Università
Ca'Foscari
Venezia

CORSO DI LAUREA IN

ECONOMIA E FINANZA

Tesi di Laurea

Il rischio informatico: sviluppo di un modello per la determinazione del livello di rischio in caso di un evento di Data Breach

Relatore
Ch. Prof. Simone Mazzonetto

Correlatore
Ch. Prof. Andrea Veller

Laureanda
Erika Argentieri
Matricola 867019

Anno accademico
2021/2022

Sommario

“E il vostro dubbio può divenire una buona qualità, se lo ‘educate'. Esso deve diventare conoscenza, deve farsi critica. Domandategli, ogni volta che vuole guastarvi qualche cosa, ‘perché' la tal cosa sia brutta, esigete dimostrazioni da lui, esaminatelo, e lo troverete forse inerme e confuso, anche forse arrogante. Ma non cedete, sollecitate prove e agite così, attento e conseguente, ogni singola volta, e verrà giorno in cui da distruttore diverrà uno dei vostri migliori lavoratori - forse il più accorto di tutti quelli che edificano la vita.

E per il resto lasciatevi accadere la vita. Credetemi: la vita ha ragione, in tutti i casi.”

Rainer Maria Rilke

INTRODUZIONE

Quasi da un giorno all'altro, l'emergenza pandemica ha costretto il mondo bancario a porre in essere cambiamenti radicali incentrati sull'utilizzo massiccio delle piattaforme tecnologiche.
I canali digitali rivolti ai clienti sono stati rafforzati e migliorati, le piattaforme di lavoro a distanza sono state ampliate e gli strumenti emergenti, come i software di analisi dei dati, sono diventati parte integrante dei processi organizzativi interni.
In un contesto senza precedenti, nel quale all'immediatezza di cambiamenti epocali si è purtroppo associata spesso una mancata informativa sulle più elementari nozioni di sicurezza digitale, gli attacchi informatici sono aumentati sfruttando la maggiore esposizione cibernetica dei soggetti attaccati e la minore attenzione degli utenti causata dalla situazione di emergenza, ampliando così la platea dei potenziali rischi da gestire.
L'identificazione, la gestione e la prevenzione di questi rischi attraverso l'automazione costituiscono il fulcro della resilienza digitale aziendale, poiché consentono di incorporare i controlli in modo coerente ed efficiente, a condizione, ovviamente, che le infrastrutture e i processi stessi siano immaginati per essere resilienti.

Questa tesi ha l'obiettivo di proporre un modello prototipale, da applicarsi nel caso di attacco informatico, che possa restituire un indicatore di rischio in base alle variabili utilizzate.

Il lavoro è suddiviso in quattro capitoli.
Nel primo viene analizzato il concetto di rischio dagli albori del pensiero filosofico greco fino ad arrivare ai giorni nostri ed al cyber risk.
Nel secondo viene offerto un excursus normativo soffermandosi sul GDPR 679/2016, sulle linee guida e gli orientamenti dell'EBA, il regolamento DORA, fino all'analisi della Circolare 285 del 17 dicembre 2013 di Banca D'Italia.
Nel terzo capitolo il focus è stato incentrato sugli attacchi ai sistemi informatici delle istituzioni finanziarie. Lo sviluppo della finanza digitale ha infatti ampliato il rischio di manipolazioni fraudolente, di malicious software e di fenomeni riferibili al social engineering. Si rende quindi quanto mai opportuna la definizione di una efficace governance informatica che minimizzi il rischio di successo per questo tipo di attacchi,

governance essenziale per la credibilità stessa delle istituzioni finanziarie e la solidità del rapporto fiduciario con la clientela.
L'insieme di questi passaggi ha costituito la base propedeutica per il completamento del quarto capitolo, ovverosia la predisposizione di un modello prototipale da applicare al verificarsi di uno degli eventi di Data Breach già descritti nell' elaborato.

Il fine ultimo del modello risiede nella restituzione di un indicatore di rischio per ogni evento preso in considerazione, cui consegua l'assegnazione di un punteggio al quale associare dei determinati livelli di rischio.

Vengono infine presentate le conclusioni di questo studio, con l'intento di contribuire alla sensibilizzazione degli addetti ai lavori e della comunità degli utenti sull'evoluzione in atto nel campo della finanza digitale e sull'importanza dei presidi di sicurezza informatica ad esso preposti.
Una risposta efficace alla gravità degli attacchi informatici cui il sistema finanziario è sempre più esposto deve prevedere necessariamente il costante aggiornamento delle procedure interne poste a tutela delle reti aziendali nonché, soprattutto, una proficua attività di formazione ed educazione digitale rivolta al personale delle istituzioni finanziarie ed ai clienti delle stesse.

CAPITOLO 1: IL RISCHIO

1.1 Il concetto di rischio

Il concetto di rischio e le metodologie di contenimento dello stesso sono ormai assurte a veri e propri tratti distintivi delle società contemporanee.
Il nostro modo di essere e, di riflesso, quello della società in cui viviamo, è costantemente condizionato dall'esigenza di monitorare, prevenire ed eventualmente gestire una platea di rischi tendenzialmente sempre più ampia.
Gli eventi potenzialmente dannosi per l'equilibrio individuale e quindi sociale si presentano sottocategorie estremamente diverse, di volta in volta avvertite come preminenti: dall'emergenza sanitaria a quelle imputabili ai cambiamenti climatici in atto (scioglimento dei ghiacciai e siccità come ultimi esempi), dalle minacce alla stabilità globale rivenienti dagli attacchi terroristici (11 settembre, Bataclan) all'incubo di un conflitto bellico alle porte di casa. I rischi sono dunque teoricamente infiniti e possono influenzare direttamente o indirettamente le nostre vite in numerosi modi, dall'impatto sulla sicurezza alla diminuzione della nostra tranquillità, dalle disponibilità reddituali alla qualità dell'ambiente in cui viviamo.
Ma da dove nasce questa interrelazione e come mai il rischio è diventato un elemento così importante nella nostra società?
In primo luogo, dobbiamo considerare, pur non essendone ormai pienamente consapevoli, che il rischio è in realtà un concetto relativamente moderno.
La mitologia greca associava e sovrapponeva a quello che oggi definiamo rischio l'idea del caso, inteso come somma di eventi non altrimenti governabili. La stessa Cosmogonia greca, l'ordine originario del mondo, risentiva di questa impostazione filosofica. Zeus, Poseidone e Ade, dopo epiche battaglie primordiali, si spartirono l'universo giocando con gli astragali (gli antenati ossei dei nostri dadi); e fu così che il caso volle Zeus padrone delle terre, Poseidone dei mari e il perdente Ade relegato negli inferi.
Per i greci il rischio non era il prezzo da pagare per ottenere opportunità, ma essenzialmente la condizione umana di sottoposizione costante a pericoli causali. Gli uomini potevano solo tentare di prepararsi ad affrontarli, ma non a gestirli o evitarli. Nell'antica Grecia il rischio rappresentava unicamente un altro volto del fato e del destino,

quello nefasto. L'uomo non era artefice del proprio destino, il cui corso risiedeva nelle mani spesso capricciose degli Dei e di Zeus primo fra tutti.

L'umanità era costretta a coesistere con la volubilità degli intendimenti divini che condiziona inevitabilmente il corso degli eventi. Questo è un concetto chiave della cultura greca: l'uomo non può illudersi di avere il controllo delle proprie azioni e di ciò che lo circonda.

Il mito di Prometeo[1] imprime nella consapevolezza della società greca il destino di colui il quale osi sfidare Zeus per cambiare il destino dell'umanità.

L'uomo riceve dal Parnaso il fuoco, cioè il controllo del mezzo fondamentale per l'affermarsi della "tecnica" e per la nascita della tecnologia. I mortali si ritrovarono e si percepirono così come "liberi", cioè affrancati dalla volontà divina, consumando un tradimento insopportabile dell'ordine precedentemente costituito che costò a Prometeo una terribile condanna: rimanere incatenato per l'eternità ad una roccia del Caucaso e lì sopportare il dolore lancinante che un'aquila, dilaniandogli il fegato, gli avrebbe procurato in continuazione[2].

La potenza del mito e le sue implicazioni sono alla base delle analisi del filosofo ed antropologo Stefano Maso[3], riflessioni tese all'individuazione di una categoria ontologica in cui il concetto stesso "dell'osare", dell'agire umano, assume una valenza fondamentale.

"Chi è che può "osare", cioè che può ipotizzare di slanciarsi oltre i confini abituali della propria azione e della propria riflessione? Solamente colui che, libero (almeno in parte) da una serie di vincoli, può autonomamente "decidere" di agire in modo autonomo, disposto ad accettare le inevitabili conseguenze della propria decisione. Ciò significa "rischiare", mettere a repentaglio se stessi, il proprio futuro e, in assoluto, la propria vita con il proposito – di fatto paradossale – di "vivere".

Ma che senso ha "rischiare", allorché l'assenza di rischio sembrerebbe comportare un quieto permanere (e cioè un vivere) a proprio agio e, per converso, sembrerebbe escludere di fatto l'incognita del cambiamento e del futuro?"

Questo dilemma, questa antitesi tra l'aspetto razionale e quello emozionale coesistenti all'interno dell'animo umano trovarono una soluzione nel prodigioso sviluppo del

[1] In greco antico: Προμηθεύς, Promethéus, «colui che riflette prima», in latino: Prometheus

[2] "egò d'ho tolmes": io fui colui che osò

[3] Stefano Maso, La Ricerca Folklorica , ottobre 2012, No. 66, Antropologia del rischio (ottobre 2012), pp. 85-95

pensiero filosofico greco, che cominciò a porre un argine alla forza del "mythos"[4] contrapponendo allo stesso la fiducia nel "logòs"[5].

La sintesi perfetta tra questi due aspetti all'apparenza inconciliabili viene raggiunta da Platone nel "Fedone", il dialogo in cui viene descritto l'ultimo giorno di vita di Socrate nella primavera del 399 a. C. Preparandosi a morire Socrate affronta il problema della vita dopo la morte e si prefigura una sopravvivenza per l'anima, così evidenziando l'esistenza di un rischio sia nella vita che nella morte.

La necessità per l'essere umano di correre dei rischi è quindi per Platone evidente, così come il concetto di sfida, di mettersi alla prova, che questo implica.

La sfida non comporta necessariamente l'esistenza di un avversario bensì di un limite specifico che ciascuno interiormente abbia inteso determinare. Il superamento del limite prestabilito necessita sia dell'aiuto che la scienza (sophia) e la tecnologia applicata (technè) offrono ma anche, inevitabilmente, di uno stimolo incosciente in cui l'azzardo (tolan) e l'irrazionale (alogon) incombono.

Nel "Lachete", il dialogo dedicato al coraggio, questa virtù viene delineata come una particolare forza d'animo da mostrare nelle situazioni difficili, supportata dalla scienza, da non confondersi con la temerarietà, una tendenza istintiva prossima alla follia.

L'impegno dell'uomo lungo il corso della sua vita si accompagna quindi alle situazioni di rischio in cui si può arrivare a sperimentare il proprio valore, le proprie competenze tecniche e, più in generale, la propria sapienza. Se tali occasioni di pericolo non si presentassero l'essere umano non potrebbe nemmeno verificare nel concreto il suo carattere ed il suo temperamento.

In definitiva, l'uomo è costretto perennemente a misurarsi con il pericolo e con il fatto di dover rischiare: per riuscire a scegliere la vita migliore per sé stesso deve rincorrere il giusto equilibrio tra le conoscenze acquisite e la sua forza morale.

Con il passaggio dal mondo greco a quello romano l'impostazione filosofica testé descritta esce rafforzata anche dal punto di vista filologico. Alcuni interpreti[6] ravvisano infatti nel verbo latino "resecare" il fondamento della parola rischio, evocando quindi la scelta umana di recidere, di intervenire direttamente in un processo esterno decidendone le sorti.

---

[4] In greco antico: μῦθος «parola, discorso, racconto, favola, leggenda»

[5] In greco antico: λόγος «parola, discorso, ragione»

[6] Giovanni Semerano

Il soggetto che agisce mutando il corso degli eventi è consapevole di misurarsi con gli ostacoli frapposti dalla realtà, di cui accetta il "periculum"[7] che potrà superare solo qualora sia "peritus"[8].

Nel primo Medioevo, tuttavia, la società non percepiva ancora l'evento avverso come fattore condizionante la quotidianità dell'esistenza.

Molti dei pericoli che gli uomini affrontavano in quel periodo, come le epidemie, le carestie, i disastri naturali, venivano semplicemente considerati alla stregua di manifestazioni divine, spesso punitive, con le quali l'uomo doveva imparare a convivere non potendo esercitare sulle stesse alcun controllo.

Unica eccezione a questa convinzione erano gli eventi bellici, variabile umana costantemente presente per secoli, cui probabilmente deve essere attribuita la paternità del vocabolo rischio.

Infatti, sia la radice araba "rizq" che quella bizantina "rizikon" stanno ad indicare il denaro con cui erano pagati i soldati di ventura, quegli uomini cioè che rischiavano per denaro la propria vita.

Altri studiosi fanno risalire l'emergere del concetto di rischio alle prime compagnie di navigazione dell'era premoderna. Secondo Ewald[9] questa nozione apparve per la prima volta nel Medioevo con riferimento al commercio marittimo per indicare i pericoli che mettevano a rischio un viaggio: «a quel tempo, il termine rischio indicava l'eventualità di un pericolo oggettivo, un atto di dio, una forza maggiore, una tempesta o qualche altro pericolo del mare non imputabile a una condotta sbagliata».

Termini come *resecáre* o *risciare* erano usati dai mercanti veneziani dediti al commercio marittimo nel senso di «fendere le onde a ritroso, vogare all'indietro»[10], in modo pericoloso.

In conclusione, è estremamente interessante osservare come la percezione del concetto di rischio si affianchi al progressivo sviluppo all'interno del pensiero occidentale dell'idea dell'uomo come artefice dell'evoluzione e dei cambiamenti sociali.

[7] La cui etimologia, non a caso, deriva dal greco "peira", prova

[8] Esperto, formato nelle arti e nelle scienze

[9] Ewald F. (1993): Two infinities of risk in: Massumi B. (a cura di): The Politics of Everyday Fear - Minneapolis, Minn, University of Minnesota Press, p.226.

[10] L'Oxford English Dictionary sostiene che questa argomentazione si adatti al contesto marittimo di molti primi usi della parola in inglese e nelle lingue romanze

Nel corso del Rinascimento le scoperte scientifiche in tutti i campi, dall'astronomia alla medicina all'architettura, posero definitivamente al centro della Storia l'uomo.
L'essere umano che si avvale delle proprie conoscenze per affinare tecnologie sempre più raffinate consolida il proprio potere sulla natura fino ad affrancarsi definitivamente dalla soggezione divina secondo i principi illuministici prima e positivistici in seguito.
Dalla consapevolezza di poter modificare l'ordine del creato consegue anche l'ardire (o la presunzione…) dell'uomo contemporaneo di voler prevedere ed anticipare gli eventi contrari all'ordine delle cose non più inteso in senso divino ma assolutamente umano.
È in questo contesto logico ed emozionale che maturano le diverse moderne teorie di approccio al rischio e di contenimento e gestione dello stesso in ogni ambito sociale.

1.2.1 L'evoluzione del rischio e gli approcci allo stesso

Nel linguaggio comune spesso il concetto di rischio viene associato ad un'accezione esclusivamente negativa, in quanto riferito all'eventualità del concretizzarsi di eventi negativi o comunque lesivi dell'ordinario assetto (individuale o sociale) delle cose.
Questa interpretazione non è ovviamente accettabile in campo economico, dove il presupposto stesso dell'attività d'impresa è la consapevolezza di dover affrontare la variabilità degli orientamenti e della domanda rivenienti dal mercato.
La comprensione della natura del rischio, la valutazione dello stesso ed il suo contenimento, sono passaggi alla base della nostra economia moderna.
Ogni decisione posta in essere dagli operatori economici nel perseguimento degli obiettivi stabiliti comporta l'assunzione di rischi. Dalle indicazioni operative quotidiane ai compromessi fondamentali in sede di consiglio di amministrazione, il rischio è parte integrante del processo decisionale.
Anche l'inazione, la propensione a differire le decisioni, in realtà sono esse stesse delle scelte, delle assunzioni di rischio in quanto dal non agire derivano sempre delle conseguenze.
L'assunzione del rischio può essere frutto di un approccio istintivo, emotivo (il c. d." sesto senso") così come di una pianificazione attenta che valuti i pro e i contro dei diversi scenari oggetto di valutazione.
Esistono comunque situazioni di rischio che non rientrano nella nostra sfera previsionale o decisionale in quanto insite nelle situazioni, negli eventi che possono manifestarsi e che

in generale derivano da circostanze esterne su cui non è possibile esercitare alcun controllo.

Non sempre il rischio esogeno può essere oggetto di una previsione ragionevole, come nell'ipotesi dei cosiddetti "cigni neri"[11], cioè di accadimenti difficilmente preventivabili.

Il rischio è quindi un fattore immanente, presente in qualsiasi attività o processo umano, da cui può conseguire un evento positivo così come un risultato negativo.

L'analisi del rischio potrebbe essere sintetizzata in una semplice domanda: 'what if ...?' Chiedersi cosa potrebbe accadere a fronte di un evento (normalmente avverso, ma non necessariamente), in modo da configurare gli interventi da porre in essere al verificarsi dello stesso o per prevenirlo.

La valutazione del rischio è ormai comunemente ritenuta una metodologia indispensabile al fine di assicurare la sicurezza e la continuità operativa delle organizzazioni, metodologia supportata da processi, norme e strumenti tecnici. Inserita nelle pratiche migliori e oggetto di certificazioni aziendali, viene sempre più spesso richiesta dal Legislatore (si pensi alla normativa in materia di trattamento dei dati personali) come elemento fondamentale per lo sviluppo di cicli virtuosi di miglioramento continuo e responsabilizzazione.

La gestione del rischio in azienda ha ormai assunto criteri propri delle prassi scientifiche, che ne consentono la ponderazione in sede di formulazione delle strategie e degli obiettivi organizzativi in modo da ottimizzare la performance dell'impresa.

Le metodologie di valutazione e mitigazione aziendale del rischio sono migliorate notevolmente negli ultimi decenni.

Il Global Risks Report rilasciato nell'ambito dell'undicesima edizione del World Economic Forum già nel 2016 poneva ad oggetto della propria analisi "la crescente volatilità, complessità e ambiguità del mondo". Le organizzazioni del lavoro sono chiamate ad affrontare sfide che hanno un forte impatto sull'affidabilità e la fiducia che gli stakeholder richiedono oggi al mercato. Le leadership vengono valutate in virtù delle capacità di "leggere" le opportunità offerte dal contesto economico compatibilmente con un livello di rischio assunto come accettabile anche eticamente. La gestione del cambiamento

[11] La teoria del cigno nero si riferisce a quegli eventi che sono difficili da prevedere nel normale corso degli affari. Si tratta di eventi casuali, inaspettati, ma di grande impatto. Questi eventi sono considerati outlier, perché non esistono dati passati che ne indichino il verificarsi in un futuro prevedibile.

continuo cui è sottoposta qualsiasi attività d'impresa richiede una capacità strategica in cui la corretta valutazione del rischio acquista una centralità prima sconosciuta.
Nel contesto dei mercati finanziari questi assiomi devono essere declinati non solo in funzione preventiva di eventuali perdite o di ricavi inferiori alle attese, ma anche, e soprattutto, in funzione premiale del rischio d'investimento affrontato
I mercati sono quindi arrivati a considerare il rischio come una caratteristica intrinseca, ineliminabile, di ogni attività di business, che per sua natura è caratterizzata dal fatto di espletare i suoi risultati nel futuro che, essendo per definizione non perfettamente intellegibile, può generare differenti esiti.

1.2.2 L'analisi del rischio

Analogamente al World Economic Forum, ed in linea con la sua missione generale, il COSO[12] Board ha commissionato e pubblicato nel 2004 l'Enterprise Risk Management-Integrated Framework.
Il fine ultimo di questa ricerca era quello di offrire al sistema economico e finanziario un valido strumento per bilanciare efficacemente la ricerca di utili elevati con la mitigazione dei rischi necessari per il loro conseguimento: *"value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives." (*Enterprise Risk Management—Integrated Framework, Executive Summary, COSO (2004).)
Nel corso degli anni le sue conclusioni sono state recepite da svariate organizzazioni del lavoro nell'ambito delle politiche aziendali di gestione del rischio.
La necessità di adeguati processi di valutazione del rischio è stata oggetto di specifica regolamentazione in primo luogo da parte delle Autorità competenti nel campo bancario e finanziario, geneticamente più sensibili alle esigenze di tutela degli utenti del mercato,

[12] Il Committee of Sponsoring Organizations of the Treadway Commission (COSO) è un'iniziativa congiunta per combattere le frodi aziendali. È stato fondato negli Stati Uniti da cinque organizzazioni del settore privato, con l'obiettivo di guidare il management esecutivo e gli enti governativi negli aspetti rilevanti della governance organizzativa, dell'etica aziendale, del controllo interno, della gestione del rischio aziendale, delle frodi e dei rapporti finanziari. Il COSO ha stabilito un modello comune di controllo interno rispetto al quale le aziende e le organizzazioni possono valutare i propri sistemi di controllo.

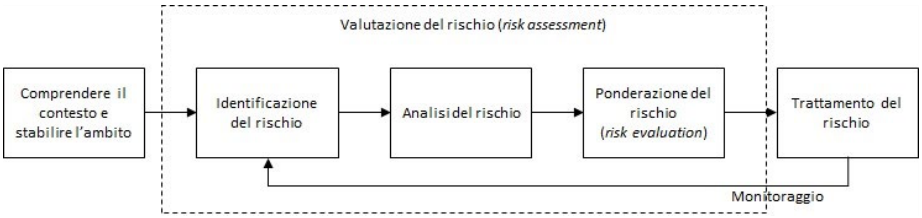
per poi interessare anche altri comparti economici in cui le governance aziendali devono essere supportate da un efficace quadro normativo.

Ovviamente ogni istituzione, finanziaria e non, presenta caratteristiche propria che influenzano le modalità di gestione e monitoraggio del rischio. Per determinare e applicare tali fattori è utile applicare un quadro di gestione del rischio come parte di un approccio globale alla pianificazione, all'esecuzione e al monitoraggio della gestione complessiva dei vari rischi.

È inoltre importante tenere presente che l'obiettivo del processo di gestione del rischio, nel contesto di un quadro di riferimento ampio, non può essere certo quello di eliminare completamente tutti i rischi, ma di determinare livelli accettabili degli stessi. I processi operativi interni devono essere quindi tesi a contenere i fattori di rischio entro i limiti prestabiliti.

I passi che seguono aiutano a determinare e ad applicare azioni specifiche a tal fine.

Figura 1: Valutazione del rischio



Fonte: Clusit – Associazione Italiana per la Sicurezza Informatica

Il processo di gestione del rischio si articola in diverse fasi:

1. Identificazione degli obiettivi e del Risk Appetite

La definizione degli obiettivi aziendali deve essere preliminarmente supportata dall'analisi degli eventuali rischi che il perseguimento delle dette finalità comporta.

In altre parole, è necessario chiedersi fino a che punto vogliamo spingerci per ritenerci soddisfatti dei risultati raggiunti, quale sia il nostro "appetito". Un piano di sviluppo aziendale che non sia accompagnato da una ponderazione realistica degli eventuali imprevisti, scostamenti, da affrontare espone inesorabilmente l'attività d'impresa al rischio concreto di porsi degli obiettivi difficilmente raggiungibili o di impegnare risorse

economiche ed umane in modo eccessivo e sproporzionato. L'efficiente allocazione delle risorse a disposizione è un tema centrale per la pianificazione degli investimenti, soprattutto in un'industria particolare come quella finanziaria caratterizzata da una volatilità estrema. Il vincolo cui riferirsi deve essere quindi la definizione del proprio capitale di rischio. Questo principio ha assunto rilevanza strategica in occasione della gravissima crisi dei sub prime[13] che nel 2008 / 2009 dagli Stati Uniti si è propagata all'intero sistema finanziario mondiale. La rincorsa continua di livelli di target sempre più elevati, unita ad una remunerazione eccessiva dei vertici aziendali legata esclusivamente ai profitti di breve periodo, aveva portato a sottostimare il processo di valutazione dei rischi relegandolo ad un aspetto puramente tecnico/formale e svilendone la funzione strategica. Alla luce dell'instabilità globale dei mercati finanziari, il Comitato di Basilea ha individuato delle regole stringenti per risolvere il problema dello scollamento tra le decisioni strategiche delle istituzioni finanziarie e l'effettiva ponderazione dei rischi in queste insite. È stato introdotto l'obbligo per gli organi decisionali delle banche di formalizzare il Risk Appetite così da rapportarlo al patrimonio aziendale. Il Financial Stability Board ha poi esteso a tutte le istituzioni finanziarie il suddetto obbligo di formalizzazione facendolo confluire nel Risk Appetite Statement, rappresentativo della complessiva propensione al rischio dell'intera azienda. In ottemperanza a questi interventi, il Risk Appetite aziendale deve essere sempre minore o uguale rispetto alla Risk Capacity.

2. Individuazione dei rischi.

La seconda fase del processo di valutazione dei rischi consiste nella mappatura dei potenziali eventi avversi. Questo processo deve avviarsi con la revisione delle finalità, degli obiettivi d'impresa comparandoli con le risorse a disposizione. I professionisti del

[13] La crisi finanziaria del 2007-08, detta anche crisi dei mutui subprime è stata una grave contrazione della liquidità nei mercati finanziari globali che ha avuto origine negli Stati Uniti a seguito del crollo del mercato immobiliare statunitense. Ha minacciato di distruggere il sistema finanziario internazionale; ha causato il fallimento (o quasi) di diverse grandi banche d'investimento e commerciali, istituti di credito ipotecario, compagnie assicurative e associazioni di risparmio e prestito; ha fatto precipitare la Grande Recessione (2007-09), la peggiore recessione economica dalla Grande Depressione (1929-c. 1939).

rischio spesso applicano un approccio top-down e bottom-up per individuare gli elementi di rischio. La parte top-down considera i programmi mission-critical che non dovrebbero mai essere compromessi (come le transazioni di vendita in un negozio al dettaglio o i processi produttivi in una fabbrica), per poi individuare le condizioni che potrebbero compromettere l'effettivo raggiungimento degli obiettivi prefissati. La parte bottom-up, invece, prende in considerazione le diverse potenziali fonti di minaccia conosciute (terremoti, attacchi ransomware, crisi economiche) per poi riflettere sull'impatto che potrebbero avere sull'azienda. Poiché il rischio è, per definizione, qualsiasi incertezza che possa influire sugli obiettivi, un rischio è tale solo se ha un impatto. Più si ritiene che un rischio possa avere un impatto, maggiore sarà la priorità della sua mitigazione.

L' "Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)" fornisce indicazioni sullo sviluppo degli scenari di rischio. Secondo il rapporto, per configurare un rischio potenzialmente dannoso è necessario che ricorrano i seguenti quattro elementi:

a) un bene o una risorsa di valore che verrebbe colpita;
b) una fonte di un'azione minacciosa che agisca contro quella risorsa;
c) una condizione preesistente (o vulnerabilità) che consenta alla fonte della minaccia di agire;
d) un impatto dannoso derivante dallo sfruttamento della vulnerabilità da parte della fonte della minaccia.

Alla luce di questi elementi è possibile configurare un'ampia serie di scenari di rischio da analizzare, classificare e trattare. Descrivere il rischio come scenario aiuta a comunicare le condizioni di rischio, ad analizzare la probabilità e l'impatto dello stesso nonché ad individuare idonee misure preventive. Nel considerare i vari tipi di rischio risulta sicuramente utile organizzarli in categorie, così da facilitarne il monitoraggio da parte di società specializzate. Il Committee of Sponsoring Organizations of the Treadway Commission, un'iniziativa congiunta di organizzazioni professionali che fornisce indicazioni sulla gestione del rischio, ha suggerito un'organizzazione dello stesso nelle seguenti quattro aree:

a) rischio strategico (reputazionale, relazionale, d'innovazione tecnologica);

b) rischio finanziario e di reporting (volatilità del mercato, legislazione fiscale, accesso al credito);
c) rischio di compliance e governance (codici etici, assetto regolamentare, relazioni internazionali, profili di privacy);
d) rischio operativo (sicurezza informatica e tecnologica, normativa sulla privacy, filiera di approvvigionamento, problemi di lavoro, disastri naturali).

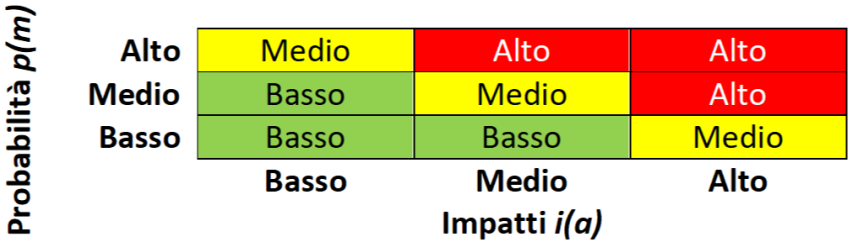
Le categorie di rischio aiutano anche a integrare le informazioni, consentendo al management di pianificare gli interventi di mitigazione, di aggiornare gli scenari operativi di contesto e di individuare gli strumenti utili al contenimento degli eventi avversi.

3. Analisi della probabilità e dell'impatto del rischio

Il presupposto ultimo perché un evento si definisca fattore di rischio è che dallo stesso possa verificarsi un impatto e che questo sia misurabile. I diversi fattori esterni o interni al processo economico che siano potenzialmente in grado di determinare danni all'attività imprenditoriale devono poter essere ponderati in maniera tale da creare una scala di priorità dei rischi da contrastare. Le misure di contrasto e mitigazione del rischio comportano infatti costi importanti per l'approntamento di strumenti tecnici ed organizzativi, costi che devono essere sopportati in misura proporzionale all'intensità prevista del danno. Le politiche aziendali di gestione dei rischi non potranno essere quindi improntate all'esigenza di rispondere indiscriminatamente a tutti i rischi, ma solo a quelli sufficientemente grandi ed il cui impatto sia stimato come rilevante. Le metodologie di analisi del rischio hanno nel corso degli anni assunto una propria rilevanza scientifica nella determinazione delle probabilità che un evento si verifichi e nello stimare l'impatto delle conseguenze che ne deriverebbero. Calcolare l'impatto di un rischio è attività particolarmente complessa in quanto presuppone l'analisi di eventi non necessariamente immediati ma spesso procrastinati nel medio lungo periodo. Molte organizzazioni del lavoro utilizzano termini generali o qualitativi per esprimere questi valori. Una matrice di probabilità e impatto è una griglia per la mappatura della probabilità di accadimento di ciascun rischio e del relativo impatto sugli obiettivi del progetto nel caso in cui tale rischio si verifichi. La tecnica qualitativa più diffusa, che permette di giungere a un ordinamento dei rischi individuati, è la "matrice probabilità-impatto". Si basa sulle due componenti del rischio, la probabilità che si verifichi e l'impatto sugli obiettivi nel caso in cui si manifesti.

La matrice è una griglia bidimensionale che mappa la probabilità che i rischi si verifichino e il loro effetto sugli obiettivi del progetto. Il punteggio del rischio, spesso indicato come livello o grado di rischio, viene calcolato moltiplicando i due assi della matrice. Rischio = Impatto x Probabilità. Questa formula considera da un lato le probabilità che un certo rischio si concretizzi e dall'altro l'entità del suo effetto. La dimensione di un rischio si calcola moltiplicando questi due elementi: probabilità e conseguenze. Poiché l'impatto e la probabilità possono essere descritti sia in modo relativo che numerico, anche il punteggio di rischio viene definito nello stesso modo. Più alte sono le valutazioni combinate, più alto è il punteggio e quindi il livello di rischio. Queste valutazioni sono generalmente definite da basso ad alto o da molto basso a molto alto. Le valutazioni della probabilità e dell'impatto vengono effettuate utilizzando le opinioni raccolte durante le interviste. Queste valutazioni devono essere classificate da ciascuna organizzazione in modo specifico per ogni attività. Ogni istituzione, finanziaria e non, è chiamata a stabilire il proprio grado di tolleranza del rischio. La predisposizione di queste scale dei livelli di impatto e probabilità può contribuire a ridurre l'influenza di eventuali pregiudizi nella mappatura dei rischi. I risultati delle matrici di rischio vengono utilizzati per stabilire la priorità degli stessi, identificarli per una loro valutazione quantitativa, pianificare la risposta aziendale, delineare una guida nell'allocazione delle risorse. Attribuendo un punteggio la matrice consente di suddividere i rischi del progetto in gruppi di priorità. Particolare attenzione deve essere posta alla valutazione della qualità dell'obiettivo influenzato dal rischio: un evento che configuri un elevato rischio per la sicurezza o la salute dovrà essere ponderato prioritariamente rispetto ad un altro che presenti un rischio finanziario anche molto elevato.

Figura 2: Matrice del rischio



Fonte: Clusit – Associazione Italiana per la Sicurezza Informatica

I rischi sono valutati in termini di rischio inerente (rischio in assenza di qualsiasi intervento) e di rischio residuo (rischio residuo dopo aver attuato interventi per ridurlo). Il rischio *inerente* è il rischio che grava su un'organizzazione in assenza di qualsiasi azione in grado di alterare la probabilità e/o l'impatto del rischio stesso; rappresenta l'impatto lordo di un fattore di rischio, cioè la massima perdita realizzabile in seguito al suo manifestarsi e alla mancanza di azioni tese a limitarne gli effetti.
Il rischio *residuo* è il rischio che rimane dopo la risposta al rischio, cioè dopo l'effettiva implementazione delle azioni tese alla mitigazione del rischio inerente. La differenza tra i benefici dell'azione e gli effetti complessivi che i fattori di rischio hanno sugli obbiettivi aziendali determina il rischio residuo, cioè l'impatto netto riconducibile ai fattori di rischio. Il processo di valutazione dei rischi si focalizza prima sui rischi inerenti e successivamente dopo lo sviluppo di adeguate risposte al rischio, su quelli residui.

4. Definizione dei piani di risposta al rischio

Una volta individuati i rischi e definita la scala di priorità degli stessi, si rende necessario procedere alla valutazione delle opzioni disponibili per il loro controllo e mitigazione. Gli strumenti utili al raggiungimento di un livello di rischio ritenuto accettabile sono molteplici. Se il rischio, in base al Risk Appetite Statement, sia già ponderato come sopportabile non sono, ovviamente, necessari ulteriori trattamenti di sorta. Qualora si configuri l'eventualità di condividere una parte dell'impatto con altra istituzione (ad esempio, una compagnia assicurativa, un fornitore di servizi), tecnicamente sarà possibile trasferire all'esterno dell'azienda una parte del rischio.

Se invece non risulti possibile applicare alcuno strumento di contenimento del rischio, i responsabili aziendali saranno tenuti ad eliminare le attività o le esposizioni che prefigurerebbero lo scenario in esame. I piani di gestione del rischio, qualsivoglia sia la tipologia degli eventi valutati, devono essere comunque economicamente sostenibili, prevedendo una commisurazione ottimale tra il valore delle attività censite e le risorse da destinare alla loro protezione.

