logninv(rand, mu, std_dev); %perdita simulata se
   evento

   else

       sim_loss = 0; %perdita simulata altrimenti

   end

  res(k) = sim_loss; %per ogni scenario restituisce la perdita

end
```

Il punto di partenza per la simulazione consiste nell'estrazione di un numero casuale[7]da una distribuzione uniforme[8]. Tale numero può essere interpretato come un indicatore che segnala se l'evento si sia verificato o meno. Immaginando un segmento di lunghezza unitaria, è possibile individuare su di esso una "banda di accadimento" i cui estremi sono l'origine del segmento (lo zero) a sinistra e la probabilità media dell'evento calcolata in precedenza a destra; se il numero casuale risulta appartenente a tale zona, allora l'evento si è verificato, diversamente no. In seguito, un secondo numero casuale uniforme viene estratto per stabilire in che modo l'evento abbia impattato, ovvero la magnitudine delle perdite che esso ha generato, distribuite secondo una lognormale con media e deviazione standard calcolate in precedenza. Tale procedimento viene ripetuto per il numero di scenari indicati al codice come dato di input: lo scopo è quello di verificare più casi possibili in modo che tutte o quasi le combinazioni possano effettivamente verificarsi.[9]

[7]Sarebbe più opportuno utilizzare l'espressione "pseudocasuali" in quanto i software di analisi numerica come MATLAB utilizzano specifici algoritmi deterministici per estrarre un numero da una certa distribuzione specificata. Essi non derivano da un processo puramente casuale, ma possono essere considerati tali a seguito di appositi test statistici sulla loro distribuzione e correlazione

[8]Una variabile casuale estratta da questo tipo di distribuzione ha la medesima probabilità di estrazione di tutte le altre, come, ad esempio, l'uscita di un certo esito in seguito al lancio di un dado bilanciato.

[9]All'aumentare del numero di scenari generati le variabili tendono ad oscillare attorno al valore

Tabella 4.6: Risultati della simulazione Monte Carlo per 100.000 scenari nel caso di implementazione e non dei controlli

$Scenario$	$Perdita_{sim}$	$Perdita\,residua_{sim}$
1	–	–
2	–	18.222.397,7785
3	–	–
4	5.194.690,7926	–
5	–	–
6	24.092.827,8906	–
7	–	–
8	–	–
9	–	–
10	–	76.323.743,2106
...	...	...
10.000	52.016.229,8980	22.891.349,8588
...	...	...
25.000	–	–
...	...	...
50.000	27.451.975,1674	–
...	...	...
75.000	61.168.739,5113	–
...	...	...
100.000	72.633.549,1501	–

Visto il valore contenuto della probabilità di accadimento del rischio, gran parte degli scenari restituiscono valore nullo per le perdite, in quanto in esse la minaccia non si è verificata: nello specifico, per la simulazione riportata, si è manifestata 4340 volte per il caso senza controlli e 2875 per quello con i controlli implementati (su 100.000 casi verificati). Alla luce di questo fatto, nell'istogramma di seguito si sono escluse le perdite nulle poiché comprometterebbero di fatto l'aspetto della figura, rendendo pressoché invisibili le frequenze più piccole.

medio con movimenti via via sempre meno percettibili, motivo per cui non si è soliti generare un numero troppo elevato di simulazioni, risparmiando capacità computazionale.

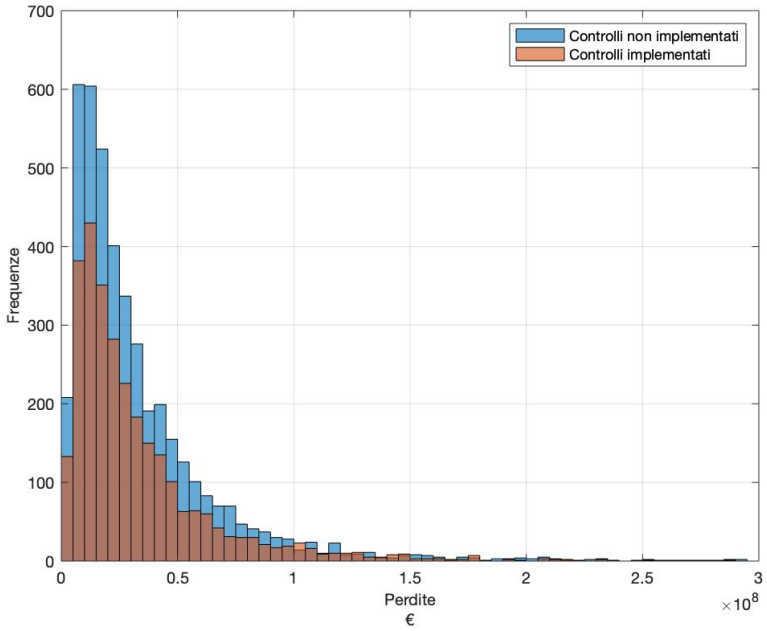

Figura 4.5: Istogramma delle perdite con e senza controlli implementati

Come si evince dalla figura precedente, l'effetto dei controlli prende forma diminuendo sensibilmente le perdite in tutte (o quasi) le classi considerate. Si noti anche come, coerentemente con le ipotesi di partenza, la maggior parte delle perdite si concentra verso valori intermedi ma sono comunque presenti alcune osservazioni in valori decisamente più alti. Come detto in precedenza, lo scopo della simulazione risiede nell'ottenere una stima della distribuzione finale delle perdite: a tal scopo si è creato un fit basato su una distribuzione lognormale, in modo da ottenerne i parametri fondamentali.

Tabella 4.7: Riepilogo dei parametri ottenuti dal fit - caso senza controlli

$Media$	$Varianza$	μ_{est}	σ_{est}
$3{,}4475e+07$	$1{,}5899e+15$	16,9312	0,9215

Tabella 4.8: Riepilogo dei parametri ottenuti dal fit - caso con controlli

$Media$	$Varianza$	μ_{est}	σ_{est}
$3{,}4389e+07$	$1{,}4851e+15$	16,9465	0,9019

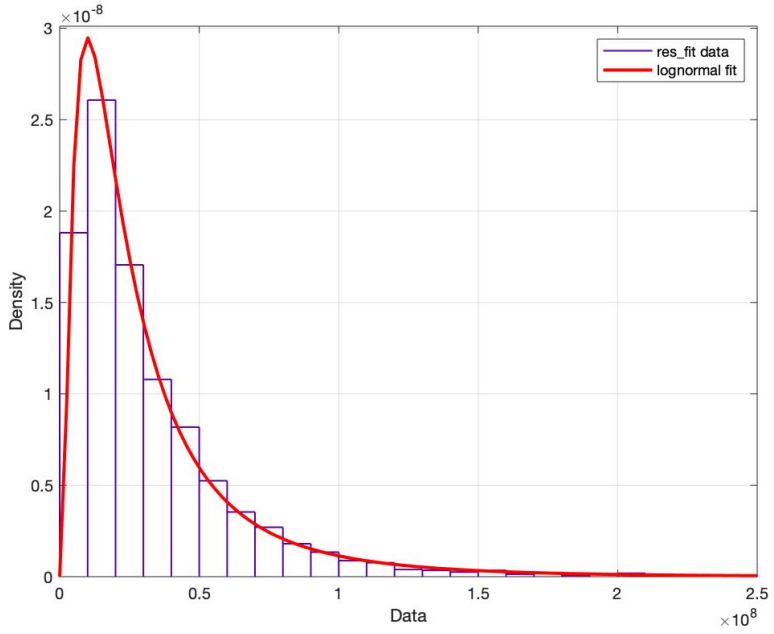

Figura 4.6: Istogramma delle perdite e curva di fit per controlli non implementati

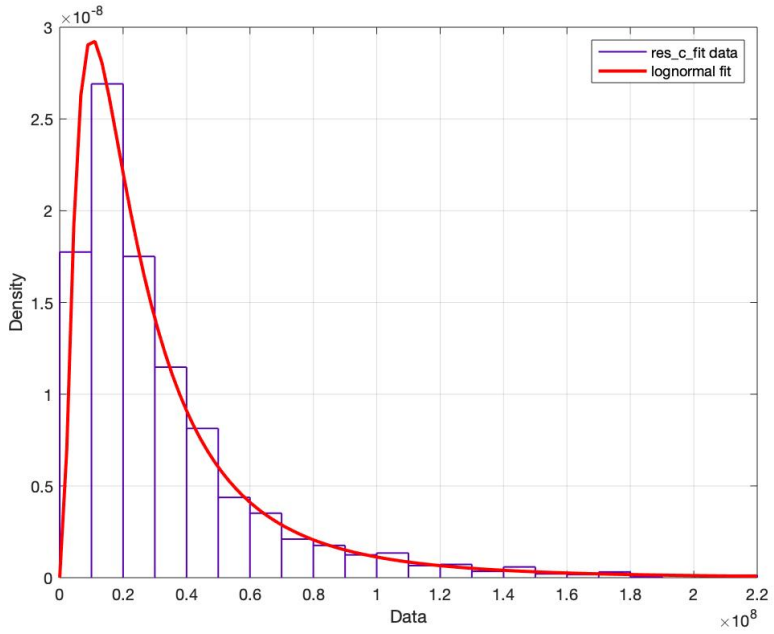

Figura 4.7: Istogramma delle perdite e curva di fit per controlli implementati

4.5 Dalla matrice alle curve di rischio

Nell'ambito del risk management si fa largamente utilizzo della matrice di rischio (detta anche "heat map"), ovvero uno strumento in due o tre dimensioni nel quale dispongono sulle coordinate probabilità, impatto e altre variabili in maniera arbitraria, rappresentandole su una di una scala ordinale[10] qualitativa da uno a tre (o cinque) livelli, in ordine di severità. In ciascuna porzione dello spazio si individuano poi dei punti, ognuno corrispondente ad un singolo rischio e caratterizzato da un livello (alto, medio o basso) di criticità. Nell'ambito della cybersecurity i vari framework e standard internazionali incentivano e promuovono l'utilizzo della matrice come parte integrante del risk assesment.

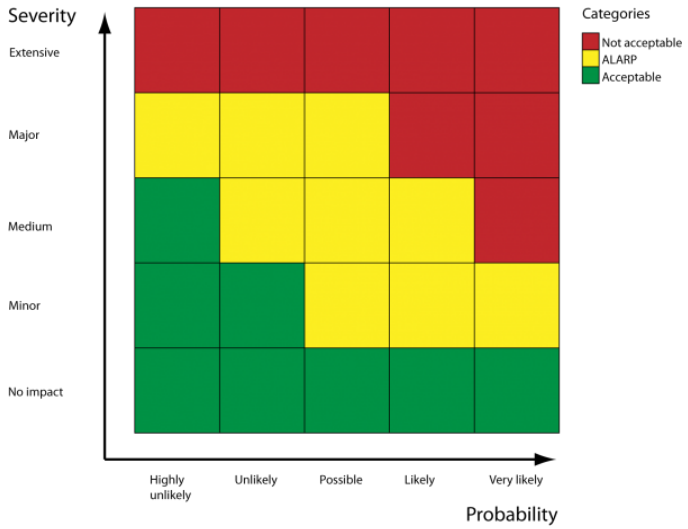

Figura 4.8: Una tipica matrice di rischio o heat map (fonte: [59])

I trend globali con cui gli attacchi informatici stanno evolvendo e raggiungendo i target più disparati, dalle infrastrutture critiche, portali universitari, compagnie telefoniche ecc. rendono necessaria l'adozione di metodi e strumenti maggiormente evoluti:

1. Non vi è, infatti, alcuna evidenza che i metodi qualitativi migliorino la capacità di giudizio e l'attività decisionale di risposta al rischio, bensì essi aumentano la possibilità di compiere degli errori per via della loro soggettività e per le disperse interpretazioni associate a concetti verbali come "molto probabile",

[10]Nella teoria delle scale di misura, si definisce ordinale quella scala che ha come operazione empirica la determinazione di non equivalenza, ha come permutazione ammissibile la permutazione ed utilizza come misura di posizione e dispersione la mediana e i frattili.

"mediamente probabile" o "molto improbabile" da parte di ciascun soggetto. [11]

2. Secondo un altro studio, nel momento in cui si assegnano varie forme di scale ordinali riferendosi a valori definiti nel continuo (come, appunto, probabilità e impatto), è possibile si verifichi quello che gli autori definiscono il fenomeno della "range compression", ovvero un errore di approssimazione che porta a considerare due differenti rischi, ciascuno con diverse ascisse e ordinate, appartenenti alla stessa zona o addirittura alla stessa cella di severità all'interno della matrice [61]. Questo è, ovviamente, una pratica da evitare perché porterebbe a considerare critiche alcune minacce che in realtà non lo sono, e, viceversa, a non dare il giusto peso verso altre degne di maggiore attenzione.

3. Tra il 2008 ed il 2009, Hubbard Research ha compiuto un'indagine su cinque differenti organizzazioni operanti nel settore della cybersecurity riguardo all'utilizzo delle matrici di rischio. Nello specifico, sono state raccolte più di duemila risposte riguardanti score assegnati da ciascun individuo ad alcuni rischi e si è potuto osservare che il 76% delle risposte si concentrava nella zona medio-alta della matrice, ovvero quella racchiusa dai valori "tre" e "quattro" su di una scala da uno a cinque [62]. In altre parole, si è verificato un ulteriore clustering dei rischi, aumentando di fatto l'errore di approssimazione, già insito di natura in una matrice.

4. Anche il design della matrice stessa, inteso come il principio logico con cui essa comunica è stato oggetto di approfondimenti. In uno studio del 2014 si mostra come, invertendo i valori tipicamente associati al ranking (quindi cinque per bassi valori di probabilità e impatto e viceversa) e moltiplicando i valori delle coordinate, non necessariamente si mantiene l'ordinamento degli score, conducendo a errori interpretativi e mostrando come la scelta arbitraria di una matrice piuttosto che l'altra possa essere determinante nella categorizzazione dei rischi. Sempre nello stesso articolo, è stata posta l'attenzione su di parametro, tipico di ogni strumento, detto "Lie Factor": esso indica sostanzialmente in che modo l'informazione all'interno di un grafico risulti distorta. Per le matrici di rischio, il valore ottenuto dagli autori è risultato maggiore di cento. Se si pensa che ad una "menzogna" sia associato tipicamente un valore di circa quindici, è intuitivo come la matrice di rischio presenti, se non altro, delle controversie nel suo utilizzo incondizionato [63].

[11] Ci si riferisce ad una ricerca dello psicologo David Budescu condotta su 223 studenti dell'Università dell'Illinois, ai quali è stato richiesto di associare una probabilità soggettiva a diverse categorie qualitative, da "molto probabile" o "estremamente improbabile". I risultati mostrano che le associazioni sono del tutto disperse: ad esempio per la categoria "molto probabile" è stato indicato un range che va dal 43% al 99%, per "estremamente improbabile" l'intervallo è compreso tra l'8% e il 66%, per "probabile" 45%-84% e per "molto improbabile" 3%-75% [60].

Alla luce di queste considerazioni, è quindi possibile affermare che un approccio quantitativo e più oggettivo sia quantomeno consigliabile nell'ambito della sicurezza informatica, applicando al Cyber Risk Management i medesimi strumenti già largamente utilizzati negli ambiti più tradizionali della gestione del rischio. Secondo uno studio condotto su alcune imprese del settore petrolifero, è emersa una relazione piuttosto significativa tra performance economica e utilizzo di metodi quantitativi, come la simulazione Monte Carlo descritta in precedenza [64]. L'utilizzo di strumenti di self-assesment soggettivi, come la matrice, non deve comunque essere del tutto abbandonato ma può essere conservato come mezzo di partenza per un'analisi preliminare, o a livello comunicativo. Ad esempio, la NASA fa tutt'ora utilizzo di simulazioni storiche, in aggiunta a metodi qualitativi basati su considerazioni soggettive per la gestione dei propri rischi [65].

A questo punto, analizzate le principali criticità dovute all'utilizzo di metodi puramente soggettivi per la quantificazione del rischio, è possibile introdurre un nuovo strumento, interpretabile come una naturale evoluzione della classica matrice: le *curve di rischio*. Esse collegano probabilità (sull'asse verticale) e impatto (sull'asse orizzontale, qui rappresentato con il logaritmo in base dieci) in termini monetari, ponendo il focus sulla possibilità di osservare una perdita di una certa entità nella propria organizzazione, una volta verificatosi il rischio in questione. Sostanzialmente, le curve di rischio permettono di rispondere alla seguente domanda:

