LUISS

Corso di laurea in Economia e Management

Cattedra: Matematica Finanziaria

“Definizione, regolamentazione e quantificazione del rischio cibernetico: da temibile minaccia a terza potenza economica mondiale”

Prof. Salvatore Forte
Relatore

Andrea Santucci (270081)
Candidato

Anno Accademico 2023/2024

Indice

Introduzione

L'elaborato di tesi in esame si propone, sin dal proprio stato embrionale, di costituire un *excursus* di carattere culturale ed informativo in riferimento ad una delle tematiche di maggior attualità e rilevanza del panorama normativo, economico e politico all'interno del corrente scenario internazionale: il rischio cibernetico. Per tale motivazione si è stabilito di istituire un'analisi dettagliata e complessiva dell'argomento, in principio incentrata rispetto alla comprensione dell'effettivo valore della stessa tramite il *reportage* di informazioni derivanti da documenti redatti dalle più autorevoli testate ed organizzazioni di competenza. Inoltre, si è ritenuto funzionale all'effettiva comprensione della materia l'analisi delle fasi essenziali della relativa evoluzione intertemporale, illustrandone, dunque, le corrispondenti misure di tutela e prevenzione, rientranti nel novero della *cybersecurity*. Quindi, si evince come la valutazione dettagliata del rischio cibernetico e delle sue cangianti tipologie abbia indotto alla definizione delle procedure atte a minimizzare potenziali effetti catastrofici in termini finanziari e reputazionali sul triplice piano individuale, aziendale ed istituzionale. Dunque, è stata condotto un approfondimento riguardante il contesto normativo e regolamentare in questione, tracciandone i tratti salienti ed individuandone le autorità competenti a seconda delle fattispecie di riferimento, al fine di fornire al lettore informazioni preziose all'apprendimento delle strategie impiegate sul piano personale, imprenditoriale e transnazionale al fine di garantire la salvaguardia dei diritti fondamentali dell'essere umano e degli enti da esso eretti. In tale prospettiva è stato ritenuto opportuno fornire una specifica descrizione dei principali strumenti di tutela preventiva, essendo in epoca moderna essenziale l'anticipazione di eventuali calamità avverse in modo da ridimensionarne i potenziali effetti nefasti, tenendo ben chiaro in considerazione il fatto che attualmente il fenomeno del rischio cibernetico rappresenti la terza potenza economica mondiale, dietro alle sole USA e Cina, sormontate, in modo da ottenere il primato, in termini di tasso di crescita annuo. Per questa ragione è risultato essere intrigante e di particolare interesse analizzare dal punto di vista analitico l'argomento, tramite la determinazione concettuale, *ab origine*, e l'interpretazione applicativa, *ex post*, di modelli idonei alla quantificazione del rischio cibernetico. Auspicando la sollecitazione dell'interesse e del coinvolgimento del corrispondente, si augura in maniera viva e sentita una piacevole lettura.

1. Il cyber risk

In epoca recente il significativo progresso nel contesto tecnologico e digitale ha apportato significativi benefici alla quotidianità di ogni singolo individuo, implementando, tra numerosi aspetti, in modo particolare l'operatività di molteplici realtà produttive. Allo stesso tempo, l'informatizzazione delle procedure di produzione e delle comunicazioni ha generato per i soggetti e le aziende un rilevante incremento di vulnerabilità con conseguenti danni potenzialmente irreparabili.

Nello specifico, la gestione da parte delle imprese di una sostanziosa mole di dati ed informazioni riguardanti il proprio know-how o i soggetti con i quali esse interagiscono, quali clienti o fornitori, ha esposto tali attività al fenomeno del *cyber risk*. Quest'ultimo risulta essere un rischio di tipo informatico, derivante dall'uso della tecnologia, capace di comportare danni economici, anche noti come rischi diretti, o reputazionali, definiti come rischi indiretti. Tale utilizzo abusivo di *network* informatici da parte di determinate figure risulta essere generalmente finalizzato al danneggiamento di un determinato ente sul mercato o all'acquisizione di elementi sensibili relativi all'*asset* aziendale.

1.1 Definizione e contestualizzazione del rischio cibernetico

Innanzitutto, è opportuno considerare il rischio cibernetico come specifica tipologia di rischio operativo. Quest'ultimo è descritto dalla Banca d'Italia, in seno al recepimento dell'accordo internazionale Basilea II[1], come "rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni"[2] Dunque l'*operational risk* riguarda le molteplici incertezze dinanzi alle quali potrebbe ritrovarsi un'impresa durante lo svolgimento delle proprie attività produttive o commerciali all'interno di un certo settore di mercato.

Il *cyber risk*, o rischio cibernetico, è comunemente definito come un rischio legato al mondo informatico consistente nel trattamento illegittimo ed improprio di informazioni inerenti al sistema hardware-software o alle banche dati di una determinata impresa.

---

[1] Basilea II è la denominazione abbreviata del documento di vigilanza prudenziale intitolato "*International Convergence of Capital Measurement and Capital Standards*" siglato nel 2004 presso il Comitato di Basilea per la Supervisione Bancaria. Tale accordo mira a rafforzare le normative riconducibili al precedente protocollo Basilea I finalizzato all'individuazione di standard comuni per la gestione del credito da parte delle banche divenuta poco prudente.

[2] Citazione ricavata dal documento "RISCHI OPERATIVI (Metodi Avanzati - AMA)", Banca d'Italia, Luglio 2006

Queste componenti risultano essere oggetto di violazione, acquisizione irregolare o cancellazione e possono giungere sino alla compromissione persino di dati personali. Tali fenomeni presentano una duplice natura a seconda della quale vengono qualificati come: accidentali, ovvero involontariamente generati dagli stessi dipendenti adibiti all'utilizzo del complesso informatico dell'azienda, come ad esempio guasti tecnici o l'uso di tecnologie obsolete; dolosi, i quali consistono in atti intenzionali, da parte di soggetti non autorizzati al trattamento di specifici dati, con finalità lesive per le aziende, tra i quali attacchi hacker.

Inoltre, è possibile riportare, secondo quanto illustrato dal CRO Forum[3] nel 2016, che il concetto di *cyber risk* riguardi anche i danni psicologici da esso causati, le responsabilità derivanti dall'utilizzo o trasferimento di particolari dati e la disponibilità, integrità o confidenzialità dell'informazione in formato elettronico.

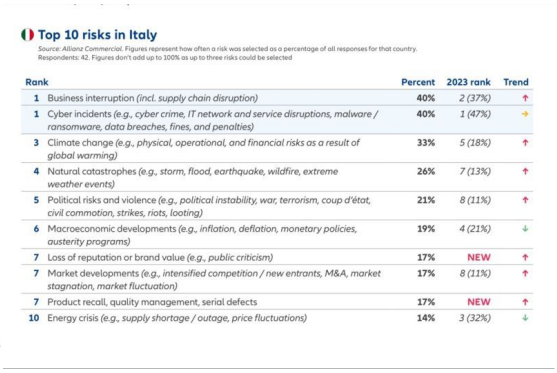
In epoca odierna l'esposizione al *cybercrime* risulta essere riportata al primo posto nella graduatoria, rappresentata dall'Allianz Risk Barometer, dei rischi maggiormente temuti dalle aziende, non soltanto in Italia ma anche nel mondo. Dunque, nel 2024 il cyber risulta essere il principale rischio per imprese ed aziende nel panorama nazionale e globale, apportando maggiore preoccupazione rispetto a fenomeni particolarmente noti quali catastrofi naturali o cambiamento climatico. Tale risultato, secondo il giudizio di Petros Papanikolaou, CEO di Allianz Commercial[4], deve essere inteso come frutto delle problematiche maggiormente significative in epoca moderna per le imprese dell'intero globo, tra le quali primeggia la globalizzazione. In aggiunta a quanto esplicitato, è doveroso sottolineare che le principali incertezze aziendali coinvolgano simultaneamente grandi società, piccole e medie imprese. Bensì, si riscontra un disallineamento in termini di resilienza, in quanto, in modo particolare a seguito della crisi pandemica, le maggiori imprese hanno palesato maggiore consapevolezza del rischio, a differenza delle minori, le quali, per carenza di risorse e tempo, riscontrano

[3] Il CRO forum, dove CRO sta per *Chief Risk Officer*, è un organismo costituito dai principali responsabili del rischio all'interno delle maggiori compagnie di assicurazione nel contesto internazionale, tra i cui membri fondatori vi è l'italiana Assicurazioni Generali. Tale ente presenta come obiettivi la promozione delle *best practices* nella gestione del rischio, l'analisi di rischi emergenti e l'evoluzione dell'ambito assicurativo e delle rispettive norme o regolamenti mediante la pubblicazione di paper tematici.

[4] *Allianz Commercial*, parte dell'*Allianz Group,* è un'azienda impegnata nel settore assicurativo. Secondo l'agenzia internazionale di consulenza strategica e gestione dei marchi Interbrand, Allianz risulta essere il primo *brand* assicurativo al mondo. Esso è attivo in più di 200 paesi ed ha prodotto globalmente nel 2023 circa €18 miliardi in premi assicurativi.

maggiori difficoltà nel tutelarsi da potenziali fattori di incertezza o nel superare quest'ultimi.

Figura 1: Allianz Risk Barometer Global 2024[5]



Rank		Percent	2023 rank	Trend
1	Business interruption *(incl. supply chain disruption)*	40%	2 (37%)	↑
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	40%	1 (47%)	→
3	Climate change *(e.g., physical, operational, and financial risks as a result of global warming)*	33%	5 (18%)	↑
4	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	26%	7 (13%)	↑
5	Political risks and violence *(e.g., political instability, war, terrorism, coup d'état, civil commotion, strikes, riots, looting)*	21%	8 (11%)	↑
6	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	19%	4 (21%)	↓
7	Loss of reputation or brand value *(e.g., public criticism)*	17%	NEW	↑
7	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	17%	8 (11%)	↑
7	Product recall, quality management, serial defects	17%	NEW	↑
10	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	14%	3 (32%)	↓

Figura 2: Allianz Risk Barometer Italy 2023[6]

Ulteriori interessanti informazioni in merito alla tematica trattata risultano fornite dallo studio *"Net Losses: Estimating the Global Cost of Cybercrime"* su iniziativa del CSIS[7], il quale mette in luce intriganti statistiche in merito all'incidenza del cybercrime rispetto al PIL secondo la duplice prospettiva nazionale e globale nel 2014. La comparazione tra i dati relativi a tale periodo e quelli inerenti all'epoca contemporanea si riveleranno di estrema rilevanza al fine di evincere la crescita esponenziale del fenomeno analizzato nel corso degli ultimi anni.

Considerando l'analisi condotta dal CSIS nei riguardi dei paesi selezionati, è possibile notare che quelli maggiormente colpiti in termini percentuali rispetto al proprio PIL fossero Germania, con l'1.60%, e l'Olanda, con l'1.50%. Tali valori sono ben distanti da quelli italiani, pari a circa lo 0.04%, per motivazioni legate ad una moltitudine di ragioni, tra le quali è possibile menzionare la mancanza di sufficienti informazioni qualificate, per cui nazioni con economie simili e sistemi di tutela analoghi presentano livelli di perdite dissimili. Ad esempio, il costo per la violazione o appropriazione della proprietà intellettuale si presenta come uno dei più complicati da stimare, ma allo stesso tempo uno dei maggiormente rilevanti. Inoltre, appaiono evidenti le oscillazioni di rendimento osservando le stime nazionali a disposizione. Infatti, le economie dominanti

[5] Fonte: *Allianz Commercial*, Gennaio 2024, "*Allianz Risk Barometer Results appendix 2024*"
[6] Fonte: *Allianz Commercial*, Gennaio 2024, "*Allianz Risk Barometer Results appendix 2024*"
[7] Il CSIS, anche noto come *Center for Strategic and International Studies,* è un think tank statunitense, ovvero un organismo tendenzialmente indipendente dalle forze politiche impegnato nell'analisi delle politiche pubbliche. Nello specifico tale centro, tra i migliori al mondo nel suo genere, conduce analisi riguardanti temi politici, economici e di sicurezza in ottica internazionale.

presentavano un danno medio dello 0.9% per ragioni legate ad un *report* più dettagliato, ma anche per una maggiore attrattività rispetto a nazioni maggiormente vulnerabili come quelle in via di sviluppo, con una perdita media dello 0.2%. Come precedentemente accennato, a causa del fenomeno dell'*underreporting* le cifre riportate potrebbero in realtà rivelarsi ben maggiori.