5. Monitoraggio dei risultati della gestione del rischio.

L'intero processo di mappatura e classificazione dei rischi in virtù della loro probabilità di produrre impatti negativi, nonché i piani aziendali di contenimento e mitigazione degli eventuali danni, deve essere costantemente sottoposto a monitoraggio affinché corrisponda in ogni momento alla policy definita dagli organi decisionali dell'azienda. Le condizioni di rischio possono infatti cambiare rapidamente, i valori degli asset fluttuare e le preferenze degli stakeholder modificarsi. Un aspetto fondamentale dell'attività di monitoraggio consiste nell'assicurare un flusso informativo in tempo reale al management aziendale cosicché venga aggiornato sui progressi attuativi dei piani di gestione del rischio e sulle eventuali modifiche agli stessi da cui potrebbero risultare degli impatti organizzativi. Man mano che i vari team dell'organizzazione intraprendono azioni per identificare, analizzare e rispondere ai rischi, i risultati delle stesse a loro volta informano e perfezionano l'iterazione successiva.

1.3 La Percezione Del Rischio

Che se ne abbia o meno la consapevolezza, la maggior parte delle decisioni individuali vengono assunte considerando l'esposizione o meno a determinate tipologie di rischio. A differenza degli specialisti del settore, la percezione del rischio della maggior parte delle persone non deriva da sofisticate valutazioni dello stesso o da modelli matematici. Non passiamo la giornata a calcolare costantemente se ci possa accadere o meno qualcosa di negativo, tendiamo invece ad affidarci a giudizi più intuitivi sul rischio.
Questi giudizi intuitivi si definiscono tipicamente percezioni del rischio, percezioni influenzate dal nostro modo di essere, dal nostro vissuto e dai condizionamenti esterni cui siamo sottoposti. In definitiva, sono giudizi soggettivi che gli individui esprimono sulle caratteristiche, la gravità e la probabilità del rischio. Alcuni rischi non suscitano un grande

senso di paura: li corriamo deliberatamente giorno per giorno, ad esempio guidando troppo velocemente. Altri rischi incutono una grande paura, come un attacco terroristico, ma la probabilità di essere vittima di un incidente stradale è maggiore rispetto a quella di essere coinvolti in atti di terrorismo. Come possiamo spiegare questa discrepanza e quali fattori influenzano la nostra percezione del rischio?

Lo studio scientifico sulla percezione del rischio cerca di rispondere ad alcune di queste domande.

Questa tematica ha riscosso sempre più attenzione a partire dagli anni '60 e sorge dall'osservazione della diversa percezione dei rischi insiti nell'adozione di nuove tecnologie da parte degli esperti in materia rispetto alla generalità del pubblico. Molte delle prime ricerche sulla percezione del rischio si sono quindi concentrate sull'esistenza di un divario di conoscenze, di informazioni tra la categoria dei tecnici e la platea dei consumatori. Si presumeva che se questi ultimi avessero potuto accedere alle nozioni scientifiche e comprenderle, molto probabilmente le considerazioni su determinati rischi sarebbero state simili a quelle degli esperti.

Tuttavia, nel corso degli anni successivi la ricerca ha rivelato che la conoscenza non è l'unico fattore che determina la percezione del rischio. Quali sono dunque questi altri fattori?

In genere percepiamo i rischi che conosciamo bene come meno pericolosi rispetto a quelli a noi meno noti: abbiamo meno paura dei rischi associati a una radiografia in ospedale in confronto a quelli rivenienti dalla vicinanza di una centrale nucleare.

In secondo luogo, tendiamo a considerare certe attività più rischiose quando abbiamo un grado di controllo personale molto basso su di esse.

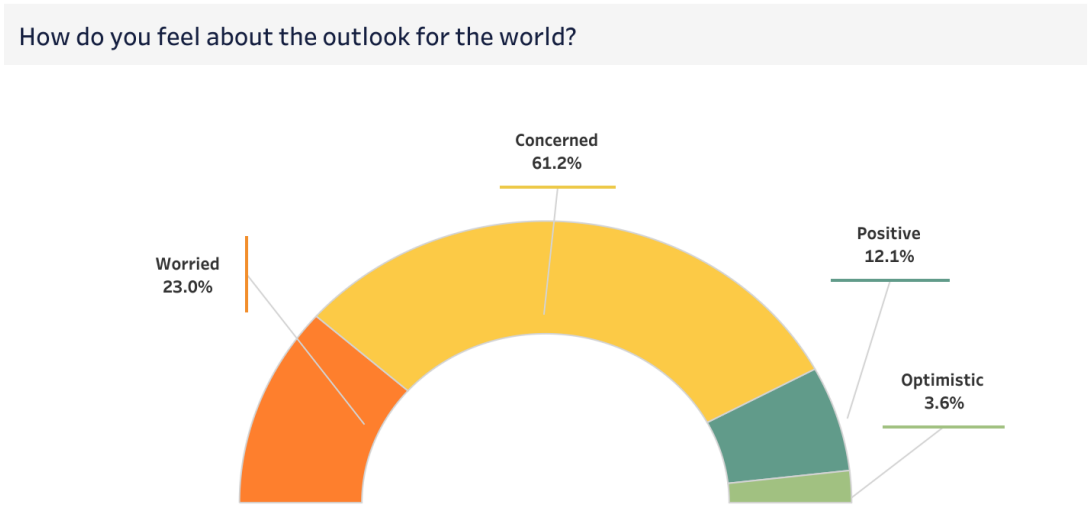
Infine, la nostra percezione del rischio è influenzata dalla volontarietà o meno dell'esposizione allo stesso.

Il World Economic Forum ha pubblicato quest'anno la 17esima edizione del 'Global Risk Report' con l'obbiettivo di analizzare la percezione dei rischi a livello globale.

È stato chiesto a 100 esperti e decision maker dei vari settori dell'economia globale di tracciare un bilancio degli ultimi due anni per capire un po' di più dove si trovasse il mindset globale. Da questo sondaggio è emerso che i rischi sociali - sotto forma di "erosione della coesione sociale", "crisi dei mezzi di sussistenza", "deterioramento della salute mentale" – sono quelli percepiti come maggiormente pericolosi a seguito della crisi pandemica globale.

Se ai rischi sociali si affiancano anche quelli rivenienti dalla grave instabilità geopolitica ed economica indotta dal conflitto in Ucraina o dalle tensioni intorno a Taiwan, non risulterà sorprendente l'insorgenza di una visione pessimistica del prossimo futuro. Solo il 16% degli intervistati infatti manifesta fiducia ed ottimismo sulle prospettive del mondo e solo l'11% ritiene che la ripresa globale accelererà. La maggior parte dei partecipanti allo studio prevede invece che i prossimi tre anni saranno caratterizzati da una volatilità costante e da molteplici incognite, oppure da traiettorie frammentate che determineranno una frattura netta tra la minoranza che ne trarrà vantaggi e la maggioranza che ne sarà travolta.

Figura 3: Visione del futuro



Fonte: World Economic Forum Global Risks Perception Survey 2021-2022

Le conseguenze economiche e sociali della pandemia da Covid-19[14] continuano a rappresentare una potenziale minaccia per l'economia globale le cui prospettive di crescita per il 2024 risultano essere inferiori del 2,3% rispetto allo scenario teorico depurato dagli effetti dell'emergenza sanitaria.

Il rapporto sui rischi globali evidenzia che nei prossimi 5-10 anni le maggiori preoccupazioni per la coesione sociale ed economica sono rappresentate dai cambiamenti climatici, in particolare dagli eventi metereologici estremi e dalla scomparsa della

[14] La pandemia COVID-19, nota anche come pandemia da coronavirus, è una pandemia globale in corso di malattia da coronavirus 2019 (COVID-19) causata dal coronavirus 2 della sindrome respiratoria acuta grave (SARS-CoV-2).

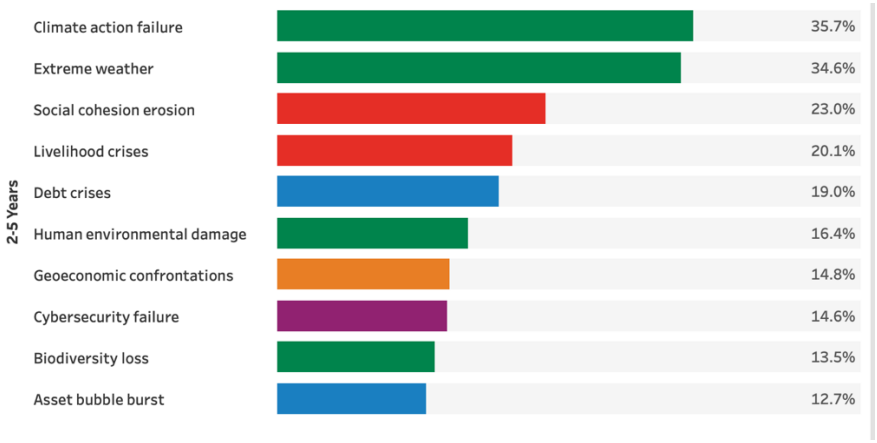
biodiversità, nonché dall'eventuale fallimento delle politiche di contenimento degli stessi a livello globale.

Gli impatti economici della pandemia e delle crisi geopolitiche in atto (Ucraina e Taiwan in primis) si riflettono pesantemente sulle catene di approvvigionamento dei prodotti improvvisamente ristrette, sui prezzi delle materie prime (alimentari ed energetiche) sottoposti ad aumenti incontrollati, traducendosi in un tasso inflattivo tornato ai livelli degli anni '70 del secolo scorso.

A questo scenario corrisponde una crescita dei diversi debiti pubblici (in primis quello italiano) cui molto difficilmente le Banche Centrali potranno rispondere ancora con politiche monetarie espansive, mettendo così a rischio la realizzazione dei piani nazionali di transizione ambientale, infrastrutturale ed economico-sociale europei (PNRR). Un' eventuale crisi dei debiti sovrani simile a quella vissuta nel 2008-2011 rappresenta per gli intervistati una ulteriore fonte di preoccupazione.

I rischi tecnologici, come la "disuguaglianza digitale" e il "fallimento della cybersicurezza", sono avvertiti come minacce critiche a breve e medio termine ma non nel lungo periodo, così determinando un possibile punto cieco nella percezione del rischio.

Figura 4: Percezione del Rischio



Fonte: World Economic Forum Global Risks Perception Survey 2021-2022

Il GRPS 2021-2022 ha incluso anche delle domande circa l'efficacia delle politiche internazionali di mitigazione del rischio.

"Intelligenza artificiale", "sfruttamento dello spazio", "attacchi informatici transfrontalieri e disinformazione", "migrazione e rifugiati" sono le aree in cui la maggior parte degli intervistati ritiene che lo stato attuale degli sforzi di attenuazione del rischio non siano all'altezza delle sfide poste, ovvero che gli stessi risultino "non avviati" o in "fase iniziale di sviluppo".
Per quanto concerne invece alla "facilitazione del commercio, alla "criminalità internazionale" e alle "armi di distruzione di massa", la maggior parte degli intervistati ritiene che gli sforzi di mitigazione del rischio siano "consolidati" o "efficaci".
Per quanto attiene specificatamente al mondo imprenditoriale, l'attenzione è principalmente rivolta all' ESG[15] ed è sempre più evidente che livelli ottimali di governance aziendali ed una effettiva capacità di resilienza si possano ottenere realisticamente soltanto con piani di gestione del rischio collaborativi, credibili e sofisticati.
Gli attacchi informatici non costituiscono una novità assoluta, ma la loro intensificazione negli ultimi due anni induce a ritenere che tali minacce stiano crescendo più rapidamente della capacità di prevenirle e gestirle efficacemente.

Le aziende sopravvissute alla crisi pandemica sono state indotte dal mercato ad intensificare le politiche tese all'automazione e digitalizzazione dei processi produttivi, ma nonostante questi ingenti sforzi permane l'utilizzo di tecnologie obsolete che hanno consentito una maggiore esposizione agli attacchi informatici. La percezione del rischio risulta molto alta quando riferita alla possibilità di fallimenti di infrastrutture critiche, ai furti di identità digitali, alle modifiche procedurali interne per adeguarsi a dettami normativi sempre più stringenti e, in particolare, alla possibile incapacità di realizzare efficacemente la trasformazione digitale delle imprese.

1.4.1 Il Rischio Operativo

Il rischio operativo può essere definito come l'eventualità che le operazioni aziendali falliscano a causa di inefficienze o guasti nei processi interni, nelle persone e nei sistemi d'impresa.

[15] Environmental, social and corporate governance

Con riferimento specifico al comparto bancario, il "Comitato di Basilea[16] per la vigilanza bancaria" ha descritto il rischio operativo come il *"rischio di perdite derivanti da processi interni, persone, sistemi o eventi esterni inadeguati o falliti"*.

1.4.2 La Circolare 263 di Banca d'Italia e il Comitato di Basilea

A livello di regolatore nazionale la Banca d'Italia (Circolare n. 263 "Nuove disposizioni di vigilanza prudenziale per le banche" - Titolo II – Capitolo 5) intende il rischio operativo come "*il rischio di subire perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni".*
L'ambito di applicazione del rischio operativo è quindi estremamente ampio e arriva ad includere eventi negativi anche molto diversi tra di loro, come le frodi, la violazione della sicurezza aziendale, le minacce ai dati personali sensibili, i rischi legali, i rischi fisici (come la indisponibilità dei sistemi) o ambientali (catastrofi naturali). La cennata Circolare della Banca d'Italia n. 263, nello specificare che nel rischio operativo è compreso il rischio legale, non include nello stesso i rischi strategici e di reputazione.
I rischi operativi possono avere un impatto notevolmente ampio sull'attività d'impresa nel suo complesso, essendo in grado di condizionare la soddisfazione dei clienti, la reputazione aziendale, la creazione di valore per gli azionisti e, più in generale, di aumentare al contempo la volatilità dei risultati operativi.
Tutti questi rischi devono essere gestiti con un approccio gestionale sempre più sofisticato che garantisca all'azienda di prosperare e crescere, nella consapevolezza, comunque, che il rischio operativo è connaturato all'attività d'impresa.

Prima delle revisioni normative in materia di vigilanza bancaria introdotte in occasione di "Basilea II"[17], il rischio operativo era considerato una categoria residuale in cui annoverare le tipologie di rischi di difficile quantificazione e mitigazione, il cosiddetto "paniere degli altri rischi".

[16] Il Comitato di Basilea per la vigilanza bancaria è un comitato di autorità di vigilanza bancaria istituito nel 1975 dai governatori delle banche centrali dei Paesi del Gruppo dei Dieci. È composto da alti rappresentanti delle autorità di vigilanza bancaria e delle banche centrali di Belgio, Canada, Francia, Germania, Italia, Giappone, Lussemburgo, Paesi Bassi, Spagna, Svezia, Svizzera, Regno Unito e Stati Uniti. Si riunisce solitamente presso la Banca dei Regolamenti Internazionali a Basilea, dove ha sede il suo Segretariato permanente.
[17] International Convergence of Capital Measurement and Capital Standards

Infatti, la definizione che precedentemente era stata fatta propria da "Basilea I" era sostanzialmente di carattere negativo: per rischio operativo si intendeva qualsiasi rischio che non fosse di mercato o di credito. In virtù di questa interpretazione quindi, diverse istituzioni creditizie erano use associare il concetto di rischio operativo a quello non finanziario.
Nell'ottobre 2014, come detto, il Comitato di Basilea per la vigilanza bancaria ha proposto una revisione dello schema di capitale per il rischio operativo, prevedendo un nuovo approccio standardizzato in sostituzione di quello tradizionalmente utilizzato per calcolare il capitale necessario alla mitigazione di questo rischio.
In sostanza le banche, per poter affrontare i rischi operativi senza timore di compromettere gravemente la propria attività, devono disporre di requisiti patrimoniali in grado di sopportare i danni rivenienti dal verificarsi di eventi dannosi riconducibili all'operatività compromessa.
Queste indicazioni sono state recepite in Italia con la detta Circolare n. 263, che ha previsto tre metodi di calcolo del requisito patrimoniale (Base – Standardizzato – Avanzato) tra di loro differenti a seconda delle dimensioni del soggetto vigilato e della esposizione al rischio operativo. In particolare, le banche che utilizzano il metodo Avanzato devono disporre di una specifica funzione di controllo sui rischi operativi deputata, tra l'altro, "alla progettazione, allo sviluppo e alla manutenzione dei sistemi di gestione e di misurazione dei rischi operativi e alla determinazione del requisito patrimoniale". Stante questa maggiore complessità ed onerosità sia patrimoniale che organizzativa, l'utilizzo del metodo avanzato è subordinato ad autorizzazione specifica della Banca d'Italia secondo le modalità previste dalla Circolare n. 288 "Disposizioni di Vigilanza per gli intermediari finanziari" (Titolo I – Capitolo 10).
Il vigente assetto normativo ha istituzionalizzato il rischio operativo come categoria oggetto non solo di attenzione da parte delle Autorità di regolamento ma anche, e soprattutto, di interventi organizzativi degli organi strategici delle istituzioni bancarie, instaurando così un collegamento diretto tra l'efficace gestione del rischio operativo e una sana governance aziendale.

Eventi come gli attentati terroristici dell'11 settembre, le perdite da trading illecito di Société Générale, Barings, AIB, UBS e National Australia Bank, hanno tutti contribuito alla

maturazione definitiva nel settore bancario della consapevolezza che l'approccio alla gestione del rischio debba andare ben oltre il semplice rischio di mercato e di credito.
Le tipologie di rischi (e, in particolare, la loro portata) che le banche si trovano oggi ad affrontare spaziano dalle frodi ai guasti dei sistemi informatici, dalle semplici controversie con la clientela o i dipendenti fino agli atti di terrorismo. Tutti questi eventi avversi, così diversi tra di loro, vengono generalmente classificati nella categoria del "rischio operativo".
L'identificazione e la misurazione del rischio operativo è un problema reale e vivo per il sistema bancario contemporaneo, in particolare dopo la citata decisione del Comitato di Basilea per la vigilanza bancaria di introdurre un requisito patrimoniale specifico per questo tipo di rischio come parte del nuovo quadro di adeguatezza patrimoniale.

1.4.3 La gestione del rischio operativo

In linea teorica il rischio operativo comprende tutti gli accadimenti, come gli errori umani che si traducano in opportunità di business mancate, dai quali possa derivare un impatto sulla performance complessiva dell'organizzazione e sulla sua capacità di creare valore.
Il presupposto di una efficiente gestione del rischio operativo si basa sul principio che le attività di controllo, monitoraggio e garanzia della continuità operativa debbano basarsi su una valutazione complessiva dei rischi cui l'azienda è esposta, così da portare alla identificazione e classificazione degli stessi in funzione della loro pericolosità.
Nel determinarne l'importanza quindi, il rischio deve essere valutato in base alla probabilità di accadimento ed all'eventuale successivo impatto sull'organizzazione aziendale.
L'impatto non può essere valutato esclusivamente in termini di valore finanziario perduto, come accadeva con le metodologie tradizionali, ma inserito in un contesto più ampio riferito al raggiungimento degli obiettivi strategici dell'impresa, in primis quella bancaria. Il processo di mappatura del rischio operativo deve quindi valutare l'intera filiera che porta alla generazione di valore, dall'individuazione e generazione di un prodotto alla sua distribuzione e vendita.
Una mappatura della specie arriverà quindi a comprendere sia gli eventi di relativa rilevanza sia quelli che potrebbero mettere potenzialmente a repentaglio l'esistenza stessa dell'azienda, senza sottovalutare le conseguenze di alcuno di essi.

I danni conseguenti al verificarsi dei rischi operativi possono essere significativi nonché diversi per tipo e gravità; perdite dirette (costi di gestione dei guasti del sistema e degli errori di elaborazione), spese generali di regolamentazione (costi di audit e indagini obbligatorie), e danni alla reputazione conseguenti ad attività fraudolente e pratiche sleali.
A differenza degli altri rischi "tradizionali" (di credito, di mercato, assicurativo), i rischi operativi di solito non sono assunti volontariamente né sono determinati dai ricavi. Inoltre, non sono diversificabili e non possono essere eliminati. Ciò significa che finché le persone, i sistemi e i processi rimangono imperfetti, il rischio operativo, per definizione, non può essere completamente eliminato.

Esso è tuttavia gestibile in modo tale da contenere le perdite entro un determinato livello di tolleranza al rischio (ossia la quantità di rischio che si è disposti ad accettare per perseguire i propri obiettivi), quantificato bilanciando i costi del miglioramento con i benefici attesi. Tendenze più ampie come la globalizzazione, l'espansione di Internet e l'ascesa dei social media, nonché la crescente richiesta di una maggiore responsabilità aziendale a livello mondiale, sono tutti eventi che rafforzano la necessità di una corretta gestione del rischio.

1.4.4 Le sette tipologie di eventi

Al riguardo, si elencano di seguito le sette tipologie di eventi ufficialmente censiti in occasione di "Basilea II", corredati da alcuni esempi propri di ciascuna categoria:

- *Frode interna*: appropriazione indebita di beni, evasione fiscale, errata indicazione intenzionale di posizioni, corruzione
- *Frode esterna*: furto di informazioni, danni da hacking, furto e falsificazione da parte di terzi.
- *Pratiche di impiego e sicurezza sul posto di lavoro*: discriminazione, risarcimento dei lavoratori, salute e sicurezza dei dipendenti.
- *Clienti, prodotti e pratiche commerciali*: manipolazione del mercato, antitrust, commercio improprio, difetti dei prodotti, violazioni fiduciarie, churning dei conti.
- *Danni alle attività fisiche*: disastri naturali, terrorismo, vandalismo.

- *Interruzione dell'attività e guasti ai sistemi:* interruzioni di servizio, guasti al software, guasti all'hardware.
- *Esecuzione, consegna e gestione dei processi:* errori di inserimento dati, errori contabili, mancato reporting obbligatorio, perdita negligente di beni del cliente

Il prerequisito essenziale ai fini della corretta gestione e misurazione del rischio operativo è quello di procedere ad una definizione dello stesso non generalizzata ma tarata sulle dimensioni e peculiarità della singola azienda. Ogni banca, o più precisamente ogni gruppo bancario, deve sviluppare una definizione di rischio operativo coerente con le proprie caratteristiche aziendali e organizzative, nell'ambito di una visione integrata e coordinata della gestione del rischio. È quindi possibile, e probabilmente opportuno, che la definizione aziendale di rischio operativo non sia uniforme e omogenea per tutti i gruppi bancari e tutte le banche. Pertanto, da questo punto di vista il rischio operativo si differenzia dalle altre categorie di rischio per le quali esiste invece da tempo una definizione univoca, chiara e coerente.

Il 15° aggiornamento della più volte menzionata Circolare 263 della Banca d'Italia detta al riguardo delle disposizioni specifiche con le quali viene richiesta ai vertici delle banche una particolare attenzione alla definizione delle politiche e dei processi aziendali di maggior rilievo, "quali quelli riguardanti la gestione dei rischi, lo sviluppo e la convalida dei modelli interni di misurazione dei rischi non utilizzati a fini regolamentari". In particolare, le norme enfatizzano il ruolo dell'organo con funzione di supervisione strategica nella definizione del modello di business e del Risk Appetite Framework; a tale organo viene richiesto anche di "favorire la diffusione di una cultura dei controlli attraverso l'approvazione di un codice etico al quale sono tenuti a uniformarsi i componenti degli organi aziendali e i dipendenti".

La Circolare evidenzia come, diversamente dagli altri rischi di "primo pilastro", per i quali la banca, in base alla sua propensione al rischio, assume consapevolmente posizioni creditizie o finanziarie per raggiungere il desiderato profilo di rischio/rendimento, l'assunzione di rischi operativi risulta implicita nella decisione di intraprendere un determinato tipo di attività. "In tale contesto, il sistema dei controlli interni deve costituire il presidio principale per la prevenzione ed il contenimento di tali rischi". Una specifica

attenzione deve essere assicurata alla valutazione del rischio informatico (rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione) e del rischio informatico residuale, ovverosia quello cui l'intermediario è esposto una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi.

1.4.5 I rischi informatici

In apparenza, i rischi informatici e alcuni altri rischi operativi sono molto simili. Infatti, entrambi possono comportare il malfunzionamento di un processo o di una tecnologia che potrebbe paralizzare un'azienda e potenzialmente avere conseguenze ancora più ampie.

In realtà però, come evidenziato da un recente studio[18] ad un'analisi più attenta il cyber risulta speciale sotto due aspetti:
a) il modo in cui si verifica lo shock;
b) l'impatto dello shock dopo che si è verificato.

Sebbene la trasmissione all'economia in generale avvenga attraverso canali noti, la natura unica dello shock e l'impatto successivo implicano che la risposta normativa appropriata sarà probabilmente diversa.
La minaccia informatica può assumere più di una forma. Alcuni attacchi causano l'interruzione dei sistemi informatici, rallentando o bloccando completamente i processi critici. Altri colpiscono i dati che supportano tali processi, ottenendo un accesso non autorizzato o corrompendo i dati.
Entrambi i tipi di shock informatici hanno caratteristiche comuni, tipiche, che li distinguono da altri shock operativi.

[18] Kashyap, Anil K., and Anne Wetherilt. 2019. "Some Principles for Regulating Cyber Risk." AEA Papers and Proceedings, 109: 482-87.

Innanzitutto, l'*intento*. Gli attacchi dirompenti sono condotti con intento malevolo e progettati per infliggere il massimo danno, magari combinando le azioni malevoli a più sistemi o selezionando una data critica.

In secondo luogo, la *probabilità*. Tra gli esperti è diffusa l'opinione che la probabilità di successo sia oggi molto più alta rispetto al recente passato e che un evento ad alto impatto sia una questione di "quando", piuttosto che di "se".

Terzo, la *tempistica*. L'attacco potrebbe comportare una fase nascosta, in cui venga inserito un codice dannoso e i dati vengano compromessi e manipolati per creare il massimo danno possibile. Una volta che l'attacco divenga noto può comunque risultare difficile valutare l'entità del danno e identificare soluzioni efficaci. Ad esempio, gli esperti ritengono che allorché nel 2017 si diffuse il virus NotPetya[19] lo stesso fosse presente già da diverse settimane nell'hardware preso di mira.

Inoltre, i nuovi strumenti e le nuove tecniche a disposizione degli aggressori informatici riducono il costo degli attacchi e ne aumentano l'impatto, consentendo agli autori delle minacce di individuare vulnerabilità precedentemente non sfruttate ed incrementando, al contempo, il costo degli strumenti di protezione.
Diversi shock operativi, come anche l'attività terroristica, condividono queste caratteristiche risultando maliziosi e adattivi.
Peraltro, i cyber shock si differenziano da altri eventi similari per un altro aspetto, ovverosia per l'impatto diffuso sulle organizzazioni e sul sistema finanziario in generale. In parte, ciò è dovuto al fatto che l'interconnessione del sistema finanziario rende possibile un'interruzione su larga scala. Il software dannoso può essere infatti introdotto direttamente nelle reti aziendali o indirettamente attraverso le loro controparti o terze parti, creando così diversi varchi che gli aggressori possono sfruttare. Attraverso gli attacchi alla catena di approvvigionamento la criminalità informatica può facilmente

[19] NotPetya prende il nome dal ransomware Petya, diffuso un anno prima, che criptava i file e richiedeva il pagamento di valuta digitale in cambio della decriptazione.

accedere a dati riservati da un'ampia gamma di fonti, contando anche sulla circostanza dell'utilizzo di software sempre più comuni.[20] .

Un'altra caratteristica peculiare del cyber risk deriva dalle ripercussioni della fase silenziosa e nascosta preliminare all'attacco informatico. Un terrorista "tradizionale" potrebbe passare molto tempo a pianificare un attacco i cui effetti sarebbero però immediatamente visibili. Al contrario, l'impatto di un attacco informatico può rimanere sconosciuto per un lungo periodo, salvo poi procurare danni indefiniti nella loro ingenza per la difficoltà di comprendere fino a che punto l'integrità dei dati sia stata compromessa. Non è un caso, infatti, se gli attacchi informatici che causano danni o furti di dati risultino in genere essere i più costosi per le organizzazioni che debbano procedere al loro reintegro.

1.5.1 La Tassonomia dei Rischi Operativi

La tassonomia dei rischi operativi per la sicurezza informatica è strutturata su una gerarchia di classi, sottoclassi ed elementi.

Le classi prese in considerazione sono quattro:

- *Azioni delle persone*. Per tali si intendono le azioni, attuate o mancate, intraprese dalle persone, deliberatamente o accidentalmente, che abbiano un impatto sulla sicurezza informatica.

- *Guasti ai sistemi e alla tecnologia*, ovverosia i guasti alle componenti hardware, al software e ai sistemi informativi.

- *Processi interni falliti*. Sono costituiti dai problemi nei processi aziendali interni che abbiano un impatto sulla capacità di implementare, gestire e sostenere la sicurezza informatica, come la progettazione, l'esecuzione e il controllo dei processi.

- *Eventi esterni*. Criticità insorte al di fuori del controllo dell'organizzazione, come i disastri naturali, le controversie legali e le dipendenze dai fornitori di servizi.

[20] Come nel caso del cosiddetto incidente Wannacry, che nel 2017 ha sfruttato una vulnerabilità comune nei sistemi Windows di diverse organizzazioni e settori per provocare danni ingenti agli utenti coinvolti, coinvolgendo oltre 300.000 computer in 150 Paesi.

È opportuno considerare come i rischi possano essere a cascata: i rischi di una classe possono innescare quelli di un'altra. In questa ipotesi, l'analisi di un particolare rischio può coinvolgere più elementi di classi diverse. Ad esempio, un guasto del software dovuto a impostazioni di sicurezza non corrette potrebbe essere causato da uno qualsiasi degli elementi di azioni involontarie o deliberate delle persone.
Ciascuna delle quattro classi è ulteriormente scomposta in sottoclassi le quali, a loro volta, sono composte da elementi propri.

1.5.2 Azioni delle persone

Le azioni delle persone descrivono una classe di rischio operativo caratterizzata da problemi causati dalle azioni intraprese o non intraprese dagli individui in una determinata situazione. Questa classe comprende quindi le azioni di persone interne ed esterne all'organizzazione. Le sue sottoclassi di supporto includono le azioni involontarie (generalmente da parte di insider), le azioni deliberate (da parte di insider o outsider) e l'inaction (generalmente da parte di insider).
La prima sottoclasse si riferisce ad azioni *non intenzionali* intraprese senza intento malevolo o dannoso e sono solitamente, anche se non esclusivamente, associate a un individuo interno all'organizzazione.

Questa sottoclasse è composta dai seguenti elementi.

- Errore: individuo a conoscenza della procedura corretta che compie accidentalmente un'azione non corretta
- Errore: individuo non a conoscenza della procedura corretta che compie un'azione non corretta
- Omissione: persona che non pone in essere un'azione corretta nota, spesso a causa dell'esecuzione frettolosa di una procedura.

La seconda sottoclasse si riferisce alle azioni deliberate e descrive quelle intraprese *intenzionalmente,* con l'intento di arrecare danno, da parte di soggetti interni ed esterni all'organizzazione.

Questa sottoclasse è descritta dai seguenti elementi:

- Frode: un'azione deliberata intrapresa per avvantaggiare sé stessi o un collaboratore a spese dell'organizzazione.
- Sabotaggio: un'azione deliberata intrapresa per causare un guasto a un asset o a un processo organizzativo, generalmente condotta contro asset chiave individuati da qualcuno in possesso di informazioni riservate o comunque con accesso diretto a queste ultime.
- Furto: il prelievo intenzionale e non autorizzato di beni aziendali, in particolare quelli informativi.
- Vandalismo: il danneggiamento intenzionale di beni dell'impresa, spesso realizzato in modo casuale.

La terza sottoclasse, quella dedicata all' *"inaction",* descrive la mancanza di azione o l'incapacità di agire in una determinata situazione.

Gli elementi dell'inaction includono l'incapacità di agire a causa della mancanza di competenze adeguate, di conoscenze, di orientamento e della indisponibilità di soggetti in grado di agire.

1.5.3 I guasti ai sistemi interni e alla tecnologia

I guasti ai sistemi e alla tecnologia descrivono una classe di rischio operativo caratterizzata da un funzionamento problematico, anomalo o inatteso degli asset tecnologici.
Le sue sottoclassi di supporto includono guasti di hardware, software e sistemi integrati.
La sottoclasse hardware riguarda i rischi riconducibili a guasti delle apparecchiature fisiche dovuti a:
- Capacità o meno di gestire un determinato carico o volume di informazioni.
- Prestazioni. Si intendono per tali le competenze professionali utili al completamento di istruzioni o all'elaborazione di informazioni entro parametri accettabili (velocità, consumo energetico, calore).
- Manutenzione: mancata esecuzione della manutenzione ordinaria o a richiesta dell'apparecchiatura.

- Obsolescenza: funzionamento dell'apparecchiatura oltre la durata di vita prevista.

La sottoclasse del software affronta i rischi derivanti dalle risorse software di tutti i tipi, compresi i programmi, le applicazioni e i sistemi operativi.
Gli elementi delle carenze del software sono la compatibilità, la gestione della configurazione, il controllo delle modifiche, le impostazioni di sicurezza, le pratiche di codifica e i test.
- Compatibilità, ovverosia l'incapacità di due o più software di funzionare insieme come previsto.
- Gestione della configurazione. Si realizza con l'applicazione e gestione non corretta delle impostazioni e dei parametri appropriati per l'uso previsto.
- Controllo delle modifiche apportate all'applicazione o alla sua configurazione da un processo privo di autorizzazione, revisione e rigore appropriati.
- Impostazioni di sicurezza applicate non correttamente, in maniera eccessivamente restrittiva o poco incisiva.
- Pratiche di codifica. Fallimenti dovuti a errori di programmazione, compresi problemi di sintassi o di logica e la mancata osservanza di pratiche di codifica sicure.
- Test inadeguati o atipici, dell'applicazione o della configurazione software.

La sottoclasse dei sistemi si occupa dei guasti ai sistemi integrati che non funzionano come previsto.
I guasti dei sistemi sono descritti dagli elementi:

- Progettazione inadeguata del sistema per l'applicazione o l'uso prestabilito.
- Specifiche. Consiste nella definizione errata o inadeguata dei requisiti o mancato rispetto degli stessi durante la costruzione del sistema.
- Integrazione. Il mancato funzionamento congiunto o interfacciamento corretto dei vari componenti del sistema; comprende anche l'inadeguatezza dei test del sistema.
- Complessità del sistema o numero eccessivo di interrelazioni tra i componenti.

1.5.4 Il fallimento dei processi interni

Il fallimento dei processi interni descrive una classe di rischio operativo associata a problemi derivanti dalla mancata applicazione delle procedure aziendali in materia informatica come preventivamente stabilito.
Le relative sottoclassi includono la progettazione o l'esecuzione dei processi, i controlli dei processi e i processi di supporto.
La sottoclasse della progettazione o dell'esecuzione dei processi concerne l'incapacità dei processi di raggiungere i risultati desiderati, a causa di una progettazione inadeguata al compito da svolgere o di una cattiva esecuzione di un processo progettato correttamente.
Gli elementi della progettazione o dell'esecuzione dei processi sono i seguenti:
- Flusso del processo. Progettazione carente del movimento degli output del processo verso i consumatori previsti.
- Documentazione del processo inadeguata in riferimento agli input, agli output, e agli stakeholder del processo.
- Ruoli e responsabilità. Definizione e comprensione insufficienti dei ruoli e delle responsabilità degli stakeholder del processo.
- Notifiche e avvisi inadeguate di un potenziale problema o problema di processo.
- Flusso di informazioni. Progettazione carente della circolazione delle informazioni di processo alle parti interessate e agli stakeholder.
- Escalation dei problemi. Incapacità della gestione ordinaria di condizioni anomale o inattese per l'intervento del personale appropriato.
- Accordi sul livello di servizio. La mancanza di accordo tra gli stakeholder del processo sulle aspettative di servizio potrebbe causare il mancato completamento delle azioni previste
- Task hand-off. La "perdita della palla" dovuta all'inefficienza del passaggio di un task in corso da una parte responsabile a un'altra.