> «Nell'ipotesi che la minaccia si manifesti, con quale probabilità è possibile osservare una perdita maggiore o uguale a quella che si vuole verificare?»

Analizzando il grafico in figura 4.9 è possibile individuare tre differenti curve:

1. La *curva dei rischi*, ovvero la probabilità che il rischio provochi un certo impatto senza che si implementino i controlli.

2. La *curva dei rischi residui*, che indica la perdita potenziale ne caso in cui si attuino le contromisure necessarie alla mitigazione del rischio.

3. La *curva del rischio tollerato*, ovvero un insieme di punti soggettivamente stabiliti che rappresenta la propensione ad accettare o meno, con una certa probabilità, una data perdita. Essa divide il piano in due regioni: la prima, detta "zona di tolleranza" indica quei valori di probabilità e impatto che si ritngono accettabili, mentre la seconda evidenzia una zona di allerta in cui la possibilità che il rischio generi una data perdita sia inaccettabile.

Le curve di rischio sono anche note in letteratura con la sigla LEC (Loss Exceedance Curves) e rappresentano un valido metodo per rappresentare quantitativamente probabilità contro impatto. Come si evince dalla figura 4.9, la curva dei rischi residui è, per ogni valore delle ascisse, sovrastata da quella tratteggiata

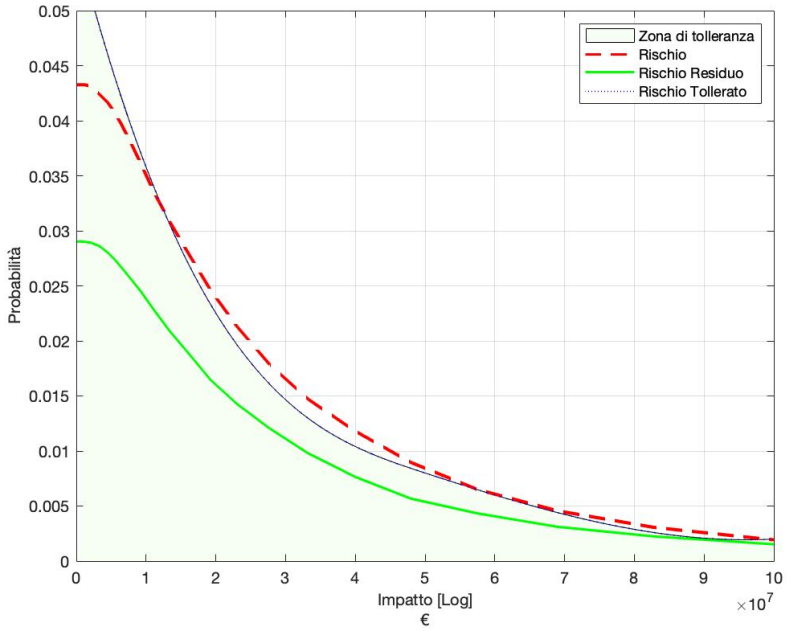

Figura 4.9: Curve di rischio per la minaccia "Data breach"

dei rischi, coerentemente con l'adozione dei controlli che contribuisce di fatto ad abbattere la probabilità di accadimento di un certo evento rischioso. Inoltre, è possibile osservare come, per tutti i valori delle ascisse, la curva di rischio residuo sia sovrastata dalla curva di tolleranza, mentre quella dei rischi "lordi" violi la soglia per i valori iniziali della scala: in questo caso è possibile affermare che la curva blu "domina stocasticamente" quella verde. Al fine di costruire una soglia di tolleranza, è necessario rispondere alla seguente domanda:

> «Con quale probabilità accetto di subire una perdita di importo maggiore o uguale, in riferimento all'orizzonte temporale di un anno?»

Tabella 4.9: Probabilità e perdite utilizzate per la costruzione della curva di tolleranza

Perdita	500.000	5.000.000	50.000.000	60.000.000	100.000.000
Prob. toll. [%]	5,5	4,5	0,7	0,5	0,3

Non sono necessari molti punti per ottenere la curva definitiva. Nell'esempio in figura il software utilizza come dati di input cinque coppie di probabilità e impatto

ritenute sensibili dall'organizzazione, e procede all'interpolazione mediante la funzione spline[12], ma è possibile utilizzare anche l'interpolazione lineare, che conduce una semplice una linea spezzata per i punti indicati. Nel modello è stato anche implementato un calcolatore di probabilità data una certa perdita richiesta, in modo da poter dare una risposta puntuale nel caso in cui si voglia porre il focus su un particolare ammontare di impatto. Di seguito si riportano alcuni risultati significativi ottenuti:

Tabella 4.10: Alcuni output di probabilità in base all'impatto richiesto

Perdita	1.000.000	3.000.000	5.000.000	10.000.000	50.000.000
Prob. toll. [%]	2,93	2,857	2,708	2,306	0,551

4.6 Calcolo del VaR, Expected Shortfall ed una considerazione sui controlli

Dai risultati della simulazione Monte Carlo è possibile calcolare alcuni indicatori fondamentali di rischio come il Value at Risk e l'Expected Shortfall, permettendo alla propria organizzazione di ottenere degli indicatori di rischio globale in termini monetari (per le definizioni di questi due concetti si rimanda al capitolo 3). Nel modello si fa utilizzo del VaR non parametrico, dal momento che i dati necessari al calcolo sono risultato di una simulazione. Il punto di partenza risiede nel calcolare l'Expected Loss (o perdita attesa) secondo la seguente formula:

$$Expected\,Loss = \frac{\sum_{i=1}^{n.\,simulazioni} Perdita\,simulata_i}{n.\,simulazioni} \tag{4.21}$$

Nel caso in esame il numero di simulazioni viene dato come input al modello ed è stato posto a pari a 100.000 iterazioni. A questo punto è possibile calcolare il Value at Risk come:

$$VaR = Expected\,Loss - Perdita_{\alpha-esimo\,quantile} \tag{4.22}$$

[12]L'interpolazione spline è una tecnica largamente usata nell'analisi numerica. Essa si basa sull'utilizzo delle funzioni spline, le quali suddividono l'intervallo considerato in molteplici sottointervalli e generano, per ciascuno di essi, un polinomio di grado variabile (solitamente piccolo). L'interpolazione lineare utilizza polinomi del primo grado, per cui è considerabile come un caso particolare di quella mediante spline.

La perdita all'α-esimo quantile corrisponde al quantile delle perdite ottenute dalla simulazione riferita al livello di confidenza desiderato (in questo caso 99%). A questo punto si procede quindi nel calcolare l'Expected Shortfall come la media delle perdite superiori al VaR:

$$Expected\,Shortfall = E[Perdite|Perdite > VaR] \tag{4.23}$$

Come detto in precedenza, l'ES è una misura molto importante di rischio, poiché prende in considerazione quelle perdite che superano un valore fondamentale, ovvero il VaR. Nella tabella di seguito si riportano i risultati ottenuti dal modello per il rischio "Data Breach".

Tabella 4.11: Principali indicatori di rischio - controlli non implementati

$Expected\,Loss$	$Value\,at\,Risk$	$Expected\,Shortfall$
1.539.490,4609	42.978.137,2315	84.776.626,2597

Tabella 4.12: Principali indicatori di rischio - controlli implementati

$Expected\,Loss$	$Value\,at\,Risk$	$Expected\,Shortfall$
980.763,0492	29.607.117,8640	85.691.228,4025

Lo scopo di questo modello risiede nel poter dare a chi lo utilizza un supporto ad alcune decisioni di carattere operativo. Una di questa riguarda certamente l'allocazione delle risorse destinate all'implementazione dei controlli, o, più semplicemente, a quanto si deve spendere per ottenere un certo impatto sulle perdite ottenibili. A tal proposito è stato implementato un semplice indicatore chiamato Return On Control, la cui formulazione è la seguente:

$$Return\,On\,Control = \frac{Expected\,Loss - Expected\,Loss_c}{Costo\,del\,controllo} - 1 \tag{4.24}$$

L'indicatore restituisce sinteticamente la diminuzione percentuale delle perdite attese prima e dopo aver implementato i controlli, ottenute in seguito alla simulazione Monte Carlo.

Tabella 4.13: Indicatore ROC per il rischio "Data Breach"

$Costo\,dei\,controlli$	$Return\,on\,Control$
400.000,00	0,3082

4.7 Analisi quantitativa di molteplici cyber rischi aggregati

Nel modulo IT Risk® l'azienda mette a disposizione dei propri clienti uno strumento per la gestione di molteplici rischi informatici. Il risultato finale è un profilo di rischio, ovvero un "portafoglio rischi" che include all'interno differenti minacce, riferiti ad un certo asset e con i controlli ad esso associati. Con il seguente modello il cliente può compiere una ulteriore analisi supportata da metodi quantitativi per quei rischi che ritiene meritevoli di approfondimento, oppure considerandoli nella loro totalità per avere una panoramica globale, oppure ancora analizzandoli singolarmente e confrontando i risultati finali. In ogni caso, il modello è stato progettato per contenere virtualmente un numero infinito di rischi, pur considerando i dovuti limiti computazionali. Nei successivi paragrafi sono puntualmente descritti i procedimenti utilizzati, i dati di input e i principali risultati ottenuti. Per i calcoli descritti sono stati considerati quattro diversi cyber rischi, sotto l'ipotesi di correlazione nulla tra di essi, per ottenere un primo esempio sul corretto funzionamento del modello.

4.7.1 Calcolo delle probabilità di accadimento e delle distribuzioni delle perdite

Analogamente al caso in cui si è considerato un singolo rischio, per il calcolo della probabilità media di accadimento si ricorre all'utilizzo della distribuzione Beta con l'approccio "hits & misses" descritto in precedenza. Di seguito si riportano i dati di input e output restituiti dal modello.

Tabella 4.14: Panoramica sui principali dati per il calcolo della probabilità riguardo ai rischi considerati

Rischio	y_s	y_e	n_c	*Succ.*	p_α	p_β	α	β	*Prob. med.*
Data breach	2019	2020	4209	185	1	1	186	4025	4,4170%
Denial of service	2019	2020	2530	157	1	1	158	2374	6,2401%
Abuse of personaldata	2019	2020	1454	67	1	1	68	1388	4,6703%
Loss of sensitive information	2019	2020	2367	253	1	1	254	2115	10,7218%

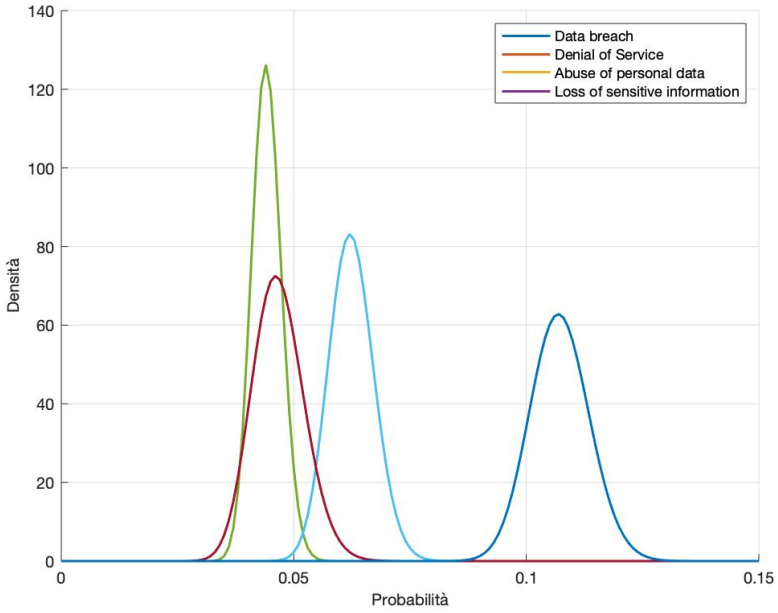

Figura 4.10: Distribuzioni di probabilità per i quattro rischi considerati

Anche per il calcolo della distribuzione delle perdite si seguono i medesimi step del caso con singolo rischio, indicando per ciascuno di essi l'intervallo di perdite che si ritiene possa ricoprire il 90% dei casi. Si osservi che, nonostante i risultati del modello siano sempre in riferimento all'orizzonte temporale di un anno, si possono utilizzare, per il calcolo della probabilità, osservazioni appartenenti a serie storiche non necessariamente riferite all'ultimo anno trascorso: l'effetto dell'ampiezza di questo intervallo è comunque preso in considerazione, come si osserva dall'equazione (4.12).

Tabella 4.15: Dati per la costruzione delle distribuzioni delle perdite

Rischio	*Limite inf.*	*Limite sup.*	μ	σ
Data breach	5.000.000	100.000.000	16,9288	0,9106
Denial of service	2.000.000	50.000.000	16,1181	0,9785
Abuse of personaldata	1.500.000	30.000.000	15,7188	0,9348
Loss of sensitive information	5.000.000	30.000.000	16,3208	0,5447

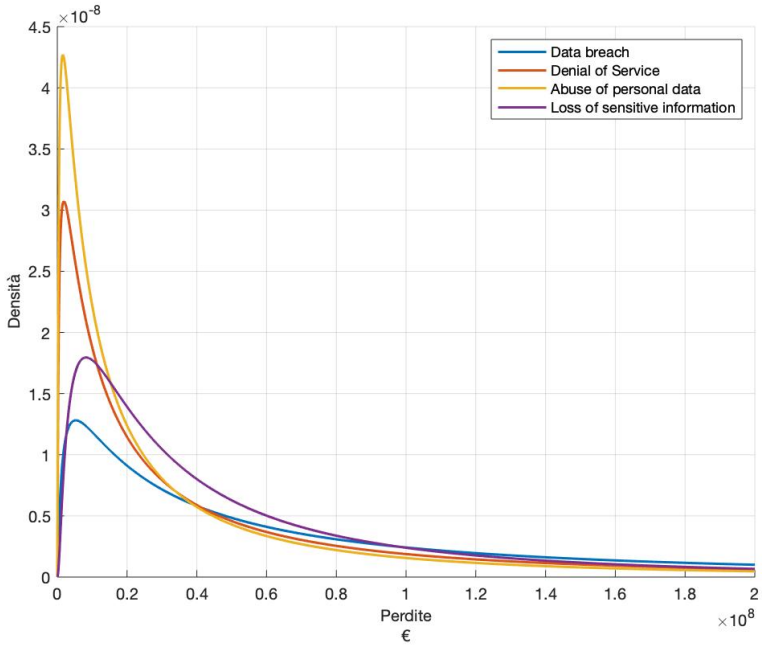

Figura 4.11: Distribuzioni lognormali stimate dagli intervalli di partenza

A questo punto è possibile calcolare con le equazioni (4.19) e (4.20) le perdite, nel caso in cui non si considerino i controlli e quelle residue, qualora si effettuino tali azioni, al fine della mitigazione dei rischi. Di seguito si riportano i risultati calcolati dal modello.

Tabella 4.16: Valori attesi delle perdite (senza controlli) e delle perdite residue (con controlli)

Rischio	C_e	*Perdita*	*Perdita residua*
Data breach	0,35	1.487.817,4457	967.081,3397
Denial of service	0,25	1.007.141,2923	755.355,9692
Abuse of personaldata	0,30	474.269,9808	331.988,9866
Loss of sensitive information	0,10	1.523.109,3964	1.370.798,4567

4.7.2 Simulazione Monte Carlo, calcolo di VaR, ES e curve di rischio

Una volta ottenuti i valori attesi delle perdite è possibile procedere alla simulazione Monte Carlo, in cui si sono generati 100.000 differenti scenari di rischio, dove per ciascuno di questi può essere che si sia verificato uno, nessuno, alcuni o tutti i

fenomeni considerati. La logica utilizzata è la medesima per il caso precedente, con la differenza che per ciascun scenario si ottiene come output il complessivo delle perdite simulate causate da ciascun rischio, nel caso in cui questi si siano verificati. Di seguito si riporta la porzione di codice utilizzata per tali iterazioni, nel caso in cui non si effettuino i controlli (i codici completi sono visibili in appendice).