Per quanto concerne i calcoli condotti su base globale, invece, il CSIS valuta il costo globale del *cybercrime* per una cifra che si aggirava all'epoca attorno ai 400 miliardi di dollari, equivalente allo 0.8% del PIL mondiale ed il 16% dell'intera *Internet Economy*[8].

L'impatto reale dei dati appena descritti può essere effettivamente compreso comparando gli stessi con altri relativi agli effetti prodotti da ulteriori iniziative criminali a livello globale, tra le quali attività di estrema risonanza quali la contraffazione ed il narcotraffico, che presentavano rispettivamente una percentuale di influenza dello 0.89% e 0.90% rispetto al PIL globale. Oltre a quanto precedentemente esposto, è assolutamente significativo ricordare come in ottica macroeconomica la soglia di tollerabilità per le azioni illecite risulta stanziata attorno al 2% del PIL. Per questa ragione è evidente come il *cyber risk* rimanesse al tempo dello studio analizzato al di sotto del citato livello limite; tuttavia, appariva già preoccupante la progressiva crescita di tale fenomeno, malgrado si trattasse, e si tratti ancora oggi, di una tipologia di infrazione che non sempre si dimostra facilmente monetizzabile.

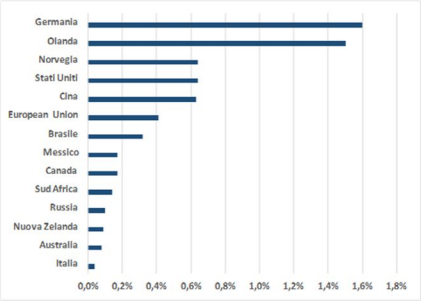


Figura 3: Incidenza del Cybercrime sul PIL[9]

Attività criminale	Costo espresso in % del PIL
Pirateria marittima	0,02% (Global)
Cybercrime	**0,80% (Global)**
Contraffazione	0,89% (Global)
Narcotraffico	0,90% (Global)
Incidenti stradali	1,00% (US)
Crimini Transnazionali	1,20% (Global)
Taccheggio	1,50% (US)

Figura 4: Impatto delle attività criminali sul PIL[10]

[8] L'*Internet economy* riguarda tutto ciò che può essere associato all'utilizzo del web e si basa sullo studio di tecnologie avanzate. Tale branca risulta essere una componente della *digital economy*, la quale riguarda in modo più generico il complesso di relazioni e processi derivanti dall'impiego della tecnologia.

[9] Fonte: CSIS *Center for Strategic and International Studies*, Giugno 2014, "*Net Losses: Estimating the Global Cost of Cybercrime*"

[10] Fonte: CSIS *Center for Strategic and International Studies*, Giugno 2014, "*Net Losses: Estimating the Global Cost of Cybercrime*"

In epoca recente, come testimoniato dall'ANSA[11] gli attacchi *cyber* si attestano come emergenza globale, al pari di eventi di assoluta notorietà come il cambiamento climatico e la criminalità organizzata, dal valore di 6 trilioni di dollari, equiparabile al 6% del PIL mondiale ed al 400% del PIL italiano. Tale cifra risulta addirittura ancora maggiore facendo testo al Microsoft Data Security Index[12] report, il quale indicizza il *cybercrime* come la terza potenza economica mondiale dal valore di 8 trilioni di dollari, collocandosi alle spalle soltanto di colossi nazionali come USA e China. Il dato in merito al quale il rischio cibernetico primeggia persino dinanzi ai due citati *totem* dell'economia moderna risulta essere la crescita relativa annuale del 15%. L'analisi dettagliata di queste cifre stupefacenti permette di comprendere realmente le potenzialità della manipolazione di dati in una società interconnessa e globalizzata come quella attuale, che sfondano il muro dell'ambito informatico arrivando ad influenzare in maniera diretta la stabilità, le politiche e la sicurezza dell'intero globo.

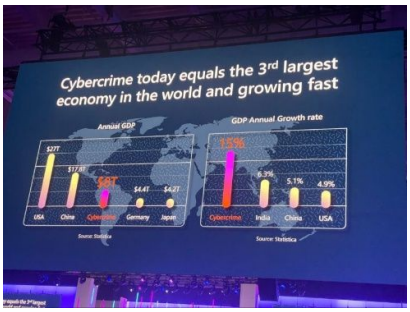


Figura 5: il cybercrime come potenza economica mondiale[13]

Per quanto concerne la valutazione dei settori maggiormente colpiti dagli effetti del rischio cibernetico il riferimento individuato è al rapporto Clusit-Associazione Italiana per la Sicurezza Informatica[14]sulla sicurezza ICT[15] inerente al primo semestre del 2023,

[11] L'ANSA, acronimo di Agenzia Nazionale Stampa Associata, è una delle principali agenzie di informazione multimediali in Italia e nel mondo. Lo scopo di tale ente è la pubblicazione di notizie relative ai principali avvenimenti nel panorama internazionale, perseguito tramite cinquanta sedi in cinque continenti.

[12] *Microsoft Data Security Index* è il frutto del coinvolgimento di più di 800 esperti di sicurezza impegnati nell'identificazione in tale contesto di *trend* e *best practices*.

[13] Fonte: *Microsoft Data Security Index*, 2024, "*Microsoft Data Security Index report"*

[14] Clusit è un'associazione italiana impegnata nell'ambito della sicurezza informatica con una moltitudine di obiettivi, tra i quali la diffusione della cultura della sicurezza informatica, la partecipazione per l'elaborazione di normative in materia a livello nazionale e comunitario e la diffusione di metodi e tecnologie utili all'efficientamento della sicurezza per aziende, Pubblica Amministrazione e cittadini

[15] La sicurezza ICT concerne l'ambito della tecnologia dell'informazione e della comunicazione, inerente ad attività e metodologie utili alla ricezione, trasformazione e trasmissione di informazioni tramite l'interazione tra tecnologie e comunicazioni

all'interno del quale emerge un incremento degli attacchi informatici in Italia del 40% rispetto ai primi sei mesi del 2022. Il *trend* sostanziatosi nel Belpaese risulta maggiormente preoccupante se paragonato a quello mondiale, il quale ha registrato un incremento dell'11% nel primo semestre del 2023, cifra inferiore al +21% ottenuto un anno prima. Statistica addizionale di consistente rilevanza risulta essere la crescita complessiva degli attacchi *cyber* che si estende dal 2018 al 2023 nel corso del quale l'Italia ha patito un a crescita relativa del 300%, ben più significativa se paragonata al +61.5% nel contesto globale. Come illustrato da Gabriele Faggioli, presidente di Clusit, è interessante notare come l'Italia nel periodo citato abbia avuto un'incidenza del 9.6% del totale degli attacchi che si sono verificati nel panorama internazionale. Tale informazione stupisce in quanto l'Italia costituisce esclusivamente il 2% del PIL e lo 0,7% della popolazione mondiali. In più, nello scenario globale si denota un progressivo sviluppo degli attacchi *hacktivism*, perpetuati per ragioni politiche e finalizzate all'indebolimento di determinati paesi, e di quelli nell'ambito *social engineering,* che generano conseguenze per imprese, istituzioni e cittadini privati. Infine, è opportuno segnalare una sempre più marcata diversificazione delle industrie coinvolte, tra le quali è consueto menzionare sanità e pubblica amministrazione, con particolare menzione ad una sempre più notevole frequenza nel mondo della manifattura. In modo particolare, a livello globale il 34% del totale delle infrazioni nel contesto del *manifacturing* ha origine in Italia, paese nel quale gli illeciti di questo tipo primeggiano al fianco di quelli compiuti nel settore *government,* che emerge come principale in termini di numerosità nel nostro paese. Diversamente, nell'ottica internazionale il settore maggiormente danneggiato risulta essere l'*healthcare*, ovvero il settore sanitario.

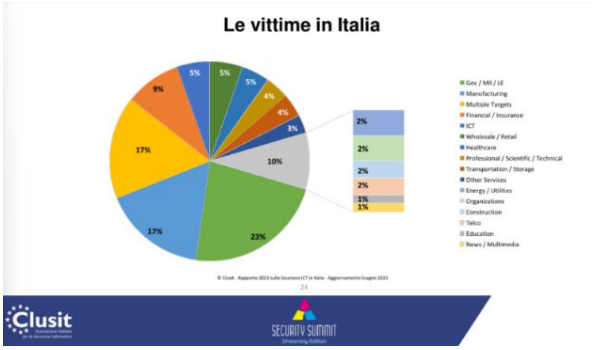


Figura 6: crescita % cyber attacks in Italia e nel mondo[16] *Figura 7: i settori colpiti dal cybercrime in Italia*[17]

1.2 L'evoluzione del cyber risk

Il fenomeno del cybercrime può certamente essere considerato come uno dei maggiormente mutevoli ed in costante fase di sviluppo, essendo la dinamicità e, dunque, l'imprevedibilità tematiche insite all'interno dello stesso. Attualmente i principali *trend* in materia risultano essere, in primo luogo, relativi ad un ampliamento dei *target,* intesi come obiettivi*,* tra cui risulta doveroso menzionare non soltanto il più dispendioso e rapido, ovvero l'appropriazione indebita di informazioni, ma anche e soprattutto la violazione dell'integrità delle stesse, che spesso vengono modificate o distrutte per finalità di carattere economico o politico. Infatti, l'oggetto degli attacchi informatici non si limita esclusivamente all'essere umano, spesso considerato come elemento sensibile ed esposto, ma si estende sino a coinvolgere il *core system* di aziende o, persino, nazioni. Per tali ragioni il rischio cibernetico presenta come potenziali effetti da un lato la semplice acquisizione illecita di dati sensibili, dall'altro presenta la possibilità di concretizzarsi come un vero e proprio strumento per l'attacco frontale ad interi paesi. Si evince pertanto come il cybercrime possa coinvolgere soggetti o enti di qualsivoglia dimensione, settore o provenienza tramite il semplice utilizzo di dispositivi tecnologici capaci di estendere progressivamente le minacce di intere *supply chain*, arrivando sino a minare l'integrità di partner di terzo o quarto livello pur di ottenere i risultati auspicati. Tutto ciò viene perpetuato nonostante molteplici individui ed imprese, essendo ormai consapevoli della pericolosità del tema in questione, abbiano ampliato sistemi di regolamentazione e tutela, i quali risultano frequentemente elusi da tecniche e metodologie di realizzazione del crimine *cyber* sempre più all'avanguardia.
Il *report* di Accenture[18] intitolato "Securing the Digital Economy" delinea chiaramente l'assunzione di particolare rilevanza da parte dell'economia digitale nel corso degli ultimi anni, ponendo in evidenza il fatto che soli 10 anni fa le imprese a puntare

[16] Fonte: Clusit-Associazione Italiana per la Sicurezza Informatica, Giugno 2023, "Rapporto 2023 sulla sicurezza ICT in Italia"
[17] Fonte: Clusit-Associazione Italiana per la Sicurezza Informatica, Giugno 2023, "Rapporto 2023 sulla sicurezza ICT in Italia"
[18] Accenture è una multinazionale statunitense attiva nel mondo della consulenza strategica e direzionale e dell'outsourcing, considerata come una delle principali a livello internazionale, come testimoniato dalla presenza nella lista Fortune 500, classifica delle prime 500 multinazionali nel mondo per fatturato. Essa compie attività di riprogettazione di processi aziendali per finanza, contabilità e controllo di gestione, consulenza strategica e cybersecurity.

sull'impiego di Internet per i propri affari fossero poco più di una su quattro, mentre attualmente la *digital economy* è identificata come essenziale vincolo di sviluppo per il 90% dei principali *business leaders*. Tuttavia, il 68% di questi riconosce una notevole crescita dei *cyber risks*, dinanzi alla quale l'80% delle aziende si configura come impreparata non accompagnando alle numerose innovazioni digitali le necessarie misure di protezione e sicurezza. In tal senso non sorprende il fatto che gli attacchi *cyber* ricoprono una posizione rilevante all'interno delle graduatorie riguardanti i rischi globali redatte dal World Economic Forum[19] nel 2024.