La sottoclasse dei controlli di processo si occupa dei fallimenti imputabili a controlli inadeguati sul funzionamento del processo.
Gli elementi di questa sottoclasse sono:
- Monitoraggio dello stato. Mancata revisione e risposta alle informazioni di routine sul funzionamento di un processo

- Metriche. Mancata revisione delle misurazioni del processo nel tempo allo scopo di determinare le tendenze delle prestazioni
- Revisione periodica. Mancata revisione periodica del funzionamento end-to-end del processo e mancata introduzione delle modifiche ritenute necessarie.
- Proprietà del processo. Incapacità di un processo di fornire i risultati attesi a causa di una cattiva definizione della sua proprietà o di pratiche di governance inadeguate.

La sottoclasse dei processi di supporto si occupa dei rischi operativi indotti a causa dell'incapacità dei processi organizzativi di supporto di fornire le risorse adeguate.

I processi di supporto interessati sono gli elementi relativi al personale, alla contabilità, alla formazione e allo sviluppo e agli approvvigionamenti.

- Personale. Incapacità di fornire risorse umane adeguate a supportare le operazioni aziendali.
- Finanziamenti. Incapacità di fornire risorse finanziarie adeguate a sostenere le operazioni aziendali.
- Formazione e sviluppo. Incapacità di mantenere le competenze adeguate all'interno della forza lavoro
- Approvvigionamenti. Incapacità di fornire i servizi e i beni acquistati necessari a supportare le operazioni.

1.5.5 Gli eventi esterni

Gli eventi esterni descrivono una classe di rischi operativi associati ad accadimenti generalmente al di fuori del controllo dell'organizzazione. Spesso quindi la tempistica o il verificarsi di tali eventi non è di facile previsione e pianificazione.
Le sottoclassi di supporto di questa classe includono disastri, problemi legali, problemi aziendali e dipendenze dai servizi.
La sottoclasse dei pericoli riguarda i rischi dovuti a eventi, sia naturali che di origine umana, sui quali l'organizzazione non ha alcun controllo e che possono verificarsi senza preavviso. Gli elementi che supportano questa sottoclasse includono eventi meteorologici, incendi, inondazioni, terremoti, disordini e pandemie.

- Evento atmosferico. Situazioni meteorologiche avverse come pioggia, neve, tornado o uragano
- Incendio all'interno di una struttura o interruzione causata da un incendio esterno a una struttura
- Alluvione. Allagamento all'interno di una struttura o interruzione causata da un'alluvione esterna alla struttura
- Terremoto. Interruzione delle operazioni organizzative a causa di un terremoto
- Disordini. Interruzione delle operazioni a causa di disordini civili, sommosse o atti terroristici
- Pandemia. Condizioni sanitarie avverse e molto diffuse che interrompono le operazioni dell'organizzazione.

La sottoclasse delle questioni legali riguarda i rischi che possono avere un impatto sull'organizzazione a causa degli elementi di conformità normativa, legislazione e conseguenti a controversie legali.

- Conformità normativa. Emanazione di nuove legislazioni governativa o mancata conformità alla normativa esistente.
- Legislazione. Nuova normativa che ha un impatto sull'organizzazione.
- Controversie legali. Azioni legali intraprese contro l'organizzazione da qualsiasi stakeholder, compresi dipendenti e clienti.

La sottoclasse dei problemi di business (descritta dagli elementi fallimento dei fornitori, condizioni di mercato e condizioni economiche) si occupa dei rischi operativi derivanti da cambiamenti nell'ambiente di business dell'organizzazione.

- Fallimento del fornitore. L'incapacità temporanea o permanente di un fornitore di assicurare all'organizzazione i prodotti o i servizi necessari.
- Condizioni di mercato. La diminuzione della capacità dell'organizzazione di vendere i propri prodotti e servizi sul mercato.
- Condizioni economiche. L'incapacità dell'organizzazione di ottenere i finanziamenti necessari per sostenere le proprie attività.

La sottoclasse dipendenze da servizi riguarda i rischi derivanti dalla dipendenza dell'organizzazione verso soggetti esterni per il proseguimento delle attività. La sottoclasse è associata agli elementi utenze, servizi di emergenza, carburante e trasporti.

- Servizi di pubblica utilità. Guasti alla rete elettrica, a quella idrica o ai servizi di telecomunicazione dell'organizzazione.
- Servizi di emergenza. Dipendenza dai servizi di risposta pubblica come i vigili del fuoco, la polizia e i servizi medici di emergenza.
- Carburante. Mancanza di forniture esterne di carburante, ad esempio per l'alimentazione di un generatore di riserva.
- Trasporti. Guasti ai sistemi di trasporto esterni, ad esempio impossibilità per i dipendenti di recarsi al lavoro e impossibilità di effettuare e ricevere consegne.

1.6 Il Cyber Risk

Che cos'è il rischio in relazione al cyberspazio?
Non esiste una risposta semplice a questa domanda, poiché nel cyberspazio i rischi si presentano sotto diverse forme e sembianze.
Uno dei rischi più concreti e ad alto impatto è quello relativo alla intangibilità delle cosiddette infrastrutture critiche. Si pensi agli acquedotti, ai sistemi di approvvigionamento alimentare e idrico, ma anche ai sistemi di trasporto o alle istituzioni sanitarie. Tutte queste architetture infrastrutturali sono ormai gestite via rete per ottimizzarne l'efficienza ed il controllo da remoto, esponendole però al rischio di attacchi informatici con rilevanti effetti negativi a livello sociale ed economico.
Di recente il Sistema Sanitario italiano è stato oggetto di gravi attacchi informatici a livello di istituzioni regionali (prima il Lazio e poi il Veneto), mentre è recente la notizia di una indebita intrusione negli archivi automatizzati dell'Agenzia delle Entrate.
A livello internazionale si sono verificati diversi episodi di manomissione delle infrastrutture digitali di Stati nazionali (Estonia, Svezia, Finlandia), spesso riferibili a tentativi di destabilizzazione imputabili, direttamente o indirettamente, ad altre Nazioni. Le stesse attività militari sono state spesso oggetto di attacchi informatici potenzialmente molto pericolosi.

I rischi per la sicurezza informatica non sono però solo un problema dei governi nazionali, delle forze armate o della comunità internazionale.

Un'ampia gamma di crimini informatici può colpire istituti di credito, industrie, singole imprese, organizzazioni del lavoro e privati cittadini.

Il furto o la manipolazione di dati informatici (cyber theft), l'indisponibilità di informazioni o servizi (hacktivisme), l'interruzione o danneggiamento di sistemi informatici attraverso il malware, sono tutti eventi fraudolenti in aumento costante ovunque le cui vittime sono principalmente persone fisiche o imprese.

Le piattaforme tecnologiche convergenti, gli strumenti e interfacce collegate sulla rete Internet che si sta rapidamente spostando verso una versione 3.0 più decentralizzata, sono fattori di creazione dei presupposti per un panorama di minacce informatiche più complesso e per un numero crescente di punti critici di fallimento.

Mentre l'intera società continua a migrare nel mondo digitale, la minaccia della criminalità informatica incombe, traducendosi in un costo per le organizzazioni del lavoro private o pubbliche stimabile in centinaia di milioni di dollari. I costi da sopportare non sono solo finanziari: anche le infrastrutture critiche, la coesione sociale e il benessere mentale sono a in pericolo. La crescente dipendenza dai sistemi digitali negli ultimi 20 anni ha modificato drasticamente il funzionamento di molte società.

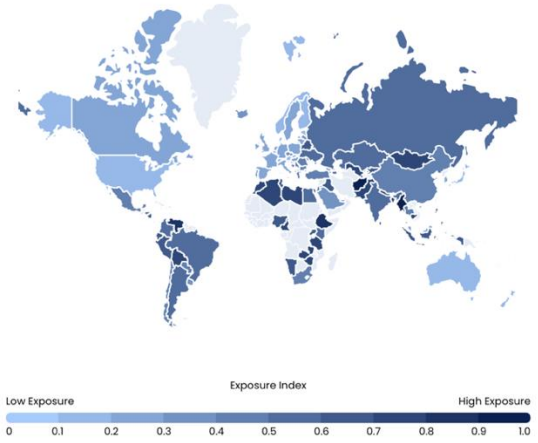
Dagli attacchi agli endpoint, progettati per ottenere un accesso non autorizzato, rubare dati ed estorcere denaro bloccando l'accesso a file o sistemi informatici, agli attacchi al cloud, ideati per compromettere le macchine virtuali, il crimine informatico può assumere molte forme.

Per questo motivo, per individuare quali siano i Paesi più e meno esposti alla criminalità informatica, è stato calcolato per 108 Paesi il Cybersecurity Exposure Index (CEI). Per determinare l'indice sono stati presi in considerazione i dati relativi a cinque dei tipi più significativi di attacchi informatici end-point e cloud e le risorse impiegate nel campo della sicurezza informatica.

I dati rivelano gli ultimi approfondimenti su quali siano i Paesi più esposti, quelli meno aggrediti e quelli che si trovano in una situazione mediana.

Da 0 a 1, il Cybersecurity Exposure Index (CEI) calcola il livello di esposizione alla criminalità informatica per Paese. Più alto è il punteggio, più alta è l'esposizione.

Figura 5: Global Cybersecurity Exposure Index 2020



Fonte: Password Managers

Il Cybersecurity Exposure Index (CEI) è stato calcolato utilizzando un sistema di classificazione.

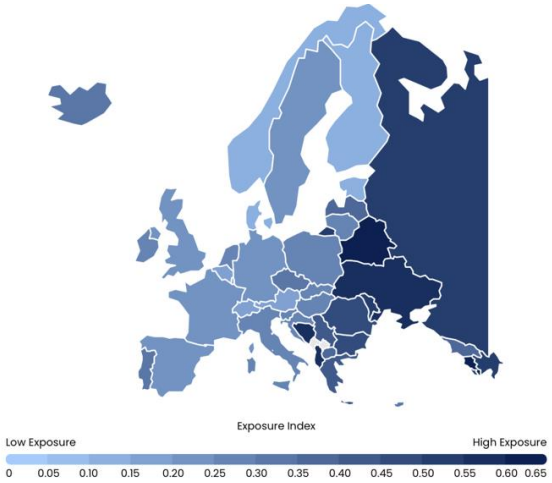
I tassi di riscontro di malware, ransomware, criptovalute, pagine di download drive-by e attacchi in entrata relativi a provider cloud sono stati classificati da alti a bassi in virtù dell'esposizione dei singoli Stati alla criminalità informatica.

Similmente, il tasso di impegno per la sicurezza informatica è stato classificato da alto a basso considerando l'insieme delle risorse impegnate a livello nazionale.

Il risultato per ciascun Paese è stato poi sommato e diviso per 290 al fine di calcolare la scala di esposizione da 0 a 1 (bassa-alta).

Limitando l'analisi al continente europeo si possono osservare i seguenti dati.

Figura 6: Europe Cybersecurity Exposure Index 2020



Fonte: Password Managers

L'Europa ha in generale il punteggio di esposizione più basso per Paese (0,329). Infatti, il 70,73% dei Paesi europei è classificato nei gruppi di esposizione bassa e molto bassa e l'Europa rappresenta il 67,44% dei Paesi a bassa e bassissima esposizione su scala mondiale. Solo due Stati sono classificati tra quelli ad alta esposizione (il 4,88% dell'intero continente), dando così luogo alla più bassa esposizione a livello globale.

L'Armenia è il Paese più esposto, seguito da Bielorussia, Bosnia-Erzegovina, Ucraina e Albania.

La Finlandia è lo stato meno esposto, seguito da Danimarca, Lussemburgo, Estonia e Norvegia.

Come noto, uno dei principali effetti sul mercato del lavoro indotti dalla crisi pandemica è stata sicuramente l'intensificazione del modello di lavoro da remoto. Il massiccio passaggio al lavoro a distanza ha accelerato l'adozione di piattaforme e dispositivi che consentono di condividere dati sensibili con terze parti (fornitori di servizi cloud, aggregatori di dati, interfacce di programmazione delle applicazioni (API) e altri intermediari tecnologici).

Questi sistemi, pur costituendo strumenti potenti per i dati e l'elaborazione, determinano però un ulteriore livello di dipendenza dai fornitori di servizi. Lo smartworking ha anche spostato gli scambi digitali dalle reti degli uffici a quelle residenziali, le quali ultime presentano una maggiore varietà di dispositivi connessi con una minore protezione contro le intrusioni informatiche.

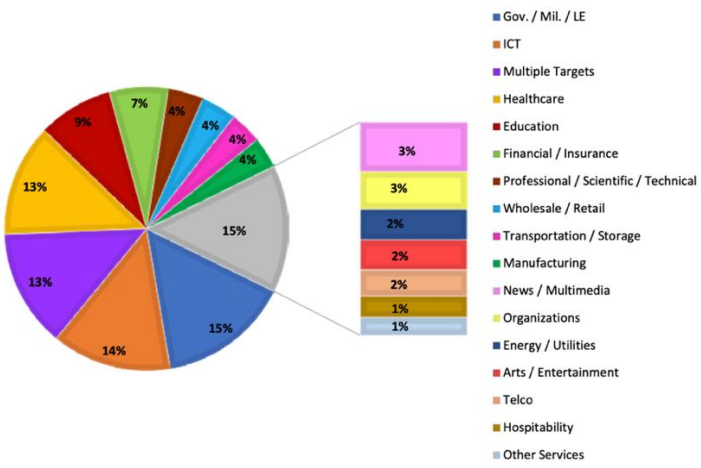
Parallelamente, cresce l'interesse per le funzionalità basate sull'utilizzo di più tecnologie che lavorano di concerto, tra cui l'intelligenza artificiale (AI)[21], i dispositivi abilitati all'Internet delle cose (IoT)/Internet degli oggetti robotici, l'edge computing[22], la

[21] L'intelligenza artificiale è un'ampia branca dell'informatica che si occupa di costruire macchine intelligenti in grado di eseguire compiti che di solito richiedono l'intelligenza umana.

[22] L'edge computing è un paradigma informatico emergente che si riferisce a una serie di reti e dispositivi in prossimità dell'utente. L'edge consiste nell'elaborare i dati più vicino al luogo in cui vengono generati, consentendo un'elaborazione a velocità e volumi maggiori e portando a risultati più incisivi in tempo reale.

blockchain[23] e il 5G[24]. Se da un lato questi prodotti innovativi offrono enormi opportunità alle aziende e alle società in genere di utilizzare le tecnologie massimizzandone l'efficacia, la qualità e la produttività, di converso queste stesse possibilità espongono gli utenti a forme elevate e più perniciose di rischio digitale e informatico.
Il Rapporto Clusit 2022[25] raffigura la distribuzione per settore merceologico dei soggetti esposti a cyber attacchi nel 2021. Nonostante le differenze percentuali, si può concludere che non esiste un settore che possa ritenersi immune da questo tipo di rischio.

Figura 7: Distribuzione delle vittime 2021



Fonte: Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

In futuro, l'interconnessione e la convergenza di questi strumenti digitali continueranno ad aumentare di pari passo con la diffusione delle più recenti versioni di Internet basate sulla tecnologia blockchain.

[23] La blockchain è un libro mastro condiviso e immutabile che facilita il processo di registrazione delle transazioni e di tracciamento dei beni in una rete commerciale. Un bene può essere tangibile (una casa, un'auto, denaro, un terreno) o intangibile (proprietà intellettuale, brevetti, diritti d'autore, marchio).
[24] The 5th generation mobile network
[25]Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

L'esempio principale di questa evoluzione sarà probabilmente costituito dal cosiddetto metaverso: una rete di spazi virtuali 3D, abilitata da criptovalute[26] e token non fungibili[27] (NFT) tra le altre tecnologie, con un'interoperabilità socioeconomica senza precedenti ed esperienze di realtà virtuale coinvolgenti. Gli utenti del metaverso saranno chiamati a superare le vulnerabilità di sicurezza insite sia nella maggiore dipendenza che nella crescente frammentazione di questo tipo di tecnologie complesse, spesso caratterizzate dalla decentralizzazione e dalla mancanza di guardrail strutturati o di sofisticate infrastrutture di onboarding.

Nel contesto di una diffusa dipendenza da sistemi digitali sempre più complessi, le crescenti minacce informatiche stanno superando la capacità delle società di prevenirle e gestirle efficacemente.

L'attività criminale prolifera non solo a causa delle crescenti vulnerabilità, ma anche perché ci sono pochi deterrenti contro i partecipanti all'industria del ransomware e pochi rischi per gli stessi di incorrere in sanzioni penali.

Il malware è aumentato del 358% nel 2020, mentre il ransomware a sua volta è aumentato del 435%, quadruplicando il valore totale delle criptovalute ricevute a titolo di riscatto.

Il "ransomware come servizio" consente anche a criminali non esperti informatici di eseguire attacchi, una tendenza che potrebbe intensificarsi con l'avvento del malware alimentato dall'intelligenza artificiale (AI). Infatti, gruppi di mercenari informatici in cerca di profitto sono pronti a fornire l'accesso a sofisticati strumenti di intrusione informatica per facilitare tali attacchi.

Inoltre, la diffusione delle criptovalute ha permesso ai criminali informatici di incassare cospicui riscatti con un rischio molto modesto di essere identificati e sanzionati.

Anche gli attacchi stessi stanno diventando più aggressivi e diffusi. Gli attori delle minacce informatiche che utilizzano i ransomware sfruttano tattiche di pressione più minacciose e si rivolgono contro obiettivi più vulnerabili, colpendo servizi pubblici, sistemi sanitari e aziende ricche di dati.

[26] Una criptovaluta è una moneta digitale o virtuale protetta dalla crittografia, che ne rende quasi impossibile la contraffazione o la doppia spesa. Molte criptovalute sono reti decentralizzate basate sulla tecnologia blockchain.

[27] Un token non fungibile (NFT) è un record su una blockchain associato a un particolare bene digitale o fisico. La proprietà di un NFT è registrata nella blockchain e può essere trasferita dal proprietario, consentendo agli NFT di essere venduti e scambiati..

L'utilizzo di sofisticati strumenti consente agli attori delle minacce informatiche di attaccare in modo più efficiente gli obiettivi di scelta, anziché accontentarsi di quelli di opportunità, sfruttando le proprie potenzialità per realizzare incursioni che in prospettiva potrebbero portare a danni finanziari, sociali e di reputazione sempre più elevati.

L'uso sempre più sofisticato di tecnologie spyware[28], ad esempio, ha permesso attacchi mirati contro giornalisti e attivisti per i diritti civili in tutte le aree geografiche, provocando un'ondata di contraccolpi politici e industriali sotto forma di sanzioni governative e azioni legali. La capacità di personalizzare gli attacchi permette anche di minare la capacità di risposta degli apparati preposti alla cybersicurezza, se impegnati al momento da altre priorità come accaduto durante il picco epidemico da COVID-19 o in occasione di gravi calamità naturali.

Gli attori delle minacce informatiche hanno inoltre accesso a informazioni di qualità superiore rispetto a quelli in possesso delle potenziali vittime. Infatti, la tecnologia deepfake consente agli attori delle minacce informatiche di migliorare gli stratagemmi di ingegneria sociale, di diffondere false informazioni e di creare scompiglio nella società, soprattutto nei momenti di maggiore volatilità.

Gli intervistati della Global Risks Perception Survey (GRPS)[29] riflettono queste tendenze, classificando il "fallimento della cybersecurity" tra i primi 10 rischi la cui percezione si è aggravata maggiormente dall'inizio della crisi COVID-19.

Inoltre, l'85% della Cybersecurity Leadership Community del World Economic Forum ha sottolineato come il ransomware stia diventando una minaccia pericolosamente crescente e rappresenti una fonte di grande preoccupazione per la sicurezza pubblica.

A livello regionale, il "fallimento della cybersecurity" si colloca tra i primi cinque rischi in Asia orientale e Pacifico e in Europa, mentre quattro Paesi - Australia, Gran Bretagna, Irlanda e Nuova Zelanda - lo hanno classificato come il principale.

Anche molte piccole economie altamente digitalizzate, come Danimarca, Israele, Giappone, Taiwan, Singapore ed Emirati Arabi Uniti, hanno classificato questo rischio tra i primi cinque più preoccupanti.

[28] Lo spyware è un tipo di software dannoso, o malware, che viene installato su un dispositivo informatico all'insaputa dell'utente finale. Si introduce nel dispositivo, ruba informazioni sensibili e dati sull'utilizzo di Internet e li trasmette a inserzionisti, società di dati o utenti esterni.

[29] World Economic Forum, The Global Risks Report 2022, 17th Edition, https://www.weforum.org/reports/global-risks-report-2022/

I professionisti nel campo dell'IT e della cybersecurity, già in difficoltà per l'ordinaria mole di lavoro, sono sottoposti a un onere crescente non solo a causa dell'espansione del lavoro a distanza, ma soprattutto per la crescente complessità delle normative in materia di dati e privacy.

Appare sempre più preoccupante la carenza di professionisti del cyber (stimata a livello globale in oltre 3 milioni di addetti) in grado di fornire un'assistenza adeguata, di testare e proteggere i sistemi e di formare le persone all'igiene digitale. Similmente alle altre materie prime, la cronica mancanza di professionisti della cybersicurezza potrebbe ostacolare la crescita economica, sebbene si moltiplichino alcune iniziative per "democratizzare" la cybersecurity (es.: cessione a titolo gratuito di strumenti di sicurezza) e aiutare in tal senso le piccole imprese o le istituzioni pubbliche di minori dimensioni.

Si teme che l'informatica quantistica potrebbe diventare abbastanza potente da rompere le chiavi di crittografia, il che rappresenterebbe un rischio significativo per la sicurezza a causa della sensibilità e della criticità dei dati finanziari, personali e di altro tipo protetti dalle stesse.

L'emergere del metaverso potrebbe amplificare le possibilità di attacchi informatici individuando un numero maggiore di punti di ingresso per il malware e le violazioni dei dati. Con la crescita del valore del commercio digitale nel metaverso (secondo alcune stime, oltre 800 miliardi di dollari entro il 2024), questi tipi di attacchi aumenteranno in frequenza e aggressività. La miriade di forme di proprietà digitale, come le collezioni d'arte NFT e i beni immobili digitali, potrebbe infatti attrarre ulteriormente l'attività criminale.

A livello intergovernativo gli sforzi per contenere la crescita della criminalità informatica risultano spesso frustrati dalla disomogeneità tra i diversi ordinamenti normativi in materia. Le spaccature geopolitiche ostacolano la potenziale collaborazione transfrontaliera, con alcuni governi che non vogliono o non possono regolamentare le intrusioni informatiche che hanno origine all'interno e impatto al di fuori dei loro confini. Non sorprende che, date le tensioni geopolitiche sulla sovranità digitale, secondo gli intervistati del GRPS "gli attacchi informatici transfrontalieri e la disinformazione" con "l'intelligenza artificiale" rappresentino le aree con le iniziative di mitigazione del rischio internazionale meno "consolidate" o "efficaci".

L'utilizzo spregiudicato da parte di entità comunque riferibili a Stati sovrani della "disinformazione a pagamento" o dello spionaggio informatico, potrebbero infatti dare

luogo a gravissimi fenomeni di tensione sociale, condizionando l'esito di elezioni politiche nei Paesi democratici e indebolendo le capacità economiche dei loro sistemi industriali e infrastrutturali. Le minacce informatiche determinano un allontanamento degli Stati, con i governi nazionali che seguono percorsi sempre più unilaterali per controllare i rischi. Con l'intensificarsi della gravità degli attacchi informatici le tensioni già forti tra i governi colpiti dalla criminalità cibernetica e quelli che sono complici della loro commissione aumenteranno, poiché la sicurezza informatica diventerà un altro cuneo di divergenza, anziché di cooperazione, tra gli Stati nazionali. Soprattutto in un'epoca di crescenti tensioni tra le superpotenze, gli attacchi informatici aprono un altro fronte di scontro la cui l'escalation è un rischio reale e gravissimo. Se l'opera di mitigazione degli effetti della criminalità informatica non decollerà, i governi nazionali continueranno a rivalersi sui responsabili (effettivi o percepiti), portando a una guerra informatica aperta e a ulteriori disagi per i sistemi economici e sociali coinvolti.

Agli stessi rischi sono esposti i gruppi industriali di maggiori dimensioni a livello globale, la cui reputazione può essere facilmente compromessa da campagne di disinformazione con conseguenti gravissimi danni d'immagine ed il cui patrimonio di conoscenze è spesso fatto attacco da intrusioni indebite che ne possono diminuire le capacità concorrenziali.
Inoltre, stante l'importanza sempre più attribuita alle istanze di natura ambientale ed etica, le istituzioni che non dimostrino una solida governance aziendale in materia di cybersecurity potrebbero subire un danno reputazionale irreversibile agli occhi degli investitori attenti ai temi ESG.
L'impatto di cyberattacchi dirompenti potrebbe essere finanziariamente devastante per le aziende che non investano in protezioni efficaci per la loro infrastruttura digitale, soprattutto qualora le Autorità nazionali decidessero di vietare il pagamento di riscatti o di penalizzare le politiche di cybersecurity ritenute inadeguate.
Il raggiungimento di livelli ottimali di sicurezza informatica comporterà inevitabilmente un aumento significativo dei costi operativi per tutte le parti interessate. Questo scenario potrebbe essere particolarmente impegnativo per le piccole e medie imprese, chiamate ad investire anche più del 4% del proprio budget operativo per la sicurezza, mentre le realtà di maggiori dimensioni dovrebbero impegnare tra l'1-2%.
È opportuno comunque evidenziare come il 95% dei problemi di cybersecurity segnalato dalle aziende sia riconducibile a errori umani e in cui le minacce interne (intenzionali o

accidentali) rappresentano il 43% di tutte le violazioni. Molto probabilmente assisteremo a prassi di maggiore segmentazione dei sistemi digitali per il contenimento del rischio insider, con potenziali perdite di efficienza del personale qualora l'accesso ai dati e alle informazioni diventasse meno agevole.

Inoltre, a causa della crescente frequenza e gravità delle richieste di risarcimento per ransomware, i prezzi delle assicurazioni cyber negli Stati Uniti sono aumentati del 96% nel terzo trimestre del 2021, segnando l'incremento più significativo dal 2015 e un aumento del 204% su base annua. La necessità di coperture assicurative si è resa sempre più impellente a seguito dell'ulteriore sviluppo del commercio on line verificatosi durante la pandemia con l'ingresso in rete di popolazioni inesperte e più vulnerabili. Si consideri inoltre che, anche in settori maggiormente "protetti" come quello del credito, nel 2021 le frodi bancarie via Internet nel Regno Unito sono aumentate del 117% in volume e del 43% in valore rispetto all'anno precedente.

La vulnerabilità digitale della popolazione è un tema di assoluta rilevanza. Circa il 40% della popolazione mondiale non è ancora connesso a Internet e questa particolare forma di diseguaglianza sociale è destinata ad acuirsi con l'avvento di Internet 3.0 e del metaverso.

Peraltro, anche all'interno delle società digitalmente avanzate le fasce sociali economicamente in difficoltà sono spesso le più a rischio dal punto di vista digitale: un recente studio condotto sui residenti a basso reddito di San Francisco - il cuore della Silicon Valley – ha rilevato come questi ultimi abbiano maggiori probabilità rispetto ai residenti più ricchi di rimanere vittime della criminalità informatica.

Un altro aspetto di fondamentale importanza è quello relativo all'identità digitale e alla sicurezza della sua inviolabilità.

La sempre maggiore diffusione dei contrassegni di identità digitale obbligatori, indispensabili per accedere a diversi servizi assicurati dalle istituzioni pubbliche e private, presuppone la garanzia che l'autenticazione biometrica non possa essere indebitamente compromessa.

Qualora questa garanzia non dovesse essere percepita come assoluta la collettività degli utenti potrebbe perdere interesse ad operare nel mondo digitale, ritenendo i rischi sull'indebito utilizzo dei propri dati personali superiori agli eventuali vantaggi rivenienti dall'utilizzo della rete.

La sensazione di ridotta autonomia potrebbe inoltre riflettersi negativamente sulla protezione delle proprie impronte digitali, come dimostra lo sviluppo tumultuoso del mercato delle applicazioni di messaggistica e le controversie insorte sulle violazioni della privacy.

Sebbene infatti siano presenti delle opzioni a tutela dei clienti ("rifiuta tutto"), i siti web sono ancora pieni di pixel di tracciamento e di script di terze parti che rimangono potenti strumenti per rilevare i comportamenti online degli utenti.

Molte Autorità nazionali si stanno adoperando per garantire la vigenza del “contratto sociale digitale”, mettendo in sicurezza le infrastrutture critiche, affrontando le minacce alla "sicurezza epistemica" derivanti dalla disinformazione, proteggendo l'integrità dei processi civici e dei servizi pubblici, legiferando contro la criminalità informatica, formando la popolazione all'alfabetizzazione informatica, regolamentando i fornitori di servizi digitali e garantendo la disponibilità di risorse (come i minerali di terre rare) per l'economia digitale.

Questa doverosa attività di supervisione dovrà però essere necessariamente bilanciata dall’altrettanto irrinunciabile libertà individuale nell’approccio al mondo digitale, libertà senza la quale i rischi di autoritarismo potrebbero divenire una triste realtà.

Con l'aumento della dipendenza dalle tecnologie digitali e con l'avvento di Internet 3.0 si dovranno necessariamente intensificare gli sforzi per costruire norme e definire regole di comportamento per tutte le parti interessate nel cyberspazio. Se da un lato i dialoghi internazionali dovranno contribuire a rafforzare i legami tra gli attori che operano nel campo della sicurezza digitale, dall'altro la cooperazione tra le organizzazioni potrebbe definire le migliori pratiche replicabili in tutti i sistemi economici Le iniziative comuni dovrebbero concentrarsi sulle tecnologie emergenti, come la blockchain, l'intelligenza quantistica e artificiale, nonché sulle modalità di scambio digitale che esse facilitano, come il metaverso.

In una società profondamente connessa, la fiducia digitale è la moneta che facilita l'innovazione e la prosperità future. Le tecnologie affidabili, a loro volta, rappresentano le fondamenta su cui si costruisce l'impalcatura di una società equa e coesa.

Se non agiamo per migliorare la fiducia digitale con iniziative intenzionali e persistenti, il mondo digitale continuerà ad andare alla deriva verso la frammentazione e la promessa di una delle epoche più dinamiche del progresso umano potrebbe andare perduta.

CAPITOLO 2: LA REGOLAMENTAZIONE

2.1 La sicurezza digitale nel settore bancario e finanziario

Quasi da un giorno all'altro, l'emergenza pandemica ha costretto il mondo bancario a porre in essere cambiamenti radicali incentrati sull'utilizzo massiccio delle piattaforme tecnologiche.

I canali digitali rivolti ai clienti sono stati rafforzati e migliorati, le piattaforme di lavoro a distanza sono state ampliate e gli strumenti emergenti, come i software di analisi dei dati, sono diventati parte integrante dei processi organizzativi interni.

La migrazione massiccia verso gli strumenti digitali per l'interlocuzione con i clienti e l'operatività interna ha conseguentemente ampliato la platea dei potenziali rischi da gestire. In particolare, la cybersecurity, le conseguenze indesiderate dell'intelligenza artificiale e i problemi di integrazione associati alla mobilità delle infrastrutture informatiche, come la migrazione al cloud pubblico, sono diventate tematiche all'ordine del giorno per i Chief Risk Officer[30] (CRO).

L'identificazione, la gestione e la prevenzione di questi rischi attraverso l'automazione costituiscono il fulcro della resilienza digitale aziendale, poiché consentono di incorporare i controlli in modo coerente ed efficiente, a condizione, ovviamente, che le infrastrutture e i processi stessi siano immaginati per essere resilienti.

La crisi sanitaria globale ha indotto tutti i settori economici ad avviare profondi cambiamenti produttivi ed organizzativi, ma per il settore bancario, già in condizioni di cronico stress imputabili al processo costante di riorganizzazione dei principali players e ad una concorrenza serrata da parte di nuovi offerenti di servizi di pagamento (si pensi a Google o Amazon), la necessità di investire rapidamente in nuove tecnologie e di trasformarsi in aziende più digitali ha assunto caratteristiche di criticità e urgenza.

Questo processo di trasformazione digitale è stato perseguito sì con velocità ma non a scapito della resilienza, dovendo la tecnologia a disposizione dei circuiti bancari e finanziari essere agile e scalabile, in grado di funzionare 24 ore su 24, 7 giorni su 7, proteggendo i dati trattati da eventuali attacchi informatici.

[30] Il Chief Risk Officer (CRO) è il dirigente aziendale incaricato di valutare e attenuare le minacce competitive, normative e tecnologiche significative per il capitale e gli utili di un'impresa.

L'introduzione di tecnologie di terze parti, un requisito comune degli sforzi di trasformazione digitale, può risultare rivoluzionaria per i clienti e per i processi operativi interni ma, al contempo, sicuramente aumenterà il profilo di rischio dell'azienda bancaria. Da un attacco informatico, un'interruzione di sistema o la mancata protezione dei dati dei clienti possono derivare effetti significativi sul patrimonio aziendale e la reputazione della banca. Nelle banche di grandi dimensioni, inoltre, con modifiche organizzative e procedurali che avvengono su larga scala e insistono su più aree operative incidendo sui processi decisionali, questi rischi possono moltiplicarsi rapidamente.

La modalità ordinaria con la quale le istituzioni finanziarie cercano di trasformarsi digitalmente è il passaggio dai sistemi IT legacy al cloud, soprattutto al cloud pubblico.

I CRO intervistati nel sondaggio continuano a nutrire preoccupazioni su come le banche possano effettuare questa migrazione in modo sicuro ed efficace. Il livello delle capacità di rischio per la sicurezza (59%) e la capacità di adattare le capacità di rischio esistenti per affrontare le incognite specifiche del cloud (46%) sono fonti di particolare preoccupazione.

La resilienza digitale può essere migliorata prevedendo all'origine gli opportuni controlli automatizzati. Le funzionalità di monitoraggio continuo, ad esempio, possono essere integrate nella fase di progettazione dei processi. Ciò può risultare di supporto ai test di rischio e di controllo, consentendo alle banche di effettuare più momenti di verifica (stress test), anziché campionamenti sporadici, e di aumentare la coerenza riducendo gli approcci manuali.

Il sistema creditizio nel suo complesso è chiamato a definire delle strategie di controllo coerenti con l'obiettivo della trasformazione e modernizzazione digitale. Dovranno essere implementate le specifiche tipologie di valutazione dei rischi, scongiurando il rischio di una ipertrofia del sistema dei controlli interni attraverso l'accurata selezione degli interventi da mettere in atto.

Gli organi decisionali dovranno quindi individuare dei processi interni di gestione dei rischi informatici attuali e prospettici in grado di combinare in maniera chiara e semplificata l'esigenza di modernizzazione digitale con l'opportunità di assicurare la dovuta resilienza delle istituzioni finanziarie.