```
r1 = rand(1,n_rischi); %vettore casuali uniformi

res = zeros(n_scenari,1);  %vettore perdite simulate agg.

p_sim = zeros(n_rischi,1); %vettore perdite simulate singole

for i = 1:n_scenari

    for j = 1:n_rischi

     if rand < prob_m(j)

      p_sim(j) = logninv(rand, mu(j), std_dev(j));

     else

      p_sim(j) = 0;

     end

    end

   res(i) = sum(p_sim(j));

end
```

Il modello genera per ogni iterazione (quindi per ogni scenario Monte Carlo) un vettore contenente numeri casuali uniformemente distribuiti (tutti diversi tra loro), che hanno la funzione logica di indicare se il rischio si sia verificato o meno, secondo il meccanismo illustrato nel caso precedente. Se la minaccia si è verificata, il codice calcola la perdita simulata, utilizzando un secondo numero casuale uniforme come argomento della funzione lognormale inversa, in quanto non si conosce la probabilità corrispondente; in caso contrario la perdita simulata si pone uguale a zero; questo passaggio è verificato per tutti i rischi inseriti come input. Al termine di questo step, si aggregano le singole perdite simulate provenienti dai rispettivi rischi e si procede allo scenario successivo. Di seguito si riportano alcuni scenari di output dei vettori `res` e `res_c` (contenente i risultati per il caso con i controlli implementati), dove sono riportate le perdite aggregate calcolate dalla simulazione.

Tabella 4.17: Risultati della simulazione Monte Carlo per 100.000 scenari nel caso di implementazione e non dei controlli per rischi aggregati

$Scenario$	$Perdita_{sim}$	$Perdita\,residua_{sim}$
1	10.326.188,6104	–
2	–	58.542.184,6385
3	160.957.804,3259	1.895.332,6732
4	9.638.239,8223	–
5	–	–
6	–	19.950.574,7164
7	–	36.725.617,2488
8	125.262.214,2454	19.950.574,7164
9	–	–
10	–	–
...	...	...
10.000	5.047.397,8987	250.640.086,6474
...	...	...
25.000	29.507.060,0216	–
...	...	...
50.000	19.439.554,0871	–
...	...	...
75.000	27.278.181,4190	555.930.586,7601
...	...	...
100.000	–	–

Intuitivamente, anche nel caso in cui si consideri l'effetto congiunto di più rischi, è possibile notare come l'effetto dei controlli abbatta significativamente il numero di occorrenze per tutte, o quasi, le classi delle perdite. Poiché si stanno considerando più eventi contemporaneamente, è lecito aspettarsi che il numero di scenari, in cui il totale delle perdite è nullo, sia maggiore rispetto al caso precedente: nello specifico, per questa simulazione, 10.732 scenari su 100.000 riportano un valore diverso da zero per il caso senza controlli implementati, mentre sono 9.450 su 100.000 quando si considerano i controlli (questi numeri sono da intendersi aventi valenza puramente esplicativa e rappresentano l'esito di un "lancio" del codice: è possibile, infatti, che i risultati ottenuti siano diversi, nonostante non dovrebbero differenziarsi molto man mano che si procede con successive verifiche). Anche in questo caso è stato costruito un fit di tipo lognormale per entrambi gli istogrammi, nei quali non sono state considerati gli scenari che hanno registrato una perdita nulla, per le ragioni descritte in precedenza Grazie al software è stato possibile ricavare i parametri caratteristici delle due distribuzioni finali ottenute in seguito alla simulazione Monte Carlo:

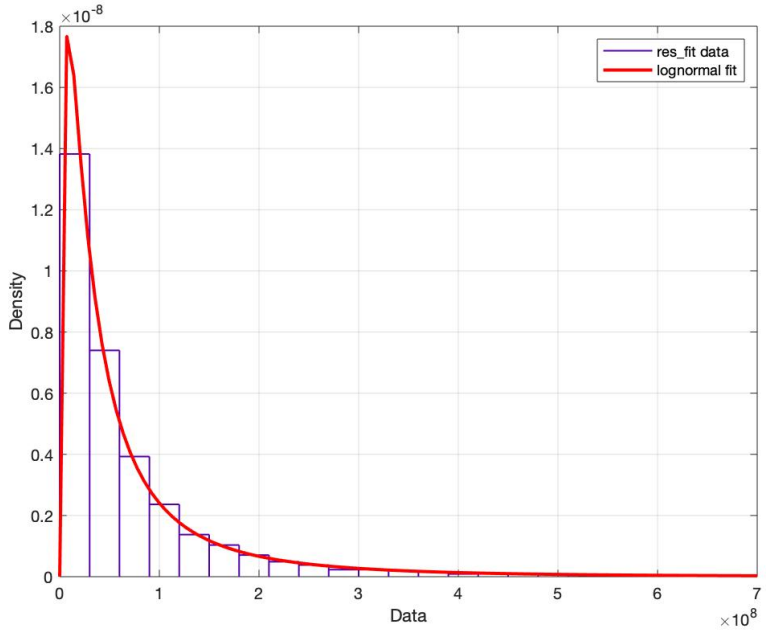

Figura 4.12: Istogramma delle perdite e curva di fit per controlli non implementati e rischi aggregati

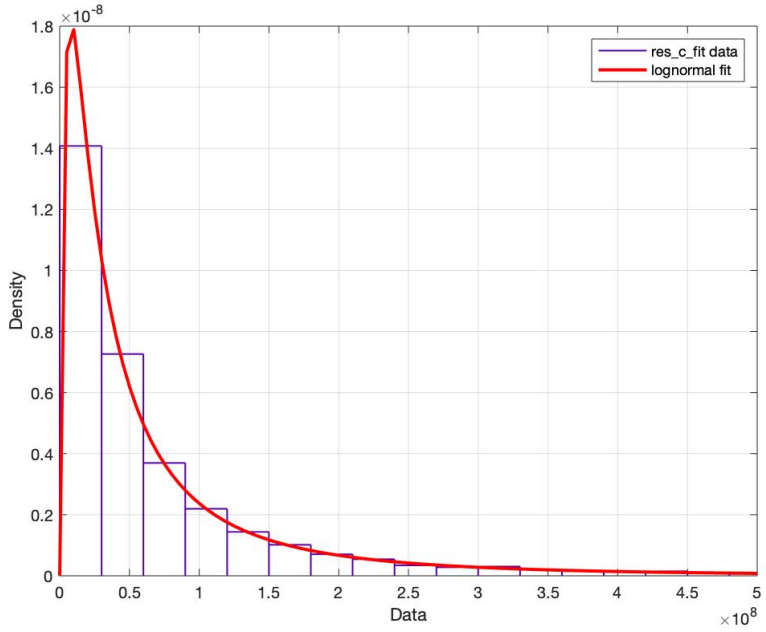

Figura 4.13: Istogramma delle perdite e curva di fit per controlli implementati e rischi aggregati

Tabella 4.18: Riepilogo dei parametri ottenuti dal fit per rischi aggregati - controlli non implementati e implementati

Classe	*Media*	*Varianza*	μ_{est}	σ_{est}
Controlli non impl.	$8{,}3851e+07$	$2{,}6604e+16$	17,4619	1,2511
Controlli impl.	$8{,}2605e+07$	$2{,}4738e+16$	17,4638	1,2357

Osservando i dati nella tabella sopra, è possibile notare (intuitivamente) come, tra le due classi di eventi, il secondo caso in cui si considerano i controlli abbia un valore della media e della varianza significativamente inferiore, indicando, ancora una volta, il ruolo essenziale che i controlli svolgono all'interno della gestione dei cyber rischi. Infine, una volta stimata la distribuzione finale delle perdite con il metodo Monte Carlo, è possibile procedere al calcolo delle curve di rischio: il metodo non differisce da quello illustrato nel caso di un singolo rischio, e anche qui si richiede di inserire come input alcuni valori di probabilità e impatto che si ritiene siano tollerabili all'interno della propria organizzazione. Analogamente al caso

Tabella 4.19: Valori per la costruzione della curva di tolleranza ai rischi

Perdita	1.000.000	5.000.000	10.000.000	50.000.000	60.000.000
Prob. toll. [%]	22	15	12	2	0,1

precedente, in cui si è considerato un singolo rischio, la curva rossa tratteggiata dei rischi "puri", ovvero senza che siano implementati i controlli, risulti dominare per ogni valore delle ascisse quella dei rischi residui, nonostante le due curve tendano a convergere verso valori estremi dell'impatto. Questo permette di fare una considerazione sull'efficacia dei controlli: si rivelano molto utili in termini di abbattimento della probabilità e delle perdite ordinari (coerentemente con quanto osservato nei risultati precedenti) ma il loro effetto si riduce, fino ad annullarsi, per quegli eventi imprevedibili che comportano effetti catastrofici. Questi sono, in linea teorica, i casi con verosimiglianza minima, ma comunque non nulla: al pari del verificarsi di una pandemia, non si possono escludere a priori eventi di questo genere e ciò deve indurre a non sottovalutare questa minaccia. Qualora si verificasse un evento con connotati sistemici, l'effetto dei controlli tradizionali tenderebbe a svanire, pertanto è necessario prendere coscienza di questa possibilità e migliorare la propria resilienza nei confronti di tali rischi.

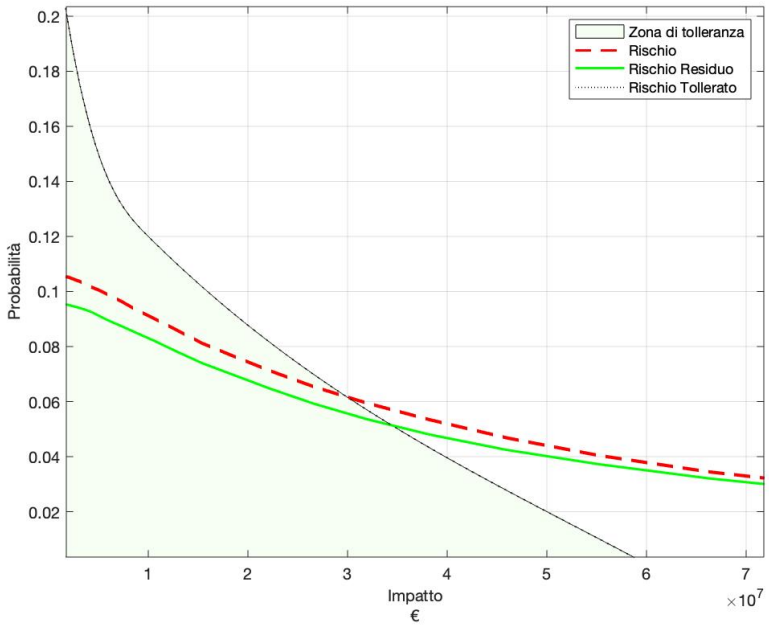

Figura 4.14: Curve di rischio nel caso di molteplici cyber rischi aggregati

A differenza del singolo caso "Data breach", qui non si osserva dominanza stocastica tra la curva dei rischi tollerati e quella dei rischi, poiché questa viola la zona di tolleranza a partire da valori intermedi delle ascisse. Per ottenere risultati che rientrino nella propria soglia di sicurezza, occorre o aumentare l'efficacia dei controlli, in modo da abbassare ulteriormente la curva dei rischi residui oppure rivedere le proprie soglie di accettazione del rischio. Nel modello è stato implementato anche il medesimo calcolatore che restituisce la probabilità di perdere un certo ammontare, inserito come output, in riferimento al vettore delle perdite residue ottenute dalla simulazione: nella tabella seguente sono riportati alcuni risultati notevoli. Tale strumento può essere utilizzato sia in ottica analitica, in quanto permette di ricevere un risultato immediato ricavato da criteri oggettivi, sia in ottica comparativa, ad esempio mettendo a confronto più portafogli rischi oppure confrontando tra loro singole minacce.

Tabella 4.20: Alcuni output del modello riguardo alle perdite benchmark

Perdita	1.000.000	3.000.000	5.000.000	10.000.000	50.000.000
Prob. toll. [%]	9,69	9,40	9,13	8,17	4,04

A partire dai risultati della simulazione, nei casi con e senza controlli, si possono ottenere i due indicatori sintetici di rischio noti come Value at Risk ed Expected Shortfall, già descritti in precedenza, utilizzando le equazioni descritte nel caso di un singolo rischio:

Tabella 4.21: Principali indicatori di rischio per rischi aggregati - controlli non implementati

Expected Loss	*Value at Risk*	*Expected Shortfall*
9.116.620,9889	190.516.161,5463	416.055.184,4784

Tabella 4.22: Principali indicatori di rischio per rischi aggregati - controlli implementati

Expected Loss	*Value at Risk*	*Expected Shortfall*
8.304.172,1644	178.722.526,2376	406.758.978,3398

Infine, anche in questo caso si può ottenere una panoramica sull'utilizzo dei controlli, mediante l'indicatore Return On Control, per ciascun rischio considerato. L'equazione utilizzata è la medesima illustrata in precedenza; di seguito si riportano i risultati ottenuti.

Tabella 4.23: Valori di ROC per i rischi considerati

Rischio	*Costo dei controlli*	*Return on Control*
Data breach	400.000	0,3082
Denial of service	200.000	0,2589
Abuse of personal data	130.000	0,9447
Loss of sensitive information	145.000	0,5042

Capitolo 5

Scomposizione dei rischi

Nei paragrafi precedenti è stato illustrato un metodo per ottenere una stima finale della distribuzione delle perdite generate da uno o più cyber rischi, dove si utilizzano come dati di input considerazioni soggettive riguardanti sia la probabilità che si verifichi l'evento, che l'impatto ad esso associato. Il modello restituisce come output diversi indicatori, che possono essere utilizzati come supporto nel momento in cui occorra avere una visione globale dei rischi della propria organizzazione. Questo rappresenta solamente il punto di partenza per l'analisi delle minacce informatiche e, al fine di ridurre l'incertezza associata al *come* un certo rischio possa manifestarsi, è possibile scomporre la magnitudine di ciascuno di essi, in modo da avere una visione più dettagliata riguardo sia alla tipologia di evento, sia al danno che può generare. Esistono svariati metodi di scomposizione: in questo modello si utilizza un *cost-driven approach*, ovvero ci si focalizza su differenti tipologie di costo che possono impattare all'interno della propria organizzazione, le quali verranno illustrati in seguito. L'utilizzo di questo focus sui rischi si basa sul concetto fondamentale che questi si verifichino sempre, a differenza di quello descritto in precedenza nei quali gli eventi possono manifestarsi o meno, questo per ragionare conservativamente e focalizzarsi sulle diverse modalità con cui possono verificarsi delle perdite.

5.1 Il criterio R.I.D. - Riservatezza, Integrità, Disponibilità

Nell'ambito della sicurezza informatica esistono tre concetti fondamentali su cui è bene concentrarsi per una corretta gestione del rischio, lungo tutto il ciclo di vita dei dati, dalla loro creazione fino al transito attraverso le vie di connessione:

1. *Riservatezza (o confidenzialità)*, ovvero garantire che i propri dati siano disponibili solamente per quei soggetti aventi diritto di accesso ed impedirlo

ad attori esterni non autorizzati. Una perdita di questo attributo può essere dovuta sia da agenti malevoli provenienti dall'esterno della propria organizzazione, i quali commettono un furto di credenziali oppure violano le misure di sicurezza adottate, sia da errori umani da parte di operatori interni, poiché non mettono in pratica le linee guida per la sicurezza delle autenticazioni o incappano semplicemente in errori accidentali. Questo tipo di evento può essere combattuto partendo dalla formazione del personale e dalla loro presa di coscienza sull'importanza di alcuni aspetti (come l'autenticazione a più fattori o l'utilizzo di password a brevi scadenze), passando all'inasprimento delle misure di sicurezza e dal rispetto delle norme di data governance.

2. *Integrità*, ovvero la veridicità e la conformità dei propri dati agli standard richiesti, senza che nessun'informazione sia in qualche modo alterata o eliminata da soggetti non autorizzati. Anche in questo caso può essere causata intenzionalmente da una minaccia esterna, oppure a causa di errori umani da parte di persone non autorizzate che apportano modifiche ai dati. La perdita di integrità dei dati può avvenire a differenti livelli, partendo dagli amministratori del software fino agli utenti finali, ed è tipicamente causata da una errata progettazione del sistema di sicurezza, ad un impiego non conforme alle policy di sicurezza oppure a vulnerabilità interne al software, che possono essere sfruttate da un agente esterno per scopi criminali. E' possibile ridurre la propria esposizione alla perdita di integrità implementando un controllo degli accessi più rigido, sistemi di rilevamento di intrusioni esterne, formazione del personale e riduzione degli accessi consentiti.