Figura 8:World Economic Forum Global Risks Perception Survey 2023-2024[20]

Il primo esemplare di attacco informatico moderno risale al 1988, quando lo studente statunitense Rober Tappan Morris diede vita al fenomeno oggi definito come "Verme di Morris", noto ancora oggi come uno dei più significativi crimini informatici della storia. Eppure, risulta doveroso ricordare come tale *malware*[21] non fosse stato progettato con finalità maliziose, bensì con la volontà di analizzare le reali dimensioni di Internet. A tal scopo era stato sviluppato con la capacità di autoreplicarsi ed installarsi all'interno dei dispositivi connessi alla rete sfruttando alcune vulnerabilità di un programma di individuazione di password, della piattaforma di posta elettronica Sendmail e del

[19] Il World Economic Forum si sostanzia come fondazione senza fini di lucro, la quale ogni inverno presso Davos in Svizzera si occupa dell'organizzazione di un evento che coinvolge protagonisti della politica ed economia internazionale, giornalisti ed intellettuali per discutere di temi di urgenza, che possono essere anche di natura sanitaria o ambientale. L'organizzazione si occupa inoltre di ricerca e progetti settoriali.
[20] Fonte: World Economic Forum, 2024, "The global Risks report 2024"
[21] Il *malware* indica un *software* dannoso capace di compromettere ogni genere di dispositivo, servizio o rete programmabile. Di norma viene impiegato al fine di estrapolare illecitamente informazioni per le quali verrà poi richiesto un riscatto generalmente in denaro.

protocollo di rete per lo scambio di informazioni Finger per l'acquisizione di dati sugli utenti di altri computer. Questo "worm" era stato programmato per cancellarsi automaticamente in caso di spegnimento del computer, bensì all'epoca i dispositivi venivano spenti raramente; pertanto, si verificò un'incontrollata diffusione del virus. Furono resi inutilizzabili circa 6000 macchinari, equivalenti all'epoca ad una probabilità di un computer su dieci, per un danno complessivo dai 100000 ai 10000000 di dollari. Il caso ebbe una tale risonanza da porre in secondo piano le elezioni presidenziali, che si sarebbero tenute da lì a poco, sulle prime pagine dei principali quotidiani dell'epoca, tra cui il New York Times. L'estensione del verme di Morris fu tale da indurre l'autore dello stesso, in collaborazione con un collega di Harvard, a diffondere in rete un messaggio anonimo contenente le istruzioni per la riparazione dei dispositivi infetti. Tra questi vi furono i sistemi di autorevoli istituzioni, tra le quali la NASA, Berkeley e Stanford per cui il governo degli Stati Uniti decise di dare vita all'ancora oggi esistente CERT, acronimo di Computer Emergency Response Team, gruppo di esperti di informatica finalizzato al contenimento ed alla prevenzione di fenomeni analoghi. Inoltre, tale ente negli anni successivi si è occupato del monitoraggio e della quantificazione di casi di *cybercrime* nell'intero panorama globale, testimoniandone un incremento esponenziale. Effettivamente, nel 1990, anno della condanna di Morris a libertà vigilata, ore di servizi sociali e $10000 di ammenda, gli attacchi informatici segnalati erano approssimativamente un centinaio, per poi raddoppiare soltanto un anno dopo, giungere sino a 56000 nella successiva decade, duplicandosi nuovamente nel 2003 sino a varcare la soglia dei 100000 casi, così inducendo il CERT ad interromperne il conteggio. Il "verme di Morris" costituisce una pietra miliare del mondo della sicurezza informatica ed è per tale ragione ancora oggi un modello per programmatori ed hacker, pertanto nel bene e nel male.

Se da un lato il "verme di Morris" costituisce il primo vero caso di *cyber attack* moderno, è opportuno illustrare le caratteristiche di uno degli esemplari di *cybercrime* maggiormente nefasti della storia: il *ransomware*[22] WannaCry. Nello specifico quest'ultimo può essere tecnicamente definito come un *crypto ransomware*, essendo caratterizzato dalla codifica di dati di terzi con dispositivi di sistema operativo

[22] Il *ransomware* è una tipologia di *malware* generalmente impiegata al fine di estorcere denaro al soggetto danneggiato in seguito alla crittografia di file resi illeggibili, nel caso del *crypto ransomware*, o impedendo l'accesso al computer, nel caso di *locker ransomware.*

Microsoft Windows, per la cui restituzione veniva richiesto un sostanzioso riscatto in Bitcoin, ovvero in criptovaluta. Il fenomeno in questione si è esteso globalmente e rapidamente nel 2017, periodo nel quale erano ancora in vigore sistemi informatici obsoleti, software poco aggiornati ed una conoscenza poco approfondita di determinati aspetti del mondo digitale. In effetti, tale attacco fu perpetuato sfruttando le vulnerabilità del sistema Microsoft Windows poste alla luce dall'iniziativa denominata EternalBlue da parte dell'NSA[23] statunitense, la quale fu smascherata e resa di pubblico dominio dal gruppo di *hacker* noto come "Shadow Brokers". A tal seguito, Microsoft ha sviluppato una *patch* di sicurezza per la tutela dei computer esposti ad EternalBlue e, di conseguenza, a WannaCry. Tuttavia, imprese e singoli individui non avendo scaricato l'aggiornamento necessario, sono rimasti esposti al rischio cibernetico ed alle conseguenti richieste del pagamento di cifre tra i 300 ed i 600 dollari in Bitcoin entro tre giorni, altrimenti i dati in ostaggio sarebbero stati cancellati in modo irreversibile. A tal proposito alcuni analisti ritengono che nessuna delle informazioni impropriamente acquisite sia stata restituita al legittimo proprietario, altri, tra cui la società di *cybersecurity* F-secure, ritengono che parte degli utenti ne abbia ripreso possesso. Ciò che rileva è che WannaCry ha apportato danni per circa 230000 dispositivi collocati in 150 paesi diversi causando, a livello complessivo, perdite per 4 miliardi di dollari e coinvolgendo attività di ogni genere, tra le quali la società di telefonia mobile Telefonica ed addirittura un terzo dei complessi ospedalieri britannici facenti capo al National Health Service. Ulteriore dato preoccupante all'epoca era rappresentato dal fatto che un anno dopo questo catastrofico attacco *ransomware* il 97% delle aziende era ancora vulnerabile esattamente come prima. Inoltre, gli Stati Uniti d'America, dopo aver pubblicamente accusato la Corea del nord per il drammatico evento in analisi, malgrado la Corea rinneghi ancora oggi la propria responsabilità, hanno identificato Park Jin Hyok come artefice di WannaCry tramite un documento di ben 179 pagine prodotto dal dipartimento di giustizia degli USA, paese storicamente impegnato nella lotta al crimine di natura informatica e capace di individuare nella fattispecie in esame una connessione server proveniente da una gamma di indirizzi IP tipicamente

[23] NSA sta per National Security Agency ed è un organismo del Dipartimento della difesa degli Sati Uniti d'America. Nello specifico tale ente si occupa della sicurezza all'interno ed all'esterno del paese tramite il monitoraggio e la raccolta di informazioni, la protezione di comunicazioni degli enti governativi degli Stati Uniti e la tutela di messaggi riservati alle ambasciate statunitensi ed al governo.

appartenenti alla Corea del Nord ed al gruppo di *cyberspionaggio* Lazarus, operante nell'interesse del paese appena menzionato.

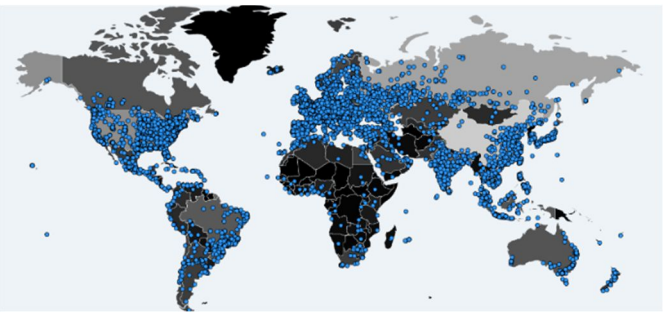


Figura 9: la schermata in cui WannaCry richiede il riscatto[24] *Figura 10: l'incredibile estensione di Mannari*[25]

In epoca moderna si è giunti a parlare persino di *cyber warfare*, anche nota come guerra informatica, la quale risulta essere frutto di una trasfigurazione dello scontro armato frutto delle trasformazioni tecnologiche, culturali e sociali degli ultimi decenni. In tale ottica il conflitto si sviluppa su un campo di battaglia inedito quale la rete, dove i soldati risultano impersonificati da *hacker* che impiegano strumenti informatici in costante aggiornamento per finalità economiche, politiche e sociali. Tale fenomeno ha origine nel periodo tra gli anni Sessanta e settanta del Novecento, dunque in piena Guerra Fredda, anni nei quali le popolazioni dell'intero globo entravano a contatto con l'era digitale. Inoltre risulta rilevante distinguere il concetto di *cyber warfare* dalla *cyberwar*, in quanto la prima riguarda iniziative strategiche condotte da professionisti dell'informatica per conto di particolari nazioni al fine di danneggiare singole entità governative, mentre la seconda è inerente ad attività di *cybercrime* che presentano effetti su un contesto più ampio, cagionando danno non soltanto ad organizzazioni e Stati, ma anche ai singoli individui, pertanto implicando scenari ben più catastrofici. In aggiunta a quanto detto, risulta opportuno specificare come tali attacchi non siano soltanto iniziativa da parte di determinati paesi, ma possono anche essere promossi da organizzazioni terroristiche o gruppi di criminali informatici intenzionati a difendere gli interessi di uno Stato ostile.

La complessità della guerra cibernetica si evince dalla poliedricità dei possibili attacchi

[24] Fonte: Cybersecurity Italia, 22 Maggio 2017, "WannaCry. Ecco la scheda tecnica completa sul micidiale ransomware"
[25] Fonte: The Two-Way: NPR, 15 Maggio 2017, "WannaCry Ransomware: What We Know Monday"

ad essa associati, uno su tutti lo spionaggio, finalizzato all'acquisizione di informazioni particolarmente delicate e generalmente non di dominio pubblico in modo tale da poter manipolare gli utenti della rete minacciata. Ulteriore casistica piuttosto frequente è quella del sabotaggio, il quale ha la potenzialità di far vacillare l'esistenza stessa di un intero Stato in seguito alla sottrazione di dati, poi eliminati o utilizzati per danneggiare l'obiettivo, forniti da vulnerabilità di natura umana quali *insider threats*, ovvero dipendenti scontenti o negligenti, o infiltrati all'interno del paese obiettivo. Infine, negli ultimi anni ha acquisito una certa rilevanza la finalità di propaganda, perseguita direzionando e manipolando la percezione, in modo particolare in ambito politico, che gli individui hanno nei riguardi dello Stato sotto attacco, il quale risulta generalmente leso o privato della fiducia popolare in seguito alla diffusione di informazioni sensibili o vere e proprie menzogne.
Uno dei casi di *cyber* warfare di maggiore notorietà è sicuramente quello perpetuato ai danni di Sony Pictures in seguito all'uscita del film "The Interview", il quale forniva una rappresentazione piuttosto critica del leader politico nordcoreano Kim Jong-un. Per tale motivazione, secondo quanto testimoniato dall'FBI, il governo della Corea del Nord avrebbe programmato un *cyber attack* ai danni dell'ente cinematografico. Secondo quanto riportato le responsabilità sarebbero state attribuite tramite l'individuazione di somiglianze con attacchi plurimi da parte dello stesso governo nordcoreano, tra cui l'impego della crittografia, la cancellazione di dati sensibili e l'impiego di particolari codici.