2.2.1 Il rischio nel trattamento dei dati personali: IL GDPR 679/2016

La diffusione di tecnologie "smart", caratterizzate dall'utilizzo di grandi database all'interno dei quali ogni giorno vanno a confluire una quantità abnorme di informazioni, comporta irrimediabilmente un sempre maggior numero di attività di trattamento degli elementi raccolti (si pensi alla diffusione di operazioni consistenti in processi decisionali automatizzati come la cd profilazione dell'utente) facendo così sorgere particolari esigenze connesse alla protezione dei dati personali.

La crescita esponenziale del fenomeno dei Big data ha prodotto il passaggio da una concezione del diritto alla privacy inteso come protezione dei dati personali verso una maggiormente incentrata sulla tutela del diritto di mantenere il controllo sulle proprie informazioni.

In questo scenario in rapida evoluzione il GDPR 679/2016 risponde alla duplice esigenza di assicurare un riscontro in termini di tutela dei dritti e delle libertà degli interessati adattabile ad un contesto in continuo divenire, nonché di uniformare l'impianto normativo di riferimento in materia di dati personali per tutti gli stati membri dell'UE, scongiurando il rischio di legislazioni nazionali divergenti in una materia così delicata.

Il Regolamento UE 2016/679 – General Data Protection Regulation - è entrato in vigore il 25 maggio 2018 al termine del biennio concesso dall'Unione Europea agli Stati membri per poter approfondire il tema e poi essere pronti ad applicarlo.

In attuazione del suddetto Regolamento il Legislatore italiano ha prima emanato il D.lgs. 51/2018 in materia di trattamento dei dati personali da parte delle Autorità competenti e, in un secondo momento, il D.lgs. 101/2018 con il quale sono state armonizzate alla citata normativa europea le previgenti disposizioni del Codice della privacy (D.lgs. 196/2003).

L'adeguamento del sistema normativo nazionale si è reso necessario al fine di coordinare la legislazione vigente con il Regolamento, assicurando un'interpretazione uniforme ed evitando asimmetrie applicative e conflitti giurisprudenziali.

L'intento del Legislatore sovranazionale si è quindi tradotto in regole concrete caratterizzate da una applicazione a largo spettro, con l'obiettivo di approntare ogni opportuna tutela a tutti i dati personali trattati con strumenti elettronici o tecnologici.

L'intero nuovo assetto legislativo costituisce una vera e propria rottura rispetto al passato, segnata dalla definizione di misure minime di sicurezza riferibili a qualsiasi

realtà, pubblica o privata, che abbia a che fare con ogni sorta di trattamento di dati personali, costruendo le proprie fondamenta sul c.d. principio di accountability o "responsabilizzazione".

Il Regolamento, unitamente alla normativa italiana di attuazione, opera quindi una sorta di *"rivoluzione copernicana"*[31] delineando un sistema di sicurezza teso a garantire la necessaria riservatezza dei dati personali nelle varie fasi del trattamento, affidando questo compito non più al Legislatore ma al Titolare del trattamento.

Il GDPR e tutto il sistema normativo nazionale ed europeo sono intesi quindi come uno strumento vivo, una "metodologia" da applicare in modo costantemente innovativo, sempre attento all'evoluzione della realtà, piuttosto che alla stregua di un corpus di norme da applicare in modo statico. Il suo fondamento ultimo, prima che giuridico, non può che essere valoriale, espressione di una visione del ruolo dell'uomo contemporaneo nell'età digitale.

Infatti, le innovazioni tecnologiche e la crescita esponenziale dell'uso dei Big Data Analysis pongono tutti gli esseri umani davanti a cambiamenti enormi potenzialmente pericolosi sotto diversi punti di vista.

Lo sviluppo inarrestabile dell'Intelligenza Artificiale e il cambio di paradigma nella trasmissione dei dati, legato alla ormai avanzata realizzazione della tecnologia e delle reti 5 G, comportano sfide sempre più alte per la tutela dei diritti e delle libertà fondamentali dei cittadini europei e per i valori fondanti della nostra eredità culturale.

È impossibile non constatare come già oggi si confrontino nel mondo tre grandi sistemi geopolitici e tecnologici, in competizione durissima tra di loro non solo in materia di sviluppo digitale ma anche, e soprattutto, sulla visione culturale e politica che guida i diversi progetti di futuro che ciascuno di essi coltiva.

Il riferimento è ovviamente al modello di sviluppo tecnologico americano, a quello cinese ed a quello europeo. Tre modelli diversi e distinti tra loro in particolare sul rilievo da attribuire al concetto di protezione dei dati personali e sulle modalità con le quali affrontare questa tematica.

[31] M.Martorana (2019), *GDPR e Decreto Legislativo 101/2018, Vademecum del professionita: obblighi, adempimenti, strumenti di tutela*, CEDAM

L'Unione Europea pone al centro della sua strategia e della sua concezione del mondo una visione della società digitale rispettosa dei diritti fondamentali, dei principi democratici, del *rule of law*.[32]
In definitiva, una visione che mette in primo piano la persona e il suo libero arbitrio.
Questa impostazione, che, si ripete, è culturale e valoriale molto prima che giuridica, impone a tutti coloro che si occupano di tutela dei trattamenti dei dati personali l'adesione a una sorta di "patriottismo europeo", o, se si preferisce, di impegno a difendere i valori fondanti della cultura occidentale.
Una sfida grandissima ci attende. Una sfida che, nella società digitale, si combatte tutta intorno al concetto di trattamento dei dati personali e al rispetto, senza se e senza ma, dei principi che sono alla base del GDPR.
Ulteriore conseguenza dell'approccio fatto proprio dal Legislatore europeo è quella di aver predisposto un corpus normativo che interviene direttamente anche nel campo economico e sociale, prevedendo degli obblighi comportamentali (etici) in capo alle aziende e agli enti pubblici che operano nel territorio dell'Unione.

2.2.2 Gli obiettivi del GDPR

La filosofia del GDPR si sostanzia nella promozione di uno sviluppo armonioso dell'economia digitale, incentivando un clima di fiducia sulle opportunità offerte da questo nuovo modello di organizzazione sociale, nella consapevolezza, al contempo, dell'esigenza imprescindibile di tutelare la sfera personale dei cittadini dell'Unione.
Alle persone fisiche deve essere infatti assicurato il controllo costante delle informazioni inerenti alla propria sfera personale, ed a tal fine il Regolamento introduce regole chiare e stringenti in materia di informativa e consenso, ponendo dei limiti effettivi al trattamento automatizzato dei dati acquisiti da terzi per finalità commerciali o amministrative.
Vengono stabiliti inoltre criteri rigorosi per il trattamento dei dati nei Paesi extra U.E. e predisposto un quadro sanzionatorio nelle ipotesi di violazioni delle norme a tutela della privacy.

[32] «*Rule of law guarantees fundamental rights and values, allows the application of EU law, and supports an investment-friendly business environment. It is one of the fundamental values upon which the EU is based on.* » *(European Commission)*

Soprattutto, viene promossa la responsabilizzazione (accountability) dei Titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali possa comportare ai diritti e alle libertà degli interessati.

2.2.3 I ruoli istituiti dal DGPR

Il Regolamento individua delle figure cui vengono attribuite delle responsabilità precise al fine di assicurare l'intangibilità dei diritti individuali.
Per Titolare del trattamento si intende colui il quale, decidendo la finalità e le modalità del trattamento, si assuma la responsabilità giuridica del rispetto degli obblighi previsti dalla normativa. Si tratta di una persona, fisica o giuridica, chiamata a mettere in atto tutte le misure tecnico/organizzative tese a garantire e comprovare che il trattamento sia stato svolto in modo conforme al Regolamento. Il Titolare è vincolato al dovere di riservatezza dei dati e quindi non può utilizzare gli stessi al di fuori del processo di trattamento.
Il Rappresentante è una persona fisica o giuridica che abbia la propria residenza nell'Unione e subentri negli obblighi propri del Titolare qualora quest'ultimo non sia a sua volta residente in un Paese dell'U. E.
Il Responsabile, laddove questa figura venga prevista, è il soggetto che, in virtù di delega formale, assuma la responsabilità di uno o più ambiti specifici del processo di trattamento dei dati.
Per Soggetto autorizzato si intende la figura autorizzata, dal Titolare o dal Responsabile se designato, ad elaborare o utilizzare materialmente i dati personali.
Ex art. 29 del GDPR le istituzioni pubbliche o private sono tenute a predisporre delle istruzioni specifiche inerenti al trattamento dei dati personali.
Il Referente Interno privacy è il soggetto cui il Titolare delega specifiche attività relative alla normativa in materia di privacy.
Il Responsabile per la Protezione dei dati, o DPO (Data Protection Officer), è la persona fisica, oppure una società o ente specializzato nella protezione dei dati, che assiste il Titolare o Responsabile del trattamento. La sua nomina in alcuni casi specifici è obbligatoria, ma non lo è per quanto riguarda le attività di e-commerce tradizionali. Come requisito sostanziale per svolgere la funzione di DPO il Regolamento prevede il possesso

di conoscenze specialistiche della normativa e delle prassi in materia di protezione dei dati nonché competenze certificate in campo informatico e di cyber security.

Il Regolamento pone inoltre con forza l'accento sulla "responsabilizzazione" (accountability, nell'accezione inglese) del Titolare e dei Responsabili nell'assunzione di pratiche conformi allo spirito del DGPR in materia di Trattamento dei dati personali:

« Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.» [33]

Viene affidato al Titolare, nell'ambito delle disposizioni normative e regolamentari, il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali.

Il Regolamento UE 2016/679 rovescia quindi la prospettiva di fondo della disciplina in materia di protezione dei dati personali, in quanto tutto il nuovo quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del Titolare del trattamento.

A quest'ultimo compete l'obbligo di acquisire in maniera formale il consenso dell'interessato al trattamento dei dati personali strettamente necessari alle finalità d'impresa o amministrative ("protection by default"), garantendo all'utente un'informativa espressa dei suoi diritti in materia.

L'art. 25 pone inoltre in capo al Titolare l'onere ("data protection by design") di garantire la protezione dei dati in suo possesso sin dall'origine, individuando strumenti organizzativi e tecnici che possano prevenire eventuali trattamenti non conformi al disposto normativo.

Inoltre, qualora i dati precedentemente acquisiti non siano più necessari o quando dovessero venire meno i presupposti del trattamento o in caso di revoca del consenso da parte dell'interessato, il Titolare è obbligato a rendere le suddette informazioni non più fruibili da alcuno.

[33] Regolamento UE 2016/679, art 23, comma 2

2.2.4 Il dato personale

Ma cosa si intende per dato personale?
Il dato personale può essere definito come qualsiasi informazione riguardante una persona fisica identificata o identificabile.
Si considera identificabile il soggetto che possa essere individuato, direttamente o indirettamente, attraverso elementi caratteristici quali il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo online, o mediante uno o più tratti della sua identità fisica, fisiologica, genetica, psichica, economica, culturale e sociale.
Il concetto di identificabilità, diretta o indiretta, è il discrimine circa l'applicabilità o meno del Regolamento UE n.679/2016.
La normativa infatti non prende in considerazione i dati anonimi, non riconducibili in maniera assoluta ad un individuo, bensì esclusivamente i dati personali c. d. pseudonimizzati[34] cioè resi parzialmente anonimi ma attribuibili ad un interessato specifico tramite l'abbinamento di informazioni aggiuntive che ne consentano la secretazione.
Ne consegue che il diritto alla protezione del dato personale costituisce, nell'ordinamento nazionale e sovranazionale, misura specifica della più ampia tutela delle persone fisiche, intendendosi l'identità come l'essenza stessa dell'essere umano, quale insieme di elementi naturali (fisici e psichici) e scelte soggettive (politica, religione, sesso, precedenti giudiziari) che lo distinguono dagli altri.
Da qui la previsione del trattamento dei dati come strumento al servizio della collettività per contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia.
Nell'alveo dei dati personali confluiscono diverse tipologie di informazioni significative.
I dati identificativi permettono l'individuazione diretta del soggetto; tra questi rientrano i dati anagrafici (nome e cognome, data e luogo di nascita, residenza), quelli bancari (IBAN), fiscali (partita IVA e codice fiscale), telematici (indirizzo IP).
I dati di contatto, invece, consentono di relazionarsi con i soggetti interessati (indirizzo e-mail, un numero di telefono fisso o mobile).

[34] Regolamento UE 2016/679, art 4, comma 5

I dati di natura particolare sono quelle informazioni, assolutamente sensibili, che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, lo stato di salute e l'orientamento sessuale della persona.
Assimilabili ai dati di natura particolare sono quelli giudiziari, quelli genetici e, da ultimo, i dati biometrici, ovverosia i dati personali ottenuti da un trattamento tecnico specifico (impronta digitale, timbro o tonalità della voce, ecc., ecc.).
Il trattamento dei dati biometrici ha assunto una particolare rilevanza durante l'emergenza pandemica, allorché l'accesso a strutture pubbliche o private è stato subordinato alla rilevazione della temperatura corporea tramite telecamere termiche (face detection). Il potenziale contrasto tra il diritto individuale alla riservatezza dei propri dati personali e quello prevalente di sanità pubblica è stato risolto grazie al principio di minimizzazione, in virtù del quale non viene ammessa la registrazione del dato relativo alla temperatura corporea rilevata ma la sola circostanza del superamento della soglia stabilita normativamente.
Più in generale, l'emergenza sanitaria ha costituito un banco di prova effettivo sulla tenuta nelle società democratiche dei presidi posti a tutela dei diritti individuali in occasione di situazioni eccezionali.

2.2.5 I diritti conoscitivi nel DGPR e la loro tutela

Come già ampiamente evidenziato, il tratto distintivo dell'impianto normativo sulla tutela dei dati personali è quello di garantire all'interessato il controllo costante dell'intero processo di trattamento delle informazioni che lo riguardano.
Questa possibilità di controllo deve essere assicurata sia nella fase iniziale di acquisizione dei dati che per tutto il tempo dell'utilizzo degli stessi, fino ad arrivare al diritto alla distruzione delle informazioni raccolte quando non più necessarie o, nell'eventualità di violazioni del dettato normativo, all'accertamento delle stesse ed alla comminazione di sanzioni.
Gli artt. 13 e 14 del DGPR disciplinano il diritto all'informativa, prevedendo che il Titolare del trattamento, nell'ambito della propria autonomia organizzativa, debba assicurare l'esercizio dello stesso al momento del primo contatto con l'interessato o entro un termine breve e comunque entro il limite massimo dei trenta giorni dall'acquisizione dei dati personali.

L'informativa costituisce lo strumento principale di trasparenza assicurato al cittadino europeo, il quale ha diritto di conoscere quali dati personali saranno acquisiti e per quale finalità, come e per quanto tempo le dette informazioni saranno trattate, quali siano gli strumenti di protezione e chi siano i responsabili ultimi del procedimento.
Essa si pone come il presupposto della liceità di detenzione e trattamento dei dati personali e per tale motivo deve essere resa in un linguaggio chiaro e sintetico, così da assicurare l'effettiva consapevolezza del soggetto i cui dati vengono richiesti.
Uguale rilievo viene riconosciuto dal Legislatore al riscontro dell'interessato, ovverosia all'atto con il quale quest'ultimo manifesta la propria volontà libera da condizionamenti di sorta di accettare il trattamento dei dati che lo riguardano. Il consenso, che non può essere sottoposto a vincoli temporali in quanto revocabile in qualsiasi momento, deve essere riscontrato formalmente anche attraverso strumenti elettronici.
Dal momento in cui rilascia il consenso al trattamento dei propri dati l'interessato mantiene il pieno diritto ad accedere agli stessi, nonché a rivendicarne la distruzione (diritto all'oblio) quando siano venute meno le motivazioni circa la loro conservazione e, soprattutto, di poter adire un'Autorità indipendente qualora ravvisi usi impropri delle informazioni rilasciate.
Il Legislatore italiano ha individuato nel Garante per la protezione dei dati personali l'istituzione chiamata ad assicurare l'applicazione della normativa in materia.
Alla sua valutazione possono essere sottoposte ipotesi di violazioni, intendendosi per tali le patologie che abbiano compromesso la tutela dei dati personali comportandone l'impropria diffusione, la modifica e la distruzione parziale o totale, eventi tutti da cui possono derivare danni di diversa rilevanza civile e penale.
Il Garante funge anche da Sportello nei riguardi dei Titolari del trattamento, i quali ultimi sono obbligati a comunicare prontamente le eventuali violazioni di cui siano venuti a conoscenza specificando quali potrebbero essere le conseguenze delle stesse e le misure poste in essere per contenerle.
Il Titolare inoltre, nel caso di grave rischio all'incolumità e alla libertà delle persone fisiche, è tenuto a comunicare le violazioni anche ai diretti interessati. Come ulteriore strumento di tutela e promozione della trasparenza è prevista l'istituzione, all'interno dell'organizzazione di cui il Titolare è responsabile, di un Registro delle violazioni in cui confluiscano tutti gli eventi patologici segnalati al Garante.
Importante è l'assetto sanzionatorio previsto dal Legislatore.

Le sanzioni pecuniarie amministrative possono arrivare fino a 20 mln di euro, ma teoricamente potrebbero risultare anche di importo superiore in quanto riferite ad un parametro che va dal 2 al 4% del fatturato globale dell'azienda sanzionata.
La normativa in materia è stata integrata prevedendo anche l'eventualità di applicare misure prescrittive così da consentire la rimozione di ostacoli interni al completo rispetto dei dettami normativi.

2.2.6 I rischi nel processo di trattamento dei dati personali

Il rischio tipico insito nel processo di trattamento dei dati personali è quello della possibile insorgenza di eventi lesivi dei diritti individuali del soggetto interessato.
Il Titolare del trattamento è quindi chiamato in via preliminare a procedere alla valutazione dei rischi dell'attività posta in essere, così da poter definire analiticamente i processi meritevoli di attenzione e di particolari presidi di sicurezza.
In capo allo stesso grava una responsabilità di compliance, tesa in generale all'organizzazione dei fattori della produzione con modalità conformi alle diverse discipline normative che sovrintendono all'attività d'impresa o amministrativa.
L'individuazione del rischio costituisce attività prodromica all'approntamento di misure appropriate di contenimento dello stesso, più strettamente organizzative se improntate alla definizione di prassi operative individuali, cioè riferite ai comportamenti degli addetti partecipi del processo, o maggiormente indirizzate al controllo delle componenti tecnologiche nel caso di processi automatizzati.
L'attività di mappatura dei rischi del procedimento deve essere condotta con riferimento a principi di trasparenza, che ne consentano una valutazione preventiva sia da parte dell'interessato in sede di acquisizione del consenso che dalle competenti funzioni interne di audit per certificarne la validità.
I presidi di sicurezza individuati per il contenimento del rischio devono essere in primo luogo adeguati allo stesso, così da poter proporzionare gli assetti organizzativi agli eventuali eventi patologici.
Devono essere approntate misure che assicurino la riservatezza dei dati (impedendo la divulgazione degli stessi attraverso accessi non autorizzati), la loro integrità e disponibilità (contrastando l'eventualità di una parziale o totale distruzione delle informazioni acquisite).

I sistemi e servizi di trattamento devono essere resilienti, in grado di garantire il pronto ripristino dei presidi di sicurezza a seguito di incidenti fisici o tecnici.
Il processo di mappatura del rischio deve consentire al Titolare del trattamento di definire il livello di pericolosità dell'evento avverso, ovverosia se il rischio debba essere definito elevato o ordinario in virtù del diverso impatto che una violazione avrebbe sui diritti e le libertà individuali degli interessati.
La classificazione del rischio a seconda del livello di pericolosità, di probabilità del suo verificarsi e dei relativi potenziali danni comporta, ovviamente, l'organizzazione di un sistema di controlli interni diversificato negli approcci tecnologici e di processo finalizzato alla mitigazione del verificarsi del "data breach".
Il Legislatore comunitario ha attribuito una particolare rilevanza allo strumento del DPA, la valutazione d'impatto della privacy.
Quando un tipo di trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve preliminarmente effettuare una valutazione dell'impatto che contenga la descrizione puntuale delle finalità del trattamento, la valutazione delle necessità e proporzionalità del processo in relazione alle finalità, la effettiva ponderazione dei rischi per i diritti e le libertà dell'interessato e le misure previste per mitigare gli eventi avversi, incluse le caratteristiche di sicurezza fatte proprie dall'organizzazione aziendale.
Nell'ipotesi in cui dalla suddetta valutazione dovesse emergere l'impossibilità di predisporre strumenti tecnici e prassi organizzative in grado di attenuare adeguatamente e ragionevolmente il rischio valutato come elevato, si renderà opportuno il coinvolgimento dell'Autorità garante cui dovrà essere richiesto un intervento di carattere prescrittivo.
Il Legislatore comunitario ha infine previsto l'istituzione dei Registri di trattamento, ovverosia l'archivio documentale da tenere a disposizione per comprovare la conformità aziendale ai dettami normativi e dare sostanza probatoria al principio della responsabilizzazione.
L'autonomia del Titolare nella valutazione del rischio e nell'approntamento di una serie di misure tese al contenimento dello stesso deve poter essere riscontrabile a posteriori sia dalle funzioni di controllo interno che eventualmente dalle autorità pubbliche preposte in materia.
Questi Registri devono contenere il nome e i dati di contatto del titolare del trattamento, le finalità del trattamento, una descrizione delle categorie di interessati e delle categorie

di dati personali trattati, le categorie dei destinatari a cui i dati personali sono stati o saranno comunicati ove applicabile i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale.
La tenuta del Registro non costituisce quindi un mero adempimento formale ma uno strumento sostanziale di ulteriore garanzia di valutazione, controllo e mitigazione del rischio.

2.2.7 Violazione dei dati personali

Come comportarsi in caso di violazione dei dati personali?
Per violazione dei dati personali si intende la violazione delle misure di sicurezza dalla quale derivi, in modo accidentale o illecito, la distruzione, la modifica, la perdita o la divulgazione non autorizzata dei dati personali trattati.
La violazione dei dati personali può comportare per l'interessato un danno rilevante, di carattere materiale, biologico e quindi, sostanzialmente, economico.
Il Regolamento estende ai Titolari e Responsabili del Trattamento l'obbligo di comunicare al Garante della privacy eventuali violazioni, obbligo precedentemente in capo esclusivamente al web provider.
La segnalazione deve essere effettuata in modo chiaro e specifico, nel più breve tempo possibile (con tempistiche diverse a seconda della natura giuridica del soggetto tenuto all'inoltro) e deve riportare la natura dell'evento, le circostanze, le conseguenze e i provvedimenti adottati per contrastare gli effetti negativi della violazione.
La suddetta comunicazione, nella quale devono essere sempre indicati i dati di contatto del Responsabile della Protezione, non deve essere portata sempre a conoscenza degli utenti ma solo in casi di particolare gravità.
Le violazioni amministrative in materia di protezione dei dati personali possono essere contestate dall'Ufficio del Garante della privacy o da ogni organo di polizia giudiziaria che le abbia rilevate nel corso degli accertamenti o ispezioni poste in essere nell'ordinaria attività d'indagine.
Il dettato normativo in materia è assicurato dall'articolo 33, che detta le modalità di notifica delle violazioni, e dall'articolo 34, che invece disciplina le modalità di comunicazione delle violazioni alle persone interessate dalle stesse.

2.2.8 ARTICOLO 33: Notifica di una violazione dei dati personali all'Autorità di controllo

«1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. »[35]

L'obbligo dell'articolo 33 è un obbligo non delegabile, in quanto il soggetto individuato espressamente dalla norma è il Titolare del trattamento, il quale procede alla notificazione al Garante senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui sia venuto a conoscenza della violazione.
Non ogni violazione rende obbligatoria la notifica al garante. Infatti, il considerando 85 dispone espressamente che «*non è obbligatorio notificare all'autorità garante quando ha valutato che la violazione intervenuta nei suoi sistemi non è in grado di impattare negativamente sulla sfera dell'interessato».*[36]
Questa precisazione ci offre uno spaccato della "filosofia" del Regolamento, tesa ad assicurare una protezione sostanziale dei dati personali e non anche una burocratizzazione procedurale che, sovrastimando eccessivamente il numero delle violazioni da esaminare, conduca paradossalmente ad una tutela meno incisiva dei diritti degli utenti.

In una ottica di responsabilizzazione il Regolamento insiste moltissimo sulla particolare attenzione che il Titolare del Trattamento deve assicurare ai profili organizzativi interni. Al riguardo, l'articolo 24 dispone in capo al suddetto Titolare l'onere di definire delle corrette politiche aziendali nel trattamento dei dati personali, attraverso l'organizzazione di procedure amministrative e tecniche, di adeguate reti e piattaforme informatiche, che

[35] Regolamento UE 2016/679, art 33, comma 1 e 2
[36] Regolamento UE 2016/679, Considerando 85

siano in grado di intercettare immediatamente eventuali violazioni, di valutarle e procedere o meno ad informare delle stesse il Garante.

Il data breach è spesso infatti conseguenza non solo di problematiche nelle infrastrutture informatiche dell'azienda, ma anche di una non ottimale organizzazione interna incapace di individuare le prassi operative adeguate alla protezione dei dati personali.

Questa consapevolezza organizzativa assume rilevanza allorché si renda necessario analizzare le cause di un eventuale fallimento degli strumenti aziendali di protezione dei dati personali, stimare le conseguenze delle violazioni in riferimento al numero di utenti coinvolti e ai danni da questi subiti e, soprattutto, individuare le misure più opportune per mitigare gli effetti negativi insorti e rafforzare nel futuro la sicurezza delle procedure operative interne.

Una valutazione della specie costituirà anche la base informativa della comunicazione da rendere al Garante, corredata dai dettagli tecnici delle violazioni, dalla descrizione degli impatti susseguenti le infrazioni e delle misure da mettere in pratica per ridurre i danni occorsi agli interessati.

L'inesistenza di un obbligo assoluto di comunicazione al Garante e agli interessati delle violazioni di dati personali non deve però essere estesa alla documentazione delle stesse.

La documentazione degli eventi avversi, di qualsiasi entità o gravità, costituisce infatti il presupposto per una efficace attività di revisione interna dei processi, tesa a rafforzare la sicurezza complessiva nel trattamento dei dati personali posto in essere dall'azienda attraverso l'individuazione di idonee misure preventive di carattere tecnico ed organizzativo.

Per questo motivo il Legislatore comunitario ha introdotto con l'articolo 33 l'obbligo di documentare qualsiasi violazione dei dati personali, disponendo l'istituzione di un Registro delle violazioni in cui confluiscano in forma libera tutte le informazioni raccolte in occasione di ogni evento avverso che abbia riguardato dati personali di terzi. La valenza di questo Registro è quindi non solamente di carattere statistico ma soprattutto di supporto alla funzione aziendale di controllo e mitigazione dei rischi.

2.2.9 ARTICOLO 34: Comunicazione di una violazione dei dati personali all'interessato

«1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). »[37]

Il disposto normativo intende assicurare una pronta informativa all'interessato quando dalla violazione dei dati personali possa derivare per lo stesso un grave rischio per la sua libertà personale o per i suoi diritti.
Assume inoltre una particolare rilevanza il richiamo all'opportunità dell'utilizzo di un linguaggio semplice e chiaro, scevro quindi da eccessivi tecnicismi, che consenta all'interessato di comprendere appieno la portata del danno subito e gli strumenti individuati dal Titolare del trattamento per mitigarne gli effetti negativi.

2.3 Le linee guida e gli orientamenti dell' EBA – il regolamento DORA

Come noto, l'EBA, European Banking Authority, è l'Autorità responsabile della vigilanza sul settore bancario a livello europeo. È stata creata dall'Unione Europea nel 2011, con la riforma seguita alla crisi finanziaria iniziata nel 2008, insieme alla European Securities and Markets Autorithy (ESMA) e alla European Insurance and Occupational Pensions Autorithy (EIOPA), con le quali costituisce il Sistema europeo di vigilanza finanziaria, l'European System of Financial Supervisor (ESFS).
L'attività dell'EBA (che riunisce e coordina le singole autorità di vigilanza nazionali) è focalizzata sull'analisi dei singoli intermediari creditizi e non anche sui rilievi macro-prudenziali, cioè sulle interrelazioni tra il settore bancario e quello economico in generale,

[37] Regolamento UE 2016/679, art 34, comma 1 e 2

che sono invece di competenza dell'European Systemic Risk Board (ESRB). I compiti dell'EBA sono sostanzialmente due: promuovere una vigilanza comune e di alta qualità nel territorio dell'Unione, favorendone l'applicazione uniforme in tutti gli Stati membri, e condurre analisi di rischio riferite al sistema bancario europeo (stress test) allo scopo di verificarne il grado di solidità e l'adeguatezza dei requisiti patrimoniali

Il 28 novembre 2019 l'Autorità bancaria europea ha pubblicato la relazione finale sugli orientamenti sulla gestione del rischio ICT e della sicurezza (EBA/GL/2019/04) al fine di stabilire i requisiti per gli enti creditizi, le imprese di investimento e i prestatori di servizi di pagamento (PSP) in materia di mitigazione e gestione dei rischi ICT e di sicurezza.

L'obiettivo delle Linee guida è quello di stabilire i requisiti per gestione dei rischi legati alle ICT e alla sicurezza, rischi aumentati negli ultimi anni a causa della crescente digitalizzazione del settore finanziario e della maggiore interconnessione con le altre istituzioni finanziarie e con terze parti attraverso i canali di telecomunicazione.

Le disposizioni, entrate in vigore il 30 giugno 2020, hanno definito i principi ai quali tutte le istituzioni finanziarie devono ispirare i piani di gestione dei rischi interni ed esterni legati alle ICT e alla sicurezza cui possono essere esposti.

Le Linee Guida, in sintonia con le finalità dell'EBA, rappresentano un ulteriore passo avanti nel percorso di armonizzazione dell'approccio alla gestione dei rischi ICT e di sicurezza nel mercato unico europeo. Esse recepiscono le indicazioni già rivolte a tutti i Prestatori di servizi di pagamento (PSP) nelle Linee Guida del 2017[38] ai sensi della Direttiva (UE) 2015/2366 (PSD2) - EBA/GL/2017/17.

La ratio che le ispira è che l'ICT[39] (Information and Communication Technology), più comunemente nota come IT (Information Technology), sia ormai una risorsa chiave nello sviluppo e nel supporto dei servizi bancari alla stregua dei fondamentali patrimoniali. Le istituzioni finanziarie hanno avviato una digitalizzazione su larga scala e si affidano all'uso delle ICT per elaborare e analizzare le informazioni e reingegnerizzare le operazioni.

Le ICT possono essere implementate dalle istituzioni finanziarie per migliorare i processi interni o per offrire servizi innovativi e nuove funzioni ai clienti, al fine di soddisfare al meglio le loro aspettative ed esigenze sempre crescenti. Tuttavia, la complessità delle

[38] Misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento

[39] «*Tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli utenti di creare, immagazzinare e scambiare informazioni. Rilevanti incentivi economici favoriscono questo processo di integrazione, promuovendo la crescita delle imprese attive nel settore.*» (Enciclopedia Treccani)

tecnologie adottate e la continua crescita della dipendenza da esse può condurre ad un aumento degli incidenti legati alle ICT e alla sicurezza.

Secondo la definizione fornita nelle Linee Guida, il concetto di rischio ICT implica l'esistenza di un rischio di perdita dovuto alla violazione della riservatezza e dell'integrità dei sistemi e dei dati, all'in appropriatezza o indisponibilità degli stessi, all'incapacità di modificare la tecnologia dell'informazione in tempi e costi ragionevoli al mutare degli obiettivi aziendali.

I rischi per la sicurezza sono imputabili invece a processi interni inadeguati o falliti, a eventi esterni o ad un contesto ambientale in cui la sicurezza fisica sia inadeguata.

Il concetto di rischio così definito appare coerente con l'approccio al rischio operativo (ossia agli eventi negativi derivanti da processi interni) perché, se l'evento si realizza, si traduce in una perdita.

Di conseguenza, i rischi operativi, ICT, di sicurezza delle informazioni e quelli più specifici sono ora direttamente correlati tra loro.

La correlazione con i rischi operativi è ulteriormente prescritta dalle attuali Linee Guida dell'EBA sul processo di revisione e valutazione prudenziale (SREP), emanate in virtù dell'art.74 della Direttiva 2013/36/UE con la quale l'Autorità è stata incaricata di armonizzare la governance delle istituzioni finanziarie. Queste disposizioni, volte a promuovere procedure e metodologie comuni per il processo di valutazione della vigilanza, prescrivono alle Autorità nazionali di valutare il rischio ICT e di sicurezza come una sottocategoria del rischio operativo.

In effetti, nel più ampio contesto della Direttiva sui requisiti patrimoniali IV[40], la gestione del rischio ICT e di sicurezza svolge un ruolo cruciale nella calibrazione dei requisiti patrimoniali aggiuntivi a copertura dei rischi rilevanti. Le Linee Guida evidenziano anche il nuovo ruolo della gestione del rischio ICT e di sicurezza come acceleratore per le istituzioni finanziarie nel miglioramento della loro resilienza operativa all'evoluzione delle minacce informatiche.

Gli orientamenti del 2019 definiscono dei principi diversificati per ambito di attività al fine di mitigare per ciascuno di essi i rischi ICT e di sicurezza, principi di seguito sinteticamente descritti:

[40] CRD V

- Gestione della continuità operativa: creazione di un solido processo di gestione della continuità operativa che includa l'analisi dell'impatto sul business, la pianificazione della continuità operativa e le attività di pianificazione della risposta e del ripristino.
- Governance e strategia: allineamento della strategia ICT con la strategia aziendale complessiva così da configurare una governance unica e adeguata.
- Quadro di gestione del rischio ICT e di sicurezza: creazione di un quadro di gestione del rischio ICT e di sicurezza supportato dall' esecuzione di valutazioni periodiche del rischio e dall'attività di audit e reporting.
- Gestione dei progetti e dei cambiamenti ICT: implementazione dei processi che regolano e supportano l'acquisizione del sistema ICT, la gestione dei cambiamenti ICT e la gestione dei progetti ICT.
- Gestione delle operazioni ICT: implementazione di processi documentati per gestire le ICT in modo controllato, inclusa la gestione della capacità, la gestione degli incidenti e la risoluzione dei problemi.
- Sicurezza delle informazioni: documentazione e sviluppo di processi aziendali tesi al raggiungimento di livelli adeguati di sicurezza logica e fisica, anche attraverso la formazione del personale e l'attività di monitoraggio costante.

Ad integrazione delle Linee guida del 2019 il 10 giugno 2021 l'EBA ha pubblicato la versione finale degli Orientamenti sulla segnalazione degli incidenti gravi ai sensi della Direttiva sui servizi di pagamento (PSD2) (gli "Orientamenti" - EBA/GL/2021/03), con la quale sono stati rivisti i principi sulla segnalazione individuati nel 2017 di concerto con la Banca Centrale Europea.

Nel corso del 2020, infatti, l'EBA aveva avviato la revisione biennale degli orientamenti[41] valutando le segnalazioni ricevute fino a quel momento. Scopi del processo revisionale erano quello di ottimizzare e semplificare il processo e i modelli di segnalazione, di concentrarsi sugli incidenti con un impatto significativo sui PSP e di migliorare la rilevanza delle informazioni da segnalare riducendone l'onere.