3. *Disponibilità*, ovvero quando le informazioni sono accessibili agli utenti autorizzati per il tempo stabilito dalle proprie norme, senza che ci siano interruzioni e garantendo una corretta erogazione del servizio in questione. Le cause di questo fenomeno possono essere le più svariate, come il malfunzionamento del software e la rottura degli asset hardware che veicolano i dati. Da menzionare anche il fatto che, talvolta, le cause possano provenire da fattori ambientali esterni o eventi catastrofici che causano interruzioni del servizio nelle infrastrutture a monte della propria, ad esempio impedendo l'apporto di energia elettrica. Infine, particolare rilievo assumono gli attori esterni che compiono attacchi mirati all'istituzione volti a rendere inaccessibile le informazioni (come i DoS). Anche in questo caso gioca un ruolo importante l'errore umano, che scaturisce nell'utilizzo non corretto degli asset fisici o la rimozione di dati non intenzionale. Dal punto di vista della prevenzione, si agisce tipicamente sul design delle proprie reti, rendendole adatte all'erogazione del servizio nel caso in cui si verifichino guasti o incidenti e limitando le vulnerabilità in esse presenti.

Nel modello è stata fatta l'assunzione che le perdite di riservatezza e integrità si verifichino congiuntamente, permettendo quindi di passare da tre possibili tipologie

di eventi a due. Alla base di questo ragionamento vi è il fatto che la disponibilità dei dati o di certe informazioni rende necessario conoscere alcune variabili oggettive tipiche di questo processo (ovvero di quando viene meno la disponibilità), rendendo di fatto la stima dell'impatto più complicata. Inoltre, si può, per semplicità, assumere che, nel caso di un'istituzione finanziaria, perdite di riservatezza e integrità siano complementari e possano essere modellate dal medesimo range di partenza. Il metodo utilizzato ha come obiettivo il computo della distribuzione finale delle perdite come conseguenza di un certo tipo di evento, in modo da poter offrire un focus su come impattino i differenti costi associati a ciascun evento. Analogamente al caso precedente si fa utilizzo del metodo Monte Carlo per verificare iterativamente 100.000 scenari di rischio differenti. La scomposizione in questione è stata applicata ai medesimi rischi utilizzati nel capitolo precedente, per verificare il loro effetto congiunto, questa volta secondo una visione più dettagliata; è comunque possibile applicare questo ragionamento ad un singolo rischio e confrontare i risultati con quelli ottenuti per un'altra minaccia.

5.1.1 Altre possibili scomposizioni

Al fine di ridurre l'incertezza relativa ad un rischio si possono utilizzare differenti approcci e quindi considerare numerose variabili. Ad esempio, un aspetto di rilevante importanza può essere la criticità di un certo processo informativo, data, ad esempio, dal numero di operatori che questo coinvolge, dall'importanza dei dati trasmessi e, in generale, dall'importanza in termini "finanziari" che questo ricopre (per una generica azienda si potrebbe parlare, ad esempio, di processi che implicano la vendita di beni o servizi). In un'ottica che predilige l'analisi dei costi associati ad un certo evento, è possibile anche considerare il numero di risorse (quindi il capitale) da impiegare nel momento in cui il rischio si sia verificato e occorra quindi investigare sulle cause ma soprattutto porvi rimedio: questo è tipico dei sistemi informativi, per i quali occorrono spesso più individui per la risoluzione del guasto. Sempre per quanto concerne i costi, possono assumere una notevole rilevanza l'incombenza di sanzioni pecuniarie nel caso in cui si verifichi un'anomalia all'interno dei processi sottoposti ad un certo regolamento legale. La scelta del criterio sul quale basare la scomposizione è del tutto arbitraria e va fatta considerando le proprie necessità ed il livello di dettaglio desiderato, avendo cura di non introdurre eccessive variabili che renderebbero il modello poco interpretabile dal personale.

5.2 Stima delle distribuzioni delle perdite

Il metodo utilizzato per la costruzione delle distribuzioni delle perdite è il medesimo già utilizzato nei due casi precedenti (quando sono stati considerati i rischi singolarmente oppure aggregati): si richiede di indicare un valore stimato dei limiti superiori e inferiori per ciascuna tipologia di evento, avendo cura di inserire

delle stime che coprano il 90% dei casi. Nei seguenti paragrafi saranno descritte le modalità con cui si è inteso modellare le differenti tipologie di eventi in questione e le assunzioni che stanno alla base di tali ragionamenti. Per continuità e facilità di interpretazione, si ipotizza che tutte le variabili associate all'impatto delle varie tipologie di rischio si distribuisca secondo una lognormale, poiché si ritiene che possa modellare abbastanza fedelmente tali variabili. Tuttavia, nulla vieterebbe di utilizzare funzioni differenti, per semplificare il modello, approfondirlo oppure per verificare la solidità dei risultati ottenuti. Anche in questo caso, dove non specificato, i dati riportati nelle tabelle sono espressi in euro.

5.2.1 Eventi di tipo R/I - danneggiamento della riservatezza e integrità dei processi

Come detto in precedenza, parlando di "riservatezza" delle informazioni ci si riferisce a un utilizzo improprio dei dati in esse contenuti, mentre per "integrità" si intende la modifica, intenzionale o no, delle informazioni o parte di esse. Il modello richiede come dati di input una stima soggettiva, oppure dati storici di settore (qualora fossero disponibili) per costruire l'intervallo di confidenza. Anche in questo caso, si utilizzano per il calcolo della media e deviazione standard le equazioni (4.17) e (4.18). Per i quattro rischi considerati si sono ottenuti i seguenti output:

Tabella 5.1: Valori di media e deviazione standard calcolati per eventi R/I

Rischio	*Limite inf.*	*Limite sup.*	μ	σ
Data breach	50.000	5.000.000	13,1223	1,3998
Denial of service	10.000	10.000.000	11,8595	1,1892
Abuse of personaldata	30.000	6.000.000	12,9581	1,6106
Loss of sensitive information	70.000	1.500.000	12.6886	0,9316

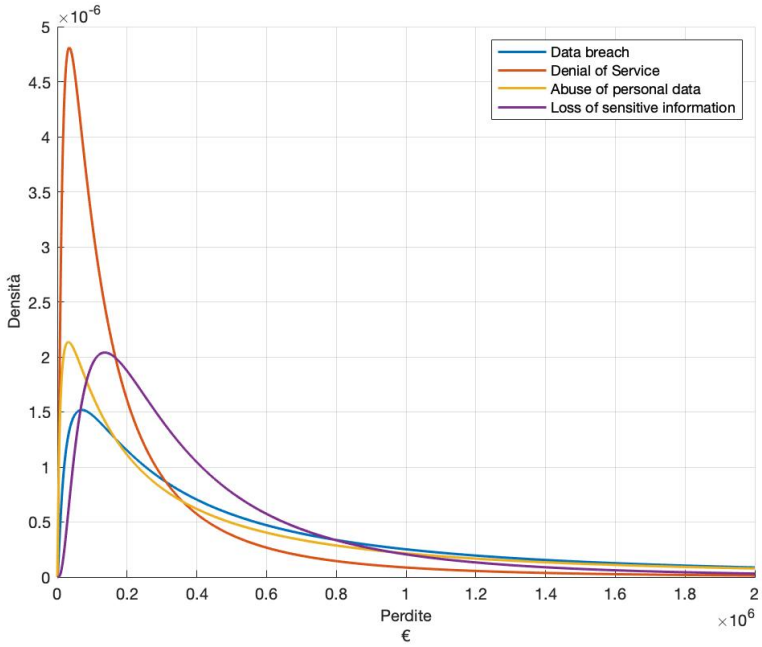

Figura 5.1: Funzioni di densità di probabilità per eventi R/I

5.2.2 Eventi di tipo D - danneggiamento della disponibilità dei processi

Come anticipato in precedenza, la perdita di disponibilità di un certo processo informativo è stata modellata facendo ricorso a due variabili, che descrivono sinteticamente il modo in cui questa tipologia di rischi impatta all'interno di una organizzazione:

- *Durata dell'interruzione*, ovvero l'intervallo temporale minimo e massimo che si ritiene possa rappresentare il 90% dei casi possibili.

- *Costo dell'interruzione*, ovvero l'ammontare orario del danno conseguito nel momento in cui non sia possibile erogare un servizio o accedere alle informazioni necessarie.

Per entrambe le variabili è stata fatta l'ipotesi che esse seguano una distribuzione lognormale: ambedue non possono assumere valori negativi ed è possibile, seppur poco probabile, che si possano raggiungere valori molto elevati di durata e costo. I dati riportati nel modello sono i seguenti, per i quali sono state utilizzate le equazioni (4.17) e (4.18):

Tabella 5.2: Valori di media e deviazione standard calcolati per la durata dell'interruzione (espressi in ore)

Rischio	*Limite inf.*	*Limite sup.*	μ	σ
Data breach	2	4	1,0397	0,2107
Denial of service	1	12	1,2424	0,7553
Abuse of personal data	1	3	0,5493	0.3339
Loss of sensitive information	4	9	1,0986	0,2465

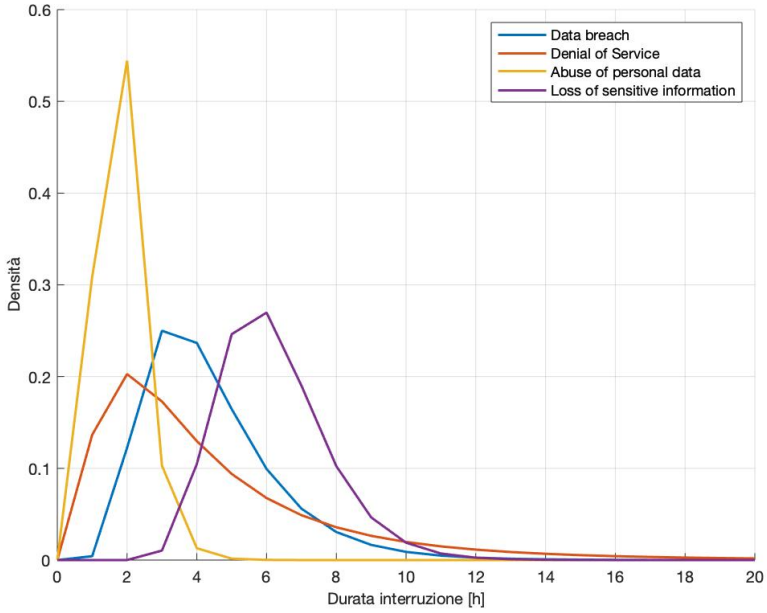

Figura 5.2: Funzioni di densità di probabilità per eventi D - durata dell'interruzione

Tabella 5.3: Valori di media e deviazione standard calcolati per il costo dell'interruzione

Rischio	*Limite inf.*	*Limite sup.*	μ	σ
Data breach	50.000	5.000.000	13,1223	1,3998
Denial of service	10.000	10.000.000	11,8594	1,1892
Abuse of personal data	30.000	6.000.000	12,9581	1,6106
Loss of sensitive information	70.000	1.500.000	12,6886	0,9316

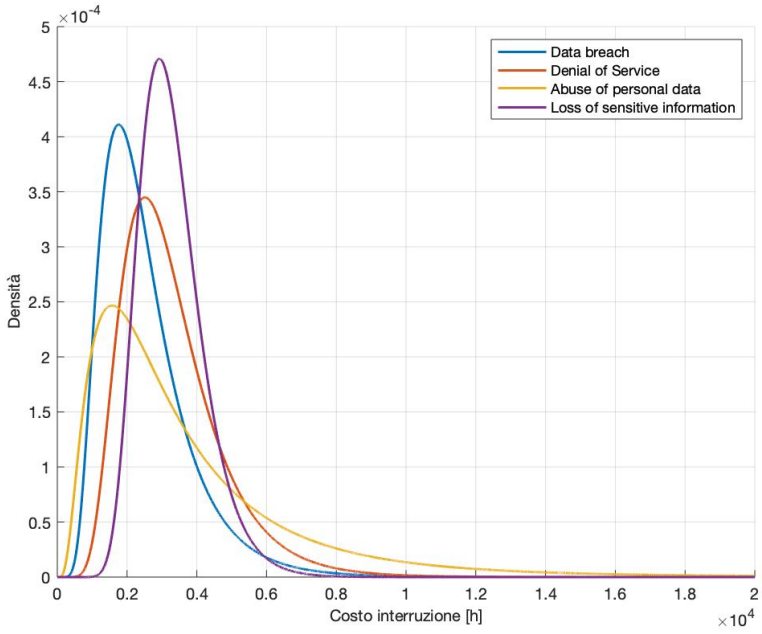

Figura 5.3: Funzioni di densità di probabilità per eventi D - costo dell'interruzione

5.3 Determinazione logica di accadimento singola e congiunta

Lo scopo di questo modello risiede nel trasmettere informazioni riguardo ad un singolo rischio, qualora esso si verifichi, spostando l'attenzione sulla tipologia del rischio e sull'impatto associato. Da una certa minaccia è possibile che si verifichi una perdita di disponibilità, un danneggiamento di riservatezza e integrità oppure entrambi: al fine di modellare questo comportamento, si associa per ogni rischio una probabilità soggettiva che si ritiene possa indicare il tasso di accadimento medio con cui un rischio impatti una o l'altra categoria. Più semplicemente, ci si pone la seguente domanda:

> «In che percentuale può, un certo rischio, riguardare la perdita di disponibilità oppure di riservatezza e integrità»

Siccome risulta pressoché impossibile stabilire con correttezza tali probabilità, poiché non vi sono metodi precisi o dati storici, si sono inseriti dei valori ritenuti essere ragionevoli e conservativi. Definite $q_{R/I}$ e q_D, rispettivamente, le probabilità che un evento sia del tipo R/I e del tipo D, si può calcolare la probabilità che sia di entrambe le tipologie con la seguente formula:

$$q_{BOTH} = 1 - (q_{R/I} + q_D) \tag{5.1}$$

Questi tre valori possono essere interpretati come tre soglie che individuano, su di un segmento unitario, tre bande di accadimento differenti, ciascuna per ogni categoria. Una volta che si sono definiti tali valori, si ricorre all'estrazione di alcuni numeri casuali uniformemente distribuiti per stabilire come l'evento si sia manifestato. Nel modello si sono generati due vettori binari, inizializzati a 0, le cui celle vengono aggiornate secondo i processi logici qui sotto riportati.

$$logic_{R/I} = \begin{cases} 1 & \text{se } rand < q_{R/I} \text{ o } rand > 1 - q_{BOTH} \\ 0 & \text{altrimenti} \end{cases} \tag{5.2}$$

$$logic_D = \begin{cases} 1 & \text{se } q_{R/I} < rand \wedge (q_{R/I} + q_D) > rand \parallel rand > (q_{R/I} + q_D) \vee rand > 1 - q_{BOTH} \\ 0 & \text{altrimenti} \end{cases} \tag{5.3}$$

Una volta compilati i vettori, è possibili stabilire la tipologia di impatto di ciascun rischio e calcolare quindi le perdite generate.

5.4 Calcolo dei valori attesi e simulati delle perdite scomposte con il metodo Monte Carlo

Secondo le ipotesi di partenza, si assume che entrambe le tipologie di impatto seguano una distribuzione lognormale, per cui è possibile calcolare il valore atteso di tali perdite con le equazioni seguenti:

$$Perdita\,attesa_{R/I} = [e^{\mu_{R/I} + \frac{\sigma^2_{R/I}}{2}}](q_{R/I} + q_D) \tag{5.4}$$

$$Perdita\,attesa_D = [e^{\mu_h + \frac{\sigma^2_h}{2}}][e^{\mu_c + \frac{\sigma^2_c}{2}}](q_{BOTH} + q_D) \tag{5.5}$$

Dove i pedici h e c indicano i parametri di media e varianza riferiti rispettivamente alle variabili contenute in tabella 5.2 e 5.3. Le perdite attese corrispondono quindi ai valori attesi di ciascuna distribuzione moltiplicati per i valori soggettivi delle probabilità di un certo tipo di impatto. Per i dati di input utilizzati in precedenza si sono ottenuti i seguenti valori:

Tabella 5.4: Output delle perdite attese

Rischio	$Perdita\,attesa_{RI}$	$Perdita\,attesa_D$
Data breach	665995.02443	8813.9473
Denial of service	200764.4115	12085.3670
Abuse of personal data	931228.7397	6259.8877
Loss of sensitive information	350069.5123	10166.2912

Calcolati i valori attesi, si procede al lancio della simulazione Monte Carlo su 100.000 scenari di rischio. Come affermato in precedenza, questo modello non utilizza come dati di input la probabilità media di accadimento per stabilire se il rischio si sia verificato o meno, bensì si basa sul fatto che il rischio si verifichi (quasi) certamente, pertanto non viene simulato il *se* ma il *come* una minaccia abbia impattato. Di seguito si riportano le linee di codice per la simulazione:

```
res_ri = zeros(n_scenari,1); %vettore scenari R/I

p_sim_ri= zeros(1,n_rischi); %vettore perdite simulate R/I

for i = 1:n_scenari

  for j = 1:n_rischi

    p_sim_ri(j) =logninv(rand,mu_ri(j),sigma_ri(j))*logico_ri(j);
  end
res_ri(i) = sum(p_sim_ri(j));

end
p_sim_d = zeros(1,n_rischi); %vettore scenari D

res_d = zeros(n_scenari,1);  %vettore perdite simulate D

for i = 1:n_scenari

   for j = 1:n_rischi

     p_sim_d(j) =

logninv(rand,mu_int(j),sigma_int(j))*logninv(rand,mu_costo(j),
   sigma_costo(j))*logico_d(j);

   end

res_d(i) = sum(p_sim_d(j));

end
```

Per entrambe le tipologie di evento, il modello genera dei numeri casuali uniformi corrispondenti al quantile delle distribuzioni lognormali (con media e deviazione standard calcolate prima) delle perdite, producendo ogni volta un valore differente degli impatti. Per stabilire se si sia verificata una tipologia piuttosto che l'altra, le perdite sono moltiplicate per i corrispondenti vettori logici binari definiti in precedenza. Una volta lanciato lo *script* si ottengono due tabelle (nello specifico i due vettori `res_ri` e `res_d`) che riportano al loro interno i valori calcolati.

Tabella 5.5: Valori per istogramma delle perdite R/I e D

$Scenario$	$Perdita\, simulata_{R/I}$	$Perdita\, simulata_{D}$
1	361.618,13225	13.501,7397
2	1.884.104,7063	14.382,3620
3	119.376,3090	46.228,1148
4	1.646.415,4609	30.368,1286
5	1.318.246,4917	20.128,5898
6	393.030,4976	98.90,0157
7	693.077,1009	20.261,1868
8	95.385,1220	14.753,4647
9	1.141.385,6886	34.803,5037
10	149.110,7192	17.928,5095
...	...	...
10.000	304.428,1922	10.092,0736
...	...	...
25.000	905.944,7463	30.890,5464
...	...	...
50.000	592.180,3729	19.059,3176
...	...	...
75.000	168.216,5037	18.720,4671
...	...	...
100.000	288.502,5593	35.409,3928

Dai dati riportati nella tabella sopra si può osservare quanto detto in precedenza, ovvero che il modello è inteso come un'ulteriore approfondimento dei rischi, riferendosi ai casi in cui questi si siano sempre verificati. Come nel caso precedente, si è eseguito su ogni istogramma un fit di tipo lognormale per avere una stima dei parametri caratteristici della distribuzione finale delle perdite generate da ciascun evento. Per la simulazione in questione si sono ottenuti i seguenti valori:

Tabella 5.6: Riepilogo dei parametri ottenuti dal fit per le categoria di evento

$Tipologia\, evento$	$Media$	$Varianza$	μ_{est}	σ_{est}
R/I	501.844	$3{,}5426e+11$	12,6869	0,93714
D	20368,2	$6{,}1593e+07$	9,8525	0,3721

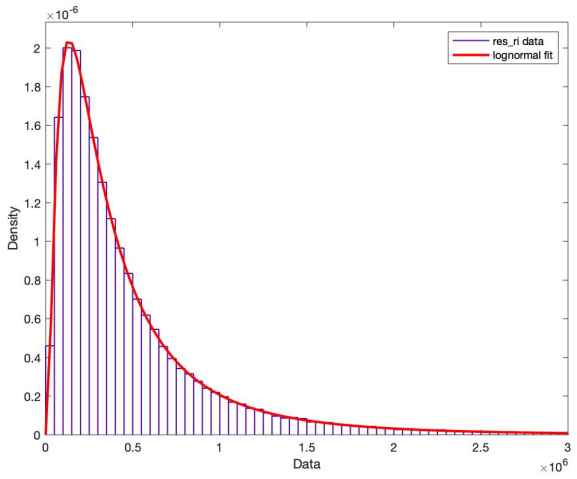

Figura 5.4: Istogramma per eventi R/I con curva di fit lognormale

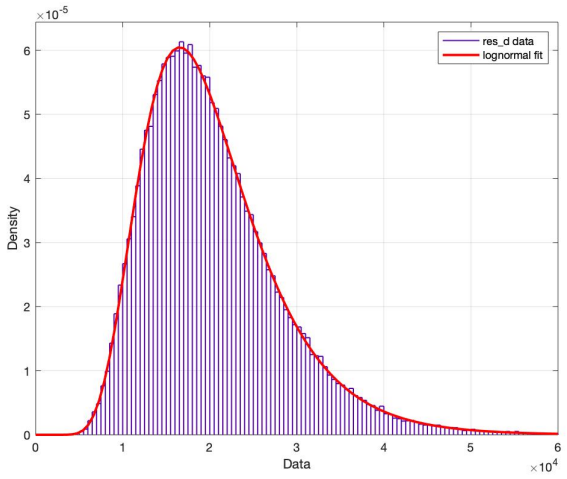

Figura 5.5: Istogramma per eventi D con curva di fit lognormale

5.5 Curve di Rischio, calcolo di Value at Risk ed Expected Shortfall

L'ultima parte del modello è dedicata all'ottenimento delle curve di rischio come strumento per l'analisi probabilistica delle potenziali perdite, in riferimento sempre all'orizzonte temporale di un anno. L'approccio metodologico è lo stesso dei casi con uno o più rischi aggregati: si parte dall'istogramma ottenuto con la simulazione e si verifica quanti dei 100.000 scenari generati superino una certa perdita

benchmark, in modo da ottenere un valore per la probabilità. In questo caso non sono riportate delle curve di tolleranza al rischio, nonostante non sarebbe affatto un errore implementarle nel proprio modello.

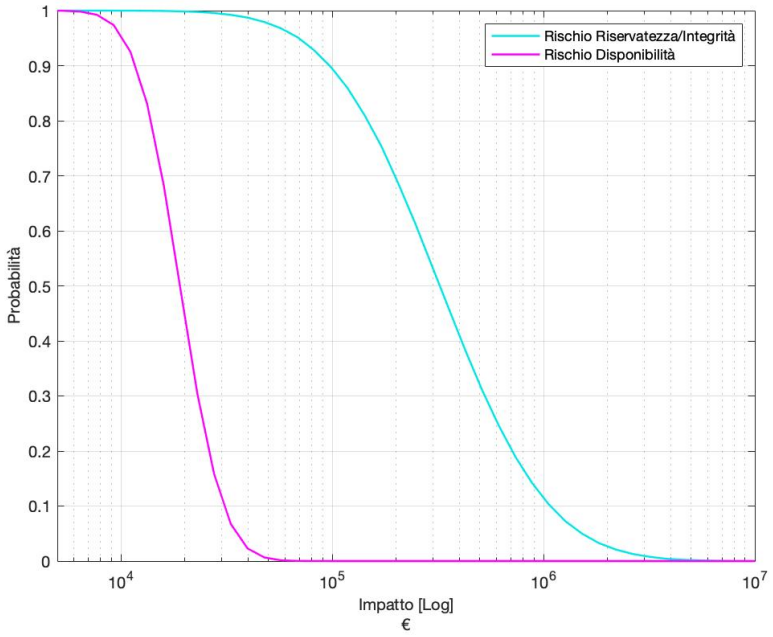

Figura 5.6: Curve di rischio per gli eventi R/I e D

E' possibile osservare come, per i dati di input inseriti, gli eventi di tipo D siano meno impattanti rispetto a quelli di tipo R/I, pertanto essi hanno una curva di rischio corrispondente più inclinata, suggerendo che questi possano provocare perdite con una probabilità significativa solamente per valori piuttosto modesti degli impatti. Al contrario, la curva R/I risulta sottendere un'area decisamente più estesa del piano, indicando una maggiore incidenza. Nel modello sono state inoltre considerati il VaR e l'ES per restituire un valore sintetico del rischio per le tipologie di evento considerate, e per il loro calcolo si sono utilizzate le medesime equazioni del caso con singolo rischio.

Tabella 5.7: Principali indicatori di rischio per gli eventi R/I e D

Tipologia evento	*Expected Loss*	*Value at Risk*	*Expected Shortfall*
R/I	502.210,4099	2.378.183,7497	351.125,4841
D	20.366,7180	24.757,3907	31.341,7012

Capitolo 6

Conclusioni

La cybersecurity rappresenta, ora più che mai, una nuova frontiera dei rischi operativi e, in quanto tali, richiede un approccio che permetta la sua analisi sotto più punti di vista. Il cybercrime finanziario ha subito una ulteriore evoluzione nel corso dell'ultimo anno, sia nella tecnica e tattica dei gruppi criminali che nella loro organizzazione: il cyber crimine è, ad oggi, dominato da gruppi internazionali, ben guidati e strutturati. La frode finanziaria risulta essere la principale minaccia osservabile in ambito europeo, e si verifica, quasi sempre, attraverso il furto delle credenziali delle vittime. Inoltre, frequenti sono i casi in cui le banche e altri intermediari finanziari subiscano attacchi DoS, campagne di phishing e di hackeraggio dei propri asset. In un contesto globale incerto e in assenza di linee guida e strumenti univoci per la gestione dei cyber rischi occorre che l?approccio alla sicurezza di ciascuna organizzazione sia unico, e che esso si basi sull?allineamento tra strategia di sicurezza e business, includendo la definizione dei driver di rischio e l?implementazione dei controlli di sicurezza volti a garantire l'integrità delle risorse aziendali e la protezione dalle minacce. Il processo di *cyber resilience* deve essere implementato partendo, anzitutto, dalla sensibilizzazione dei singoli individui nei confronti dei numerosi rischi insiti nell'era digitale, incentivando all'adozione di pratiche di sicurezza apparentemente banali (come l'utilizzo di password a breve scadenza o l'autenticazione a due fattori) ma che abbattono fin da subito la possibilità di un attacco informatico. Ciascuna organizzazione deve poi dotarsi di flessibilità operativa e di conformità agli standard e alle normative, verificando periodicamente il proprio livello di maturità nei confronti delle tecniche di mitigazione adeguati e stabilendo veri e propri programmi di incentivi alla sicurezza informatica.

Nei capitoli di questa tesi si è voluto indagare, mediante alcuni metodi statistici tipicamente utilizzati nella gestione del rischio, le peculiarità di ciascun evento dal punto di vista della probabilità e dell'impatto, compiendo un analisi multi-scenario in grado di restituire una visione globale delle potenziali perdite associate, tenendo

in considerazione l?efficacia dei controlli effettuati e i costi ad esso associati. I risultati permettono di compiere alcuni riflessioni importanti sulle prospettive di perdita generate dai rischi e su come queste siano determinate dai numerosi parametri di input utilizzati dal modello. Nello specifico, si ottiene di una distribuzione "bulk" delle perdite, ottenuta grazie al metodo Monte Carlo, dalla quale si possono calcolare le Curve di rischio, strumento interpretabile come evoluzione complementare alla matrice di rischio e particolarmente utile come supporto all'analisi decisionale. Dai risultati della simulazione si possono computare anche alcuni indicatori essenziali di rischio "tradizionali" utilizzati in tutti tutti gli ambiti del risk management: l'Expected Loss, il Value at Risk e l'Expected Shortfall. Inoltre si permette una analisi *what-if* in merito all'utilizzo dei controlli, della valutazione della loro efficacia e del loro impatto sulle perdite risultanti. Nel modello si compiono anche considerazioni in merito ai concetti di *risk tolerance*, confrontando differenti profili di rischio e valutandone la conformità o meno agli standard aziendali. Infine, per compiere un'ulteriore indagine sugli impatti associati a ciascun obiettivo di sicurezza, è stata proposta una scomposizione dei rischi mediante il criterio R.I.D.,con il quale si differenziano le perdite in base alla loro tipologia.

Questi modelli rappresentano un primo passo verso l'implementazione di metodi quantitativi per la cybersecurity negli intermediari finanziari e possono essere intesi come punto di partenza per eventuali sviluppi futuri. Le tecniche utilizzate sono quelle già largamente impiegate sia in letteratura che in ambito operativo e, nonostante siano di facile comprensione anche per quei soggetti aventi poca familiarità con la materia, permettono di compiere alcune valide riflessioni. Tuttavia, è bene specificare alcune limitazioni e mancanze riscontrabili all'interno dei modelli che potrebbero essere oggetto di possibili revisioni e miglioramenti futuri. Un primo aspetto piuttosto critico nella gestione dei rischi operativi (quindi anche quelli informatici) rappresenta la stima dei coefficienti di correlazione tra i singoli rischi. E' intuitivo osservare che numerose minacce siano tra loro correlate e, nel momento in cui si considerano più cyber rischi aggregati, sarebbe meglio considerare questi legami, al fine di ottenere risultati più affidabili e conservativi. Inoltre, sarebbe opportuno utilizzare distribuzioni alternative alla lognormale (come le già citate triangolare e la Legge di Potenza) per verificare la solidità dei calcoli. Infine, un aspetto di fondamentale importanza è la possibilità di compiere osservazioni per il calcolo della probabilità di accadimento: non sempre è possibile ottenere numeri esatti e le informazioni sono spesso nascoste, anche per via della poca propensione delle banche a diffondere determinate notizie che ne comprometterebbero la reputazione. In caso non fosse possibile ottenere questi dati, si potrebbe ricorrere alla logica di Bayes oppure ancora utilizzare una probabilità soggettiva, avendo cura di inserire valori *unbiased* e di evitare risultati troppo ottimistici. Numerose altre considerazioni potrebbero essere compiute e gli scenari di sviluppo sono innumerevoli: nel corso dei prossimi anni si assisterà all'adozione di standard quantitativi sempre più frequenti anche nell'ambito della sicurezza informatica.