1.3 Le tipologie di cybercrime

Al giorno d'oggi il *cybercrime* è un fenomeno di una tale estensione da includere in sé una moltitudine di categorie differenti, entro le quali poter individuare peculiarità singolari e caratteristiche specifiche. La prima di esse, nonché una delle più generiche e frequenti, è certamente il *malware*, che può essere identificato come *software* capace di cagionare danno ad un dispositivo penetrando nello stesso in modo illecito e silente. Non sorprende in tal senso il fato che molto spesso la vittima dell'attacco non sia neppure in grado di realizzare di essere oggetto di un crimine cibernetico. In questo modo l'*hacker* è in grado di appropriarsi di informazioni da criptare o diffondere al fine di apportare danni o malfunzionamenti ad un intero sistema ed agli apparecchi ad esso connessi. Ulteriore fine ultimo associato al *malware* è la richiesta di ingenti somme di

denaro per il riscatto dei dati sottratti alla vittima, il cui accesso ad informazioni teoricamente private risulta compromesso.

In seguito è doveroso descrivere una particolare tipologia di *malware*, definita *ransomware*, il quale limita o impedisce completamente l'accesso ai sistemi infettati, il cui ripristino alla situazione antecedente all'attacco avviene in cambio di una somma di denaro in genere non particolarmente elevata al fine di indurre la vittima al riscatto. Si registrano due tipologie di *ransomware*: i *crypto ransomware*, capaci di crittografare file rendendoli inutilizzabili; i *locker ransomware*, che si limitano a rendere inaccessibile il dispositivo avvisando la vittima con una schermata di blocco. Tale categoria di attacco informatico si presenta come una delle più diffuse e dannose per le organizzazioni. Non sorprende dunque che il rapporto intitolato "State of the Phish 2023" stilato da Proofpoint[26] abbia rilevato che il 64% delle organizzazioni intervistate ha testimoniato di essere stata colpita da *ransomware* nell'anno antecedente e che di tali aziende ben due su tre siano state danneggiate più volte. In più, a giudizio di molteplici esperti i numeri effettivi di casi sarebbero ben maggiori di quanto illustrato. In tale ottica tra i settori più colpiti spiccano la sanità, con un tasso di pagamento dei riscatti dell'85%, e le istituzioni scolastiche.

Addizionale frode informatica di particolare rilevanza è certamente il *phishing*, il quale prevede la sottrazione di informazioni personali all'utente tramite la diffusione di *e-mail* apparentemente attendibili che inducono il singolo all'inganno spingendolo a fornire dati sensibili. Tale categoria di attacco informatico impiega le tecniche di *social engineering* al fine di raggirare persone ed imprese per acquisirne dati individuali. Il *phishing* risulta altamente impiegato in quanto semplice, economico ed efficace. Infatti, raccogliere numerosi indirizzi *mail* richiede uno sforzo minimo ed allo stesso tempo contattare quest'ultimi risulta un'operazione sostanzialmente priva di costo. Dunque, dal punto di vista dei criminali informatici un'iniziativa del genere è chiaramente di estrema convenienza in quanto consente potenzialmente il furto d'identità a costo zero. Il citato concetto di identità si estende da elementi di identificazione personale, come numeri di carte di credito o tessere sanitarie, sino a componenti aziendali private, tra cui contatti dei clienti o *know-how* dei prodotti e delle tecnologie impiegate. Pertanto,

[26] Proofpoint è una società americana di sicurezza informatica aziendale, la quale fornisce *software* come servizi e prodotti per la sicurezza di e-mail, la difesa da minacce a dati personali, prevenzione dalla perdita di dati ed informazioni riguardanti il modo elettronico.

questa particolare di rischio cibernetico permette agli *hacker* di penetrare all'interno di specifiche infrastrutture aziendali per poi perpetuarsi ad interi settori.
Per quanto concerne lo *spamming*, esso è caratterizzato dall'invio indiscriminato e sostanzioso di messaggi di posta elettronica al netto del consenso del destinatario, il quale ritrova al proprio indirizzo contenuti di pubblicità o inviti ad iscrizioni e servizi da parte di indirizzi generici non verificati o sconosciuti. Molteplici sondaggi testimoniano come attualmente lo *spam* sia considerato dalla maggioranza degli utenti uno degli elementi di Internet maggiormente tediosi. Non a caso tale fenomeno è perseguito dagli *Internet Service Provider* anche per i costi del traffico conseguenti all'invio indiscriminato e l'impiego di identità anagrafiche false o rubate. Per concludere lo *spamming* è oggetto di molteplici dibattiti di giurisprudenza inerenti alle fattispecie secondo le quali esso si configura come reato o semplice illecito, definizione che spesso dipende dal sistema legislativo di riferimento. Ad esempio in Italia l'invio di messaggi non sollecitati è semplicemente soggetto a sanzioni.
A tal punto è opportuno illustrare un'ulteriore rilevante categoria di crimine informatico: l'attacco DDoS, ovvero Distributed Denial of Service, il quale ha come fine ultimo l'inutilizzabilità di un servizio online, i cui server risultano sovraccaricati da una quantità di traffico dalle molteplici fonti tale da generare il collasso della rete e la conseguente incursione nel sistema da parte dell'*hacker*. L'attacco DDoS può essere indirizzato: al livello applicativo, nel caso in cui punti a minimizzare le risorse della vittima comportando l'interruzione dei servizi minando il livello al quale le pagine Web vengono prodotte dal server in risposta ad una specifica *query* dell'utente; al protocollo, quando comportano l'interruzione di servizio a causa di un consumo eccessivo di risorse del server o delle apparecchiature di rete; al volume, amplificando il traffico con l'obiettivo generare un intralcio consumando l'intera larghezza di banda tra Internet e la vittima.
Gli attacchi DDoS per essere ultimati molto spesso si servono di *botnet*, cioè reti di computer manipolate dai cyberciminali da remoto per diffondere *spam*, monitorare l'attività degli utenti o analizzare dati di sistema. Il controllo da parte degli *hacker* risulta essere esercitato in seguito all'installazione sugli apparecchi dei bersagli di un *malware*, che rende il macchinario colpito soggetto ai comandi di attivazione dell'attaccante.

In aggiunta a quanto precedentemente riportato, è possibile fornire una distinzione del *cybercrime* orientata dall'oggetto dello stesso. Secondo tale prospettiva, la prima categoria individuabile è quella dell'attacco alla proprietà, il quale permette l'accesso a dati strettamente personali, correlati al patrimonio dell'utente, al fine di utilizzare il conto corrente del bersaglio, ultimare truffe consistenti o ultimare acquisti online. Altrettanto rischioso è certamente il crimine cibernetico ai danni della sfera individuale, ponendo in bilico la sicurezza informatica e reputazionale di singoli individui tramite la diffusione di materiale privato o diffamatorio come materiale pornografico o elementi da stalking informatico. L'ultima specie di *cybercrime* secondo l'ottica citata è il rischio *cyber* cui risulta sottoposto lo Stato, le cui potenzialità sono estreme, tali da indurre a parlare di *cyber* terrorismo. Quest'ultimo espone istituzioni governative, enti statali e persino le forze dell'ordine alla fuga di informazioni utilizzabili in termini denigratori o da cedere a paesi nemici. Inoltre, è possibile riconoscere come il fine ultimo del *cybercime* possa essere diversificato. In tal senso mirato in primo luogo alla minaccia nei confronti della confidenzialità e della *privacy* delle comunicazioni online in modo da acquisire dati personali, aziendali o di natura finanziaria. In seconda battuta la falsificazione delle informazioni consistenti in documentazioni non autentiche o registrazioni digitali ingannevoli. In seguito, l'obiettivo dei cybercriminali può consistere in frodi informatiche, volte all'inganno, alla manipolazione o alla richiesta di un riscatto. In ultima fascia, la compromissione di interi sistemi informatici, minando la fiducia nei confronti degli stessi o compromettendone l'integrità.

2. La cybersecurity

La crescita esponenziale negli ultimi decenni del fenomeno del *cybercrime* ha indotto gli esperti del settore a richiedere maggiori investimenti nell'ambito della *cybersecurity*, intesa come branca della sicurezza informatica. Quest'ultima concerne conoscenze, tecnologie e procedure finalizzate alla tutela della disponibilità, confidenzialità ed integrità delle componenti informatiche. Nello specifico, invece, la *cybersicurezza* è incentrata rispetto alla resilienza, robustezza e reattività di una specifica tecnologia, capace pertanto di respingere attacchi incentrati sul comprometterne il regolare funzionamento. Dunque, l'obiettivo primario risulta, senza ombra di dubbio, la salvaguardia dell'informazione in quanto elemento pivotale del complesso sistema informatico essendo motivo della sua esistenza, dalla progettazione allo sviluppo

passando per la manutenzione. In tal senso è imprescindibile garantirne la riservatezza, cioè la capacità di monitorare il soggetto, la tempistica e le modalità di accesso ai dati, i quali è necessario che si presentino autentici, ovvero inalterati al netto di autorizzazioni, e reperibili su richiesta in tempi adeguati ai soggetti che ne hanno diritto. Quanto appena esposto rientra nella definizione internazionale di CIA factors, il cui equivalente in lingua italiano sono i parametri RID, ovvero le precedentemente citate confidenzialità, integrità e disponibilità necessarie alla custodia dell'informazione. Quest'ultima non necessita esclusivamente del fattore tecnologico, dunque delle risorse che costituiscono il complesso informatico, ma anche di un'affidabile componente umana, ovvero la preparazione e competenza dei singoli individui spesso individuati come l'elemento della sicurezza informatica maggiormente imprevedibile. Per tale ragione è possibile evincere che la *cybersecurity* implica effettivamente in primo luogo la protezione del dato, ma implicitamente induce a preservare l'utente, meglio noto come *end point*, essendone il principale utilizzatore, nonché possibile bersaglio del rischio cibernetico.

Inoltre le iniziative di reazione al *cyber risk* risultano essere cangianti essendo generalmente di natura preventiva, quindi mirate al minimizzare la probabilità o l'eventuale effetto dell'attacco informatico, bensì potendosi rivelare di carattere assicurativo, pertanto volte alla copertura economica del potenziale danno, sino all'accettazione del rischio al netto di interventi di ridimensionamento del rischio.

In modo specifico nel contesto aziendale la *cybersicurezza* assume un valore assolutamente estremo in quanto in un mondo globalmente interconnesso come quello odierno anche il minimo rallentamento del *core business* può generare ingenti perdite in termini economici e di efficienza, alleviando la produttività di interi sistemi produttivi e pertanto cagionando danno non soltanto alle imprese, ma anche alla rispettiva clientela. Quest'ultima, in aggiunta a quanto illustrato, è probabile risulti vittima di *data breach*, ovvero fuga di dati, così come le aziende dalle quali acquistano prodotti e servizi, le quali si espongono pertanto da un lato ad un collasso delle vendite e dall'altro alla dispersione di progetti finanziati o delicate informazioni fiscali, sintomo di perdita di ulteriore concorrenzialità rispetto ai propri *competitor*. Per tale motivazione essere frequente bersaglio di attacchi informatici espone intere attività ad una seria e difficilmente retroattiva problematica di reputazione, essendo l'inefficacia del sistema di

sicurezza digitale, ove esistente, sintomo di inaffidabilità e, di conseguenza, ragione di perdita di clientela e difficoltà nell'individuazione di nuovi acquirenti. Per le ragioni indicate, in epoca moderna, più di ogni altro periodo storico, la necessità di sistemi di sicurezza informatica per il monitoraggio proattivo del panorama digitale è imprescindibile per salvaguardare il proprio lavoro, la propria privacy e quella dei soggetti con i quali si interagisce, anche sporadicamente, e, eventualmente, intervenire in maniera tempestiva nel caso vi sia l'insorgenza di plausibili rischi di natura cibernetica. In tale ottica si configura come essenziale un'efficace *governance* delle risorse nella propria disponibilità garantendo in maniera simultanea l'implementazione del Sistema di Gestione della sicurezza informatica, inerente al complesso di iniziative utili alla tutela delle piattaforme impiegate.

2.1 Origini ed avanzamento della cybersecurity

Innanzitutto, è doveroso considerare come la *cybersecurity* sia un'innovazione piuttosto recente essendo stata ideata nel corso del ventesimo secolo. Malgrado ciò, è possibile individuare una moltitudine di processi evolutivi ad essa correlati sino a giungere alla definizione del complesso di strumenti e strategie dal valore di 2.15 miliardi di euro nel 2023, secondo quanto riportato dall'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano.