Le disposizioni rinnovate stabiliscono i criteri, le soglie e la metodologia che i Prestatori di servizi di pagamento (PSP) devono osservare per determinare se un incidente operativo o di sicurezza debba essere considerato grave e, nell'ipotesi che venga così

[41] Direttiva europea 2015/2366, ex art. 96, par. 4

qualificato , come tale incidente debba essere notificato all'autorità nazionale competente (ANC), ai sensi dell'articolo 96, paragrafo 2, della PSD2.

L'obiettivo principale dell'attività di consultazione era quello di conseguire un'economia procedurale che consentisse di conciliare le esigenze di segnalazione con l'opportunità di ridurre drasticamente gli oneri a carico dei prestatori di servizi.

Di conseguenza, si è ritenuto opportuno circoscrivere l'obbligo di segnalazione degli incidenti operativi solo a quelli effettivamente gravi e quindi di interesse per le Autorità nazionali, superando definizioni precedentemente adottate del concetto di violazione dei sistemi di sicurezza troppo generiche e diseconomiche. Questa modifica, che è la più sostanziale, ha lo scopo di restringere la portata del criterio, evitare qualsiasi sovrapposizione con altre modalità di classificazione e fornire un criterio più tangibile che non richieda una valutazione e un'attuazione complesse.

Le disposizioni si concentrano sulle azioni dolose che hanno compromesso la rete o i sistemi informativi relativi alla fornitura di servizi di pagamento, prevedendo comunque la possibilità di segnalare ulteriori incidenti di sicurezza che potrebbero essere di interesse per le autorità di vigilanza.

Per ridurre l'onere di segnalazione in capo ai PSP sono state eliminate alcune fasi del processo ritenute non più necessarie, stabilito un termine perentorio (24 ore) entro il quale l'incidente deve essere classificato, determinato il lasso temporale massimo (4 ore) per l'inoltro della segnalazione, circoscritta l'ipotesi di presentazione di rapporti intermedi e concesso più tempo (20 giorni) per la presentazione della relazione sulla risoluzione dell'incidente.

I nuovi orientamenti hanno peraltro ulteriormente semplificato e ottimizzato il modello di segnalazione standardizzato, modifiche queste che si presume porteranno a una riduzione di oltre il 10% degli incidenti da segnalare così facilitando i prestatori di servizi di pagamento nella loro attività.

Lo scenario normativo sinora descritto è però destinato a mutare drasticamente a breve con la prossima emanazione del Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario (DORA).

Il Regolamento fa parte del cosiddetto "Pacchetto di finanza digitale dell'Unione Europea" che comprende, oltre a Dora, altre normative[42] nell'ambito delle cripto-attività e una serie

[42] MiCa, infrastrutture di mercato basate sulle DLT

di modifiche a precedenti direttive volte a garantire un quadro regolamentare armonizzato.
La strutturazione definitiva della normativa di prossima emanazione è stata comunicata nel Documento rilasciato il 23 giugno 2022 concordemente dal Parlamento, il Consiglio e la Commissione europea.
In esso viene evidenziato come, sebbene il settore finanziario dell'Unione sia regolamentato da un codice unico armonizzato e disciplinato da un sistema europeo di vigilanza finanziaria, le disposizioni sulla resilienza operativa digitale e sulla sicurezza delle ICT non sono tuttavia armonizzate in maniera completa e coerente.
Tali lacune ed incoerenze hanno condotto alla proliferazione di iniziative nazionali (per esempio in materia di test) e di approcci di vigilanza (in particolare per quanto riguarda le dipendenze da terze parti nel settore delle ICT) non coordinati, dando luogo a sovrapposizioni, duplicazioni di requisiti ed elevati costi amministrativi e di conformità per le imprese finanziarie e transfrontaliere.
Il Regolamento mira quindi a predisporre un quadro normativo sulla resilienza digitale grazie al quale tutte le imprese potranno garantire di far fronte a tutti i tipi di malfunzionamento e minacce connessi all'uso delle ICT, così da prevenirli o mitigarli.
La portata storica di DORA sarà nel suo perimetro di applicazione, stante l'elevatissimo numero di soggetti destinatari della normativa che va ben oltre gli enti finanziari propriamente detti: si stima al riguardo che saranno oltre 20.000 i soggetti che dovranno attenersi alle nuove disposizioni.

2.4.1 Circolare n. 285 del 17 dicembre 2013

La Banca d'Italia incoraggia da sempre la digitalizzazione del sistema finanziario nella convinzione che, attraverso l'evoluzione delle architetture informatiche, si possano creare le condizioni per garantire lo sviluppo e la modernizzazione dell'industria finanziaria nel suo complesso.
Nell'ambito di questo processo una particolare attenzione è sempre stata prestata ai profili di sicurezza ICT, inizialmente interpretati alla stregua di presidi contro i rischi operativi nell'ambito delle strategie per garantire la continuità operativa. È proprio in questo contesto che è progressivamente emersa la consapevolezza della minaccia informatica.

La Banca d'Italia presiede il "Comitato per la continuità di servizio della piazza finanziaria italiana" (Codise), un'unità di continuità operativa istituita nel 2003 per coordinare la gestione delle crisi nel mercato finanziario italiano. Al Comitato partecipano gli operatori del settore finanziario sistemico e la Consob. Il Codise effettua regolarmente simulazioni di crisi a titolo di esercitazione, le quali, già nel 2008, includevano la possibilità di attacchi informatici.

Con l'evoluzione della tecnologia e la proliferazione degli attacchi, in aggiunta alla continuità operativa anche altre aree di attività aziendali hanno acquisito importanza. La Banca d'Italia sta ponendo in essere una serie di attività per rafforzare la sicurezza delle architetture informatiche bancarie e del sistema finanziario in genere. Conduce inoltre ricerche sulla cybersecurity dell'economia nel suo complesso, nella consapevolezza che le vulnerabilità in altri settori potrebbero influire anche sulla sicurezza del sistema finanziario.

La Banca d'Italia è responsabile della cybersecurity nel sistema finanziario e, in qualità di istituzione garante della stabilità del sistema bancario sul quale esercita attività di regolamentazione e supervisione, ha introdotto requisiti specifici per la gestione dei sistemi informativi delle banche attraverso l'emanazione delle "Disposizioni di vigilanza per le banche" (Circolare n. 285/2013).

Tali previsioni includono misure di sicurezza ICT per i soggetti vigilati, nonché l'obbligo di segnalare gli incidenti di sicurezza rilevanti, ivi compresi gli attacchi informatici.

Nell'ambito dell'SSM la Banca d'Italia partecipa alla valutazione del rischio informatico delle banche cosiddette "significative", ovverosia di quelle istituzioni che per dimensioni, volumi di operatività e potenziali rischi sistemici sono sottoposte alla vigilanza diretta da parte della BCE e non delle singole BCN. Questa attività ha avuto inizio nel 2015 con l'invio di un questionario di autovalutazione alle banche per individuare quali fossero le più esposte, in modo che potessero essere oggetto di una più approfondita vigilanza cartolare e on site. Inoltre, in ambito europeo la Banca d'Italia partecipa alla stesura delle linee guida dell'EBA sui rischi ICT e di sicurezza per gli intermediari bancari e finanziari. Infine, a livello internazionale, nell'ambito del Senior Supervisory Group e del Comitato di Basilea per la vigilanza bancaria, sta collaborando alla definizione di best practice per la cybersecurity.

Dal 1° gennaio 2014 è divenuta applicabile la disciplina armonizzata per le banche e le imprese di investimento contenuta nel regolamento CRR (Regolamento UE 575/2013, Capital Requirements Regulation) e nella direttiva CRD IV (Direttiva 2013/36/UE, Capital Requirements Directive IV), che recepiscono nella normativa comunitaria gli standard definiti dal Comitato di Basilea per la vigilanza bancaria.
Sono stati introdotti alcuni adempimenti in capo al settore creditizio volti a rafforzare i requisiti patrimoniali delle banche, attraverso l'accantonamento di quote di capitale proporzionali al rischio derivante dai crediti erogati.
Il quadro normativo si completa con l'emanazione delle misure di esecuzione, contenute in norme tecniche di regolamentazione o di attuazione adottate dalla Commissione europea su proposta dell'Autorità bancaria europea (ABE) e, in alcuni casi, delle altre Autorità europee di supervisione (ESA).
Nella Circolare n. 285 la sezione III del capitolo 4 è espressamente dedicata all'analisi del rischio informatico.
La valutazione del rischio informatico deve essere posta in essere in occasione delle iniziative di sviluppo di nuovi progetti e di modifica rilevante del sistema informativo.
Il processo va ripetuto con una periodicità adeguata alla tipologia delle risorse ICT e dei rischi, nonché, tempestivamente, al verificarsi di situazioni che possano influenzare il complessivo livello di rischio informatico.
La valutazione del rischio informatico costituisce un presidio fondamentale per garantire la sana e prudente gestione dell'organizzazione bancaria nel suo complesso e, come tale, è oggetto di monitoraggio continuo da parte delle Autorità di settore.

2.4.2 Governo e organizzazione del sistema informativo

All'organo societario con funzioni di supervisione strategica compete la responsabilità organizzativa di dirigere e controllare i sistemi informativi al fine di ottimizzare l'uso delle risorse tecnologiche a sostegno della strategia aziendale (governance ICT).

In questo ambito è chiamato a:

- approvare la strategia di sviluppo dei sistemi informativi, tenendo conto dell'evoluzione del settore di riferimento e allineandola al consolidamento attuale e futuro delle unità di business, dei processi e delle strutture aziendali;

- approvare la policy aziendale in materia di sicurezza informatica;
- determinare le linee guida per la selezione del personale con capacità tecniche e per l'acquisizione di sistemi, software e servizi, compreso il ricorso a fornitori esterni;
- favorire lo sviluppo, la condivisione e l'aggiornamento delle conoscenze ICT interne;
- ricevere tempestivamente le segnalazioni di eventuali problemi di rilievo nelle operazioni dell'azienda derivanti da incidenti o guasti nei sistemi informativi;
- adottare un quadro organizzativo e metodologico per l'analisi del rischio informatico;
- promuovere l'uso appropriato delle informazioni sul rischio tecnico all'interno della funzione ICT e la loro integrazione con i sistemi di misurazione e gestione del rischio (in particolare, operativo, reputazionale e strategico).

L'organo aziendale avente funzioni gestionali è responsabile di garantire l'integrità, l'adeguatezza, la funzionalità (efficienza ed efficacia) e l'affidabilità del sistema informativo. In particolare, ad esso compete:

- la definizione del quadro organizzativo, metodologico e procedurale per il processo di analisi del rischio informatico e ricercare un adeguato livello di comunicazione con la funzione di gestione del rischio per il processo di valutazione del rischio operativo;
- l'approvazione, salvo il caso di full outsourcing, della struttura del processo di gestione del sistema informativo, assicurandone l'efficienza e l'efficacia, nonché l'integrità e la coerenza complessiva (tenendo conto, tra l'altro, della distribuzione funzionale dei compiti e delle responsabilità, dell'affidabilità dei controlli e dell'adeguatezza dei supporti metodologici e procedurali);
- la definizione degli standard di gestione dei dati, le procedure di gestione delle modifiche ai piani operativi per le iniziative IT, verificando che siano coerenti con le esigenze informative e con la strategia aziendale.
- la valutazione complessiva del rischio informatico in relazione alle tendenze di rischio identificate;
- l'organizzazione di un flusso informativo adeguato sul livello di rischio residuo delle varie risorse informatiche, sull'attuazione delle misure di mitigazione del rischio, sull'evoluzione delle minacce e degli incidenti registrati durante il periodo di riferimento.
- il monitoraggio costante dell'efficacia dei processi di gestione e controllo dei servizi ICT e l'attuazione delle opportune azioni correttive qualora vengano rilevate anomalie;

- l’assunzione di decisioni tempestive in occasione dei principali incidenti di sicurezza informatica;
- l’assicurazione di un flusso informativo immediato ed esaustivo all'organo con funzione di supervisione strategica quando un incidente o un guasto informatico possa comportare problemi significativi per l'attività dell'azienda.

Le molteplici attività e responsabilità in capo all’organo avente funzioni di gestione presuppone, logicamente, il possesso delle competenze tecniche e manageriali adeguate alle dimensioni operative, alla complessità delle relazioni organizzative e al posizionamento sul mercato finanziario del singolo intermediario.
La struttura organizzativa della funzione ICT dipende da fattori quali la complessità della struttura aziendale, le dimensioni, il settore di attività, la strategia aziendale e la strategia di gestione.
Sulla base dei criteri di funzionalità, efficienza e sicurezza vengono definiti chiaramente i compiti e le responsabilità individuali, assicurate peraltro dalla sussistenza di determini presidi organizzativi.
Al riguardo, devono essere definite delle linee di report diretto con la funzione d’indirizzo gestionale al fine di garantire un approccio univoco al fenomeno dei rischi informatici e l'applicazione uniforme delle regole per i sistemi informativi. Le unità di sviluppo distribuite sotto il controllo delle linee di business sono comunque riunite all'interno di un disegno architetturale più generale e operano, secondo le regole definite a livello aziendale, per la pianificazione e gestione dei portafogli di progetti IT e dei sistemi informativi. Infine, deve essere assicurata l’implementazione di meccanismi appropriati per interagire con le funzioni di business, in particolare per quanto riguarda la definizione e la pianificazione delle iniziative IT.

2.4.3 L’analisi del rischio informatico

L'analisi del rischio informatico costituisce il principale strumento per garantire l'efficacia e l'efficienza delle misure di protezione delle risorse ICT, graduando le misure di mitigazione nei diversi ambienti in base al profilo di rischio dell'intermediario.
Questa attività viene svolta nell'ambito di iniziative di sviluppo di nuovi progetti o di modifiche importanti ai sistemi informativi, ripetendosi ciclicamente per valutare la

congruità delle risorse stanziate in rapporto ai rischi presumibili. Il processo di valutazione viene invece eseguito tempestivamente qualora si verifichino eventi che possano influire sul livello complessivo di rischio informatico.
La mappatura del rischio informatico comporta la stima preventiva delle risorse ICT da assicurare nell' ipotesi di scenari di rischio rilevanti che potrebbero compromettere la sicurezza dei processi aziendali. L'obiettivo finale è quindi quello di individuare delle misure (organizzative, procedurali e tecniche) di mitigazione del rischio e dei danni da esso potenzialmente derivanti.

L'analisi del rischio si conclude con la determinazione dei rischi residui da sottoporre all'accettazione formale dell'utente responsabile.
Qualora il rischio residuo dovesse superare la propensione al rischio IT precedentemente approvata dall'organo con funzione di supervisione strategica, dovranno essere portate all'attenzione dell'organo con funzioni di gestione ulteriori misure di gestione del rischio alternative o aggiuntive.
Il programma di attuazione del piano e le eventuali misure compensative organizzative o procedurali devono essere documentate prima dell'attuazione, presentate all'utente responsabile e adottate formalmente. In ogni caso, le misure di sicurezza che riguardano le componenti critiche vengono aggiornate senza ritardi ingiustificati.
I risultati del processo (livello di classificazione, rischi potenziali e residui, elenco delle minacce considerate, elenco delle azioni protettive identificate), i successivi aggiornamenti, gli scenari presi in considerazione e le decisioni assunte sono documentati e comunicati all'organo di gestione aziendale.

2.4.4 La sicurezza delle informazioni

La sicurezza delle informazioni e delle risorse informatiche è garantita da misure di sicurezza a livello fisico e logico, la cui intensità viene gradualmente adattata in base ai risultati della valutazione dei rischi.
Le misure di sicurezza sono organizzate su più livelli di progressiva intensità, in modo tale da garantire l'effettività della tutela anche nell'ipotesi di una violazione della prima linea di difesa ("difesa in profondità").

Il primo presidio di sicurezza, per quanto apparentemente scontato, è costituito dalla preventiva autorizzazione e dal relativo controllo per l'accesso fisico ai sistemi e ai dati(ad esempio, barriere perimetrali con punti di ingresso sicuri, stanze controllate con registri di accesso).
I diritti di accesso logico alle reti, ai sistemi e ai database sono solitamente concessi sulla base di un'autorizzazione formale, che tenga conto delle mansioni, del livello gerarchico rivestito dall'addetto incaricato e, soprattutto, delle effettive esigenze aziendali ("principio della necessità di sapere"). Il personale adeguatamente formato, supervisionato e ritenuto affidabile viene abilitato informaticamente con il rilascio di appositi profili di autorizzazione, profili periodicamente sottoposti a revisione e controllo. Sui dipendenti abilitati gravano alcuni oneri specifici (quali il rispetto dei principi di autorità minima), garantiti dalla separazione dei compiti e dalla rotazione delle mansioni, nonché dalle procedure specifiche di autorizzazione e certificazione ("quattro occhi" e controlli giornalieri successivi).
La gestione dei prodotti, degli strumenti e delle procedure associate ai processi di controllo degli accessi garantisce che tali processi siano protetti da tentativi di violazione o elusione, in particolare per quanto riguarda la sottoscrizione, la consegna, la cancellazione o il ritiro degli stessi.

In particolare, viene assicurata la conformità agli standard interni e alle normative applicabili per quanto riguarda l'associazione chiara delle credenziali di accesso di ciascun utente, la protezione della riservatezza dei fattori di autenticazione, la composizione e la gestione delle password, la limitazione dei tentativi di accesso e la lunghezza delle chiavi di crittografia.
Anche l'accesso dei terzi ai sistemi e ai servizi critici attraverso i canali disponibili al pubblico (ad esempio, l'electronic banking e altri canali digitali su Internet) deve essere adeguatamente protetto, così da assicurare requisiti di sicurezza rigorosi e fornire un livello di protezione commisurato ai rischi affrontati. I servizi di pagamento via Internet sono soggetti agli orientamenti finali dell'EBA sulla sicurezza di queste transazioni.

Per proteggersi dagli eventi valutati nell'analisi del rischio informatico come aventi un alto livello di rischio potenziale si rende necessario implementare metodologie e tecnologie di sviluppo di software volti a contrastarli.

Per prevenire e controllare gli incidenti di sicurezza delle informazioni, gli accessi ai sistemi informatici e le operazioni poste in essere sono monitorati attraverso l'analisi dei log e dei registri di audit. Le minacce alla sicurezza sono continuamente monitorate tenendo conto dei fattori endogeni ed esogeni significativi, in riferimento alle attività aziendali e ai rapporti con gli interlocutori esterni.
Le azioni organizzative da cui potrebbero derivare degli impatti significativi sui sistemi informativi aziendali (ad esempio, modifiche rilevanti alle componenti critiche, adeguamenti a seguito di una fusione o di una vendita, migrazione verso altre piattaforme informatiche) devono essere preventivamente comunicate alla Banca Centrale Europea o alla Banca d'Italia per i profili di competenza.

2.4.5 La gestione degli incidenti di sicurezza informatica

Gli incidenti di sicurezza informatica sono gestiti secondo procedure formalmente definite per ridurne al minimo l'impatto e garantire che i servizi e le risorse TIC coinvolti siano ripristinati in modo tempestivo.

Secondo la Circolare n. 285 un incidente di sicurezza informatico può essere definito come: *«ogni evento, o serie di eventi collegati, non pianificati dalla banca che interessa le sue risorse informatiche e che i) ha o potrebbe avere un impatto negativo sull'integrità, la disponibilità, la riservatezza, l'autenticità e/o la continuità dei servizi o dei processi dell'intermediario; oppure ii) comunque implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi)»*[43]

Gli incidenti più gravi legati al rischio di continuità operativa vengono portati all'attenzione dell'organo aziendale competente per l'eventuale dichiarazione di una situazione di crisi.
Un incidente di sicurezza informatica è considerato grave qualora dallo stesso consegua, o possa conseguire, almeno una delle seguenti ripercussioni:
a. gravi perdite economiche o interruzione a lungo termine dell'attività dell'intermediario, anche a seguito di ripetuti incidenti di minore entità;

[43] Circolare n.285 del 17 dicembre 2013, Titolo IV, Capitolo 4, Sezione I

b. gravi perturbazioni ai clienti e ad altri soggetti (ad esempio, intermediari e infrastrutture di pagamento): la valutazione della gravità tiene conto del numero di clienti o controparti potenzialmente interessati e dell'entità del rischio;
c. rischio di compromissione della capacità della banca di rispettare i requisiti o gli obblighi di legge o di vigilanza
d. danni alla reputazione in caso di pubblicità all'esterno, attraverso i media o altri canali informativi, degli incidenti di sicurezza informatica.
Gli incidenti di sicurezza vengono sottoposti al vaglio delle competenti funzioni di audit aziendale alle quali spetta il compito di individuare le azioni correttive da porre in essere al fine di evitare il ripetersi di eventi della specie.
Questo processo, formalmente documentato, comporta la revisione integrale dei sistemi informatici aziendali ed il monitoraggio degli accessi agli stessi e delle operazioni effettuate. Costituisce parte integrante dell'attività revisionale la valutazione della resilienza organizzativa in occasione del verificarsi di incidenti informatici e l'efficacia delle procedure di segnalazione degli eventuali problemi da parte degli utenti interni ed esterni. Obiettivo dell'attività di internal audit è quello di intraprendere azioni preventive e definire indicatori di allerta precoce che siano in grado di intercettare gli eventi avversi nella fase iniziale di sviluppo.

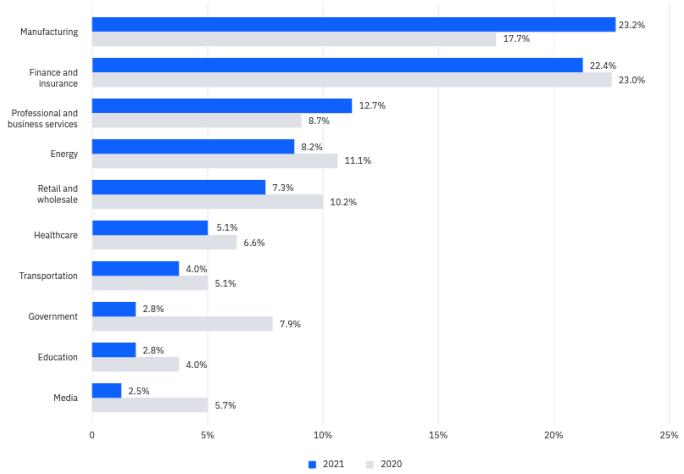
Le procedure individuate per gli incidenti critici di sicurezza informatica devono prevedere la cooperazione con le autorità competenti e con gli altri operatori o organizzazioni coinvolti.
Gli incidenti critici di sicurezza informatica devono essere tempestivamente segnalati alla Banca d'Italia inviando una relazione sintetica che includa la descrizione dell'incidente, le eventuali inadempienze degli utenti interni e dei clienti e qualsiasi altro dato o informazione richiesto dalla normativa vigente

CAPITOLO 3: GLI ATTACCHI INFORMATICI NEGLI ISTITUTI CREDITIZI

3.1 La cybersecurity negli istituti finanziari

La cybersecurity nell'operatività degli istituti finanziari (FI) è divenuta ormai da anni una tematica d'importanza cruciale, stante l'enorme mole di dati trattati e le implicazioni patrimoniali, finanziarie, legali e reputazionali che conseguono agli attacchi informatici.
L'esistenza stessa delle aziende che operano nei mercati finanziari è condizionata dall' esigenza di assoluta intangibilità dei dati e delle reti di trasmissione degli stessi, in un contesto di estrema interrelazione tra gli operatori dei sistemi di pagamento e delle infrastrutture finanziarie.
Parallelamente allo sviluppo delle tecnologie digitali, nell'attività degli istituti finanziari si è assistito nel tempo al proliferare continuo dei tentativi di accesso indebito ai sistemi informativi da questi gestiti.
Dal 2015 ad oggi il settore finanziario e assicurativo è stato quello maggiormente interessato a livello globale dalle minacce informatiche.
Una ricerca di IBM X-Force evidenzia come nel 2021 il 70% degli attacchi alle imprese finanziarie sia stato rivolto alle banche, il 16% alle compagnie di assicurazione e il 14% ad altre istituzioni finanziarie. Il diverso peso percentuale riveniente dallo studio è imputabile a diversi fattori, tra i quali in primo luogo gli investimenti posti in essere per massimizzare la sicurezza aziendale, l'operatività in sistemi cloud ibridi, le dimensioni e la complessità delle infrastrutture e degli archivi dati gestiti.

Figura 8: Ripartizione degli attacchi ai 10 principali settori industriali, 2021 vs 2020



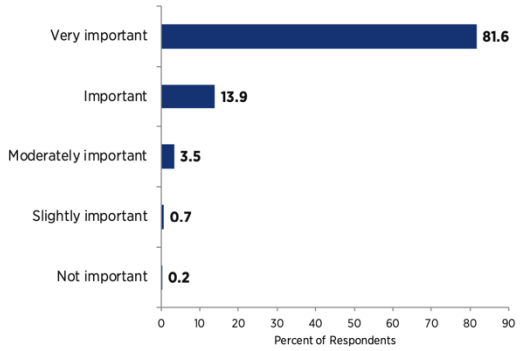
Fonte: IBM Security X-Force

Un Rapporto di BCG dimostra inoltre che i servizi finanziari (FS) hanno 300 volte più probabilità di essere vittime di un attacco informatico rispetto ad altri settori commerciali ed industriali.

Questo scenario di grave pericolosità si riflette ovviamente sulla percezione che di questi rischi hanno le istituzioni operanti nel settore finanziario.

Da un sondaggio effettuato dalla Conference of State Bank Supervisors (CSBS) nel settembre 2021, il rischio di cybersecurity è stato giudicato "estremamente importante" da oltre l'80% degli operatori intervistati, risultando di gran lunga il principale rischio operativo tra quelli ordinariamente valutati e mitigati.

Figura 9: Quanto è importante il cyber risk?



Fonte: Conference of State Bank Supervisors

La crisi pandemica ha indubbiamente svolto un ruolo di acceleratore del processo già in atto di innovazione digitale dei servizi di pagamento e finanziari proposti all'utenza, dispiegando i propri effetti anche nella diversa organizzazione del lavoro interno riorientata verso un modello ibrido in cui le prestazioni offerte da remoto hanno assunto una enorme rilevanza.

Più in generale, lo sviluppo della finanza digitale (FinTech) e la maggiore presenza sul mercato creditizio di banche operanti esclusivamente on line hanno spostato sulle infrastrutture digitali una massa enorme di transazioni finanziarie, esponendo queste ultime al rischio di manipolazioni fraudolente.

Sin dai primi mesi di restrizioni seguite all'emergenza sanitaria si era potuto assistere ad una escalation degli attacchi informatici al settore finanziario, aumentati nel trimestre febbraio-marzo 2020 del 238%.

Considerando il costo medio di una violazione grave di dati in ambito finanziario, stimata da fonti autorevoli in 5,72 milioni di dollari, si capisce perché la Presidente della BCE, Christine Lagarde, intervenendo alla conferenza annuale del Comitato Europeo per il rischio sistemico (ESRB) abbia definito come tale i diffusi attacchi informatici al sistema finanziario europeo.

«Gli attacchi informatici agli ospedali in Europa durante la crisi COVID-19 e l'attacco alla Colonial Pipeline negli Stati Uniti ci hanno dato un assaggio di ciò che potrebbe accadere in futuro. Un attacco di questo tipo è probabilmente una questione di "quando", non di "se" [..] Collettivamente, dobbiamo essere preparati a gestire le conseguenze sulla stabilità finanziaria di un grave incidente informatico. Se si verificasse un evento del genere, sarà essenziale una risposta coordinata e rapida per preservare la fiducia e ristabilire informazioni affidabili. Ciò potrebbe richiedere nuove forme e meccanismi di cooperazione e comunicazione. Le autorità finanziarie devono adattarsi a questo nuovo ambiente, poiché anche il panorama delle minacce informatiche è in continua evoluzione.»

Le conseguenze dei data breach sono sempre più allarmanti, sia in termini economici che di responsabilità legale. Le violazioni dei dati personali danno sempre più spesso luogo a contenziosi giurisdizionali, con l'attuale marcata diffusione di una serie di azioni collettive nel Regno Unito e negli Stati Uniti.
Nel 2019 la violazione dei dati della banca Capital One, una delle più gravi mai verificatesi, ha portato alla comminazione da parte dell'Autorità di controllo di una sanzione pecuniaria da 80 milioni di dollari e a una miriade di azioni legali da parte dei clienti danneggiati.
Non meno gravi per le istituzioni finanziarie sono le minacce alla continuità operativa, in primis dei sistemi di pagamento, che hanno dimostrato la vulnerabilità della resilienza aziendale agli attacchi informatici e alle conseguenti richieste di riscatto.
Nell'ottobre 2020 un guasto tecnico dalle cause incerte ha bloccato le contrattazioni delle borse giapponesi, mentre solo un paio di mesi prima la borsa neozelandese era stata costretta ad interrompere le contrattazioni a seguito della segnalazione di un attacco prolungato DDoS (Distributed Denial of Service) subito da un prestatore dei servizi di rete. Questi incidenti sono avvenuti a distanza di poco tempo dal verificarsi di un attacco

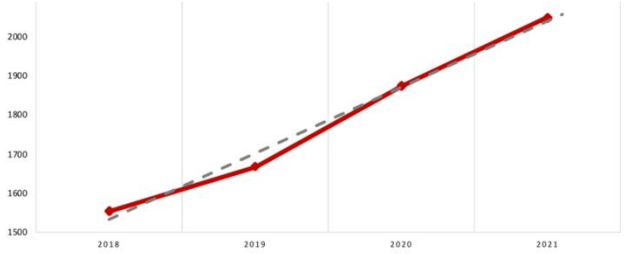
ransomware che ha causato il blocco operativo per quasi un mese della società di cambio Travelex, con gravi ripercussioni sui servizi offerti da diverse istituzioni finanziarie.
Al riguardo, nel Regno Unito la Financial Conduct Authority (FCA) ha recentemente introdotto regole e linee guida sulla resilienza operativa per banche e assicurazioni. Le norme, entrate in vigore il 31 marzo 2022, prescrivono alle imprese finanziarie l'adozione di misure interne idonee ad affrontare le interruzioni di importanti servizi aziendali dovute a una serie di eventi, tra cui attacchi informatici, guasti tecnici e interruzioni di corrente.

In Europa invece è di prossima emanazione il Regolamento la sulla resilienza operativa digitale (DORA) che introdurrà un quadro normativo comunitario sulla resilienza operativa digitale per un'ampia gamma non solo di imprese di servizi finanziari, con particolare attenzione alla continuità operativa e alla gestione del rischio di terzi.
La resilienza degli istituti alle vecchie e nuove minacce informatiche è quindi avvertita come un fattore vitale non solo per le istituzioni finanziarie, ma per la stabilità economica complessiva. Da qui la rinnovata attenzione verso la sicurezza informatica che vediamo già ben rappresentata nell'evoluzione normativa che da Basilea II ci sta portando a DORA.
Per difendersi dal cybercrime, essere pronti a contrastare le nuove minacce informatiche e adeguarsi a normative di settore sempre più stringenti le istituzioni finanziarie sono chiamate ad attuare un riposizionamento strategico delle politiche aziendali di gestione del rischio, in particolar modo di quello informatico.

Ma quali sono nello specifico i rischi che le banche e le altre istituzioni finanziarie devono oggi affrontare?

Lo scenario attuale degli attacchi di cui si ha notizia pubblicamente è quello proposto dal Rapporto CLUSIT, aggiornato a maggio 2022, che riporta un trend in forte crescita sia dei tentativi di intrusione fraudolenta nei sistemi informatici in genere che di quelli andati a buon fine e causa di danni patrimoniali e non.

Figura 10: Crescita dei cyber attacchi per anno 2018 - 2021

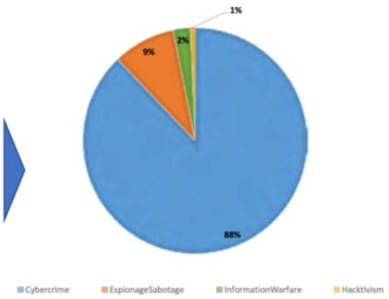


Fonte: Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Il Rapporto illustra in dettaglio gli eventi che hanno avuto conseguenze gravi proponendo una matrice molto interessante.

Figura 11: Tipologia di attacchi

ATTACCANTI PER TIPOLOGIA	2018	2019	2020	2H 2020	1H 2021	1H 2021 su 2H 2020	Trend 2021
Cybercrime	1.229	1.381	1.518	764	925	21.1%	↑
Espionage-Sabotage	203	203	264	150	95	-36.7%	↓
Hacktivism	64	48	48	21	7	-66.7%	↓
Information Warfare	58	35	44	22	26	18.2%	↑
Espionage-Sabotage + Inf. Warfare	261	238	308	172	121	-29.65%	↓

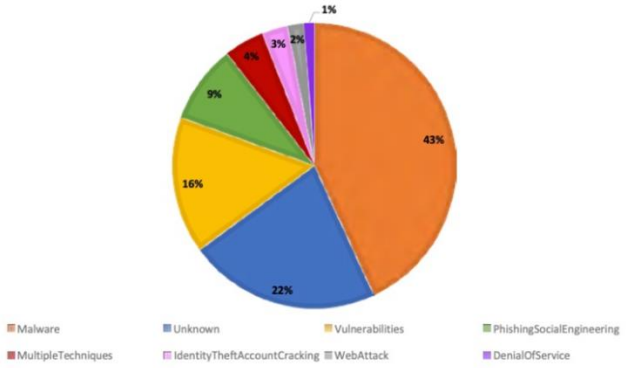


Fonte: Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Il cybercrime presenta una crescita esponenziale legata anche ad eventi di carattere geopolitico di cui non possono essere ignorate le conseguenze strategiche per i Paesi direttamente coinvolti.

La matrice cybercrime cresce del 20% annuo ed è uno degli elementi su cui bisogna focalizzarsi nel valutare tutti i rischi che incombono sull'intero ecosistema finanziario, in primo luogo sugli utenti dei prodotti bancari e finanziari.

Figura 12: Tecniche di attacco – 1H 2021

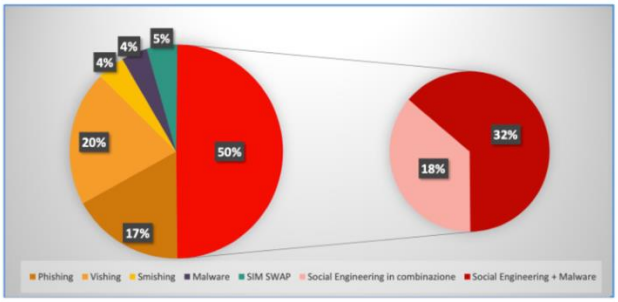


Fonte: Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Altra tecnica di attacco che ha assunto una rilevanza sempre maggiore (come è possibile desumere agevolmente dal grafico sovrastante) è costituita dai malware.

Seguono poi i ransome, sempre più all'attenzione dei media per la peculiarità di porre in essere ricatti a scopo estorsivo.
Ancora, gli attacchi basati su vulnerabilità note costituiscono il 16% del totale, mentre il phishing si attesta al 9%.
Quest'ultimo fenomeno è forse quello più comune, in quanto rivolto quasi esclusivamente contro la clientela del sistema bancario con notevole pervasività, nonostante gli accorgimenti tecnici e normativi via via posti in essere per meglio proteggere l'utenza privata.