Bibliografia e sitografia

[1] Norbert Wiener. *Cybernetics: or Control and Communication in the Animal and the Machine*. 2ª ed. Cambridge, MA: MIT Press, 1948.

[2] Dan Craigen, Nadia Diakun-Thibault e Randy Purse. "Defining cybersecurity". In: *Technology Innovation Management Review* 4.10 (2014).

[3] Ronald Deibert e Rafal Rohozinski. "Liberation vs. control: The future of cyberspace". In: *Journal of democracy* 21.4 (2010), pp. 43–57.

[4] *National Information Assurance Glossary.Committee on National Security Systems (CNSS) Instruction No. 4009*. 2010.

[5] Richard A. Kemmerer. "Cybersecurity". In: *25th International Conference on Software Engineering, 2003. Proceedings.* IEEE. 2003, pp. 705–715.

[6] Edward Amoroso. *Cyber security*. New Jersey: Silicon Press, 2006.

[7] URL: `https://www.lexico.com/definition/cybersecurity`.

[8] James A Lewis. "Cybersecurity and critical infrastructure protection". In: *Center for Strategic and International Studies* (2006).

[9] URL: `https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C`.

[10] Lisa R. Cebula James L. e Young. *A taxonomy of operational cyber security risks*. Rapp. tecn. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2010.

[11] Claudia Canongia e Raphael Mandarino. "Crisis Management: Concepts, Methodologies, Tools and Applications". In: Cybersecurity: The New Challenge of the Information Society. IGI Global, 2014. Cap. 3, pp. 60–80.

[12] ITU. *Overview of Cybersecurity. Recommendation ITU-T X.1205.* Rapp. tecn. Geneva: International Telecommunication Union (ITU), 2009.

[13] Public Safety Canada. *Canada's Cyber Security Strategy*. Rapp. tecn. Ottawa: Public Safety Canada, Government of Canada, 2010.

[14] CPS. *Cybercrime - prosecution guidance*. Rapp. tecn. The Crown Prosecution Service (CPS), 2019.

[15] James J Cebula, Mary E Popeck e Lisa R Young. *A taxonomy of operational cyber security risks version 2*. Rapp. tecn. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2014.

[16] URL: `https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors`.

[17] Boston Consulting Group. *Reigniting Radical Growth*. 2019.

[18] Patrick Schueffel. "Taming the beast: A scientific definition of fintech". In: *Journal of Innovation Management* 4.4 (2016), pp. 32–54.

[19] Dominik Sadlakowski e Anna Sobieraj. "The development of the FinTech industry in the Visegrad group countries". In: *World Scientific News* 85 (2017), pp. 20–28.

[20] URL: `https://carnegieendowment.org/`.

[21] CLUSIT. *Rapporto CLUSIT sulla sicurezza ICT in Italia- ottobre 2020*.

[22] CLUSIT. *Rapporto CLUSIT 2021 sulla sicurezza ICT in Italia*.

[23] ESRB. *Systemic cyber risk - February 2020*. Rapp. tecn. European Sysetmic Risk Board, 2020.

[24] P Testi. "Liquidity contingency plan". In: *Atti del convegno Paradigma "Il rischio di liquidità", Milano* 18 ().

[25] Anil K Kashyap e Anne Wetherilt. "Some principles for regulating cyber risk". In: *AEA Papers and Proceedings*. Vol. 109. 2019, pp. 482–87.

[26] Basel Committee on Banking Supervision (Basel). "Review of the Principles for the Sound Management of Operational Risk". In: *Technical Report* (2014).

[27] Philippe Artzner et al. "Coherent measures of risk". In: *Mathematical finance* 9.3 (1999), pp. 203–228.

[28] Mr Andreas A Jobst e Mr Dale F Gray. *Systemic contingent claims analysis: Estimating market-implied systemic risk*. International Monetary Fund, 2013.

[29] Carlo Acerbi e Dirk Tasche. "Expected shortfall: a natural coherent alternative to value at risk". In: *Economic notes* 31.2 (2002), pp. 379–388.

[30] Carlo Acerbi e Dirk Tasche. "On the coherence of expected shortfall". In: *Journal of Banking & Finance* 26.7 (2002), pp. 1487–1503.

[31] Anton N Didenko. "Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond". In: *Uniform Law Review* 25.1 (2020), pp. 125–167.

[32] Commissione Europea. *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace*. 2013.

[33] Commissione Europea. *Cybersecurity. Resilience, Deterrence and Defence. Building strong cybersecurity in Europe*. 2017.

[34] General Data Protection Regulation. "Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016". In: *Official Journal of the European Union* (2016).

[35] *REGOLAMENTO (UE) N. 575/2013 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 giugno 2013 relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento.*

[36] *DIRETTIVA 2013/36/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 giugno 2013 sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento*. 2013.

[37] URL: `https://www.bankingsupervision.europa.eu/press/publications/newsletter/2019/html/ssm.nl190213_4.en.html`.

[38] *DIRETTIVA (UE) 2015/2366 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno*. 2015.

[39] *REGOLAMENTO DELLA BANCA CENTRALE EUROPEA (UE) N. 795/2014 del 3 luglio 2014 sui requisiti di sorveglianza per i sistemi di pagamento di importanza sistemica (BCE/2014/28)*. 2014.

[40] ECB. *Revised Oversight Framework for Retail Payment Systems*.

[41] ECB. *Cyber resilience oversight expectations for financial market infrastructures*. Rapp. tecn. Banca Centrale Europea, 2018.

[42] *REGOLAMENTO (UE) N. 648/2012 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 4 luglio 2012 sugli strumenti derivati OTC, le controparti centrali e i repertori di dati sulle negoziazioni.*

[43] *DIRETTIVA 2009/138/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2009 in materia di accesso ed esercizio delle attività (Solvibilità II).*

[44] *REGOLAMENTO (CE) N. 1060/2009 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 settembre 2009 relativo alle agenzie di rating del credito.*

[45] *REGOLAMENTO (UE) N. 909/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli.*

[46] *DIRETTIVA 2014/65/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 15 maggio 2014 relativa ai mercati degli strumenti finanziari.*

[47] *REGOLAMENTO (UE) N. 600/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 15 maggio 2014 sui mercati degli strumenti finanziari.*

[48] *REGOLAMENTO DELEGATO (UE) 2017/589 DELLA COMMISSIONE del 19 luglio 2016.*

[49] *FinTech action plan: For a more competitive and innovative European financial sector*. Rapp. tecn. European Commission, 2018.

[50] *Cyber-resilience: Range of practices*. BCBS.

[51] *REGOLAMENTO (UE) N. 575/2013 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 26 giugno 2013 relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento*.

[52] URL: `https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/8101`.

[53] *ISO/IEC 27001 - Information Security Management*. International Organization for Standardization e International Electrotechnical Commission.

[54] *ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls*. International Organization for Standardization e International Electrotechnical Commission.

[55] *Cybersecurity Framework*. National Institute of Standards e Technology.

[56] *CIS controls*. Center for Internet Security.

[57] *Cybersecurity Assessment Tool*. Federal Financial Institutions Examination Council.

[58] *Data Breach Investigation Report*. Verizon. 2019.

[59] URL: `https://cio-wiki.org/wiki/Risk_Matrix`.

[60] David V Budescu, Stephen Broomell e Han-Hui Por. "Improving communication of uncertainty in the reports of the Intergovernmental Panel on Climate Change". In: *Psychological science* 20.3 (2009), pp. 299–308.

[61] Louis Anthony (Tony) Cox Jr. "What's wrong with risk matrices?" In: *Risk Analysis: An International Journal* 28.2 (2008), pp. 497–512.

[62] Douglas Hubbard e Dylan Evans. "Problems with scoring methods and ordinal scales in risk assessment". In: *IBM Journal of Research and Development* 54.3 (2010), pp. 2–1.

[63] Philip Thomas, Reidar B Bratvold, Eric Bickel et al. "The risk of using risk matrices". In: *SPE Economics & Management* 6.02 (2014), pp. 56–66.

[64] GS Simpson et al. "The application of probabilistic and qualitative methods to asset management decision making". In: *SPE Asia Pacific Conference on Integrated Modelling for Asset Management*. Society of Petroleum Engineers. 2000.

[65] Claude W Freaner et al. "An assessment of the inherent optimism in early conceptual designs and its effect on cost and schedule growth". In: *Presentation to the Planetary Science Subcommittee, NASA Advisory Council* (2008).

Elenco delle tabelle

Elenco delle figure

Appendice A

Codici MATLAB

Nelle seguenti pagine si riportano per intero i codici originali, in linguaggio MATLAB®, utilizzati per il calcolo degli output descritti nei capitoli precedenti. Per ciascuno è indicato anche il tempo di esecuzione impiegato dal software (MATLAB R2021a, macOS Big Sur 11.2.2, CPU i7 quad core 2,2 GHz, RAM 16 GB 1600 MHz DDR3, ROM SSD 256 GB, GPU Intel Iris Pro 1536 MB).

A.1 Analisi di un singolo cyber rischio