In primo luogo, si segnala come negli anni '50 la violazione di un dispositivo elettronico, connesso ad un proprio omologo tramite le prime reti, implicava un accesso fisico a quest'ultimo per tale motivazione comportando un crimine non correlato allo spionaggio cibernetico, bensì più vicino ad un'infrazione della proprietà privata. In seguito alla nascita di Internet nel 1960 mediante il sistema di reti di ARPA[27], funzionale alla comunicazione tramite computer su grandi distanze, si delinea la definizione del *cyberpazio*, entro il quale inizia a sostanziarsi l'idiosincrasia tra le prime tipologie di *malware* e, di conseguenza, le corrispettive misure di cautela per la protezione dei dati. Nel corso di tale periodo, non a caso, è possibile annoverare lo sviluppo del primo vero *software* di sicurezza, noto come Reaper. Quest'ultimo, ideato

[27] ARPA, acronimo di Advanced Research Project Agency, è stata una divisione di ricerca nell'ambito tecnologico del dipartimento della Difesa degli Stati Uniti. Tale ente è noto per l'invio di un messaggio dall'Università della California a Los Angeles all'indirizzo di un macchinario collocato dall'altra parte dello Stato, appartenente allo Stanford Research Institute. Tale evento corrisponde a giudizio di numerosi esperti alla nascita di Internet

dall'inventore dell'*e-mail* Ray Tomlinson, era capace di individuare e rimuovere il virus maggiormente diffuso all'epoca, ovvero il programma Creeper in grado di operare indipendentemente dall'essere umano diffondendosi tramite il passaggio da un dispositivo all'altro.

Nel corso degli anni successivi un utilizzo gradualmente più evoluto di ARPAnet ebbe come effetto il deposito di una mole rilevante di informazioni private e governative all'interno di macchinari connessi ad Internet, ragione per la quale il governo degli Stati Uniti avviò il finanziamento di progetti finalizzati al ridurre gli accessi impropri ed illeciti a dati sensibili, introducendo l'iniziativa Protection Analysis, monitorata da ARPA e mirata all'individuazione di misure di sicurezza automatizzate mediante il coinvolgimento di numerose grandi aziende impegnate nella fornitura di computer, chip e sistemi operativi. Ulteriore investimento in tale ambito fu realizzato da alcuni ricercatori di IBM[28] , supportati da esponenti della NASA, fu il Data Encryption Standard, ovvero un protocollo di crittografia funzionale, al punto da essere impiegato persino dall'NSA, ideato per la tutela di informazioni archiviate o trasmesse tramite rete.

Le fondamenta di *cybersicurezza* penetrano definitivamente nell'immaginario popolare nel corso degli anni '80, nel corso dei quali gli emittenti giornalistici e televisivi iniziano a diffondere con frequenza sempre maggiore notizie riguardanti crimini informatici ai danni di note istituzioni, sino a giungere al successo cinematografico del film WarGames- Giochi di Guerra, riguardante la storia di un *hacker* capace di accedere ai sistemi di controllo delle bombe atomiche. In tal modo il mercato della sicurezza informatica ebbe un ampliamento sostanziale che portò alla commercializzazione globale dei primi antivirus e di applicazioni sviluppate da esperti del settore, consacrando la *cybersecurity* moderna. Quest'ultima induce molteplici individui ad ambire all'utilizzo di Intenet non esclusivamente per ragioni lavorative o belliche, ma anche per finalità formative o ludiche. Per tale motivazione compagnie come Microsoft iniziarono ad offrire versioni dei propri sistemi operativi, tra cui Windows, maggiormente incentrate sulle necessità dei singoli consumatori, così come le offerte sul

[28] IBM, che sta per International Business Machines, è una società informatica degli Stati Uniti ed è nota come uno dei pionieri di tale settore. Ad oggi è attiva in oltre 130 paesi in tutto il mondo producendo macchinari da ufficio, impegnandosi nello sviluppo di *software* per l'elaborazione dati e nella ricerca e consulenza informatica.

mercato per l'acquisto di dispositivi tecnologici divenne ben più accessibile in termini economici, generando in modo direttamente proporzionale l'incremento di rischi di natura cibernetica appartenenti al novero del *social engineering*, relativo allo sfruttamento delle vulnerabilità umane non sufficientemente tutelate dai sistemi di *cybersecurity* dell'epoca. Pertanto la moltitudine di crimini informatici aventi ad oggetto la negligenza umana estese ulteriormente la consapevolezza della necessità di solide forme di cautela per l'informazione privata sino a rendere la difesa dai *cybercriminali* una questione di sicurezza personale e nazionale, come testimoniato dalla scelta del governo americano di ideare la National Cyber Security Division, sezione del Dipartimento di Sicurezza Interna degli Stati Uniti d'America pienamente dedita al tema della sicurezza informatica. Successivamente la diffusione di *smartphone* e *social network*, esponendo gli utenti più di ogni altro periodo antecedente, comportò la diffusione delle prime VPN, ossia reti private virtuali utili alla crittografia di dati ricevuti e trasmessi online, nonché sistemi di sicurezza digitale basati su *cloud*[29], diffusi da aziende quali Panda Security[30] e McAfee[31] ed utilissimi in quanto permettevano di sorvolare la problematica dello spazio occupato da applicazioni su dispositivi dalla memoria al tempo piuttosto limitata. L'impiego di tali sistemi di protezione fu in seguito incentivato dalle casistiche di spionaggio ai danni di potenze economiche e militari mondiali come l'Iran e dalla maggiore considerazione della tematica *privacy online*, essendo divenute di dominio pubblico nei primi anni del 2000 l'utilizzo da parte di piattaforme come Google e Facebook di rilevanti quantità di dati personali, impiegati per personalizzare offerte pubblicitarie o semplicemente vendute per la monetizzazione delle stesse. La relazione tra *privacy* e sicurezza informatica è stata oggetto di ulteriore legittimazione nel corso della pandemia, durante la quale l'espansione del fenomeno *smart working*, dell'*e-commerce* o di annunci correlati alla diffusione del virus hanno alimentato in maniera sostanziale le potenzialità dei crimini informatici portando

[29] Il *cloud* è un sistema costituito da *software* dei computer dell'intero globo e delle relative risorse di elaborazione accessibili tramite Internet da qualsiasi luogo senza dover utilizzare obbligatoriamente un particolare dispositivo, potendo utilizzare i propri dati o applicazioni liberamente quando e dove si vuole.
[30] Panda Security è un'azienda statunitense di sicurezza informatica, capace di ideare l'antivirus autonomo Panda, utile alla protezione del proprio PC anche senza connessione Internet una volta installato e capace di aggiornarsi automaticamente.
[31] McAfee è un'azienda americana impegnata nell'ambito della sicurezza informatica, impegnata nello sviluppo di sistemi capaci di analizzare i siti nei quali si naviga e di segnalare all'utente eventuali rischi e di sistemi antivirus particolarmente all'avanguardia.

quest'ultimi ad essere persino il mezzo di aggressione da parte di potenze internazionali quali la Russia nei confronti di paesi ostili. Quanto appena detto è attestato dall' iniziativa di *hacker* russi ai danni prima dell'azienda americana di trasporto carburante Colonial Pipeline, capace di far schizzare il prezzo della benzina alle stelle, e poi nei confronti dell'Ucraina, tramite messaggi intimidatori inerenti all'imminente guerra su piattaforme governative. Dunque una coalizione di Stati europei, capitanati dalla Lituania, ha investito nella promozione del Cyber Rapid Response Team, costituito da esperti di *cybersicurezza* per la collaborazione con l'Ucraina al fine di tutelare tale paese da ulteriori minacce di natura cibernetica.

L'intera storia della *cybersecurity* può essere ricondotta all'individuazione fondamentalmente di tre periodi, primo dei quali il controllo degli accessi, caratterizzato dall'impedimento all'acquisizione di informazioni private presenti all'interno dei dispositivi, i quali dopo essere stati integralmente connessi alla rete e, pertanto, ad Internet hanno comportato la diffusione di modelli di rilevamento di virus mirando a limare le vulnerabilità delle piattaforme digitali e rafforzare le infrastrutture aziendali nell'era del rilevamento, poi superata dall'epoca delle persone, nel corso della quale è sorto il *cloud*, che ha sorvolato limiti fisici da proteggere ed ha spinto i *cybercriminali* ad avere come bersaglio singoli individui mediante programmi di *social engineering.*

2.2 Le discipline di cybersecurity

La *cybersicurezza* riguarda in maniera diretta una moltitudine di specifiche discipline dalle peculiari caratteristiche ad essa riconducibili, essendo tale ambito complesso ed in continua evoluzione. In primo luogo, tra queste, spicca la sicurezza della rete, dove si verificano gran parte dei crimini informatici per finalità differenti, tra cui il furto d'identità o l'acquisizione impropria di dati, rispetto a cui divengono imprescindibili misure di tutela come l'Identity Access Management o il Data Loss Prevention. Quest'ultimo è uno strumento di estrema rilevanza per la protezione di dati sensibili entro la rete aziendale, la quale risulta spesso varcata intenzionalmente o accidentalmente dai dipendenti. L'altro, invece, acquisisce utilità nell'identificare i soggetti che utilizzano particolari applicazioni o visualizzano dati specifici, in modo tale da poter riconoscere eventuali accessi illegittimi. Inoltre la sicurezza di rete si estrinseca su un triplice piano: fisico, al fine di garantire fisicamente l'utilizzo di particolari elementi della rete come i *router* esclusivamente ai soggetti autorizzati; tecnico,

salvaguardando le informazioni transitanti o memorizzate sul *network*; amministrativo, tramite il quale è possibile monitorare l'operato dei vari utenti

In seguito è doveroso menzionare un ulteriore rilevante contesto quale il *cloud security*, di fondamentale rilevanza nel vigilare non soltanto su *asset* aziendali archiviati nel *cloud,* ma anche nell'interesse di tutti i soggetti che interagiscono con quest'ultimo, considerandone provenienza, tipologia e settore d'iniziativa. In aggiunta a quanto appena descritto, è doveroso riportare che, come definito all'interno del modello di responsabilità condivisa[32], i *Cloud Service Provider* si occupano della tutela fisica delle infrastrutture, mentre i clienti ed il reparto IT delle imprese gestiscono i criteri di sicurezza, gli accessi e le informazioni contenute nella nuvola, il cui efficientamento in termini di protezione risulta essenziale considerando che secondo quanto osservato da Venafi[33] l'81% delle aziende nel corso del 2023 è stata vittima di problematiche di sicurezza inerenti al *cloud* ed il 45% ha denunziato di averne subite addirittura quattro o più.

Successivamente è opportuno analizzare il fenomeno dell'*endpoint security*, il quale riguarda la protezione dei dispositivi utilizzati dal singolo individuo, comunemente definito come utente finale, tramite vigilanza inerente alla rete, sistemi di *threat prevention* avanzati quali l'*anti-phishing* o l'*anti-ransomware* e tecnologie di informazione forense come l'Endpoint Detection and Response. La tutela dell'utente finale risulta essere estremamente rilevante per le aziende, essendone spesso una delle principali vulnerabilità a causa della complicata gestione ad esso inerente. Tra i principali strumenti di *endpoint security* è possibile citare Bitfender GravityZone, applicazione di salvaguardia completa per il fruitore di macchinari tecnologici caratterizzato da un sistema di rilevamento comportamentale come utile sistema di precauzione, o ESET Endpoint Security, il quale si presenta come mezzo di protezione multilivello che impiega il *cloud* associando l'apprendimento automatico all'intelligenza collettiva al fine di prevenire *malware* e *ransomware*.

Per quanto concerne la *mobile security*, quest'ultima è riconducibile ad oggetti come

[32] Il modello di responsabilità condivisa riguarda in maniera specifica le responsabilità per quanto concerne la sicurezza di *provider* e clienti *cloud*, le quali dipendono dalle caratteristiche del servizio *cloud* utilizzato.