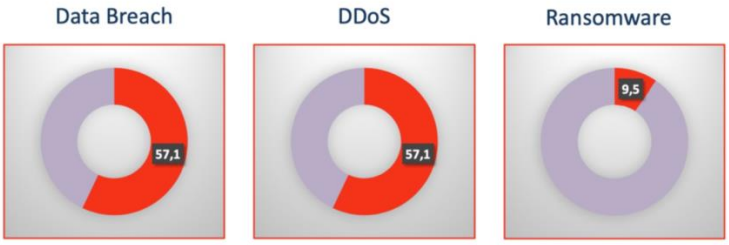
Figura 13: Clientela Retail – Tipologie di frode rilevate su canale Internet



Fonte: CERTIFIN

Focalizzando l'attenzione sulla clientela retail è possibile osservare come una forte componente degli attacchi, intorno al 50% degli stessi, sia collegata al social engineering, ovverosia al tentativo di porre in essere azioni malevole non più in riferimento alla componente tecnologica ma alla sfera sociale dell'utente.

Figura 14: Percentuale di rispondenti interessati dagli attacchi

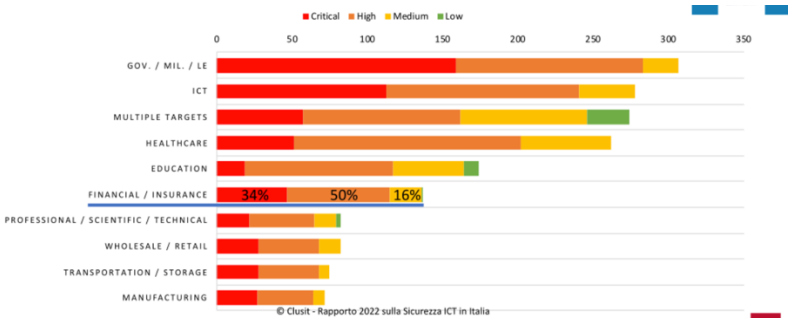


Fonte: CERTIFIN

Tornando invece ad analizzare le tipologie di attacchi cui sono sottoposte direttamente le istituzioni finanziarie, gli eventi malevoli maggiormente ricorrenti sono il ransomware, rivolto contro le infrastrutture DDoS per minare la disponibilità dei servizi offerti, ed i data breach, ovverosia gli accessi indebiti ai dati dei clienti.

È bene tener presente che il concetto di dato sensibile, quando riferito ad una istituzione finanziaria, è da considerarsi in un perimetro molto ampio (si pensi solo alle informazioni relative alla solvibilità della clientela). Di conseguenza, l'interesse della criminalità informatica a poter disporre di una miniera di informazioni da rivendere o scambiare illecitamente è sempre più incalzante.

Figura 15: Severity per TOP10 Vittime 2021



Fonte: Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Nella rilevazione statistica degli attacchi in virtù della gravità degli stessi, quelli perpetrati specificatamente contro il settore finance e insurance costituiscono il sesto target per interesse, sebbene, si ripete, il reiterarsi continuo di normative sempre più stringenti in tema di cybersecurity.

Inoltre, nell'ambito di questa categoria di azioni malevoli quelle segnalate come "critiche", ovverosia con con caratteristiche di massima rilevanza e massimo impatto nei confronti della singola istituzione finanziaria, costituiscono la stragrande maggioranza. Infatti, solo il 15% degli attacchi vengono censiti come di gravità media o bassa.

Questa peculiarità, la maggiore gravità, è propria esclusivamente del settore bancario. Elemento che non è caratteristico di altri settori, tranne alcuni casi specifici, ma solo del settore bancario.

I dati CERTIFIN ci consegnano infine un aumento di otto volte delle transazioni anomale, una prevalenza delle tecniche miste di attacco e la preferenza della clientela retail come obiettivo criminale.

È pur vero però che, a seguito dei maggiori investimenti effettuati sul fronte della sicurezza (aumentati di circa il 20% rispetto al budget precedente) e all'adozione di regolamentazioni più incisive, la gestione complessiva delle operazioni fraudolente resta ancora efficace almeno nell'83% dei casi, dato questo di assoluta rilevanza soprattutto considerando la complessità dell'intera "filiera" del sistema bancario (agenzie e clientela remota in primis).

3.2 Malware

Malware è l'abbreviazione di malicious software, ossia software dannoso.
Un malware sostanzialmente è un codice dannoso che può compromettere un sistema informatico, forzare l'accesso allo stesso o consentire la sottrazione di dati, permettendo la realizzazione di attacchi la cui gravità può arrivare a compromettere l'esistenza stessa del sistema violato.
Si tratta quindi di un programma o un file intenzionalmente dannoso per un computer, una rete o un server.
Nel concetto di malware rientrano i virus informatici, worm, cavalli di Troia, ransomware e spyware. Questi programmi maligni rubano, criptano ed eliminano dati sensibili, alterano o dirottano le funzioni informatiche principali e monitorano l'attività informatica degli utenti finali. Il malware può infettare reti e dispositivi ed è progettato per danneggiare in qualche modo gli stessi e/o i loro utenti.
Gli effetti sull'utente o sull'endpoint variano a seconda del tipo di malware e del suo obiettivo. In alcuni casi il danno prodotto è relativamente lieve, mentre in altri può essere disastroso. Indipendentemente dalla singola modalità d'intrusione, tutti i tipi di malware sono progettati per sfruttare i dispositivi a spese dell'utente e a vantaggio dell'hacker, ovvero della persona che ha progettato e/o distribuito il software dannoso.
I criminali informatici utilizzano una vasta gamma di mezzi fisici e virtuali per diffondere il malware che infetta dispositivi e reti.
I programmi dannosi possono essere veicolati in un sistema grazie ad una chiavetta USB, attraverso i più diffusi strumenti di collaborazione e tramite download drive-by, che scaricano automaticamente programmi dannosi senza l'approvazione o la consapevolezza dell'utente.
Una modalità assai comune di distribuzione di malware è costituita dal phishing, ovverosia da e-mail mascherate da messaggi legittimi contenenti invece collegamenti o allegati dannosi che recapitano il file eseguibile del malware agli utenti ignari.
Gli attacchi di malware più sofisticati sono spesso caratterizzati dall'uso di un server di comando e controllo che consente agli attori delle minacce di comunicare con i sistemi

infettati, di estrapolare dati sensibili e persino di controllare da remoto il dispositivo o il server compromesso.
I ceppi emergenti di malware includono nuove tecniche di evasione e offuscamento progettate per ingannare non solo gli utenti, ma anche gli amministratori della sicurezza e i prodotti antimalware. Alcune di queste tecniche di evasione si basano su tattiche semplici, come l'utilizzo di proxy web per nascondere il traffico dannoso o gli indirizzi IP di origine.
Le minacce più sofisticate consistono nell'utilizzo del malware polimorfico che può cambiare ripetutamente il codice sottostante per evitarne l'individuazione da parte degli strumenti di rilevamento basati sulle firme; nelle tecniche anti-sandbox che consentono al malware, una volta individuato, di ritardare le azioni per la sua mitigazione; nel malware senza file che si limita a risiedere temporaneamente nella RAM del sistema per evitare di essere scoperto.

3.3 Ransomware

Il ransomware è un tipo di malware che impedisce o limita l'accesso degli utenti al proprio sistema o ai propri dati, cui segue la minaccia di pubblicare o vendere i dati rubati qualora la vittima dell'attacco informatico non paghi un riscatto all'aggressore.

Il settore bancario è stato colpito in modo sproporzionato da questa attività malevola, registrando un aumento del 1.318% su base annua degli attacchi della specie nella prima metà del 2021rispetto al semestre precedente.
Il leader mondiale della sicurezza informatica Trend Micro Incorporated (TYO: 4704; TSE: 4704) ha annunciato il 14 settembre 2021 di aver bloccato 40,9 miliardi di minacce e-mail, file dannosi e URL dannosi per i clienti nei primi sei mesi dell'anno, con un aumento del 47% in rapporto al periodo precedente.
Secondo Trellix, inoltre, il settore bancario/finanziario ha rappresentato il 22% degli attacchi ransomware totali nel terzo trimestre del 2021.
Si può quindi affermare che questa minaccia sia ormai consolidata da diversi anni e non sembra destinata a scomparire presto. Il motivo principale della sua proliferazione è dato dal fatto che si tratta di un'attività ad alto profitto e basso rischio per gli autori delle stesse.

Figura 16: I 5 settori più colpiti dal ransomware nella prima metà del 2021

Fonte: Attacks From All Angles: 2021 Midyear Cybersecurity Report

Nelle sue prime manifestazioni il ransomware impediva alle organizzazioni di accedere ai propri dati, crittografando i file nei sistemi infetti e trattenendo la chiave di decrittazione come arma di ricatto per estorcere denaro.

Con il passare del tempo però la maggior parte delle istituzioni finanziarie si è adattata agli attacchi di crittografia dei file, migliorando le proprie procedure di backup dei dati così da rendere ininfluente la minaccia criminale.

Gli attacchi hacker si sono però evoluti nell'esfiltrazione dei dati critici prima della loro crittografia e nella minaccia di una divulgazione delle informazioni così acquisite qualora non venga pagata la somma richiesta. Ovviamente, questo non è un problema che possa essere risolto con il semplice ripristino dei backup. Secondo il rapporto Coveware 2021, oltre l'80% degli attacchi ransomware prevede l'esfiltrazione dei dati oltre alla crittografia dei file. Questa combinazione di minacce realizza quindi un fenomeno di doppia estorsione ai danni delle vittime, le quali non possono neanche contare sulla certezza, nel caso di pagamento, della definitiva rimozione dei dati sensibili sottratti.

Oltre alla crittografia e all'esfiltrazione dei dati, i criminali informatici pongono in essere altre pratiche estorsive, come la minaccia di interrompere le operazioni con attacchi DoS (denial of service), di informare direttamente della violazione i clienti e gli stakeholder dell'istituto finanziario vittima e, soprattutto, di vendere dati sensibili ai concorrenti. Nel novembre 2021 l'FBI ha allertato il sistema finanziario sull'alta probabilità che gli autori di ransomware prendano di mira e sfruttino le organizzazioni vittime attraverso eventi significativi come fusioni e acquisizioni.

La realizzazione di queste attività malevoli viene preceduta da una ricerca scrupolosa delle informazioni pubblicamente disponibili sugli obiettivi degli attacchi, contando sull'obbligatorietà della diffusione generalizzata di una notevole mole di informazioni.
I danni che possono seguire alla riuscita di queste infiltrazioni criminali edal mancato pagamento delle richieste di riscatto sono potenzialmente incalcolabili, insistendo su di un mercato, quello finanziario, in cui la fiducia sulle qualità reputazionali della singola istituzione assume una valenza economica immensa.
Stante quest'elevato profilo di rischio si è ritenuto proporre di seguito una serie di blog sul ransomware.

Tendenza 1 - Ransomware come servizio (RaaS)

La prima tendenza è quella del ransomware come servizio (RaaS).

Per poter comprendere appieno questo fenomeno è necessario però definire preliminarmente il Cybercrime as a Service (CaaS).
Il Cybercrime as a Service (CaaS) è la vendita o il noleggio di strumenti di hacking e servizi illegali a persone sul dark web. Il Cybercrime as a Service è una tendenza significativa perché consente a una gamma più ampia di attori delle minacce, compresi quelli non tecnici, di diventare criminali informatici con un investimento minimo.
Il ransomware era infatti inizialmente rivolto contro gli utenti privati, ma le capacità di social engineering della criminalità informatica si sono evolute fino a compromettere anche le reti aziendali. Di conseguenza, il ransomware è diventato un servizio che può essere affittato o venduto sui forum del Dark Web.
Questa tendenza ha creato le premesse per il modello Ransomware as a Service.
Il Ransomware as a Service (RaaS) è un modello di business criminale che consente a chiunque abbia conoscenze tecniche di base di lanciare attacchi ransomware semplicemente iscrivendosi a un servizio sul dark web, dove questo tipo di attività viene proposto alla stregua della vendita di un qualsiasi altro software legittimo. La relativa facilità nell'accedere al servizio e l'alta remunerazione delle azioni estorsive ha fatto sì che attualmente il RaaS è diventato il tipo più comune di CaaS.

Tendenza 2 – Tipologie di estorsione

Il profitto illecito riveniente dal ransomware, come abbiamo visto, si basa sull'estorsione, cioè sulla richiesta di un riscatto a fronte di una minaccia informatica. Con il passare del tempo gli autori delle stesse hanno perfezionato le modalità estorsive, modalità di cui di seguito si offre una breve panoramica.

1. Crittografia dei file - Estorsione singola

Richiesta di riscatto in cambio dell'accesso ai dati crittografati e ai sistemi compromessi. In questa ipotesi per così dire "classica" di estorsione, le vittime pagano per recuperare l'accesso ai dati crittografati e ai sistemi informatici la cui funzionalità sia stata compromessa a causa dei file crittografati.

2. Esfiltrazione dei dati - Doppia estorsione

La diffusione degli attacchi ransomware è stata contrastata dalle istituzioni finanziarie soprattutto migliorando le procedure di backup dei dati, ovverosia la capacità di recuperare gli stessi in caso di violazione. La criminalità informatica si è a sua volta adeguata cominciando ad esfiltrare i dati delle vittime prima di crittografarli per poi minacciare la loro divulgazione nell'ipotesi di mancato pagamento del riscatto.

Secondo il rapporto Coveware, oltre l'80% degli attacchi ransomware prevede l'esfiltrazione dei dati oltre alla crittografia dei file. La minaccia con la combinazione di crittografia ed esfiltrazione dei dati realizza quindi una doppia estorsione.

3. Negazione del servizio - Tripla estorsione

Alcune volte le istituzioni sotto attacco preferiscono, una volta recuperati i dati, correre il rischio di divulgazione degli stessi piuttosto che cedere ai ricatti estorsivi. Gli autori degli attacchi sono passati quindi a minacciare la funzionalità stessa dei sistemi informatici aziendali, arrivando a bloccarli attraverso il sovraccarico di traffico del server o della rete. Questa modalità estorsiva viene definita triplice in quanto combina attacchi di negazione del servizio con minacce di crittografia e divulgazione dei dati.

4. Contattare i clienti e gli stakeholder della vittima - Quadrupla estorsione

Oltre ai metodi di estorsione appena considerati, gli operatori di ransomware spesso contattano direttamente i consumatori e gli stakeholder dell'organizzazione vittima (tramite appositi call center), così da aumentare la pressione su quest'ultima. In questo caso si parla di estorsione quadrupla.

5. Contattare i concorrenti della vittima - Quintupla estorsione

In questa ulteriore modalità estorsiva gli autori delle minacce ransomware esercitano una ulteriore pressione sulla vittima, minacciando o di vendere i dati rubati a concorrenti interessati ai segreti commerciali dell'istituzione violata o di utilizzare le informazioni rubate per l'insider trading.

Tendenza 3 - Broker di accesso iniziale (IAB)

Gli Initial Access Brokers sono gli autori di minacce finanziarie che traggono profitto dalla vendita di accesso remoto alle reti aziendali in forum clandestini. La loro attività consiste nell'individuare sistemi vulnerabili effettuando una scansione massiva delle reti alla ricerca di possibili accessi sui sistemi remoti.

Questo tipo di minaccia informatica è estremamente conveniente per i criminali informatici. Secondo recenti analisi, infatti, a fronte di un costo medio sopportato per accedere ad una rete di circa 5.400 dollari, il riscatto medio pagato dalle vittime delle violazioni assomma a 170.000 dollari. Questo elevato margine di profitto induce gli I. A. B. a moltiplicare i tentativi di accesso fraudolento. Darkside Group ha di recente annunciato sui forum clandestini di essere alla ricerca di partner in grado di fornire l'accesso ad aziende statunitensi con un fatturato annuo di almeno 400 milioni di dollari.

3.4 Social Engineering

«Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems, or data. » [44]

L'espressione "ingegneria sociale" comprende un'ampia gamma di comportamenti, tutti accomunati dalla circostanza di fare leva su alcune caratteristiche umane universali: l'avidità, la curiosità, l'educazione, la deferenza verso l'autorità e così via.

Nel contesto della sicurezza informatica con il termine social engineering si descrive un tipo di attacco in cui l'aggressore sfrutta le vulnerabilità umane con mezzi quali l'influenza, la persuasione, l'inganno, la manipolazione e l'induzione, in modo da ottenere informazioni classificate, violare sistemi e reti informatiche, ottenere l'accesso non autorizzato ad aree riservate o violare gli obiettivi di sicurezza (come la riservatezza, l'integrità, la disponibilità, la controllabilità e la verificabilità) di elementi del ciberspazio (come infrastrutture, dati, risorse, utenti e operazioni).

In sintesi, l'ingegneria sociale è un tipo di attacco in cui l'aggressore sfrutta la vulnerabilità umana attraverso l'interazione sociale per violare la sicurezza del cyberspazio.

Sebbene alcune forme di social engineering si manifestino nel "mondo reale", la maggior parte degli attacchi di questo tipo avviene nel mondo virtuale dove si concentra la maggior parte delle interazioni sociali quotidiane.

Nella comunità degli hacker il social engineering è una modalità intrusiva già piuttosto diffusa fin dagli anni Settanta. Rispetto agli attacchi informatici classici, come il cracking delle password e lo sfruttamento delle vulnerabilità del software, le azioni di ingegneria sociale si concentrano sull'individuazione delle vulnerabilità umane, così da poter aggirare o superare le barriere di sicurezza senza dover contrastare firewall o software antivirus mediante una codifica profonda degli stessi. Peraltro, non esistendo allo stato un sistema informatico che non si affidi almeno in parte alle azioni dell'uomo, l'esistenza di margini di manovra affidati all'essere umano espone le reti e le infrastrutture digitali al rischio di vulnerabilità da parte di attaccanti esperti.

L'attacco di social engineering (SEA) si concretizza quindi nell'incrocio tra l'intelligenza umana malevola, la suscettibilità o ingenuità delle vittime e le necessarie competenze

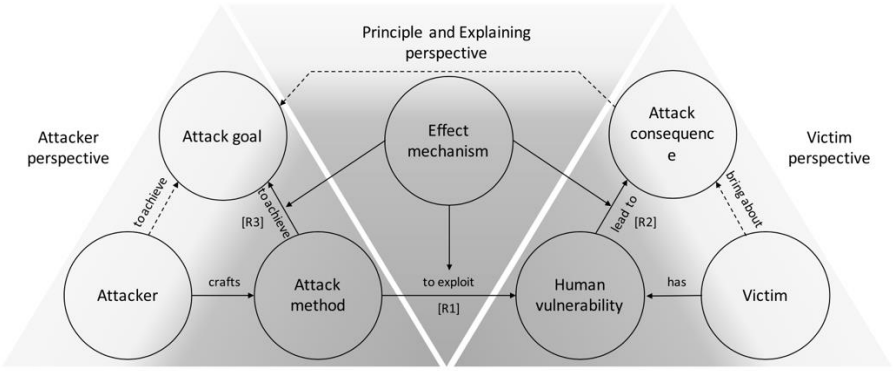
[44] https://www.csoonline.com/article/3648654/social-engineering-definition-examples-and-techniques.html

tecniche informatiche. In questo incrocio pericoloso l'attaccante interagisce socialmente con le vittime per ottenere le informazioni richieste.
Molte organizzazioni, in particolare le istituzioni finanziarie, spendono milioni di dollari per implementare gli strumenti difensivi e applicare rigidi standard di sicurezza, ma hanno la tendenza a concentrarsi principalmente sulle misure tecniche (hardware e software) investendo meno nella formazione del personale in materia di cybersecurity. Questa falla probabilmente costituisce la causa principale dell'aumento costante degli episodi di social engineering.
Si rende quindi quanto mai opportuna, in primis nel settore bancario, la definizione di una efficace governance informatica che minimizzi il rischio di successo per questo tipo di attacchi, esiziali per la credibilità delle istituzioni finanziarie e la solidità del rapporto fiduciario con la clientela. Il quadro di governance da applicare deve variare ovviamente da banca a banca, in virtù di numerosi fattori quali il budget annuale disponibile, il numero del personale complessivo, l'ambiente e l'infrastruttura della banca, la capacità dei referenti informatici di diffondere efficacemente la politica di sicurezza aziendale e la flessibilità del top management aziendale nell'adozione delle linee strategiche.

Per ridurre le SEA di successo e il loro impatto negativo, alcune ricerche raccomandano l'impiego dei c.d. ottimizzatori di social engineering, ovverosia esperti in grado di analizzare la pervasività di alcuni comportamenti umani.
Gli "ingegneri sociali" infatti cercano di individuare costantemente le vulnerabilità naturali dell'essere umano e quel frutto invece della sua evoluzione individuale e sociale, agendo quindi in uno spazio teoricamente infinito e potenzialmente molto dannoso.
L'essere disponibili nei confronti della clientela, qualità tradizionalmente sinonimo di professionalità, costituisce paradossalmente uno dei comportamenti maggiormente a rischio di social engineering. Un dipendente disponibile potrebbe aiutare inconsapevolmente un estraneo che mostri urgenza o indossi un badge simile a quello aziendale ad accedere nei locali della banca eludendo le misure di sicurezza previste (impronte digitali, caratteristiche biometriche, documento di identità). Anche la ricezione ed il successivo inoltro di e-mail non sufficientemente verificate, con le quali un presunto cliente chieda di avere un contatto con il proprio responsabile diretto, può costituire lo strumento utile per carpire le credenziali del manager.

La curiosità umana è una lusinga fondamentale per gli ingegneri sociali, in quanto le notizie su pubblicità, offerte per le vacanze e altri eventuali vantaggi di ogni sorta possono far abbassare la guardia e rendere gli utenti informatici vulnerabili agli attacchi semplicemente aprendo allegati o link.
La maggior parte dei dipendenti è efficiente nello svolgere più attività in parallelo, come scansionare documenti e rispondere contemporaneamente al telefono, ma se l'interlocutore è un malintenzionato a caccia di informazioni utili un eventuale deficit di attenzione potrebbe tradursi nella sottrazione di dati anche rilevanti.
Inoltre, la minaccia dell'ingegneria sociale cresce di pari passo allo sviluppo tecnologico e alla creazione di nuovi ambienti informatici. I siti di social network (SNS), la comunicazione mobile, l'Internet industriale e l'Internet delle cose (IoT) generano non solo grandi quantità di informazioni sensibili su persone e dispositivi, ma anche maggiori canali di accessi non autorizzati e fraudolenti.

Figura 17: Un modello concettuale per descrivere il funzionamento e l'efficacia degli attacchi di social engineering.



Fonte: Z. Wang, H. Zhu and L. Sun, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," in IEEE Access, vol. 9, pp. 11895-11910, 2021, doi: 10.1109/ACCESS.2021.3051633.

Come dimostra lo schema in alto, esistono tre possibili prospettive per capire quali possano essere gli effetti degli attacchi di social engineering.

- Dal punto di vista dell'autore della minaccia: l'individuazione di un metodo di attacco costituisce il presupposto per il successo di un'azione di ingegneria sociale.
- Dal punto di vista della vittima: le vulnerabilità umane sfruttate dall'aggressore costituiscono gli strumenti inconsapevoli per la riuscita di un'azione malevola. Altre caratteristiche di vulnerabilità (come quelle relative al software) possono essere utilizzate di concerto con quelle umane, ma non sono strettamente necessarie negli attacchi di ingegneria sociale.
- Dal punto di vista del principio e della spiegazione, i meccanismi di effetto spiegano come i metodi di attacco riescano a far sì che le vulnerabilità umane producano un danno. Essi descrivono [R1] le modalità utilizzate per far leva sulle debolezze degli utenti e spiegano [R2] perché da queste ultime derivino delle conseguenze dannose e (in corrispondenza) [R3] come i metodi di attacco raggiungano gli obiettivi prefissati. In altre parole, i meccanismi di effetto possono essere definiti come la relazione strutturale che indica cosa, perché o come le conseguenze di specifici attacchi corrispondono a specifiche vulnerabilità umane, in specifici scenari di attacco.

Pertanto, il meccanismo di effetto, la vulnerabilità umana e il metodo di attacco possono essere tre entità fondamentali per comprendere come funzionano e hanno effetto gli attacchi di ingegneria sociale.

L'ingegneria sociale, infine, può rappresentare un singolo passo in una catena di attacchi più ampia e di gravità crescente come il phishing.

3.5 Phishing

L'attacco informatico definito di phishing, diventato ormai uno dei crimini finanziari più comuni, si traduce in un'attività illecita che, utilizzando tecniche di ingegneria sociale, consente ai phishers di acquisire in modo fraudolento informazioni sensibili, come password, dati della carta di credito, informazioni sui documenti d'identità, ecc. ecc.

Il phishing (da «to fish», «pescare», perché la vittima viene «presa all'amo» dal truffatore) si realizza tramite un messaggio ingannevole che arriva via e-mail, con il quale il destinatario viene indotto a compiere una determinata attività (come cliccare su un link o scaricare una app) a seguito della quale subirà la sottrazione della sua identità digitale o dei suoi dati personali ed il conseguente accesso di terzi ai conti bancari, alle carte di credito o ad altri dispositivi finanziari a lui intestati.

Gli attacchi di phishing inducono quindi le vittime a consegnare i loro dati e le loro credenziali attraverso e-mail, messaggi di testo e altre forme di messaggistica diretta. Gli aggressori prendono di mira le vittime inviando messaggi che sembrano provenire da un mittente fidato e che esprimono l'urgenza di cliccare su un collegamento ipertestuale. Il sito web viene modificato per sembrare legittimo, consentendo all'aggressore di intercettare i dati immessi dagli utenti o di rubare le informazioni inserite, come nomi utente e password che possono essere utilizzati per commettere un più ampio furto di identità. Il phishing può avere un impatto enorme sulle aziende, in genere provocando violazioni di dati che causano danni finanziari e di reputazione.

Spesso i phishers, dopo aver avuto accesso alle informazioni finanziarie di un singolo utente che si avvalga dell'online banking, arrivano a compromettere la complessiva sicurezza informatica dell'istituzione attaccata realizzando un'ampia gamma di attività illegali (come il trasferimento illecito di fondi, l'acquisto di beni e le frodi finanziarie).

Gli autori di azioni riconducibili al fenomeno del phishing violano la sicurezza dei siti web delle banche utilizzando tecnologie sofisticate come il Man-in-the-Middle, gli attacchi ingannevoli, i malware e le azioni basate su DNS.

L'attacco Man-in-the-Middle è una attività informatica con la quale gli hacker si frappongono tra le banche e i clienti mentre questi ultimi movimentano online i loro conti correnti. Pertanto, sia le banche che gli utenti finali non si rendono conto che le transazioni sono collegate ai criminali informatici finché non si realizza un danno patrimoniale in capo ai clienti. Di recente sia Citibank che diverse altre istituzioni finanziarie statunitensi ed australiane sono state oggetto di attacchi della specie con rilevanti conseguenze economiche.

Negli attacchi ingannevoli gli hacker, presentandosi come interlocutori aziendali, inviano un messaggio agli utenti della banca, spesso millantando motivazioni di urgenza quali la segnalazione di un falso problema nell'attivazione o nella gestione del conto corrente, al fine di indurre i clienti ad interagire immediatamente aprendo un link di un sito web, simile a quello della banca ma in realtà fraudolento, incluso nell'email. Una volta entrato nel falso sito l'utente può essere indotto facilmente a fornire le proprie credenziali, offrendo così ai criminali informatici la possibilità di effettuare transazioni sui rapporti di conto ormai accessibili.

Il phishing basato su malware si realizza attraverso l'installazione di particolari software (keylogger) sui computer dei clienti. Questo tipo di attacco si verifica generalmente

allorché i clienti o i dipendenti della banca visitino un sito web non autorizzato o scarichino dei software infetti nei loro computer. La non sufficiente attenzione alle più elementari prescrizioni di sicurezza informatica diventa così la chiave di accesso ai sistemi aziendali da parte della criminalità informatica.
Quando il cliente con un computer infetto visita il sito web della banca di conto e inserisce le proprie credenziali finanziarie (come nomi utente, password e numeri di token), il malware registra le sequenze di tasti inserite durante la digitazione delle informazioni riservate. In questo modo, il keylogger raccoglie le informazioni richieste e le invia all'aggressore sotto forma di file.
Nel 2005 la Bank of London è stata vittima di una striscia di intrusioni perpetrate attraverso dei trojan keylogger che hanno causato ingenti perdite alla clientela.

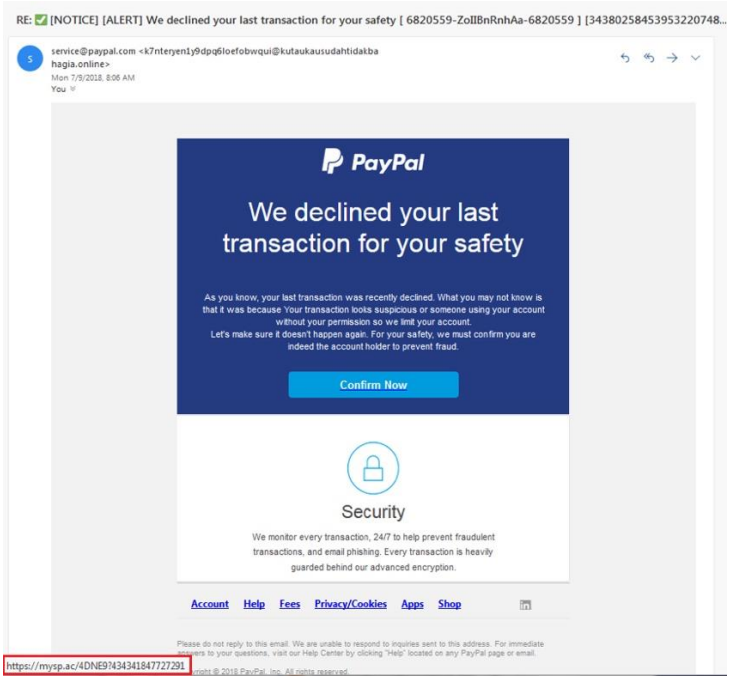
Tra le diverse forme di phishing quella attuata via e-mail è sicuramente la più comune, diffusa fin dagli albori della posta elettronica. L'aggressore invia un'e-mail presentandosi come un referente affidabile o comunque familiare (rivenditore online, funzionario di banca o di società di social media, ecc.), per poi chiedere all'utente di fare clic su un link o di scaricare un allegato per concludere un'operazione presentata come urgente.
Alcuni esempi specifici di phishing via e-mail sono:

- La compromissione della posta elettronica aziendale. L' attacco di tipo "business email compromise" (BEC) prende di mira un addetto del comparto contabile di un'organizzazione, spesso il direttore finanziario, cercando di ingannarlo per indurlo ad effettuare trasferimenti di denaro. Gli aggressori solitamente utilizzano tattiche di social engineering per convincere il destinatario dell'improcrastinabilità dell'operazione richiesta.
- Il clone phishing, con il quale viene creata una copia, o un clone, di e-mail legittime precedentemente consegnate contenenti un link o un file allegato. Questi ultimi vengono sostituiti con dei trojan che, una volta cliccati, consentono l'accesso ai sistemi informatici delle vittime. Peraltro, il phisher, una volta contraffatta l'identità della vittima, può replicare la clonazione contro altri dipendenti o clienti della medesima istituzione finanziaria.
- Le truffe 419/Nigeriane. Sebbene possa apparire quasi incredibile, l'invio di una verbosa e-mail da parte di qualcuno che affermi di essere un principe nigeriano costituisce una delle prime e più longeve truffe circolanti su Internet. Il

fantomatico "principe" subordina l'invio di ingenti somme di denaro alla ricezione di piccoli importi richiesti con le motivazioni più disparate (spese amministrative o necessità improvvise). Il numero "419" associato a questa truffa si riferisce in realtà all'articolo del Codice Penale nigeriano che configura e punisce il reato specifico.

Quello che segue è invece un esempio di phishing tramite e-mail con il quale viene simulato un avviso di PayPal contenente richiesta al destinatario di fare clic sul pulsante "Conferma ora". Qualora l'incauto utente aderisse alla richiesta fraudolenta verrebbe indirizzato verso una destinazione dell'URL evidenziata nel rettangolo rosso.

Figura 18: Simulazione evento phishing tramite PayPal



Fonte: Malwarebytes

La risposta alla gravità degli attacchi di phishing deve passare necessariamente attraverso una costante attività di aggiornamento delle procedure aziendali in materia di sicurezza informatica e, soprattutto, rivolgendo una particolare attenzione all'attività di formazione ed educazione digitale rivolta al personale delle istituzioni finanziarie ed ai clienti delle stesse.

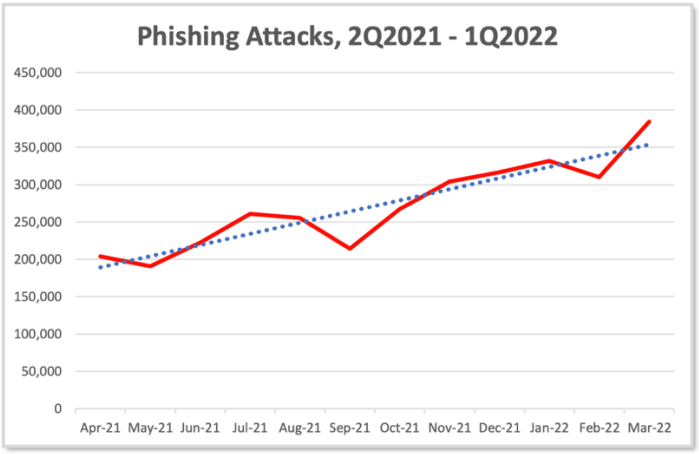
Le banche sono chiamate ad aggiornare regolarmente le procedure interne al fine di garantire la sicurezza delle transazioni con la propria clientela, introducendo ulteriori misure di sicurezza come l'autenticazione a due fattori o altri software di protezione.
Le istituzioni finanziarie potrebbero trarre enormi benefici dall'attivazione di progetti educativi rivolti alla clientela sui rischi insiti negli attacchi di phishing e sulle modalità con le quali potrebbero verificarsi degli accessi non autorizzati, fornendo al contempo le misure da adottare per proteggere i propri dati sensibili.
Gli utenti di prodotti bancari e finanziari dovrebbero essere infatti in grado, una volta formati, di intercettare le comunicazioni sospette individuando gli elementi (logo contraffatto, nominativi di referenti aziendali inesistenti) indicativi di un potenziale attacco informatico in essere, in primo luogo verificando l'affidabilità della provenienza delle e-mail attraverso il browser web.

La consapevolezza degli utenti dovrebbe costituire quindi l'obiettivo principale delle istituzioni finanziarie per contrastare efficacemente gli attacchi di phishing e mitigare, se non annullare, i danni economici che ne conseguono.

"Ultimately, once bank customers learn about their rights and responsibilities, they can take control of their financial well-being by changing the traditional saying, "A penny saved is a penny earned" to "A penny protected is a penny earned."

Il APWG Phishing Activity Trends Report ha di recente sottoposto ad analisi i diversi tipi di phishing.
Nel mese di marzo 2022 APWG ha registrato 384.291 attacchi, il totale mensile più alto da quando sono state avviate queste rilevazioni. Similmente, nel primo trimestre del 2022 sono state censite 1.025.968 azioni malevole della specie, superando di gran lunga il dato già preoccupante di 888.585 attacchi rilevati nel quarto trimestre del 2021. In generale, Il numero di attacchi di phishing è più che triplicato dall'inizio del 2020, allorché APWG osservava tra i 68.000 e i 94.000 attacchi al mese.