```
Elapsed time is 8.064579 seconds.
```

```
%% Dati di input
%rng 'default'
format long
euro = char(8364);
fontSize = 10;
IDrisk = 'Data breach';
lim_inf = 5e6;
lim_sup = 100e6;
CI = 0.9;

%% Distribuzione delle perdite
mu = (log(lim_sup)+log(lim_inf))/2;
std_dev = (log(lim_inf)-log(lim_sup))/(2*norminv(0.5*(1-CI)));

lognorm_pd = makedist('Lognormal','mu',mu,'sigma',std_dev);
x = (0:200e6);
y = pdf(lognorm_pd,x);
lb_ln = logninv(1-CI,mu,std_dev);
ub_ln = logninv(CI,mu,std_dev);
figure(1)
plot(x,y,'LineWidth',1.5)
hold on
xline(lb_ln,':k','LineWidth',1.5);
```

```
xline(ub_ln,':k','LineWidth',1.5);
hold off
grid on
xlabel({'Perdite', euro}, 'FontSize', fontSize);
ylabel('Densità', 'FontSize', fontSize);
title({'Data Breach','Distribuzione delle perdite'}, 'FontSize',
    fontSize);
legend({'Dist. perdite','Lim. inf. [90% CI]','Lim. sup. [90% CI]'},
    'Location','northeast','Orientation','vertical');

%% Probabilità di accadimento
year_start = 2019;
year_end = 2020;
eventi = 185;
n_campione = 4209;
prior_Alpha = 0;
prior_Beta = 0;
CI_prob = 0.95;

a = eventi + prior_Alpha;
b = n_campione*(year_end - year_start) - eventi + prior_Beta;
x_beta = 0:0.001:0.15;
y_beta = betapdf(x_beta, a, b);
prob_media = a/(a+b);
l_bound = betainv(1-CI_prob, a, b);
u_bound = betainv(CI_prob,a ,b);
figure(2)
plot(x_beta,y_beta,'LineWidth',1.5);
hold on
xline(prob_media,'-r'),
xline(l_bound,':');
xline(u_bound,':');
hold off
grid on
xlim([0 0.08]);
xlabel('Probabilità', 'FontSize', fontSize);
ylabel('Densità', 'FontSize', fontSize);
title({'Data Breach','Probabilità di accadimento'}, 'FontSize',
    fontSize);
legend({'Beta PDF','Prob. media','Lim. inf. [90% CI]','Lim. sup.
    [90% CI]'},'Location','northeast','Orientation','vertical');

p_att = prob_media*exp(mu + 0.5*std_dev^2); %Calcolo perdita attesa

% Simulazione Monte Carlo
n_scenari = 100000; %numero di simulazioni effettuato

res = zeros(n_scenari,1);
for k = 1:n_scenari
```

```
69    if rand < prob_media %estrae un numero casuale uniforme e
      verifica se l'evento è accaduto
70        sim_loss = logninv(rand, mu, std_dev); %calcola la perdita
      simulata in caso di evento
71    else
72         sim_loss = 0; %perdita simlata altrimenti
73
74    end
75     res(k) = sim_loss; %per ogni scenario restituisce la perdita
      calcolata
76
77 end
78
79 % Output parametri
80 Expected_loss = mean(res);
81 nn_percent_loss = quantile(res, 0.99);
82 VaR = nn_percent_loss - Expected_loss;
83 Expected_shortfall = mean(res(res > VaR));
84
85
86 %% Controlli implementati
87
88 ce = 0.35; %indice di efficacia controlli
89 cost_c = 400000; %costo dei controlli
90 p_att_c = (1-ce)*prob_media*exp(mu + 0.5*(std_dev^2)); %Calcolo
      perdita attesa
91
92 % Simulazione Monte Carlo
93 res_c = zeros(n_scenari,1);
94 for k = 1:n_scenari
95    if rand < prob_media*(1-ce)
96          sim_loss_c = logninv(rand, mu, std_dev);
97     else
98         sim_loss_c = 0;
99     end
100    res_c(k) = sim_loss_c;
101 end
102
103 figure(3)
104 edges = (0.1:5e6:300e6);
105 h = histogram(res,edges);
106 hold on
107 h_c = histogram(res_c,edges);
108 hold off
109 lgd = legend('Controlli non implementati','Controlli implementati')
      ;
110 c = lgd.TextColor;
111 lgd.TextColor = 'black';
112 grid on;
113 xlabel({'Perdite',euro}, 'FontSize', fontSize);
```

```
114 xlim([0 3e8]);
115 ylabel('Frequenze', 'FontSize', fontSize);
116 title({'Data Breach','Simulazione Monte Carlo - Istogramma delle
       perdite'}, 'FontSize',fontSize);
117
118 % Output parametri
119 Expected_loss_c = mean(res_c);
120 nn_percent_loss_c = quantile(res_c,0.99);
121 VaR_c = nn_percent_loss_c - Expected_loss;
122 Expected_shortfall_c = mean(res_c(res_c>VaR));
123
124 ROC = ((p_att - p_att_c)/cost_c) - 1;
125
126 %% Calcolo Curve di Rischio
127
128 %introdurre funzione di tolleranza al rischio
129 x_perdite_toll = [5e5 5e6 5e7 6e7 1e8];
130 prob_toll = [0.055 0.045 0.008 0.006 0.002];
131 xx=linspace(x_perdite_toll(1),x_perdite_toll(end),1000);
132 yy=interp1(x_perdite_toll,prob_toll,xx,'spline');
133
134 x_perdite = zeros(1,500);
135 for i=1:length(x_perdite)
136     x_perdite(1) = 1;
137     x_perdite(i+1) = x_perdite(i)*1.2;
138 end
139
140 for i = numel(x_perdite):-1:1
141     prob(i) = sum(res >= x_perdite(i))/n_scenari;
142
143 end
144
145 for k = numel(x_perdite):-1:1
146     prob_c(k) = sum(res_c >= x_perdite(k))/n_scenari;
147 end
148
149 figure(4)
150 area(xx,yy,'FaceColor',[247/255 1 245/255])
151 hold on
152 semilogx(x_perdite,prob,'r--','LineWidth',1.5);
153 semilogx(x_perdite, prob_c,'g','LineWidth',1.5);
154 semilogx(xx, yy,':b','LineWidth',0.8)
155 hold off
156 grid on
157 xlabel({'Impatto [Log]',euro}, 'FontSize', fontSize);
158 ylabel('Probabilità','FontSize', fontSize);
159 title({'Data Breach','Curve di Rischio'}, 'FontSize', fontSize);
160 legend({'Zona di tolleranza','Rischio','Rischio Residuo','Rischio
       Tollerato'},'Location','northeast','Orientation','vertical')
161 xlim([0 1e8]);
```

```
ylim([0 0.05]);

%calcolo probabilità di una certa perdita benchmark
val_cercato = 3e6;
nless = sum(res_c < val_cercato);
nequal = sum(res_c == val_cercato);
prob_val_cercato = (100 - 100 * (nless + 0.5*nequal) / length(res_c
    ))/100;

res_fit = nonzeros(res);
res_c_fit = nonzeros(res_c);
```

A.2 Analisi di molteplici cyber rischi aggregati

```
  Elapsed time is 62.592131 seconds.
```

```
%% Dati di input
%rng ('default')
euro = char(8364);
fontSize = 10;
n_scenari = 100000;  %Numero di simulazioni effettuate
CI = 0.9;
n_rischi = 4;
IDrisk = ["Data breach" "Denial of Service" "Abuse of personal data
    " "Loss of sensitive information"];
lim_inf = [5e6 2e6 1.5e6 5e6]; %limite inferiore delle perdite
lim_sup = [100e7 50e7 30e7 30e7]; %limite superiore delle perdite
year_start = [2019 2019 2019 2019];
year_end = [2020 2020 2020 2020];
eventi = [185 157 67 253];
n_campione = [4209 2530 1454 2367];
prior_Alpha = [1 1 1 1];
prior_Beta = [1 1 1 1];

%% Probabilità di accadimento
a = eventi + prior_Alpha;
b = zeros(1,n_rischi);
for i = 1:n_rischi
    b(i) = n_campione(i)*(year_end(i) - year_start(i)) - eventi(i)
    + prior_Beta(i);
end

prob_m = zeros(1,n_rischi); %vettore delle probabilità medie di
    accadimento
for i = 1:n_rischi
    prob_m(i) = a(i) /(a(i)+b(i));
end

x_beta = 0:0.001:0.20;
```

```
y_beta = zeros(length(x_beta), n_rischi);
figure(1)
hold on;
for i = 1:n_rischi
    y_beta(:,i) = betapdf(x_beta,a(i),b(i));
    plot(x_beta,y_beta(:,i),'LineWidth',1.5);
end
hold off
grid on
xlim([0 0.15]);
xlabel('Probabilità', 'FontSize', fontSize);
ylabel('Densità', 'FontSize', fontSize);
title('Distribuzioni di probabilità', 'FontSize', fontSize);
legend(["Data breach" "Denial of Service" "Abuse of personal data"
   "Loss of sensitive information"],'Location','northeast','
   Orientation','vertical');

%% Distribuzione delle perdite
mu = (log(lim_sup)+log(lim_inf))/2;
std_dev = (log(lim_inf)-log(lim_sup))/(2*norminv(0.5*(1-CI)));

x_dist = (0:200e6);
y_dist = zeros(length(x_dist),n_rischi);
figure(2)
hold on;
for i = 1:n_rischi
      y_dist(:,i) = lognpdf(x_dist,mu(i),std_dev(i));
      plot(x_dist, y_dist(:,i),'LineWidth',1.5);
end
hold off
grid on
xlabel({'Perdite', euro}, 'FontSize', fontSize);
ylabel('Densità', 'FontSize', fontSize);
title('Distribuzioni delle perdite', 'FontSize', fontSize);
legend(["Data breach" "Denial of Service" "Abuse of personal data"
   "Loss of sensitive information"],'Location','northeast','
   Orientation','vertical');

%% Controlli non implementati
p_att = prob_m.*exp(mu + 0.5.*(std_dev.^2)); %calcolo perdita
   attesa

r1 = rand(1,n_rischi); %vettore di numeri casuali uniformi
res = zeros(n_scenari,1); %vettore delle perdite simulate aggregate
p_sim = zeros(n_rischi,1); %vettore delle perdite simulate (singolo
    rischio)
for i = 1:n_scenari
    for j = 1:n_rischi
     if rand < prob_m(j)
        p_sim(j) = logninv(rand, mu(j), std_dev(j));
```