[33] Venafi è una compagnia di sicurezza informatica privata impegnata nello sviluppo di *software* finalizzati alla salvaguardia di chiavi crittografiche e certificati digitali. Tale azienda di fama mondiale è inoltre impegnata nella prevenzione di rischi cibernetici.

smartphone, laptop e tablet utilizzati non soltanto per scopi personali, ma spesso veicolo di preziosi dati societari, che hanno orientato il *cybercrimine* ad impiegare in tale contesto pericolose componenti quali *phishing* o attacchi *Instant Messaging.* Eventi di rilievo quali l'espansione della pandemia e la conseguente affermazione dello *smart working* hanno fatto incrementare notevolmente i rischi connessi a tale ambito, costituito da macchinari non collegati ad una singola rete aziendale come i sistemi *deskt*op*,* bensì dinamici e, di conseguenza, esposti anche al rischio di smarrimento. Quest'ultimo comporta la possibilità ad eventuali autori del furto di un dispositivo di porre in essere iniziative di *brute-force*; dunque, cercando di individuare la *password* della schermata di blocco per avere accesso ai contenuti dell'apparecchio, i quali grazie a determinate applicazioni vengono distrutti o risultano non trasferibili in seguito ad una moltitudine di tentativi di accesso falliti. Ulteriore minaccia di particolare rilevanza è rappresentata dall'installazione di applicazioni di terze parti su dispositivi personali oggetto del fenomeno di *rooting*, attraverso cui gli *hacker* hanno modo di alterare interi sistemi operativi, appropriandosi illecitamente di informazioni private. In conclusione risultano dotati di particolare rischiosità i dispositivi Bring Your Own Device, tramite i quali penetrare all'interno del complesso di macchinari collegati ad una particolare rete al fine di sfruttarne le vulnerabilità potendosi sostanziare un furto di identità oppure un attacco *man in the middle*[34].

Altra disciplina di particolare importanza nel novero della *cybersicurezza* è certamente l'*Internet of Things Security*, riguardante tecnologie collegate al *cloud*, raramente dotate di sistemi di tutela all'avanguardia, tra cui oggetti di impiego quotidiano quali frigoriferi o televisori, ma anche numerosi apparecchi aziendali. Tali strumenti essendo caratterizzati da un sistema operativo distinto rispetto a quello dei dispositivi mobili, implicano ulteriori problematiche oltre alla dispersione di dati ed alla tutela della piattaforma di archivio, come ad esempio l'autenticazione degli utenti, la crittografia dei dati trasmessi nel *cloud* o la necessità di aggiornamenti. Tale tipologia di sicurezza, non essendo dotata di modelli standard, dipende interamente dalla preparazione degli individui che li utilizzano e di coloro i quali li collocano sul mercato.

Ulteriore disciplina meritevole di menzione è certamente la sicurezza delle applicazioni,

[34] L'attacco *man in the middle* è una tipologia di iniziativa che consente al criminale informatico di intercettare la trasmissione di informazioni sulla rete tra due soggetti e ne implica dunque la capacità di alterare i contenuti a seconda dei propri interessi.

inerente alle molteplici fasi di progettazione, sviluppo e distribuzione entro le quali DataDog[35] ha individuato dati preoccupanti, tra cui l'esposizione ad attacchi informatici del 74% delle informazioni di identificazione personale, mentre per il 70% delle applicazioni la mancanza di una tra la protezione WAF e la connessione HTTPS. Quest'ultima sta per Hypertext Transfer Protocol Secure, ovvero il sistema di comunicazione crittografata tra utenti, *browser* e *server* utile a garantire ai fruitori della rete l'affidabilità ed autenticità di siti *web*, oltre alla riservatezza dei dati trasmessi. Il traffico HTTP è sorvegliato tramite WAF, acronimo di Web Application Firewall, strumento utile al fine di scannerizzare ed analizzare i dati che migrano da una rete locale ad una globale o di dimensioni maggiormente rilevanti.
Per concludere, si analizza il modello di sicurezza Zero Trust, fondato sulla necessità di verificare sempre in maniera oculata l'attendibilità di sistemi informatici, persino nel caso in cui quest'ultima sia precedentemente stata certificata. Per tale motivazione esso è caratterizzato da un approccio granulare consistente in minuziose fasi quali la micro-segmentazione, lo *screening* costante ed il monitoraggio assiduo degli accessi, tutelando informazioni delicate, *endpoint* ed infrastrutture. Una delle piattaforme di *zero trust* di maggior rilievo è Zero Trust Exchange, correlata al *cloud* ed attiva in 150 *data center* nel globo. Essa definisce la sicurezza di un sistema informatico a seconda del contesto, costituito da svariate componenti quali la collocazione dell'individuo, le informazioni trasferite ed il profilo di sicurezza del macchinario che permettono di individuarne l'eventuale fruibilità garantendo all'utente l'impiego di reti sicure e non direttamente associabili a quelle aziendali.

2.3 Prospettive future della cybersecurity

La complessità e dinamicità di un ambito articolato come quello della *cybersecurity* impongono un'aspettativa ben definita in riferimento al futuro: il relativo rinnovamento ed il progressivo incremento della variabilità. Tali prospettive risulteranno a giudizio degli esperti probabilmente colte tramite l'impiego dell'*Artificial Intelligence*, tecnologia capace di rivoluzionare l'interazione tra l'individuo e la macchina efficientando il pensiero del primo attribuendo alla seconda le capacità di apprendimento automatico dall'errore e di ragionamento tipicamente umano. Tali

[35] Data Dog è una società americana che analizza applicazioni su *cloud* analizzandone *server* e servizi tramite un sistema di analisi dati basato su Software as a Service.

qualità, associate all'estrema potenza di calcolo del macchinario, si ritiene possano rivelarsi cruciali nell'individuazione di potenziali minacce alle infrastrutture digitali mediante processi di *deep learning.* Quest'ultimo è fondato sull'apprendimento da sostanziose moli di dati, la cui ricezione e conseguente analisi consentono al dispositivo di intraprendere riflessioni analoghe a quelle pertinenti all'apparato cerebrale umano tramite il funzionamento di reti neurali artificiali costituite da moderni algoritmi. Tale sistema è capace di elaborare contemporaneamente informazioni provenienti da molteplici fonti in tempo reale ed al netto dell'intervento da parte dell'essere umano, divenendo così strumento di estrema utilità e produttività nella risoluzione di problemi decisionali sequenziali o nel perfezionamento del processo di raccolta dati. In aggiunta a quanto appena accennato, l'Intelligenza Artificiale può essere considerata come strumento "democratizzante" in quanto utile all'incremento dell'accessibilità per l'individuo e le imprese ad applicazioni di sicurezza informatica ed a nozioni ad essa relativa ampliando la conoscenza di dominio pubblico a riguardo mediante uno sforzo culturale che discenda dall'alto e riguardi indistintamente l'intera popolazione. In modo particolare, nell'ambito *business* la dottrina richiede una sostanziale integrazione tra le misure di sicurezza cibernetica e le strategie aziendali in modo tale da rendere le spese in tale contesto non soltanto semplici costi per la difesa dei propri *asset*, ma degli investimenti fruttiferi utili al mantenimento di vantaggi competitivi, alla continuità imprenditoriale ed alla realizzazione della crescita finanziaria e settoriale. In tale ottica si delinea di estrema utilità la nomina di un *Chief Informaton Security Officer* che sia capace di realizzare un *focus* strategico sulle iniziative in materia di *cybersicurezza*, comunicando in merito direttamente al Consiglio di amministrazione. A tal proposito la società di ricerca Gartner[36] riporta che entro il 2026 il 70% dei Consigli di amministrazione sarà dotato in un professionista esperto in materia di sicurezza *cyber*. Nel contesto lavorativo si ipotizza, peraltro, che l'automatizzazione coinvolgerà in maniera permeante numerosi ruoli professionali rimpiazzando professionisti della sicurezza cibernetica e portando quest'ultimi a dedicarsi maggiormente alla pianificazione strategica, sviluppando piani di azione efficienti nel rispetto delle *best*

[36] Gartner è una società per azioni americana impegnata nel settore della consulenza strategica. Inoltre, essa compie ricerche di mercato e studi specifici inerenti alle tecnologie dell'informazione. Attualmente è considerata una delle principali società a livello globale, nonché la società di analisi più grande al mondo in quanto ha fatturato e numero di analisti.

practices ed in contrasto rispetto ai più moderni modelli di crimine informatico. Secondo tale punto di vista, l'*Artificial Intelligence* avrà come effetto lo sviluppo di incarichi lavorativi inediti caratterizzati dalla produzione, gestione ed integrazione delle più moderne tecnologie al fine di rendere le aziende ed i privati estremamente più protetti da iniziative di *cybercrime*.

Secondo la prospettiva dei *cybercriminali,* il progresso incessante della tecnologia lascia presupporre un altro scenario piuttosto curioso, costituito dalla de-responsabilizzazione rispetto alle iniziative criminali di intere compagini, nazionali o meno. Tale espressione indica la difficoltà nell'individuazione di chiari indici di colpevolezza nel caso di illeciti informatici e, di conseguenza, una riduzione del rischio di esposizione da parte degli *hacker*, capaci di danneggiare in maniera non retroattiva intere nazioni con conseguenze catastrofiche al netto di severe sanzioni. Per tale motivazione si auspica che lo sviluppo di misure di cautela adeguate viaggi ad un ritmo maggiormente consolidato in modo da garantire la tutela dei complessi digitali. Tale speranza è suffragata dalla considerazione del fatto che il valore dei dati acquisibili tramite iniziative illecite è in crescita a partire dal periodo caratterizzato dalla pandemia, durante il quale imprese e governi si sono rivelate sempre più dipendenti da piattaforme informatiche, archiviando *online* moli di dati massicce utilizzate dagli *hacker* per manipolare il pensiero pubblico riguardo questioni politiche oppure richiedere ingenti riscatti in denaro per la restituzione delle informazioni impropriamente ottenute. Inoltre la crescente accessibilità di mezzi di spionaggio informatico ha permesso anche a soggetti meno specializzati nel contesto della criminalità informatica di realizzare pericolose minacce *cyber* come ad esempio *malware* creati dall'Intelligenza Artificiale o automatizzare il processo di individuazione e sfruttamento delle vulnerabilità di particolari obiettivi.

Ulteriore tematica che si prospetta di estrema importanza in ottica futura è l'informatica quantistica, disciplina in assoluta ascesa in epoca moderna, il cui funzionamento è basato sull'utilizzo di *qubit,* ovvero unità base del calcolo quantistico utile all'analisi di enormi quantità di informazioni per la definizione di soluzioni efficienti ed innovative basate su una notevole potenza di calcolo. Il fenomeno della sovrapposizione quantistica permette a tali elementi di essere presenti in più stati simultaneamente generando capacità elaborative senza precedenti. In tal modo questo strumento si denota potenzialmente di particolare importanza nell'aggiornamento dei moderni sistemi di

cybersecurity potendo implementare programmi di crittografia, algoritmi per l'identificazione di rischi cibernetici e metodologie di *management* delle tecnologie su larga scala. In parallelo è doveroso segnalare come l'impiego nella quotidianità di tali strumenti necessiti dell'aggiornamento dei protocolli di sicurezza informatica, così come di sistemi di crittografia post-quantistica che siano in grado di neutralizzare eventuali tentativi di sfruttamento delle vulnerabilità attualmente esistenti.
In modo particolare gli scenari prossimi della *cybersicurezza* appaiono caratterizzati da un'ascesa sempre più consolidata del fenomeno definito come Zero Trust Security, analizzato in fase antecedente e sostanzialmente caratterizzato da un approccio di minima confidenzialità rispetto all'attendibilità delle infrastrutture informatiche, rispetto alle quali ci si attende un comportamento di dettagliata ispezione ed indagine. Tale condizione è dettata da un ampliamento delle metodologie secondo le quali i criminali informatici sono in grado di insidiarsi all'interno di computer o altro genere di macchinari, per tale motivazione oculatamente ispezionati tramite sistemi di autenticazione degli utenti, osservazione degli *endpoint* ed un perseverante monitoraggio delle attività in rete. In tal senso si intende realizzare un costante filtraggio delle singole operazioni che avvengono a prescindere dalla rispettiva provenienza o rete di riferimento, in modo da poter realizzare un controllo pressoché totale delle vulnerabilità e dei sistemi di tutela dei complessi digitali con a consapevolezza dell'imprevedibilità ed avanguardia *dei* moderni metodi di attacco. La speranza di un ecosistema digitale più solido e resiliente dipende, tra tanti aspetti, anche dal consolidamento delle conoscenze in materia di *cybersecurity,* il quale risulta perseguito da istituti scolastici ed universitari tramite il finanziamento di svariate iniziative, tra le quali corsi di aggiornamento, interi programmi di studio e preziosi seminari. In più recentemente hanno acquisito estrema rilevanza i progetti collaterali tra enti di formazione ed aziende del settore con il preciso intento di attribuire maggiore attenzione alla pragmaticità ed alle più recenti problematiche associate al contesto della *cybersicurezza*, settore che necessita di una maggiore numerosità e specializzazione in termini di professionisti.
Molteplici esponenti della dottrina ritengono che nel corso dei prossimi anni potrebbe assumere un ruolo pivotale per la sicurezza dei dispositivi e dei dati in essi contenuti il sistema della *blockchain*, tecnologia decentralizzata le cui peculiarità essenziali

risultano essere immutabilità, trasparenza e resistenza alla manomissione delle informazioni in essa archiviate. Tale ultima caratteristica è dovuta alla necessità del consenso della rete come forma di autorizzazione alla modifica di dati sensibili quali operazioni finanziarie o elementi di identificazione personale. A differenza dei sistemi centralizzati, la *blockchain* attribuisce maggiore indipendenza e tutela alle singole componenti dell'*Internet of Things* garantendo sostanziale sicurezza alle infrastrutture informatiche tramite l'impiego di uno strumento auto-esecutivo peculiare quale lo *smart contract*, impiegato al fine automatizzare e salvaguardare gli accordi di natura digitale in difesa delle transazioni *online.*