Figura 19: Attacchi di Phishing, 2Q2021 - 1Q2022



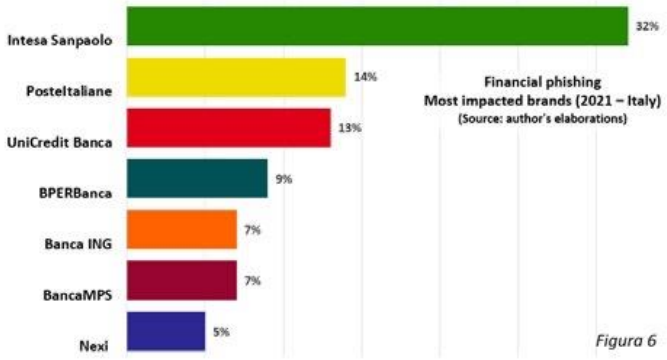
Fonte: APWG Phishing Activity Trends Report

In riferimento al primo trimestre del 2022, inoltre, OpSec Security, membro fondatore dell'APWG, ha evidenziato come gli attacchi contro il settore finanziario costituiscano la quota prevalente di tutto il fenomeno del phishing, rappresentando il 23,6% del totale. Gli attacchi contro le webmail e i fornitori di software-as-a-service (SAAS) sono rimasti preponderanti (20,5%) rispetto al trimestre precedente, mentre quelli contro i siti di commercio al dettaglio/ecommerce sono scesi dal 17,3% al 14,6% dopo la stagione dello shopping natalizio. Il phishing contro i social media è passato dall'8,5% al 12,5%; infine, quello con obiettivo le criptovalute (come gli exchange di criptovalute e i fornitori di wallet) è rimasto stabile oscillando dal 6,5% al 6,6%.

A livello nazionale il rapporto Clusit 2022 sulla sicurezza ICT in Italia rileva una media di 4,3 nuove pagine di phishing al giorno pubblicate e perfettamente funzionanti, con un'attività particolarmente intensa nei primi 5 mesi dell'anno (Figura 5). Il picco è stato raggiunto nel mese di febbraio 2021, con una media di 11 nuove pagine attivate al giorno.

Le istituzioni finanziarie interessate nel 2021 da questo fenomeno sono state 30, tra le quali quelle maggiormente colpite Intesa Sanpaolo (32% delle campagne di phishing analizzate), Poste Italiane (14%), Unicredit (13%), BPER (9%), Banca ING e Banca MPS (entrambi al 7%), Nexi (5%) e, a seguire, altri 23 player del settore per il restante 13%.

Figura 20: Phising Finanziario



Fonte: Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

3.5.2 Smishing

Il phishing via SMS è un attacco in cui l'utente riceve un messaggio di testo con il quale viene invitato a chiamare un numero di telefono, contattare un indirizzo di posta elettronica, aprire dei link a pagine web, applicazioni o interfacce utente dannose che richiedano l'inserimento delle proprie credenziali le quali, una volta divulgate, consentiranno agli aggressori di acquisire dati personali utili per le più svariate attività illecite.

L'utilizzo degli SMS rispetto alle e-mail viene preferito dalla criminalità informatica perché gli utenti tendono a rispondere più facilmente ed incontrano maggiori difficoltà nel riscontrare l'affidabilità della richiesta pervenuta. Infatti, gli attuali filtri antispam e i gateway di posta elettronica reagiscono rapidamente per bloccare un dominio di posta elettronica dannoso, utilizzando una tecnologia di sicurezza che analizza con estrema precisione le anomalie di comportamento e le possibili minacce provenienti dalle e-mail. Inoltre, con il passare del tempo l'utenza sta dimostrando una maggiore cautela nell'apertura della posta elettronica e una significativa capacità nell'identificare link e allegati sospetti.

Il phishing via SMS è noto anche come smishing, parola composta di SMS e phishing utilizzata per la prima volta il 25 agosto 2006 da David Rayhawk di McAfee.

Come detto, un SMS di smishing può incorporare un URL, un numero di telefono e/o indirizzo e-mail o essere auto rispondente.

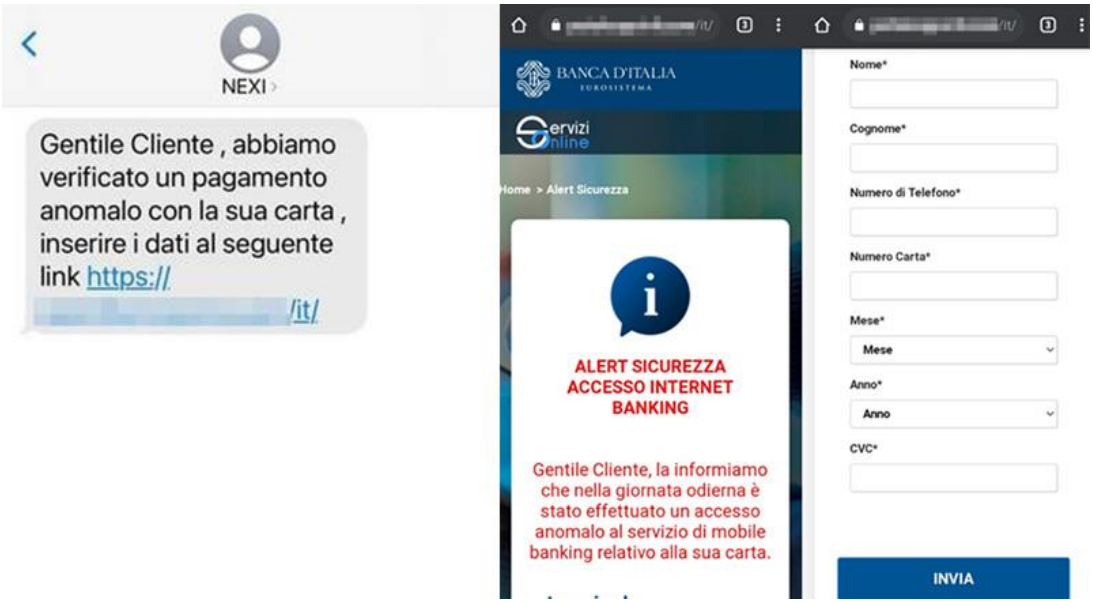
Nella prima ipotesi, cliccando l'URL l'utente scaricherà inconsapevolmente sul suo telefono un file *.apk, un malware che in seguito provocherà attività dannose, o verrà reindirizzato verso un falso sito web dove gli verrà chiesto di inserire le proprie credenziali finanziarie.

Gli SMS contenenti un numero di telefono e/o indirizzo e-mail generalmente propongono sconti, omaggi o promozioni per ottenere i quali l'utente sarà invitato a contattare i recapiti proposti fornendo progressivamente i propri dati personali.

Gli SMS auto rispondenti, infine, consistono in un messaggio di auto-risposta con il quale viene chiesto all'utente di abbonarsi o rimuovere l'iscrizione ad un servizio cliccando un link di reindirizzo verso siti web dannosi.

Di seguito si fornisce la riproduzione di SMS di phishing con l'invito ad accedere a siti web fraudolenti, cui segue la sottrazione indebita di dati personali relativi a carte di credito, rilevati dal CERT (Computer Emergency Response Team) della Banca d'Italia.

Figura 21: Riproduzione di SMS di phishing



Fonte: CERT (Computer Emergency Response Team) della Banca d'Italia

Questo genere di messaggi, ovviamente, non è in alcun modo autorizzato e non proviene dalla società NEXI S.p.A.

Nel mondo attualmente ci sono circa 6 miliardi di abbonati alla telefonia cellulare, un terzo dei quali utilizza smartphone collegati ad Internet. I dispositivi di telefonia mobile sono diventati quasi una propaggine dell'essere umano, degli strumenti indispensabili per la nostra costante interconnessione con il mondo esterno. Purtroppo, dal punto di vista della cybersecurity, un cellulare personale non è altro che un computer vulnerabile con una connessione diretta alla Rete. Quindi, proprio come i computer portatili e i dispositivi informatici tradizionali, i telefoni cellulari possono diventare piattaforme di lancio per diffondere malware, attacchi DoS e prendere il controllo di account privilegiati.
I bersagli preferiti degli attacchi smishing sono i clienti delle banche e i loro rapporti di conto corrente. Sul telefonino arrivano messaggi in cui il finto servizio clienti della banca (generalmente individuata tra le maggiori aziende del settore) segnala il blocco momentaneo del conto per l'improvvisa insorgenza di problematiche tecniche o per il ricorrere di attacchi informatici. Il recupero della piena operatività viene subordinato all'accesso ad un sito apparentemente identico a quello della banca, in cui il cliente viene invitato ad inserire i codici identificativi.
Per contenere il dilagare di questo tipo di truffa il sistema creditizio ha subordinato l'operatività on line all'autenticazione a due fattori, ovverosia l'inserimento obbligatorio da parte del cliente di un codice OTP o di una password numerica usa e getta generata automaticamente da un'apposita app dello smarphone, in assenza delle quali non è possibile compiere alcuna transazione.

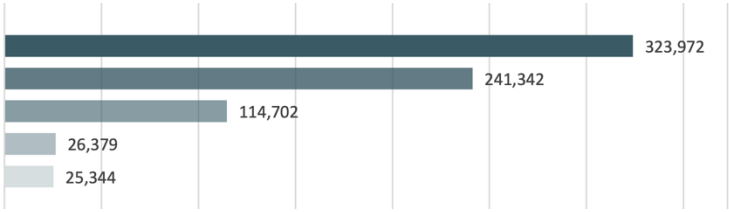
3.5.3 Vishing

Il "Vishing", termine derivante dalla composizione di voice e phishing, consiste nella pratica di avvalersi di tecnologie di messaggistica vocale basate su IP (principalmente il Voice over Internet Protocol, o VoIP) per indurre socialmente l'utente a fornire informazioni personali riservate al fine di violarne l'identità digitale. Il VoIP viene utilizzato perché, a differenza di una linea telefonica tradizionale, l'intera operazione può essere attivata e disattivata in breve tempo.

Gli autori di queste minacce informatiche si avvalgono di tecniche come lo spoofing dell'ID chiamante o sistemi automatici avanzati per convincere la vittima designata ad avviare l'operatività on line del proprio rapporto di conto. Una volta inserite le

credenziali in un sito fasullo il cliente viene contattato da un numero di telefono in tutto simile a quello della propria banca, rispondendo al quale sarà invitato da un fantomatico funzionario a comunicare un codice OTP questo sì vero che sarà purtroppo utilizzato dall'hacker per compiere operazioni fraudolente.
Il vishing è diventato ormai un problema ricorrente e costoso per il sistema finanziario, tanto che a livello globale si stima che annualmente almeno il 40% degli adulti lavoratori subisca attacchi della specie (Proofpoint, 2019), mentre negli Stati Uniti il 69% delle frodi informatiche segnalate alla Federal Trade Commission si sono verificate per telefono (FTC, 2019).
Il vishing e altri fenomeni di social engineering comportano danni enormi per centinaia di migliaia di utenti e circa il 25% delle perdite finanziarie derivanti da questi attacchi non viene mai recuperato (FBI e IC3, 2019).
Al riguardo, si riporta di seguito una recente analisi condotta dal FBI che sottolinea l'aumento costante negli anni dal 2017 al 2021 di tutti queste tipologie di crimini informatici.

Figura 22: Aumento negli anni dal 2017 al 2021 di Phishing / Vishing / Smishing / Pharming



Fonte: Federal Bureau of Investigation (FBI)

Per contrastare gli attacchi di vishing sono state implementate tecnologie di blocco delle chiamate.
Tuttavia, i visher possono falsificare le informazioni dell'ID chiamante, rendendo tali tecnologie inefficaci; di conseguenza, gli individui continuano a ricevere e a rispondere alle chiamate di vishing.
Questa forma di attacco utilizza le connessioni VoIP per convincere gli utenti a rivelare i propri dati personali. Il VoIP viene utilizzato perché l'intera operazione può essere attivata e disattivata in breve tempo, a differenza di una linea telefonica tradizionale.

Questa forma di attacco abusa della fiducia che i consumatori ripongono nella legittimità dell'infrastruttura telefonica.

3.5.4 Pharming

Il pharming (definito anche "phishing senza esca") è una particolare truffa informatica che consiste nel dirottare il traffico di rete tra un client e un web server verso siti Internet fraudolenti costruiti ad hoc, con lo scopo di sottrarre dati sensibili o per fungere da ulteriori teste di ponte per altre tipologie di attacco.
Questa tecnica, pur essendo molto simile al phishing negli scopi, è in realtà una pratica molto più insidiosa e subdola perché ingannevole anche per gli utenti dotati di evoluti strumenti di protezione.
Il pharming è infatti simile al phishing in quanto anch'essa è una minaccia che confonde gli utenti e li spinge a divulgare informazioni private, ma invece di basarsi sulle e-mail come vettore di attacco utilizza un codice dannoso installato sul dispositivo della vittima (senza che quest'ultima compia azioni particolari come il click su di un link) per reindirizzarla verso un sito web controllato dall'aggressore. Il malware viene eseguito come processo in background sul computer, non necessita di alcuna ulteriore interazione con l'utente, monitora la sua attività sul web e persiste anche in caso di riavvio del dispositivo finché non venga rimosso a seguito di bonifica dello stesso.
Esso è inoltre più mirato e preciso rispetto alle altre tipologie di attacchi informatici e si struttura in due fasi, la prima delle quali inizia con l'installazione di un codice dannoso sul computer o sul server della vittima la quale automaticamente viene reindirizzata verso un sito parassita simile a quello dell'istituzione finanziaria legittima. La seconda fase si avvia allorché il cliente, ignaro di trovarsi in un falso sito, digita le proprie credenziali fornendole così al criminale informatico che potrà porre in essere delle transazioni illegittime.

Un altro metodo utilizzato per il pharming è l'"avvelenamento" del DNS.
Il servizio di rete noto come DNS (Domain Name Server), nato per aiutare l'utente comune a districarsi nei meandri del Web semplificando l'attività di ricerca dei siti, è risultato fondamentale per la diffusione di Internet anche tra i non addetti ai lavori. Infatti, quando

si digita l'URL (Uniform Resource Locator) ovvero l'indirizzo alfanumerico di un sito Internet nella barra degli indirizzi del proprio browser, il DNS permette di tradurre l'URL in un indirizzo IP numerico.
Una truffa basata sul pharming presuppone quindi che il malware modifichi o le impostazioni DNS del computer locale, reindirizzando gli utenti a un sito dannoso quando digitano un dominio nel browser, o la cache del server DNS, cambiando le regole in esso archiviate in modo da reindirizzare il flusso informativo destinato ad un dominio legittimo verso l'indirizzo IP di un falso sito web.

3.6 L'impatto dello smart working sul rischio informatico

Le limitazioni generalizzate ai movimenti individuali imposte dalla pandemia globale Covid-19 hanno costretto le aziende di tutte le dimensioni e di tutti i settori ad adottare immediatamente pratiche di lavoro "intelligenti" per poter continuare ad operare. Nella maggior parte dei casi, la "digitalizzazione forzata" di molte attività lavorative è stata in realtà una scelta quasi obbligata.
È presumibile che il lavoro da remoto continuerà a rappresentare anche nel prossimo futuro una condizione da cui non poter prescindere e che per molte aziende il processo digitale messo in atto durante l'emergenza pandemica non potrà essere invertito.
L'urgenza di questa trasformazione digitale su larga scala e i tempi strettissimi in cui si è realizzata nel mondo del lavoro ha però esposto molte organizzazioni e utenti della rete a una serie di nuovi rischi e minacce informatiche.
In un contesto senza precedenti, nel quale all'immediatezza di cambiamenti epocali si è purtroppo associata spesso una mancata informativa sulle più elementari nozioni di sicurezza digitale, gli attacchi informatici sono aumentati sfruttando la maggiore esposizione cibernetica dei soggetti attaccati e la minore attenzione degli utenti causata dalla situazione di emergenza.
Già prima dell'insorgere della pandemia un numero crescente di dispositivi personali era connesso tramite reti locali. In molti casi, questi dispositivi non erano né adeguatamente aggiornati né adeguatamente gestiti dal punto di vista della sicurezza. Alcuni hanno addirittura presentato vulnerabilità non ancora note ai produttori.
Questa moltiplicazione esponenziale di end-point con cui gli autori di azioni malevoli possono accedere alle reti aziendali è una conseguenza diretta dell'uso dello smart

working, visto il numero sempre maggiore di datori di lavoro che consente al personale di lavorare a distanza o almeno offre l'opportunità di lavorare fuori dall'ufficio a tempo parziale.
Tuttavia, è importante che i dipendenti portino con sé in viaggio la formazione sulla sicurezza informatica. Come minimo, i dipendenti devono sapere che non devono mai lasciare incustodito un dispositivo portatile quando sono in giro per il pubblico, perché il furto di tale dispositivo porterà quasi certamente a un uso improprio.
Anche se si è vigili, gli incidenti possono comunque accadere, quindi i dipendenti devono attivare tutte le funzioni di sicurezza sul loro dispositivo ogni volta che viaggiano.
A cominciare dall'autenticazione multifattoriale, che richiede all'utente di fornire prove aggiuntive per l'autenticazione, come un codice secondario inviato a un dispositivo separato oltre alla password. Tutti i dati presenti sul dispositivo e nelle e-mail devono essere crittografati, in modo che, anche in caso di furto, l'hacker criminale non sia in grado di leggerli.
Forse l'aspetto più importante è quello di evitare reti Wi-Fi non protette.
A molte persone piace lavorare in luoghi pubblici, come treni e caffè, ma è qui che gli hacker criminali spesso creano falsi account Wi-Fi che sembrano veri ma si collegano direttamente al loro computer.
In un qualsiasi ecosistema di Smart Home i dispositivi privati (come gateway residenziali, smartphone, stampanti, fotocamere, smart-TV e assistenti vocali) possono essere tutti collegati alla stessa rete e, contestualmente, ad un PC aziendale. Ciò comporta che una singola vulnerabilità in un singolo nodo o dispositivo di rete potrebbe potenzialmente consentire a un attore di minacce informatiche di accedere al laptop aziendale e, quindi, alle sue informazioni e autorizzazioni.

Quali sono quindi i rischi “tipici” dello smart working?

- *Utilizzo di propri dispositivi*
  Molti dipendenti compensano la mancanza di dispositivi aziendali utilizzando i loro dispositivi finali personali, come laptop o smartphone, per scopi lavorativi. Di conseguenza, la funzione aziendale informatica non può ispezionare questi dispositivi per verificare l’insorgenza di eventuali problematiche.

- *Incertezza*

  Le nuove condizioni di lavoro non sono garanzia di consapevolezza del rischio informatico soprattutto in riferimento ai lavoratori più anziani con un minor grado di dimestichezza digitale. Questa situazione di incertezza si traduce in una maggiore esposizione agli attacchi informatici, tanto che si è stimato che quasi la metà degli utenti clicchi su e-mail di phishing inviate durante l'implementazione di strumenti di collaborazione.

- *Phishing*

  Gli attacchi cibernetici manipolativi, sotto forma di contatti telefonici o e-mail, si sono moltiplicati approfittando della notevole "ingenuità digitale" di gran parte degli utenti

- *Assenza di una rete di contatti sociali*

  Si è appurato che i lavoratori da remoto cliccano sulle e-mail di phishing a un tasso tre volte superiore rispetto a quelli che lavorano in ufficio. Ciò potrebbe essere in parte dovuto alla mancanza di comunicazione diretta con i colleghi ed al mancato scambio di conoscenze sul tema della sicurezza informatica.

- *Luoghi di lavoro non sufficientemente protetti*

  La diminuita presenza fisica del personale negli ambienti di lavoro ha comportato spesso un minore presidio fisico degli accessi agli stessi, consentendo così una maggiore permeabilità agli attacchi informatici.

CAPITOLO 4: MODELLO PER LA DETERMINAZIONE DEL LIVELLO DI RISCHIO IN CASO DI UN EVENTO DI DATA BREACH

4.1 Obbiettivi del modello

Nei capitoli precedenti il concetto di rischio è stato analizzato prendendo in considerazione tutti i profili dello stesso, dalla sua genesi nel pensiero filosofico greco sino alle implicazioni nei sistemi socioeconomici moderni.

All'analisi teorica si è ritenuto di affiancare un dettagliato excursus normativo soffermandosi sulle prescrizioni del GDPR 679/2016, sule linee guida e gli orientamenti dell'EBA, sui principi del Regolamento DORA di prossima emanazione e, infine, sulla normativa di vigilanza prudenziale riveniente dalla Banca d'Italia.

Il percorso illustrativo si è poi concluso con l'analisi dei pericoli di natura informatica cui sono esposte le istituzioni finanziarie, riflettendo in particolare su quanto lo sviluppo della finanza digitale abbia influito sull'incremento del rischio di eventi patologici con forti riflessi sul patrimonio delle aziende coinvolte e degli utenti di prodotti bancari e finanziari avanzati.

L'insieme di questi passaggi ha costituito la base propedeutica per il raggiungimento dell'obiettivo ultimo di questa tesi, ovverosia la predisposizione di un modello prototipale da applicare al verificarsi di uno degli eventi di Data Breach già descritti in questo elaborato.

Il fine ultimo del modello risiede nella restituzione di un indicatore di rischio per ogni evento analizzato, cui consegua l'assegnazione di un punteggio al quale associare dei determinati livelli di rischio.

Per questo modello sono stati scelti 3 differenti livelli di rischio distribuiti in un intervallo numerico (da 5 a 99) in cui il livello di rischio aumenta al crescere del punteggio.

Dalla determinazione del livello di rischio, come noto, consegue la possibilità di assumere consapevolmente le strategie aziendali, in termini di modelli organizzativi interni da adottare, di predisposizione delle politiche di mitigazione più adeguate in riferimento all'attività svolta nonché, infine, di corretta individuazione delle eventuali segnalazioni da trasmettere alle Autorità di vigilanza competenti.

Gli elementi fondamentali del modello sono dati dagli eventi, dalle tecniche di mitigazione e dal tempo di ripristino del danno.
Ogni evento, in assenza di un qualsiasi intervento teso alla sua mitigazione, rappresenta il *rischio inerente*, ossia il danno teoricamente maggiore cui l'impresa è esposta.
A seguito dell'attivazione degli strumenti atti a mitigarlo il rischio inerente si riduce in *rischio residuo*, ossia il rischio inerente meno i presidi applicati. Il punteggio attribuito a questa tipologia di rischio nel modello risentirà quindi direttamente delle tecniche di mitigazione che sono state individuate ed applicate.

Più il tempo di ripristino è lungo più il rischio aumenta e per questo motivo la variabile temporale è imprescindibile. Vengono per questo considerati 3 intervalli temporali: 24 ore, 48 ore e 72 ore.
Anche questo fattore ha un suo valore numerico, il quale, una volta applicato al rischio residuo, determina il punteggio finale.
Il punteggio finale andrà inserito in uno dei 3 intervalli di rischio scelti per il modello: *basso, medio e alto.*

Il rischio sarà basso quando lo score sarà compreso tra 5 e 35.

Il rischio sarò medio quando lo score sarà compreso tra 35 e 65.

Il rischio sarà alto quando lo score sarà compreso tra 65 e 95.

A seconda del livello di rischio raggiunto si potrà procedere con le segnalazioni.

4.2 Tecniche di mitigazione

Le tecniche di mitigazione prese in considerazione per il modello sono 5.

- *Outsourcing*

La pratica dell'outsourcing consente alle organizzazioni del lavoro di concentrarsi direttamente sulle attività in cui possono utilizzare in modo più efficiente le proprie risorse umane, remunerando altre aziende per lo svolgimento delle funzioni in cui sono invece meno efficienti. Nonostante i numerosi vantaggi immediati, in primis quello di

contrarre in maniera significativa il costo della variabile lavoro, questo processo non è esente da rischi e spesso risulta molto oneroso nel medio lungo periodo.
In ogni caso, nel corso degli ultimi anni un numero sempre maggiore di aziende ha optato per l'esternalizzazione delle attività di sicurezza informatica, con la finalità di conseguire una contrazione dell'impegno economico da sopportare o di ottenere un livello di sicurezza più elevato a parità di costi.
Sebbene questo fenomeno non possa ovviamente riguardare in astratto tutti i processi aziendali, è stato comunque dimostrato come l'outsourcing in generale, e più specificamente, l'outsourcing della sicurezza informatica, si traduca solitamente in una riduzione dei costi di produzione e nella liberazione di altre risorse per l'attività d'impresa.

Le organizzazioni generalmente procedono all'esternalizzazione di sei comparti di attività tecnica aventi caratteristiche di rilevanza:
(1) Test di penetrazione o vulnerabilità. In questa ipotesi un soggetto esterno viene ingaggiato per verificare la permeabilità e vulnerabilità dei sistemi aziendali da parte di terzi.
(2) Audit di sicurezza. La valutazione completa delle componenti tecnologiche aziendali e dei protocolli di sicurezza a presidio degli stessi viene delegata a società specializzate nel settore.
(3) Monitoraggio del sistema. Il monitoraggio continuo della rete aziendale e l'interpretazione degli eventi di sistema, compresi quelli non autorizzati e gli attacchi informatici veri e propri, vengono affidati ad aziende con una professionalità specifica.
(4) Consulenza. I contratti di consulenza prevedono l'assunzione di un'azienda esterna per fornire assistenza su tematiche generali di sicurezza informatica e in occasione di investimenti specifici o di modifiche organizzative interne.
(5) Analisi forense ed assicurativa. Le problematiche di carattere strettamente giuridico e assicurativo, aventi natura ordinaria o insorte a seguito di eventi patologici, vengono normalmente affidate a studi legali e compagnie assicurative con l'obiettivo di limitare i profili di responsabilità e i rischi di perdite patrimoniali associati all'attività informatica dell'azienda.
(6) Gestione generale del sistema. La gestione generale del sistema è la forma più invasiva di outsourcing. Si realizza quando l'intero firewall, la rete privata virtuale

(VPN), l'hardware e il software di rilevamento delle intrusioni nelle reti aziendali vengono affidate a terzi.

- Password

La password è lo strumento con il quale un utente dimostra di essere autorizzato all'accesso di un dispositivo informatico. In linea teorica può essere definita come la moderna "chiave" con la quale aprire una "porta" virtuale di accesso a "stanze" nelle quali svolgere attività lavorative o di interesse personale. Le reti aziendali, in particolare, consentono l'accesso simultaneo a più utenti, ognuno dotato di una propria chiave individuale e riservata. Alcuni dispositivi, inoltre, prevedono l'esistenza di un utente di livello gestionale ("superutente") con funzioni di controllo degli accessi.

L'accesso non autorizzato costituisce un problema potenzialmente grave per chiunque utilizzi un computer o dispositivi high-tech, che si tratti di smartphone e tablet individuali piuttosto che di sistemi informatici aziendali complessi. Le conseguenze per le vittime di queste effrazioni vanno dalla perdita di dati anche rilevanti (presentazioni, e-mail, progetti…) fino alla sottrazione di informazioni sensibili (dati bancari, sanitari…) o addirittura della propria identità, con rischi in quest'ultimo caso anche di natura penale qualora vengano posti in essere dei reati.

La modalità più comune con la quale gli hacker si introducono nei computer o nelle reti aziendali consiste nell'individuazione delle relative password di accesso. Quelle troppo comuni e semplici consentono infatti ai criminali informatici di ottenere facilmente l'accesso e il controllo dei dispositivi attaccati. Al contrario, una password difficile da decifrare rende l'intrusione proibitiva costringendo gli hacker a dirigersi verso altri obiettivi. Molto banalmente, più difficile è la password, minore è la probabilità che i dispositivi informatici siano oggetto di una violazione indesiderata.

La password costituisce quindi un presidio essenziale per la sicurezza informatica, la cui integrità deve essere salvaguardata in primo luogo attraverso un uso consapevole e riservato della stessa. La incauta gestione di una password può infatti risultare altrettanto dannosa dell'assenza stessa di strumenti di protezione dei dispositivi informatici.

-Dati Crittografati

La crittografia è una modalità di protezione dei dati riservati attraverso la conversione degli stessi in caratteri cifrati non intellegibili in assenza di una apposita chiave di

decrittazione. Questo processo si chiama “encoding" e rende estremamente difficoltoso, se non impossibile, l’accesso non autorizzato ad informazioni definite sensibili.
L’utilizzo della crittografia conferisce un ulteriore livello di sicurezza in quanto garantisce la protezione della riservatezza anche nell’ipotesi di sottrazione fraudolenta dei dati, in particolare nel contesto delle istituzioni finanziarie. L’impenetrabilità dei dati pur quando disponibili costituisce un deterrente molto efficace contro gli attacchi informatici, costringendo i potenziali autori degli stessi a preventivare un dispendio di risorse spesso insostenibile.

-Formazione dei dipendenti

Il fattore umano è probabilmente la variabile più complessa da affrontare in materia di sicurezza informatica.
Quando un ransomware colpisce un'azienda è perché spesso un dipendente della stessa ha cliccato su un link dannoso in un'e-mail di phishing, si è fidato e ha condiviso al telefono informazioni riservate con una persona non autorizzata o ha lasciato il proprio computer o dispositivo mobile esposto e incustodito in un luogo pubblico.
Per scongiurare dei comportamenti così deleteri e pericolosi si rende necessaria un’attività costante di formazione del personale tesa alla sensibilizzazione dei dipendenti verso le diverse forme della criminalità informatica.
La consapevolezza dell’esistenza di tecniche psicologiche associate all’utilizzo di strumenti informatici, come nel caso delle e-mail di phishing, costituisce un valido baluardo contro l’invasività di un fenomeno che, pur nella sua banalità, induce tuttora più di un terzo dei destinatari a cliccare su contenuti dannosi.
Una maggiore informazione ed un approccio culturalmente cautelativo consentono infatti agli addetti di comportarsi adeguatamente allorché ricevano dei contenuti apparentemente affidabili, come le false newsletter di organizzazioni note o le presunte informazioni di consegna dei fornitori di servizi di spedizione.
Gli investimenti in formazione sono inoltre in grado di innestare una spirale virtuosa, in quanto il personale formato diventa a sua volta un veicolo di informazioni verso gli altri colleghi, costituendo il primo e più efficace presidio preventivo contro i gravi incidenti di ransomware.
Un comportamento giusto al momento giusto, quindi, può salvare le aziende da danni patrimoniali e di immagine anche considerevoli.

-Firewall

Il firewall è un software che impedisce l'accesso non autorizzato a una rete. Ispeziona il traffico in entrata e in uscita utilizzando una serie di regole per identificare e bloccare le minacce.

I firewall sono tuttora considerati una componente essenziale della sicurezza di rete perché hanno avuto un'enorme influenza sulle moderne tecniche di sicurezza. Emersi agli albori di Internet, quando le reti necessitavano di nuovi strumenti in grado di gestire la crescente complessità, sono diventati da allora il fondamento della sicurezza di rete nel modello Client-Server, l'architettura centrale dell'informatica moderna. La maggior parte dei dispositivi utilizza i firewall - o strumenti strettamente correlati - per ispezionare il traffico e mitigare le minacce.

Le organizzazioni moderne li incorporano in una strategia di gestione delle informazioni e degli eventi di sicurezza (SIEM) insieme ad altri dispositivi di cyber security. Possono essere installati sul perimetro della rete di un'organizzazione per proteggersi dalle minacce esterne o all'interno della rete per creare una segmentazione e tutelarsi dalle minacce interne.

Oltre alla difesa immediata dalle minacce, i firewall svolgono importanti funzioni di registrazione e audit. Conservano una registrazione degli eventi che può essere utilizzata dagli amministratori per identificare gli schemi e migliorare i set di regole. I processi devono essere infatti aggiornati regolarmente per poter tenere il passo con le minacce alla sicurezza informatica in continua evoluzione, sviluppando patch in grado di contrastarle immediatamente.

Nelle reti domestiche, utilizzati insieme alle applicazioni antivirus, i firewall consentono di filtrare il traffico dati e avvisare l'utente di eventuali intrusioni.

Un firewall stabilisce un confine tra una rete esterna e la rete che protegge. Viene inserito in linea attraverso una connessione di rete e ispeziona tutti i pacchetti che entrano ed escono dalla rete protetta. Durante l'ispezione, utilizza una serie di regole preconfigurate per distinguere i pacchetti benigni da quelli dannosi, impedendo a questi ultimi di accedere alla rete da tutelare.

Dalle analisi poste in essere dal NETSCOUT's 14th Annual Worldwide Infrastructure Security Report è emerso come ancora nel 2018 DDoS e firewall siano risultati i due

principali servizi di sicurezza informatica richiesti dalle aziende, con una quota di mercato prossima al 30%. In questo contesto non è sorprendente che le istituzioni finanziarie siano al primo posto (72%) tra le organizzazioni che esprimono interesse per le offerte DDoS e Firewalls, seguite da vicino dalle amministrazioni pubbliche (69%).

4.3 Ponderazione

La corretta determinazione del livello di rischio residuo presuppone che ogni tecnica di mitigazione venga ponderata a seconda dell'evento preso in considerazione.

Gli eventi considerati per lo sviluppo di questo modello sono quelli già oggetto di approfondimento durante il corso di questo studio, in particolare:

- *Malware*
- *Ransomware*
- *Phishing*
- *Smishing*
- *Vishing*
- *Pharming*
- *Furto di un Computer*
- *Azioni delle persone*
- *Guasti ai sistemi*
- *Eventi naturali*

Figura 23: Ponderazione delle tecniche di mitigazione

EVENTO\TECNICHE	OUTSOURCING	PASSWORD	DATI CRITTOGRAFATI	DIPENDENTI FORMATI	FIREWALLS
MALWARE	15	20	20	10	25
RANSOMWARE	15	20	20	10	25
PHISHING	10	20	20	30	10
SMISHING	10	20	20	30	10
VISHING	10	20	20	30	10
PHARMING	10	20	20	30	10
FURTO COMPUTER	20	25	25	5	15
AZIONI DELLE PERSONE	10	10	20	30	20
GUASTI AI SISTEMI	40	5	20	15	10
EVENTI NATURALI	40	5	20	15	10

Fonte: Modello per la determinazione del livello di rischio in caso di un evento di Data Breach

Trattandosi di rischio residuo, quindi per definizione mitigato rispetto a quello inerente, la scala numerica delle ponderazioni è articolata dal valore minimo “0” fino a quello massimo “90”.

Di seguito vengono illustrate le motivazioni alla base delle ponderazioni effettuate.

Malware e Ransomware sono stati considerati insieme in quanto entrambi software dannosi che possono compromettere il sistema informatico, forzare l’accesso allo stesso o consentire la sottrazione di dati.
Per queste ragioni il peso maggiore (25) tra le tecniche di mitigazione è stato attribuito al firewall, in quanto strumento appositamente creato per contrastare la diffusione di queste tipologie di software mediante l’ispezione del traffico dati.
Seguono per rilevanza (20) la password e la crittografia dei dati, entrambi presidi necessari per la protezione dei dati, l’obiettivo finale degli atti di criminalità informatica.
Un peso importante (15) è stato riconosciuto alle compagnie di outsourcing, le quali ultime possono essere ingaggiate per gestire completamente il firewall, la rete privata virtuale (VPN), l'hardware e il software di rilevamento delle intrusioni che proteggono le attività di rete di un'azienda.
L’incidenza minore (10) è stata riferita alla formazione del personale, stante la predominanza delle caratteristiche tecniche negli eventi dannosi presi in considerazione.