```
     else
        p_sim(j) = 0;
     end
    end
   res(i) = sum(p_sim(j));
end

EL = mean(res);
VaR = quantile(res, 0.99) - EL;
ES = mean(res(res > VaR));

%% Controlli implementati

ce = [0.35 0.25 0.30 0.10]; %indici di efficacia dei controlli
cost_c = [300000 200000 200000 75000]; %costo dei controlli

p_att_c = (1-ce).*prob_m.*exp(mu + 0.5.*std_dev.^2); %Calcolo
   perdita attesa residua

res_c= zeros(n_scenari,1); %simulazione Monte Carlo
p_sim_c = zeros(n_rischi,1);
for i = 1:n_scenari
    for j = 1:n_rischi
     if rand < prob_m(j)*(1-ce(j))
        p_sim_c(j) = logninv(rand, mu(j), std_dev(j));
     else
        p_sim_c(j) = 0;
     end
    end
   res_c(i) = sum(p_sim_c(j));
end

EL_c = mean(res_c);
VaR_c = quantile(res_c, 0.99) - EL_c;
ES_c = mean(res_c(res_c > VaR_c));

figure(3)
edges = 0.1:5e6:800e6;
h = histogram(res,edges);
hold on
h_c = histogram(res_c,edges);
hold off
lgd = legend('Controlli non implementati','Controlli implementati')
   ;
c = lgd.TextColor;
lgd.TextColor = 'black';
grid on;
xlabel({'Perdite',euro}, 'FontSize', fontSize);
ylabel('Frequenze', 'FontSize', fontSize);
```

```
122 title({'Simulazione Monte Carlo';'Istogramma delle perdite'}, '
    FontSize', fontSize);
123
124 ROC = zeros(1,n_rischi);
125 for i = 1:n_rischi
126 ROC(i) = ((p_att(i) - p_att_c(i))/cost_c(i)) - 1;
127 end
128
129 %% Calcolo  Curve di rischio
130 % introdurre funzione di tolleranza al rischio
131 x_perdite_toll = [1e6 5e6 1e7 5e7 6e7];
132 prob_toll = [0.22 0.15 0.12 0.02 0.001];
133 xx=linspace(x_perdite_toll(1),x_perdite_toll(end),1e6);
134 yy=interp1(x_perdite_toll,prob_toll,xx,'spline');
135
136 x_perdite = zeros(1,500);
137 for i=1:length(x_perdite)
138     x_perdite(1) = 1e6;
139     x_perdite(i+1) = x_perdite(i)*1.2;
140 end
141
142 for i = numel(x_perdite):-1:1
143     prob(i) = sum(res >= x_perdite(i))/length(res);
144
145 end
146
147 for k = numel(x_perdite):-1:1
148     prob_c(k) = sum(res_c >= x_perdite(k))/length(res_c);
149 end
150
151 figure(4)
152 area(xx,yy,'FaceColor',[247/255 1 245/255])
153 hold on
154 semilogx(x_perdite,prob,'r--','LineWidth',1.5)
155 semilogx(x_perdite, prob_c,'g','LineWidth',1.5)
156 semilogx(xx,yy,'k:','LineWidth',0.8)
157 hold off
158 grid on
159 xlim([1e6 7e7]);
160 ylim([0 0.20]);
161 xlabel({'Impatto',euro}, 'FontSize', fontSize);
162 xlim([0 7e7]);
163 ylabel('Probabilità','FontSize', fontSize);
164 title('Curve di Rischio', 'FontSize', fontSize);
165 legend({'Zona di tolleranza','Rischio','Rischio Residuo','Rischio
    Tollerato'},'Location','northeast','Orientation','vertical')
166
167 %calcolo probabilità di una certa perdita benchmark
168 val_cercato = 50e6;
169 nless = sum(res_c < val_cercato);
```

```
nequal = sum(res_c == val_cercato);
inc_rango = (100 - 100 * (nless + 0.5*nequal) / length(res_c))/100;
%valori filtrati per fit
res_fit = nonzeros(res);
res_c_fit = nonzeros(res_c);
```

A.3 Scomposizione dei cyber rischi - criterio R.I.D.

```
Elapsed time is 2.927298 seconds.
```

```
%% Dati di input
%rng ('default')
format long
euro = char(8364);
n_scenari = 100000;  %Numero di simulazioni effettuate
CI = 0.9;
n_rischi = 4;
IDr = ['Data breach' 'Denial of Service' 'Abuse of personal data' '
    Loss of sensitive information'];
year_start = [2019 2019 2019 2019];
year_end = [2020 2020 2020 2020];
eventi = [185 157 67 253];
n_campione = [4209 2530 1454 2367];
prior_Alpha = [1 1 1 1];
prior_Beta = [1 1 1 1];
r_i = [0.2 0.2 0.1 0.5];
d = [0.5 0.3 0.4 0.3];
both = (1-(r_i+d));
r = rand(1,n_rischi); %vettore di numeri casuali

a = eventi + prior_Alpha;
b = zeros(1,n_rischi);
for i = 1:n_rischi
    b(i) = n_campione(i)*(year_end(i) - year_start(i)) - eventi(i)
    + prior_Beta(i);
end

prob = zeros(1,n_rischi); %vettore delle probabilità medie di
    accadimento
for i = 1:n_rischi
    prob(i) = a(i) /(a(i)+b(i));
end

% Determinazione vettori logici di accadimento
logico_ri = zeros(1,length(r_i));

for i = 1:length(r_i)
    if (r(i) < r_i(i)) || (r(i)>(r_i(i)+d(i)))
        logico_ri(i) = 1;
```

```
    end
end

logico_d = zeros(1,length(d));

for i = 1:length(logico_d)
    if ((r_i(i) < r(i)) && (r_i(i) + d(i)) > r(i)) || r(i)>(r_i(i)+d(i))
        logico_d(i) = 1;
    end
end
%% Eventi di tipo R/I
lim_inf_ri = [5e4 2e4 3e4 7e4];
lim_sup_ri = [5e6 1e6 6e6 1.5e6];
mu_ri = 0.5*(log(lim_inf_ri)+log(lim_sup_ri));
sigma_ri = 0.5*(log(lim_inf_ri)-log(lim_sup_ri))/norminv(0.5*(1-CI));

x_dist_ri = (0:2e6);
y_dist_ri = zeros(length(x_dist_ri),n_rischi);
figure(1)
hold on;
for i = 1:n_rischi
      y_dist_ri(:,i) = lognpdf(x_dist_ri,mu_ri(i),sigma_ri(i));
      plot(x_dist_ri, y_dist_ri(:,i),'LineWidth',1.5);
end
hold off
grid on
xlabel({'Perdite', euro}, 'FontSize', fontSize);
ylabel('Densità', 'FontSize', fontSize);
title({'Distribuzioni delle perdite','Eventi di tipo R/I'}, 'FontSize', fontSize);
legend(["Data breach" "Denial of Service" "Abuse of personal data" "Loss of sensitive information"],'Location','northeast','Orientation','vertical');

p_att_ri = zeros(1,n_rischi); %vettore delle perdite attese
for i = 1:n_rischi
    p_att_ri(i) = exp(mu_ri(i) + 0.5*((sigma_ri(i))^2))*(r_i(i)+both(i));
end

% Simulazione Monte Carlo
res_ri = zeros(n_scenari,1); %vettore scenari R/I
p_sim_ri= zeros(1,n_rischi); %vettore perdite simulate R/I

for i = 1:n_scenari
  for j = 1:n_rischi
    p_sim_ri(j) = logninv(rand,mu_ri(j),sigma_ri(j))*logico_ri(j);
  end
```

```
res_ri(i) = sum(p_sim_ri(j));
end

EL_ri = mean(res_ri);
VaR_ri = quantile(res_ri,0.99) - EL_ri;
ES_ri = mean(res_ri(res_ri>VaR_ri));

figure(2)
h1 = histogram(res_ri);
grid on
xlim([0,5e6]);
fontSize = 10;
euro=char(8364);
xlabel({'Perdite',euro}, 'FontSize', fontSize);
ylabel('Frequenze','FontSize', fontSize);
title({'Istogramma delle perdite','Eventi R/I'}, 'FontSize',
    fontSize);

%% Eventi di tipo D
int_min = [2 1 1 4];
int_max = [8 12 3 9];
c_ora_min = [1e3 1.5e3 8e2 2e3];
c_ora_max = [5e3 6e3 10e3 5e3];

mu_int = 0.5*(log(int_min)+log(int_max));
sigma_int = 0.5*((log(int_min)-log(int_max))/norminv(0.5*(1-CI)));

x_dist_int = (0:20);
y_dist_int = zeros(length(x_dist_int),n_rischi);
figure(3)
hold on;
for i = 1:n_rischi
      y_dist_int(:,i) = lognpdf(x_dist_int,mu_int(i),sigma_int(i));
      plot(x_dist_int, y_dist_int(:,i),'LineWidth',1.5);
end
hold off
grid on
xlabel('Durata interruzione [h]', 'FontSize', fontSize);
ylabel('Densità', 'FontSize', fontSize);
title({'Distribuzioni della durata interruzioni','Eventi di tipo D'
    }, 'FontSize', fontSize);
legend(["Data breach" "Denial of Service" "Abuse of personal data"
    "Loss of sensitive information"],'Location','northeast','
    Orientation','vertical');

mu_costo = 0.5*(log(c_ora_min)+log(c_ora_max));
sigma_costo = 0.5*((log(c_ora_min)-log(c_ora_max))/norminv(0.5*(1-
    CI)));

x_dist_costo = (0:20e3);
```

```
y_dist_costo = zeros(length(x_dist_costo),n_rischi);
figure(4)
hold on;
for i = 1:n_rischi
      y_dist_costo(:,i) = lognpdf(x_dist_costo,mu_costo(i),
   sigma_costo(i));
      plot(x_dist_costo, y_dist_costo(:,i),'LineWidth',1.5);
end
hold off
grid on
xlabel({'Costo interruzione',euro}', 'FontSize', fontSize);
ylabel('Densità', 'FontSize', fontSize);
title({'Distribuzioni del costo interruzioni','Eventi di tipo D'},
   'FontSize', fontSize);
legend(["Data breach" "Denial of Service" "Abuse of personal data"
   "Loss of sensitive information"],'Location','northeast','
   Orientation','vertical');

p_att_d = zeros(1,n_rischi);
for i = 1:n_rischi
    p_att_d(i) = (exp(mu_int(i)+0.5*(sigma_int(i)^2)))*(exp(
   mu_costo(i)+0.5*(sigma_costo(i)^2)))*(d(i)+both(i));
end

% Simulazione Monte Carlo
p_sim_d = zeros(1,n_rischi); %vettore scenari D
res_d = zeros(n_scenari,1);  %vettore perdite simulate D

for i = 1:n_scenari
   for j = 1:n_rischi
     p_sim_d(j) = logninv(rand,mu_int(j),sigma_int(j))*logninv(rand
   ,mu_costo(j),sigma_costo(j))*logico_d(j);
   end
 res_d(i) = sum(p_sim_d(j));
end

EL_d = mean(res_d);
VaR_d = quantile(res_d, 0.99) - EL_d;
ES_d = mean(res_d(res_d > VaR_d));

figure(5)
h2 = histogram(res_d);
grid on
fontSize = 10;
xlim([0,8e4]);
xlabel({'Perdite',euro}, 'FontSize', fontSize);
ylabel('Frequenze','FontSize', fontSize);
title({'Istogramma delle perdite','Eventi D'}, 'FontSize', fontSize
   );

```

```
%% Calcolo Curve di Rischio
x_perdite = zeros(1,200);
for i=1:length(x_perdite)
  x_perdite(1) = 500;
  x_perdite(i+1) = x_perdite(i)*1.20;
end

prob_ri = zeros(1,length(x_perdite));
for i = numel(x_perdite):-1:1
    prob_ri(i) = sum(res_ri >= x_perdite(i))/length(res_ri);

end

prob_d = zeros(1,length(x_perdite));
for i = numel(x_perdite):-1:1
    prob_d(i) = sum(res_d >= x_perdite(i))/length(res_d);
end

figure(6)
semilogx(x_perdite,prob_ri,'Color', [0, 230/255, 230/255],'
   LineWidth',1.2)
hold on
semilogx(x_perdite,prob_d,'m','LineWidth',1.2);
xlim([5e3 1e7]);
grid on
fontSize = 10;
xlabel({'Impatto [Log]',euro}, 'FontSize', fontSize);
ylabel('Probabilità','FontSize', fontSize);
title('Curve di Rischio', 'FontSize', fontSize);
legend({'Rischio Riservatezza/Integrità','Rischio Disponibilità'},'
   Location','northeast','Orientation','vertical')
```

Ringraziamenti

Questo tesi è il risultato di un lavoro durato mesi, al quale ho lavorato con interesse e motivazione affinché il risultato fosse il migliore possibile. Durante questo periodo ho avuto il piacere di intraprendere un percorso di conoscenza riguardo alla cybersecurity, tematica dall'importanza ormai assoluta, oltre che l'occasione di imparare alcuni metodi e strumenti, come MATLAB® e LaTeX, i quali ero desideroso di conoscere da tempo.

Per questo motivo, mi sento di ringraziare Augeos S.p.A. per avermi introdotto a tale argomento, oltre che per avermi concesso l'opportunità di tirocinio, in un momento storico di assoluta difficoltà per le imprese e per le persone che ne appartengono. Inoltre, ringrazio il professore Franco Varetto per l'assoluta disponibilità mostratami, sia durante i corsi universitari, che durante la stesura di questa tesi. Una menzione di gratitudine va alle persone con cui io abbia condiviso qualche momento durante tutti questi anni: da voi ho imparato molto e, spero, con la mia presenza, di avervi donato qualcosa.

Ringrazio la mia famiglia, per l'opportunità e per il supporto datomi, in particolar modo Stefano, con il quale ho condiviso gran parte della carriera universitaria, inclusi i nostri successi e i nostri fallimenti.

Infine, non posso fare altro che essere grato, per sempre, a Valentina, per il suo infinito supporto e per la pazienza con la quale mi ha accompagnato durante questo percorso di crescita culturale e, sopratutto, personale.