Infine numerosi esponenti della sicurezza informatica ritengono necessario il superamento dell'utilizzo delle *password* per accedere alle numerosissime piattaforme con le quali i singoli soggetti attualmente interagiscono, come testimoniato dall'esperta Brittany Greenfield, CEO della piattaforma Wabbi[37], secondo la quale ogni singolo utente arriva ad utilizzare sino a 40 o 50 password quotidianamente. Il dato preoccupante è rappresentato dalla constatazione del fatto che le *password* costituiscono uno strumento di sicurezza debole in quanto facilmente disperso, impiegato di frequente ed abitualmente sottratte in modo illecito. A tal proposito Microsoft stima che 150 milioni di utenti accedono a reti o applicazioni al netto dell'impiego di una password e pare che tale prospettiva possa costituire un *trend* piuttosto diffuso nel corso delle successive decadi. Ci si attende pertanto che possa sostanziarsi la progettazione di molteplici tecnologie alternative ed innovative per l'identificazione di persone e processi utilizzando nello specifico ad esempio dati biometrici, consistenti in "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici"[38].

3. Regolamentazione del rischio cibernetico

Un fenomeno in sostanziale crescita nel corso degli anni come quello della *cybersicurezza* ha necessitato di un dinamico ed aggiornato sistema di

[37] Wabbi è un'applicazione di supporto in termini di sicurezza informatica, il cui nome deriva dal concetto giapponese di *wabi-sabi*, secondo il quale l'imperfezione è vista come step per il miglioramento.
[38] Citazione ricavata dall'articolo 4, paragrafo 1, definizione numero 14 del "Regolamento europeo generale sulla protezione dei dati", anche noto come GDPR, Unione Europea, 23 maggio 2018

regolamentazione, sempre pronto ad essere modificato nell'intento di disciplinare un contesto complesso come quello in analisi. In tale prospettiva è opportuno considerare come le normative in materia di sicurezza informatica costituiscano, soltanto in primo luogo, uno strumento impiegato con l'intenzione di garantire l'affidabilità, trasferibilità e disponibilità dei dati in assoluta sicurezza. Infatti, un approccio di natura prettamente economico-finanziaria suggerirebbe una lettura del movente giuridico come una sorta di effettivo investimento da parte di attività imprenditoriali e privati, i quali mobilitano somme, spesso ingenti, di mercato al fine di dar luogo ad una precisa quadratura regolamentare. In tal modo le agenzie risultano essere esposte in prima battuta a perdite di denaro nel caso in cui i propri sistemi di tutela si rivelino non sufficientemente adeguati a salvaguardare le informazioni contenute all'interno dei dispositivi, oppure è possibile che divengano oggetto di ingenti sanzioni giustificate dalla mancanza dell'ossequio ai requisiti richiesti da regolamenti privati, nazionali o internazionali. Secondo quanto riportato dall'S&P Global Ratings[39] nello studio "Cyber risk insights: New regulations will increase resilience, at a cost" pare che nell'imminente le società saranno valutate a seconda di particolari indici di affidabilità costituiti dalla capacità di regolamentazione, conformità normativa e abilità di reazione come componenti di competitività e differenziazione rispetto ai *competitors.* Questa prospettiva identifica gli Stati Uniti d'America e l'Unione Europea come dotate di un ruolo guida nell'affermazione ed adozione di norme in materia di *cybersecurity* come oggetto di ispirazione per molteplici nazioni nel mondo.

3.1 Prime normative in materia

Le normative in materia di *cybersecurity* si differenziano, innanzitutto, tra: prescrittive, dunque inerenti alle misure di sicurezza da intraprendere ed alla definizione del concetto di sicurezza informatica; non prescrittive, incentrate rispetto all'individuazione, analisi e contenimento del rischio *cyber,* le quali hanno acquisito rilevanza con il passare degli anni malgrado ad oggi generino un *appeal* minore.

In primo luogo, l'analisi in materia si estrinseca a partire dal riferimento alle norme di certificazione della sicurezza dei prodotti informatici tra cui il TCSEC, ovvero Trusted

[39] S&P (Standard and Poor's Corporation) Global Ratings è una società privata americana impegnata nella realizzazione di ricerche ed analisi riguardanti l'ambito finanziario. È nota come una delle agenzie di *rating* più prestigiose al mondo.

Computer System Evaluation Criteria, del 1985 secondo cui la sicurezza di un determinato sistema o dispositivo era dipendente dall'adempimento a particolari funzioni essenzialmente riconducibili al controllo degli accessi. Tale criterio era impiegato per la classificazione e selezione di apparecchi tecnologici valutati in base alla capacità di analisi ed archivio di particolari informazioni. Tale criterio, anche noto come "Orange Book", dal colore della copertina del documento che lo conteneva, curato dal Dipartimento di Difesa degli Stati Uniti d'America con la volontà di rendere sistematico per la prima volta nella storia il processo di valutazione di sicurezza informatica all'epoca inerente ai sistemi tecnologici forniti dalla pubblica amministrazione ad enti militari e civili.
Successivamente, nel 1991 fu approvato l'Information Technology Security Evaluation Criteria, conosciuto ai più come ITSEC, consistente in un complesso di criteri per la valutazione della salvaguardia dei *computer* basata su un elenco di sette nuclei di sicurezza, tra cui identificazione, controllo degli accessi e tracciamento dell'utente. Tali componenti era necessario fossero non soltanto presenti all'interno del macchinario ed inerenti al rischio cibernetico al quale esso era maggiormente esposto, coprendo in tal prima battuta l'*assumption*, ma era essenziale garantirne l'*assurance*, riguardante la meticolosità con la quale gli elementi di sicurezza erano stati progettati, sviluppati e testati. Tale regolamentazione fu in prima istanza pubblicata in Francia, Germania, Olanda e Gran Bretagna erigendosi sulla documentazione in tal merito già esistente in tali paesi, per poi estenderne l'impiego tramite l'approvazione da parte della Commissione Europea per utilizzo operativo in fase di valutazione e certificazione dei dispositivi. Gran parte della logica contenuta all'interno dell'ITSEC può essere riscontrata facendo capo al documento intitolato Common Criteria, anche noto come Common Criteria for Information Technology Security Evaluation, diffuso nel 1999 e dotato di una definizione delle funzioni di sicurezza necessarie maggiormente dettagliata. Esso risulta essere lo *standard* internazionale ISO[40]/IEC[41] 15408 per la certificazione di *cybersecurity*, basata sull'assunzione di requisiti necessari a

[40] ISO sta per International Organization for Standardization ed identifica un'organizzazione non governativa ed indipendente impegnata nella definizione di standard internazionali. Tale ente è costituito da rappresentanti dei 170 paesi membri.
[41] IEC, acronimo di International Electrotechnical Commission, è un ente internazionale per lo sviluppo di criteri *standard* riguardanti l'elettricità, l'elettronica e le tecnologie ad esse correlate. Tale commissione è costituita da rappresentanti di enti di standardizzazione nazionali riconosciuti.

consolidare la tutela dei sistemi informatici, attribuendo valore al giudizio dei venditori ed aprendo all'impiego di specifici test per l'analisi dell'affidabilità dei macchinari. In tale senso diviene possibile tramite tali criteri ultimare i processi di specificazione ed implementazione della sicurezza dei dispositivi, potendo categorizzare quest'ultimi come sistemi operativi, *database* e metodi di *management*.

Per quanto concerne invece le normative di certificazione relative dei sistemi di gestione per la sicurezza delle informazioni, è opportuno far riferimento, in prima istanza, allo standard di sicurezza BS[42] 7799, la cui attuale versione è rappresentata dal documento ISO/IEC 27001, elaborato nel corso del 1994 in Gran Bretagna e caratterizzante un processo analitico fondato sui criteri fondamentali di confidenzialità, integrità e disponibilità dell'informazione. Infatti, si ritiene che i contenuti circolanti all'interno delle infrastrutture informatiche debbano essere accessibili esclusivamente ai soggetti legittimati alla visualizzazione del dato nella sua totalità ed immutabilità, salvaguardandone la possibilità di ricezione e trasmissione entro tempistiche adeguate e nel rispetto della relativa richiesta da parte degli utenti. In aggiunta a quanto appena descritto, è doveroso segnalare come tale requisito faccia capo non soltanto alla *cybersicurezza* in senso stretto, ma possa essere considerato riconducibile alla tutela fisica, inerente alla gestione delle informazioni ritenute strategiche, ed organizzativa, legata al coordinamento delle procedure necessarie alla salvaguardia dei dispositivi.

Con il passare degli anni tale normativa ha acquisito una certa notorietà in maniera progressiva prima in Italia ed i seguito in ottica internazionale, essendo di sostanziale utilità nel processo di identificazione del rischio e nella scelta delle misure di difesa maggiormente appropriate rispetto alla propria azienda o al settore nel quale essa opera.

Parallelamente, per quanto riguarda le normative incentrate rispetto all'individuazione di appropriate misure di sicurezza, risulta doveroso menzionare le misure minime AgID[43], che hanno ispirato il Cybersecurity Framework (CSF) del NIST[44], si

[42] BS, acronimo di British Standard, sono gli standard prodotti dal British Standard Institute, ovvero l'organizzazione competente in Gran Bretagna per la produzione di *standard* tecnici riguardanti prodotti e servizi, nonché relative certificazioni.

[43] AgID sta per Agenzia per l'Italia Digitale ed è un'agenzia pubblica italiana introdotta dal governo Monti al fine di perseguire l'innovazione tecnologica nello sviluppo della pubblica amministrazione nell'interesse di cittadini ed imprese. Inoltre, essa rilascia autorizzazioni per attività digitali.

[44] NIST, acronimo di National Institute of Standard and Technology, è un'agenzia del governo statunitense impegnata nella gestione di tecnologie, promozione dell'economia americana e sviluppo di *standard* tramite la collaborazione con l'industria.

sostanziano come riferimento pratico utile alle amministrazioni per il contrasto ai principali *cyber risks* tramite iniziative di tipo tecnologico, organizzativo e procedurale impiegate al fine di attribuire un riferimento operativo attuabile, verificare l'esposizione alle minacce informatiche e responsabilizzare gli enti in materia di *cybersicurezza*. Tali indicazioni risultano applicate su un triplice livello: minimo, dunque obbligatorio per ogni singola Pubblica Amministrazione a prescindere dalla propria natura o dimensione; *standard*, inteso come riferimento auspicabile per la maggior parte delle PA; alto, necessario alle organizzazioni più esposte al rischio cibernetico.