La catena di attacchi dell’ingegneria sociale è stata raggruppata in un unico gruppo composto da: phishing, smishing, vishing e pharming. In questi tipi di attacchi l'aggressore sfrutta le vulnerabilità umane con pratiche psicologiche quali l'influenza, la persuasione, l'inganno, la manipolazione e l'induzione, in modo da ottenere informazioni classificate, violare sistemi e reti informatiche, ottenere l'accesso non autorizzato ad aree riservate o violare gli obiettivi di sicurezza di elementi del ciberspazio.
Proprio in virtù di queste caratteristiche la maggiore rilevanza (30) tra le tecniche di mitigazione è stata attribuita alla formazione dei dipendenti, i quali devono acquisire gli strumenti per poter individuare e contrastare efficacemente le minacce informatiche della specie.
Gli attacchi di social engineering (SEA) si concretizzano quindi nell’incrocio tra l'intelligenza umana malevola, la suscettibilità o ingenuità delle vittime e le necessarie

competenze tecniche informatiche. In questo incrocio pericoloso l'attaccante interagisce socialmente con le vittime per ottenere le informazioni richieste. Sono proprio queste informazioni che devono essere crittografate e protette dalle password, tecniche di mitigazione alle quali è stato riconosciuto un peso elevato (20).
La rilevanza del fattore umano in queste ipotesi di rischio ha portato di conseguenza a ridimensionare l'importanza di strumenti di mitigazione maggiormente incentrati sulle componenti tecnologiche, firewall e processi di outsourcing, cui è stato attribuito un punteggio minore (10).

Nell'ultimo biennio il ricorso alle prestazioni di lavoro da remoto, principalmente a causa dell'emergenza sanitaria, è aumentato in maniera esponenziale.
I vantaggi e le potenzialità di questa nuova modalità, sperimentata forzatamente a livello di massa durante la pandemia, hanno orientato molte aziende verso una nuova organizzazione "ibrida" che combina il lavoro in presenza con quello a distanza. Ciò ha comportato l'adozione di modelli organizzativi più flessibili in cui ai lavoratori viene consentito di alternare la presenza nei luoghi di lavoro tradizionali con gli ambienti domestici, rendendo così fluidi i confini spazio-temporali nei quali rendere le prestazioni di lavoro.
Questo contesto ha indotto un utilizzo assolutamente nuovo dei dispositivi informatici in dotazione ai dipendenti, non più limitato all'ufficio propriamente detto ma anche in altri luoghi, cui è seguito quasi automaticamente l'incremento dei rischi connessi all'incolumità fisica dei pc o tablet aziendali, in primo luogo quello di un loro *furto*. Per proteggersi dalle conseguenze di un evento del genere è necessario quindi che i dati custoditi nel dispositivo elettronico siano opportunamente protetti, per cui la password e la crittografia acquistano una notevole rilevanza (25) ai fini della ponderazione come tecniche di mitigazione del rischio.
In queste ipotesi di rischio l'affidamento in outsourcing di alcuni servizi, in primis quelli di natura legale o assicurativa, riveste un peso importante (20) ai fini della mitigazione di eventuali profili di responsabilità o di gravi ripercussioni patrimoniali associati a eventi informatici.
Sia i firewall (15) che la formazione dei dipendenti (5) non risultano particolarmente performanti per il contenimento efficace dei rischi di natura informatica conseguenti al furto di un dispositivo aziendale.

Come già descritto nel primo capitolo, le *azioni delle persone* definiscono una classe di rischio operativo caratterizzata dai problemi causati dalle azioni intraprese o non intraprese dagli individui in una determinata situazione.
Logicamente quindi la tecnica di mitigazione più opportuna per una categoria di rischio connotata dalla rilevanza del fattore umano non può che risiedere nelle politiche di formazione del personale, il cui peso (30) risulta superiore rispetto all'utilizzo della crittografia (20) e dei firewall (20), strumenti chiamati ad intervenire solo successivamente al verificarsi di un errore umano al fine di tutelare comunque l'integrità dei dati. Residuale risulta invece il peso (10) da attribuire alla password ed ai processi di outsourcing nel contenimento di questa classe di rischio.

Come ultima famiglia di eventi sono stati presi in considerazione i guasti ai sistemi e gli eventi naturali, ossia tutti quegli eventi esterni che non dipendono da attacchi informatici, furti o azioni delle persone, ma bensì da cause di forza maggiore. Per far fronte a queste tipo di situazioni è auspicabile (40) il ricorso ai servizi di un soggetto cui delegare in outsourcing il monitoraggio del traffico dati 24 ore su 24, 7 giorni su 7, e l'interpretazione degli eventi di sistema in tutta la rete. Le altre tecniche di mitigazione rivestono tutte un ruolo estremamente secondario.

4.4.1 Sviluppo del modello

Al *rischio inerente* di ogni evento viene attribuito un valore pari a 100.
Da questo valore assoluto vanno decurtati i punteggi conseguiti dalle tecniche di mitigazione messe in atto, così da determinare il valore di *rischio residuo.*
Il risultato ottenuto va successivamente ponderato per il *tempo di ripristino,* il quale a seconda dei tre intervalli di tempo considerati, 24 ore – 48 ore – 72 ore, consente di giungere allo *score finale.*
Lo score finale è necessario per definire il livello di rischio: basso, medio o alto.
Questi livelli di rischio sono contenuti in un intervallo compreso tra 5 e 95.
Per lo sviluppo del modello non è stato preso in considerazione il rischio 0, non esistendo in natura la possibilità di eliminare completamente gli eventi negativi dalle azioni umane,

ritenendo invece realistico uno scenario di contenimento dello stesso sino ad un valore pari a 5.
Il valore 95 rappresenta lo scenario peggiore, corrispondente ad una situazione in cui non venga messa in atto alcuna tecnica di mitigazione e il tempo di ripristino dell'attività arrivi alle 72 ore.
I tre indicatori di rischio previsti dal modello sono i seguenti.

- Il rischio è *basso* quando lo score sarà compreso tra 5 e 35.
- Il rischio è *medio* quando lo score sarà compreso tra 35 e 65.
- Il rischio è *alto* quando lo score sarà compreso tra 65 e 95.

Vengono presentati alcuni dei risultati ottenuti per ogni evento a seconda delle diverse casistiche.

- MALWARE E RANSOMWARE

Figura 24: Applicazione del modello in caso di malware e ransomware

EVENTO\TECNICHE	Presente?	MALWARE	RANSOMWARE
OUTSOURCING	**no**	15	15
PASSWORD	**si**	20	20
DATI CRITTOGRAFATI	**si**	20	20
DIPENDENTI FORMATI	**no**	10	10
FIREWALLS	**si**	25	25
Rischio inerente		100	100
Totale mitigazione		65	65
Rischio residuo		35	35
Tempo di ripristino		24	24
Score finale		30	30

Fonte: Modello per la determinazione del livello di rischio in caso di un evento di Data Breach

In questo caso la presenza di firewall, password e dati crittografati consente di raggiungere un rischio residuo pari a 35. Questo valore, ponderato per il tempo di ripristino stimato in 24 ore, determina un punteggio finale uguale a 30.
Questo valore è compreso nell'intervallo (5 -35) e quindi il rischio è definito BASSO.

- PHISHING, SMISHING, VISHING E PHARMING

Figura 25: Applicazione del modello in caso di Social Engineering

EVENTO\TECNICHE	Presente?	PHISHING	SMISHING	VISHING	PHARMING
OUTSOURCING	si	10	10	10	10
PASSWORD	si	20	20	20	20
DATI CRITTOGRAFATI	no	20	20	20	20
DIPENDENTI FORMATI	no	30	30	30	30
FIREWALLS	si	10	10	10	10
Rischio inerente		100	100	100	100
Totale mitigazione		40	40	40	40
Rischio residuo		60	60	60	60
Tempo di ripristino		48	48	48	48
Score finale		57	57	57	57

Fonte: Modello per la determinazione del livello di rischio in caso di un evento di Data Breach

In questo caso l'assenza di una adeguata formazione in materia dei dipendenti determina un aumento significativo dei rischi derivanti dagli attacchi di social engineering, cui va inoltre aggiunto il mancato intervento del presidio di protezione offerto dalla crittografia. Il valore del rischio residuo si attesta così a 60, valore che, ponderato per un tempo di ripristino stimato in 48 ore, determina un punteggio finale pari a 57.
Essendo 57 compreso nell'intervallo (35 – 65) il livello di rischio risulta MEDIO.

- FURTO DI UN COMPUTER

Figura 26: Applicazione del modello in caso di furto di un computer

EVENTO\TECNICHE	Presente?	FURTO COMPUTER
OUTSOURCING	no	20
PASSWORD	no	25
DATI CRITTOGRAFATI	no	25
DIPENDENTI FORMATI	si	15
FIREWALLS	si	5
Rischio inerente		100
Totale mitigazione		20
Rischio residuo		80
Tempo di ripristino		24
Score finale		75

Fonte: Modello per la determinazione del livello di rischio in caso di un evento di Data Breach

Nel caso in cui venga rubato un computer e non sia stata prevista una password a protezione di dati peraltro non crittografati, l'ulteriore assenza di garanzie legali ed assicurative derivanti dalla conclusione di specifici accordi di outsourcing determina un livello del rischio residuo oggettivamente preoccupante: 80. Questo valore, ponderato per un tempo di ripristino entro le 24 ore, determina uno score finale pari a 75.

Essendo 75 compreso nell'intervallo (65 – 95), il livello di rischio è ALTO.

- AZIONI DELLE PERSONE

Figura 27: Applicazione del modello in caso di errori umani

EVENTO\TECNICHE	Presente?	AZIONI DELLE PERSONE
OUTSOURCING	**no**	5
PASSWORD	**si**	15
DATI CRITTOGRAFATI	**si**	20
DIPENDENTI FORMATI	**si**	30
FIREWALLS	**si**	20
Rischio inerente		100
Totale mitigazione		85
Rischio residuo		15
Tempo di ripristino		48
Score finale		12

Fonte: Modello per la determinazione del livello di rischio in caso di un evento di Data Breach

Qualora in occasione di un errore umano al pronto intervento dei dipendenti adeguatamente formati si potesse sommare la presenza di software accurati e di password "forti", il rischio residuo si mitigherebbe di molto attestandosi ad un valore pari a 15.

Questo valore, ponderato con un tempo di ripristino stimato in 48 ore, determina uno score finale uguale 12.

Essendo 12 un valore compreso nell'intervallo (5 – 35) il livello di rischio viene definito BASSO.

- GUASTI AI SISTEMI e EVENTI NATURALI

Figura 28: Applicazione del modello in caso di guasti ai sistemi ed eventi naturali

EVENTO\TECNICHE	Presente?	GUASTI AI SISTEMI	EVENTI NATURALI
OUTSOURCING	**no**	40	40
PASSWORD	**si**	5	5
DATI CRITTOGRAFATI	**si**	20	20
DIPENDENTI FORMATI	**si**	15	15
FIREWALLS	**si**	10	10
Rischio inerente		100	100
Totale mitigazione		50	50
Rischio residuo		50	50
Tempo di ripristino		24	24
Score finale		45	45

Fonte: Modello per la determinazione del livello di rischio in caso di un evento di Data Breach

Non aver preventivamente concluso un rapporto di outsourcing in occasione di un grave guasto ai sistemi o al verificarsi di un evento naturale come un incendio, comporta inevitabilmente un valore del rischio residuo importante: 50.
Questo valore, ponderato per un tempo di ripristino stimato in 24 ore, determina un punteggio finale pari a 45.
Il valore dello score è compreso nell'intervallo (35 - 65), per cui il livello di rischio è MEDIO.

4.4.2 Segnalazione all'Autorità Garante e a Banca d'Italia

Come ormai noto, il verificarsi di un attacco informatico produce nell'azienda interessata dallo stesso conseguenze spesso rilevanti in termini giuridici, economici e reputazionali.
Quando le tecniche di mitigazione non siano state preventivamente individuate, o comunque si siano rivelate insufficienti a contenere gli effetti negativi sopportati dall'organizzazione, si rende necessario procedere immediatamente ad una rivisitazione approfondita delle politiche di sicurezza sin qui adottate e ad una nuova mappatura dei rischi d'impresa.

La diffusione di una cultura aziendale orientata alla sicurezza informatica costituisce probabilmente il miglior presidio contro il ripetersi di azioni lesive dell'attività digitale delle imprese.
Per questi motivi è opportuno che, ancor prima della segnalazione alle autorità competenti, le violazioni rilevanti dei sistemi informatici vengano rese note all'interno dell'organizzazione per sensibilizzare ulteriormente gli organi aziendali, in primis quelli incaricati delle funzioni revisionali, sull'importanza della sicurezza informatica.
In caso di data breach è importante che l'organizzazione sappia quali misure adottare, quando farlo e a chi segnalare la violazione dei dati.
Queste fasi devono essere disciplinate accuratamente in un protocollo di violazione dei dati, affinché le conseguenze di qualsiasi evento informatico possano essere affrontate in modo responsabile e controllato. Le istituzioni, in particolare quelle finanziarie, devono essere in grado in qualsiasi momento di poter stabilire l'obbligatorietà o meno della segnalazione di una violazione dei dati attivando le competenti funzioni aziendali.
Il Garante per la protezione dei dati personali è l'Autorità cui il Legislatore ha incardinato la competenza a ricevere immediatamente le segnalazioni di avvenute violazioni all'integrità delle reti e sistemi informatici. Nell'eventualità di violazioni da cui possano derivare gravi danni alla sfera personale degli interessati è inoltre prevista l'obbligatorietà di una pronta informativa anche agli stessi di quanto oggetto di segnalazione.

Il modello proposto in questa tesi vuole quindi garantire un supporto utile, attraverso la determinazione di un punteggio finale per ogni tipologia di rischio, non solo per attivare prontamente il processo segnaletico normativamente previsto ma anche, e soprattutto, per accrescere la consapevolezza della governance aziendale sugli errori eventualmente commessi per evitare che si ripresentino in futuro.

Le imprese sono chiamate ad implementare periodicamente le misure tecniche e organizzative più adeguate al fine di garantire la sicurezza informatica.
Il data breach è spesso infatti conseguenza non solo di problematiche nelle infrastrutture informatiche dell'azienda, ma anche di una non ottimale organizzazione interna incapace di individuare le migliori prassi operative per la protezione dei dati personali.

Per questo motivo infatti Il Regolamento UE 2016/679 insiste moltissimo sulla particolare attenzione che il Titolare del Trattamento deve assicurare ai profili organizzativi interni.
È necessario definire delle corrette politiche aziendali nel trattamento dei dati personali, attraverso l'organizzazione di procedure amministrative e tecniche, di adeguate reti e piattaforme informatiche, che siano in grado di intercettare immediatamente eventuali violazioni, di valutarle e procedere o meno ad informare delle stesse il Garante.

A seconda dello score finale, e quindi del livello di rischio emerso per un determinato evento, si aprono scenari diversi.

Nei capitoli precedenti sono stati analizzati gli obblighi segnaletici così come prescritti dagli articoli 33 e 34 del GDPR e dalla Circolare della Banca d'Italia n. 285 del 17 dicembre 2013.
Entrambi gli interventi normativi sottolineano l'importanza di segnalare in modo tempestivo tutti quegli incidenti di sicurezza informatica considerati critici.

Il modello proposto in questo elaborato ha come obbiettivo quello di riuscire a restituire un indicatore di rischio che possa definire il livello di criticità richiesto dall'autorità garante.

Non tutte le violazioni dei dati personali, si ribadisce, debbono essere oggetto di segnalazione. Quando si verifica una violazione di dati personali, è necessario considerare la combinazione della gravità e della probabilità delle potenziali conseguenze negative della violazione, compreso il rischio risultante per i diritti e le libertà delle persone.
Se si ritiene probabile che dalla violazione di un dato personale consegua un rischio effettivo, è necessario procedere alla segnalazione; se invece si considera improbabile che si configuri il rischio la segnalazione non è obbligatoria.
Tuttavia, qualora si decida di non segnalare una violazione, bisogna essere in grado di giustificare questa decisione e quindi di documentarla.
La documentazione degli eventi avversi, di qualsiasi entità o gravità, costituisce infatti il presupposto per una efficace attività di revisione interna dei processi, tesa a rafforzare la sicurezza complessiva nel trattamento dei dati personali posto in essere dall'azienda

attraverso l'individuazione di idonee misure preventive di carattere tecnico ed organizzativo.

4.4.3 Analisi dei Risultati

I risultati di questo modello forniscono tre livelli di rischio da cui trarre le opportune valutazioni per procedere o meno alle segnalazioni.

- Rischio BASSO*:*

In questo caso il ridotto livello di rischio evidenzia una violazione di dati non definibile come critica, incapace quindi di impattare negativamente sulla sfera dell'interessato. La segnalazione non è obbligatoria ma deve essere conservata la documentazione dell'evento insorto.

- Rischio MEDIO e ALTO:

Al ricorrere di questi livelli di rischio è previsto l'obbligo di tempestiva segnalazione all'Autorità Garante e alla Banca D'Italia entro le 72 ore successive dal verificarsi dell'evento; qualsiasi ritardo deve essere giustificato.
Gli incidenti critici di sicurezza informatica devono essere tempestivamente segnalati alla Banca d'Italia inviando una relazione sintetica che includa la descrizione dell'incidente, le eventuali inadempienze degli utenti interni e dei clienti e qualsiasi altro dato o informazione richiesto dalla Circolare n. 285 del 17 dicembre 2013.
Se una violazione può comportare un rischio elevato per i diritti e le libertà delle persone, il GDPR prevede che oltre all'Autorità Garante vengano informati direttamente gli interessati affinché possano adeguatamente proteggersi dagli effetti della stessa.

4.4.4 Il Rischio di Reputazione

La gestione del rischio informatico assume per le aziende una notevole rilevanza non solo ai fini patrimoniali, ma anche per i riflessi sulla reputazione che le stesse possano vantare sui mercati.
È opportuno quindi adottare un approccio proattivo che preveda una risposta di comunicazione di crisi efficace e immediata. Creare una percezione di onestà e

trasparenza risulta essenziale allorché l'azienda voglia mantenere intatto il rapporto con i propri clienti ed evitare che un danno d'immagine immediato si trasformi in un disastro reputazionale di lungo periodo.

Sia Solvency II per il comparto assicurativo che Basilea II per quello bancario incorporano il rischio di reputazione nel loro quadro normativo e offrono indicazioni per la comprensione dei rischi sottostanti.
In base a Solvency II, il Comité Européen des Assurances (CEA) e il Groupe Consultatif Actuariel Europeen (2007) definiscono il rischio di reputazione come:
«Risk that adverse publicity regarding an insurer's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Reputa- tional risk could arise from other risks inherent in an organization's activities. The risk of loss of confidence relates to stakeholders, which include, inter alia, existing and potential customers, investors, suppliers, and supervisors .»

Il rischio di perdita di fiducia riguarda quindi gli stakeholder, che comprendono, tra l'altro, clienti attuali e potenziali, investitori, fornitori e autorità di vigilanza.

Anche i riflessi reputazionali debbono essere attentamente considerati quando i risultati offerti dal modello si attestino su di un livello *MEDIO – ALTO.*

Al riguardo, è opportuno evidenziare come Basilea II ritenga fondamentale per le istituzioni finanziarie preservare la propria reputazione presso la clientela, le controparti commerciali, gli azionisti, gli investitori e gli analisti di mercato. Il mantenimento della fiducia da parte degli stakeholder costituisce infatti il presupposto per lo sviluppo delle attività finanziarie ed il consolidamento sui mercati.

CONCLUSIONE

L'inizio di questa tesi è stato dedicato all'analisi del concetto di rischio così come percepito nel mondo greco antico, una società che interpretava gli eventi avversi come manifestazioni naturali del volto nefasto del destino, del fato cui l'essere umano è inevitabilmente esposto.

L'uomo non poteva illudersi di avere il controllo delle proprie azioni e tantomeno di essere artefice del proprio destino, il cui corso risiedeva nelle mani capricciose degli Dei e di Zeus primo fra tutti.

In epoca contemporanea il rischio continua ad essere un fattore ineludibile, intrinsecamente connesso a qualsiasi attività o processo umano, sul quale è difficile esercitare un controllo effettivo se insorto al di fuori della nostra sfera previsionale o decisionale.

L'uomo moderno ha però sviluppato nel tempo la capacità di elaborare una visione d'insieme delle situazioni di rischio, dotandosi degli strumenti necessari atti a prevenirle o comunque in grado di contenerne la portata negativa, rendendo così il nostro destino meno "nefasto".

Secondo Platone la condizione dell'essere umano di correre dei rischi è conseguenza evidente del suo stesso vivere, così come il concetto di sfida, di mettersi alla prova, che questo implica.

Oggi è la criminalità informatica ad essere la nostra sfida, perché in un mondo in cui le informazioni costituiscono il patrimonio più prezioso assume contestualmente una rilevanza cruciale il sistema di sicurezza ideato per proteggerle adeguatamente.

La società muta continuamente l'organizzazione dei rapporti interpersonali ed economici e quindi, inevitabilmente, anche le misure di sensibilizzazione alla sicurezza devono adattarsi alle nuove modalità con le quali rendere le prestazioni di lavoro e alla diffusione di diversi canali di comunicazione sociale. Il lavoro da remoto, nuova frontiera dell'economia digitale, ha ridefinito profondamente i ruoli e i rapporti all'interno dei processi produttivi, esponendo però questi ultimi a rischi prima sconosciuti.

Il fattore umano è probabilmente il fattore più complesso da affrontare nella definizione delle politiche di sicurezza informatica. Spesso un attacco informatico colpisce con successo un'azienda perché qualcuno al suo interno ha cliccato su un link dannoso in un'e-mail di phishing, si è fidato e ha condiviso al telefono informazioni riservate con persone

non autorizzate, ha lasciato il proprio computer o dispositivo mobile esposto e incustodito in un luogo pubblico.
I dipendenti sono gli strumenti inconsapevoli, manipolati emotivamente, con i quali la criminalità informatica accede alle reti ed ai sistemi aziendali.
Come si può evitare tutto questo? Un adeguato e continuo processo di formazione sui rischi informatici costituisce il principale presidio di sicurezza di cui le organizzazioni del lavoro, in primis le istituzioni finanziarie, possano dotarsi.
La sensibilità verso la tematica della sicurezza informatica, per essere realmente efficace, deve però essere parte integrante della cultura aziendale, condivisa e promossa dal management aziendale ai suoi massimi livelli.
Le aziende devono acquisire la consapevolezza di essere continuamente esposte a rischi di natura informatica e devono conseguenzialmente includere i target di sicurezza tra gli obiettivi strategici da perseguire.
I contesti normativi nazionali ed europei offrono al riguardo un valido supporto affinché tutti i processi decisionali siano ispirati alla valutazione dei rischi inerenti i processi produttivi ed all'individuazione degli strumenti di carattere organizzativo e tecnico idonei a mitigarne gli effetti.
Il fine ultimo delle politiche di sicurezza informatica deve essere l'adozione di best practice operative che improntino e caratterizzino l'organizzazione aziendale ad ogni suo livello, in particolare gli organi con funzioni decisionali strategiche.

Un mondo del lavoro sempre più connesso in rete comporta un aumento esponenziale del volume di informazioni gestite. La vulnerabilità o meno delle stesse dipende dal livello di competenze digitali acquisite e disponibili. Ridurre al minimo i rischi derivanti dal fattore umano diventerà quindi sempre più un elemento decisivo per il successo delle aziende sui mercati.

All'interno di questa categoria di rischi vanno compresi ovviamente anche i comportamenti posti in essere dagli utenti dei prodotti bancari e finanziari, verso i quali va indirizzata un'attenta opera d'informazione sulle peculiarità ed i pericoli della finanza digitale. L'avvento e lo sviluppo di fintech non può prescindere dalla consapevolezza di tutti gli attori del contesto circa l'importanza di poter disporre di procedure e sistemi

connotati da alti livelli di sicurezza tecnologica, in cui la riservatezza dei dati personali riveste un ruolo fondamentale.
Le misure di sicurezza di tutte le istituzioni finanziarie sono valide quanto la cultura stessa sulla sicurezza dell'organizzazione. Se i dipendenti e i clienti non saranno consapevoli dell'importanza della sicurezza informatica e delle misure di sensibilizzazione per accrescerne l'efficacia, la prevenzione e gestione delle minacce informatiche non migliorerà adeguatamente.
Questa consapevolezza va rafforzata prima che avvenga un'evoluzione dei cyber attacchi da un modello di furto di dati a un modello di furto di controllo. Infatti, in un futuro il numero e l'intensità degli attacchi informatici potrebbero aumentare sino a tendere non più alla semplice sottrazione di dati ma all'assunzione del controllo delle reti e dei dispositivi informatici.

Forse Platone al giorno d'oggi, più che di consapevolezza, parlerebbe di sapienza, la quale, accompagnata alle competenze tecniche e al valore di ogni persona, può rappresentare la forza d'animo necessaria per superare le situazioni più complesse.

BIBLIOGRAFIA

1. Agenzia Per La Cybersicurezza Nazionale, (2022). *National cybersecurity strategy 2022 – 2026*.

2. Alsayed, A. O. e Bilgrami, A. L., (2017). E-Banking security: internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and Advanced Engineering*.

3. Allianz Global Corporate & Specialty SE, (2021). *Financial services - risk trends*

4. Al Gharaibeh, Y., Abu Hammour,R. Qasaimeh,M. Al-Qassas,R., (2019). *DATA '19: Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems*. 1–7. The status of information security systems in banking sector from social engineering perspective

5. Anti-Phishing Working Group (APWG), (2022). *Phishing activity trends report, 1st quarter 2022*.

6. Armstrong, M. E., Jones, K. S., & Namin, A. S. (2021). *How Perceptions of Caller Honesty Vary During Vishing Attacks That Include Highly Sensitive or Seemingly Innocuous Requests. Human Factors.* Sage Journals

7. Basel Committee on Banking Supervision, (2014). *Review of the Principles for the Sound Management of Operational Risk.* Bank for International Settlements

8. Bourget, E., (2020). *Diagnosing accidental and malicious events in industrial control systems. cryptog- raphy and security [cs.cr]*. Thèse de doctorat de, Ecole nationale supérieure Mines-Télécom Atlantique.

9. Bouveret, *Antoine,* (June 25, 2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*

10. Bullée, J-WH, Montoya, L, Pieters, W, Junger, M, Hartel, P. On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *J Investig Psychol Offender Profil*. 2018; 15: 20– 45.

11. Cebula, J., Popeck, M., & Young, L. , (2014). *A Taxonomy of Operational Cyber Security Risks Version 2* (Technical Report CMU/SEI-2014-TN-006). Pittsburgh: Software Engineering Institute, Carnegie Mellon University.

12. Ciclosi, F., (2022). *Rischio digitale Innovazione e Resilienza Conoscere, affrontare e mitigare il rischio digitale*. Milano: Clusit Associazione Italiana per la Sicurezza Informatica, 2022.

13. Clusit, (2021). *Phishing e frodi online*.

14. Clusit, (2022). *Rapporto clusit 2022 – edizione di marzo 2022*.

15. Committee of Sponsoring Organizations of the Treadway Commission (COSO), (2017). *Enterprise risk management integrating with strategy and performance*.

16. CrowdStrike Holdings Inc, (2022). *2022 global threat report*.

17. European Systemic Cyber Group, (2019). *Systemic cyber risk*. Frankfurt am Main, Germany.

18. FBI's Internet Crime Complaint Center, (2021). *2021 internet crime report*. United States of America.

19. Federal Reserve the Conference of State Bank Supervisors (CSBS) and the Federal Deposit Insurance Corp (FDIC), (2021). *Community banking in the 21st century 2021*.

20. Frisby, J., (2020). *Cybersecurity exposure index (CEI)*.

21. Garante Per La Protezione Dei Dati Personali, (2021). *Relazione annuale 2021*.

22. Gatzert, Schmit, Kolb, N. J. A., (2014). *Assessing the risks of insuring reputation risk*. Working Paper, Department of Insurance Economics and Risk Management Friedrich-Alexander-University of Erlangen-Nürnberg.

23. Ibm Security, (2021). *Cost of a data breach report 2021*. United States of America.

24. Ibm Security, (2022). *X-Force threat intelligence index 2022*. United States of America.

25. Italia. Banca d'Italia, (2006). *Nuove disposizioni di vigilanza prudenziale per le banche.* Circolare n. 263, 27 dicembre.

26. Italia. Banca d'Italia, (2013). *Disposizioni di vigilanza per le banche.* Circolare n. 285, 17 dicembre.

27. Italia. Banca d'Italia, (2015). *Disposizioni di vigilanza per gli intermediari finanziari.* Circolare n. 288, 3 aprile.

28. A.K. Kashyap, A. Wetherilt. 2019. *Some Principles for Regulating Cyber Risk.* AEA Papers and Proceedings, 109: 482-87.

29. Lingua, M., (2021). *Modelli quantitativi per la cybersecurity negli intermediari finanziari*. Tesi di laurea magistrale, Politecnico di Torino.

30. MASO, S. (2012). Val la pena rischiare? Qualche osservazione sulla categoria filosofica di "rischio" in Platone. *La Ricerca Folklorica*, *66*, 85–95.

31. M.Martorana (2019), *GDPR e Decreto Legislativo 101/2018, Vademecum del professionita: obblighi, adempimenti, strumenti di tutela*, CEDAM

32. Mishra, S. e Soni, D., (2020). *Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis*, Future Generation Computer Systems. pp. 803–815.

33. Murphy, D. R. e Murphy, R. H., (2007). *Phishing, pharming, and vishing: fraud in the internet age.* The Telecommunications Review 2007. pp. 37–45.

34. NADDAF, G. (2009). GREEK COSMOGONY [Review of <italic>*Ancient Greek Cosmogony*</italic>, by A. Gregory]. *The Classical Review*, *59*(2), 342–344.

35. Netscout Systems Inc, (2019). *Cloud in the crosshairs: netscout's 14th annual worldwide infrastructure security report*. Westford, Massachusetts.

36. R. Locatelli E. Magistretti P. Scalerandi G. Carosio, (2001). *"Il rischio operativo"*. Università Cattolica del Sacro Cuore Facoltà di Scienze Bancarie Finanziarie e Assicurative.

37. Rowe, B., (2007). *Will outsourcing IT security lead to a higher social level of security?*

38. SoSafe, (2022). *Human risk review 2022 an analysis of the european cyberthreat landscape*. Cologne, Germany.

39. The status of information security systems in banking sector from social engineering perspective, (2019). *DATA '19: Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems*. 1–7.

40. Trend Micro Incorporated, (2021). *Attacks from all angles: 2021 midyear cybersecurity report*.

41. Unione Europea. European Banking Authority, (2019). *Orientamenti dell'ABE sulla gestione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) e di sicurezza*Guidelines n. 04, 28 novembre.

42. Unione Europea. European Banking Authority, (2021). *Relazione finale sugli orientamenti aggiornati in materia di segnalazione dei gravi incidenti ai sensi della psd2,* Orientamenti n. 03, 10 giugno.

43. Unione Europea. Parlamento Europeo, (2016). *General Data Protection Regulation.* Regolamento dell'Unione Europea n. 679, 27 aprile.

44. Z. Wang, H. Zhu and L. Sun, (2021). *"Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods,"* in IEEE Access, vol. 9, pp. 11895-11910.

45. Yeboah-Boateng, Amanor, E. O. P., (2014). Phishing, smishing & vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*. 4 aprile. p. 11.

46. Wood, O. G. (1964). Evolution of the Concept of Risk. *The Journal of Risk and Insurance*, *31*(1), 83–91.

SITOGRAFIA

1. Banca d'Italia - AVVISO. Campagna di phishing con uso fraudolento del nome della Banca d'Italia [online], (senza data). *Banca d'Italia - Il sito ufficiale della Banca Centrale Italiana*. [Consultato ad agosto 2022]. Disponibile da: https://www.bancaditalia.it/media/notizia/avviso-campagna-di-phishing-con-uso-fraudolento-del-nome-della-banca-d-italia/

2. Banca d'Italia pubblica l'elenco degli Orientamenti e delle Raccomandazioni delle Autorità europee di vigilanza (European Supervisory Authorities) - EBI - Easy Banca d'Italia [online] *EBI - Easy Banca d'Italia*. [Consultato a giugno 2022]. Disponibile da: https://ebi.sefin.it/news/banca-ditalia-pubblica-lelenco-degli-orientamenti-e-delle-raccomandazioni-delle-autorita-europee-di-vigilanza-european-supervisory-authorities-2/

3. EBA revises guidelines on major incident reporting under PSD2 [online], (senza data). *Moody's Analytics | Risk Management, Credit Ratings Research, Software*. [Consultato a giugno 2022]. Disponibile da: https://www.moodysanalytics.com/regulatory-news/Jun-10-21-EBA-Revises-Guidelines-on-Major-Incident-Reporting-Under-PSD2

4. Frodi online [online], *Banca Intesa Sanpaolo - Conto Corrente per Famiglie, Giovani e Aziende*. [Consultato ad agosto 2022]. Disponibile da: https://www.intesasanpaolo.com/it/persone-e-famiglie/bisogni/sicurezza-digitale/phishing-vishing-smishing-frode-online.html

5. Prestatori di servizi di pagamento: attuazione degli Orientamenti EBA in materia di segnalazione dei gravi incidenti ai sensi della direttiva PSD2 (EBA/GL/2021/03) - EBI - Easy Banca d'Italia [online], (senza data). *EBI - Easy Banca d'Italia*. [Consultato a giugno 2022]. Disponibile da: https://ebi.sefin.it/news/prestatori-di-servizi-di-pagamento-attuazione-degli-orientamenti-eba-in-materia-di-segnalazione-dei-gravi-incidenti-ai-sensi-della-direttiva-psd2-eba-gl-2021-03/

6. PSD2: attuati gli Orientamenti EBA sulla segnalazione di gravi incidenti - DB [online], (senza data). *DB*. [Consultato a giugno 2022]. Disponibile da: https://www.dirittobancario.it/art/psd2-attuati-gli-orientamenti-eba-sulla-segnalazione-di-gravi-incidenti/

7. Risk and control matrix: a powerful tool to understand and... [online], (senza data). *SC&H Group*. [Consultato a luglio 2022]. Disponibile da: https://www.schgroup.com/resource/blog-post/risk-and-control-matrix-a-powerful-tool-to-understand-and-optimize-your-organizations-risk-profile/

8. *Deloitte Deutschland*. [Consultato a luglio 2022]. Disponibile da: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-eba-guidelines-ict-security-risk-management.pdf

9. Solomon Fadun - Risk Management of Everything, (2021). Operational risk and the management of operational risks (operations & operational risk management) [online]. *YouTube*. [Consultato a luglio 2022]. Disponibile da: https://www.youtube.com/watch?v=s2ogL-1wdaE

10. What are smishing attacks and why are they increasing? [online], (senza data). [Consultato ad agosto 2022]. Disponibile da: https://cmap.amp.vg/web/b3lknalklab1f

11. What is pharming and how to protect against attacks | fortinet [online], (senza data). *Fortinet*. [Consultato ad agosto 2022]. Disponibile da: https://www.fortinet.com/resources/cyberglossary/pharming

12. What is phishing? | how to protect against phishing attacks | malwarebytes [online], (senza data). *Malwarebytes*. [Consultato ad agosto 2022]. Disponibile da: https://www.malwarebytes.com/phishing