La tendenza ad attribuire maggiore valore alle misure di sicurezza piuttosto che alla valutazione del rischio è confermata dalla normativa ISO/IEC 27018, la quale si presenta come estensione dell'ISO/IEC 27001 e 27002, garantendo programmi di difesa maggiormente specifici ed elaborati, in modo particolare, per garantire la tutela e la *privacy* delle informazioni di identificazione personale dei fruitori di servizi *cloud*. Tale forma di regolamentazione si basa su concetti fondamentali di riservatezza applicata a dati strettamente sensibili come la conformità ai requisiti essenziali della *privacy*, quali minimizzazione e accuratezza dei dati, o l'obbligo di collaborare con i responsabili del trattamento delle PII[45]. Si ricorda come tale documento sia stato redatto al fine di risultare applicabile all'interno di organizzazioni di molteplici dimensioni e settori operativi, pertanto adottabile da enti privati, governativi e *no-profit*, purché essi siano dotati di sistemi di analisi dell'informazione basati sul *cloud computing*.

Si ricorda come tra le prime forme di regolamentazione in materia di *privacy* si annoveri la presenza della legge 675 del 1996, intitolata "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", poi aggiornata tramite il decreto legislativo numero 467 del 2001, il quale ha apportato sostanziali garanzie ai cittadini tramite una rilevante semplificazione delle procedure, in modo particolare in riferimento alle notifiche. La normativa oggi nota ai più come "Vecchia Legge sulla Privacy", come si evince inequivocabilmente dal titolo sopra fornito, riguarda la protezione di informazioni sensibili riguardanti individui ed enti di vario genere, fornendo definizioni essenziali ed alla base della sicurezza informatica, come ad esempio la precisa

[45] PII, acronimo di Personally Identifiable Information, riguarda una certa mole di dati utili all'identificazione di un soggetto, per tale motivazione definiti dati sensibili. Tra essi rientrano ad esempio la data di nascita, il nome e cognome ed il codice fiscale. Questo tipo di dati sono particolarmente preziosi e per questo uno dei principali obiettivi dei *cybercriminali*.

distinzione tra dati personali e sensibili. Infatti, in riferimento ai dati personali, essi si qualificano come "Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale" (art.1, comma 2, lett. c, legge 675/96). Ad essi associati si configurano i dati sensibili, descritto come "I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (art. 22, comma 1, legge 675/96). In più, si ritiene doveroso valutare come, ai sensi dell'art.10 della legge sulla privacy, il professionista che filtra o analizza dati personali è tenuto ad informare il soggetto interessato in forma orale o scritta in materia di finalità e modalità del trattamento, essendo altrimenti prevista una sanzione amministrativa pecuniaria in caso di violazione (cfr. art. 39, comma 2, legge 675/96). In tale ottica si delinea il dovere di segretezza e riservatezza nell'espletamento del mandato, il quale si consolida, peraltro, come idoneo strumento a tutela di terzi nel conflitto ad indebite divulgazioni, salvo esigenze riconducibili al diritto di difesa in sede giudiziaria o alla fattispecie dello svolgimento delle investigazioni trattata dall'art.38 delle disposizioni di attuazione del codice di procedura penale.

A differenza della legge 675 del 1996, espressione di un approccio alla sicurezza caratterizzato dall'applicazione di suddette misure minime, maggiormente improntata in riferimento alla valutazione del rischio si identifica il GDPR[46] del 2016, riguardante la tutela del singolo individuo e la libera circolazione di dati personali, garantendo maggiore armonizzazione rispetto al tema tramite una pronuncia di certezza giuridica coerente e consapevole rispetto al circostante sviluppo tecnologico. Tale normativa introduce alcuni concetti innovativi, tra cui la responsabilizzazione del titolare, l'estensione delle sanzioni amministrative pecuniarie e fattispecie peculiari per la nomina di un responsabile in materia di trattamento e difesa delle informazioni. Ulteriore tematica interessante introdotta dal regolamento è certamente il diritto alla

[46] GDPR, acronimo di General Data Protection Regulation, è il regolamento 679 approvato dall'Unione Europea nel 2016, divenuto il 25 maggio 2018 applicabile in tutti gli Stati membri e riguardante il trasferimento e la protezione di dati personali. I contenuti della normativa risultano applicabili anche ad imprese localizzate all'esterno dell'Unione Europea, ma operanti all'interno del mercato Ue.

portabilità, riguardante la possibilità da parte del titolare di richiedere in un formato strutturato di uso comune le coordinate dei propri dati personali in modo tale da poter ultimare il passaggio degli stessi da un titolare del trattamento all'altro e, ove realizzabile, il trasferimento diretto dei propri dati. Questo particolare diritto risulta esercitabile nella fattispecie di trattamento legittimato dal consenso, contratto o realizzato tramite mezzi automatizzati; dunque, l'applicazione non è prevista nel caso di iniziative di interesse pubblico o inerenti all'esercizio di pubblici poteri di cui è dotato il titolare del trattamento. Nello specifico tale forma di regolamentazione non è valida nei riguardi di informazioni appartenenti ad archivi di interesse pubblico, come nel caso delle anagrafiche.

In conclusione si auspica che l'analisi delle normative citate abbia consentito di comprendere la rilevanza della coesistenza dell'approccio prescrittivo e non. Infatti, la metodologia incentrata rispetto alla definizione delle misure di sicurezza si configura come particolarmente preziosa nel fornire un solido orientamento rispetto alla tematica trattata, così come risulta maggiormente pratico in termini di verifiche. Parallelamente, l'approccio caratterizzato dalla valutazione del rischio si è dimostrato essere maggiormente adatto alla contestualizzazione delle scelte realizzata tramite una considerazione dinamica e complessiva delle più moderne innovazioni.

3.2 Normative attualmente in vigore

Attualmente il quadro normativo in materia di *cybersecurity* risulta caratterizzato dall'entrata in vigore del Regolamento UE 2023/2841 in data 7 Gennaio 2024, previa approvazione all'unanimità del Consiglio dell'Unione Europea e decorsi i 20 giorni dalla pubblicazione nell'Official Journal[47]. Tale normativa è realizzata al fine di garantire ad istituzioni ed enti dell'Unione Europea un adeguato ed omogeneo livello di *cybersicurezza*, realizzato mediante un bilanciamento tra esigenze di sicurezza informatica, innovazione tecnologica e diritti degli utenti. Pertanto, si identifica all'interno dell'atto un approccio multirischio, composto da iniziative di *management*, *governance* e monitoraggio dei rischi cibernetici perseguite tramite misure tecniche, operative ed organizzative spesso dettate dall'individuazione di minacce appresa dalla

[47] L'Official Journal rappresenta la Gazzetta Ufficiale dell'Unione Europea, tramite la quale quest'ultima pubblica ufficialmente atti giuridici ed informazioni ufficiali approvate dagli organismi competenti. Viene tradotta nelle 24 lingue ufficiali dell'UE.

condivisione di informazioni, processo imprescindibile al fine di essere sempre al passo con le più attuali forme di attacco. In tale prospettiva il regolamento prevede il riconoscimento del valore di strumenti *open source*, il cui funzionamento risulta basato su standard di trasparenza, utili all'individuazione di minacce o errori di programmazione e dotati di flessibilità estrema, rivelandosi dunque di particolare utilità per l'adattamento ai variegati interessi dei componenti dell'Unione. Ulteriore aspetto intrigante contenuto nel documento analizzato è certamente la possibilità di rivolgersi al CERT-UE, acronimo di Computer Emergency Response Team dell'Unione Europea, nel caso di incidenti riguardanti contesti ITC definiti in casi specifici e su specifica richiesta di un componente dell'Unione. Tale istituto, originariamente istituito dalla Commissione Europea, si qualifica come finalizzato all'efficientamento della sicurezza informatica di istituzioni ed organismi europei tramite servizi di consulenza tecnica specializzata o forme di supporto pratico, tra le quali programmi di prevenzione, segnalazione e coordinamento. Risulta, invece, effettivamente introdotto dal Regolamento UE 2023/2841 l'IICB, ovvero l'Interinstitutional Cybersecurity Board, competente in materia di direzione strategica ed osservazione dell'attuazione della normativa. In tal senso quest'autorità è fondamentale nella definizione di orientamenti e strategie pluriennali, così come nella formazione di gruppi competenti localmente in materia di *cybersecurity* in modo tale da facilitare l'ossequio ai dettami dell'atto giuridico, fornendo in merito informazioni, pareri ed azioni correttive o sanzioni. In aggiunta, questo istituto è legittimato alla trasmissione di raccomandazioni o alla sospensione temporanea del flusso di dati nei riguardi di componenti dell'Unione non conformi e, persino, all'istituzione di un comitato esecutivo per la delega di incarichi peculiari. CERT-UE ed ICCB collaborano in maniera sinergica in quanto il primo è competente in termini di progettazione e definizione delle direttive e strategie, la cui applicazione pratica è curata nel dettaglio dal secondo tramite servizi operativi e di consulenza finalizzati alla costituzione di un ambiente digitale sicuro e resiliente. Iniziativa addizionale realizzata con l'intento di sedimentare in maniera maggiormente approfondita i principi della sicurezza cibernetica è la direttiva NIS2, acronimo di Network & Information Security, in vigore dal 17 Gennaio 2023 e da recepire per gli Stati membri dell'UE entro il 17 ottobre 2024. Tale normativa risulta essere l'estensione della direttiva NIS del 2016, rispetto alla quale risulta più improntata sulla prevenzione.

Tra le novità maggiormente intriganti introdotte dall'atto si annovera il registro europeo delle vulnerabilità, strumento che potrà essere impiegato per l'immediata registrazione delle principali e più recenti fonti di esposizione al rischio di attacco *hacker*. Un ruolo similare in termini teoretici e formativi è ricoperto dal CyCLONe, acronimo di Cyber Crisis Liaison Organisation Network, istituito mediante la cooperazione tra Stati membri impegnati nella gestione delle crisi informatiche al fine di favorire la trasmissione di informazioni formative. Tale ente costituisce un tramite interposto tra la sfera tecnica rappresentata dal CSIRT, ovvero Comuputer Security Incident Response Team, e la direzione politica dell'UE. Inoltre, la direttiva NIS2 prevede la stesura di una relazione annuale riguardante le condizioni della *cybersecurity* in Ue in modo da avere dati di assoluta attualità in riferimento alle più recenti minacce informatiche ed alle necessità di aggiornamento dei sistemi di dotazione degli Stati membri, per i quali è legittimata la revisione *inter pares* del documento che garantisca l'attualità ed efficacia delle strategie informatiche poste in essere. In aggiunta a quanto appena riportato, è doveroso ricordare che la direttiva NIS2 risulta applicabile per l'intera catena di approvvigionamento, incluse quindi terze parti coinvolte, in modo particolare nei riguardi di organizzazioni: grandi, aventi più di 250 dipendenti; medie, dotate di un numero di dipendenti tra 50 e 250; piccole, costituite da meno di 50 dipendenti o fautrici di un fatturato annuo al di sotto dei 10 milioni di euro, ma dotate di importanza critica per la società e sottoposte a requisiti maggiormente rigorosi. Si fa notare, poi, che la direttiva è espressione di un approccio *risk based* caratterizzato dalla gestione dei *cyber risks* da parte del *management* nel rispetto delle indicazioni fornite, prevedendo in caso contrario efficaci sistemi di segnalazione alle autorità in modo tale da minimizzare i potenziali effetti di crimini informatici, salvaguardando la continuità aziendale. Nel caso in cui si verifichi una mancata conformazione alle indicazioni fornite dalla direttiva NIS2, sono previste sanzioni fino a 10 milioni di euro o al 2% del fatturato annuo globale per le organizzazioni operanti in settori classificati come "essenziali[48]", mentre nei riguardi di organizzazioni definite "importanti[49]" si prospettano multe fino a 7 milioni di euro o all'1.4% del fatturato annuo complessivo, così come si classificano

[48] I settori definiti "essenziali" dalla direttiva NIS2 sono: energetico, sanitario, trasporti, acque e acque di scarico, infrastrutture digitali, spaziale e pubblica amministrazione.
[49] I settori qualificati come "importanti" nella direttiva NIS2 sono: postale e di spedizione, gestione/trattamento rifiuti, chimico, alimentare, tecnologico e ingegneristico, servizi digitali e ricerca scientifica

come perseguibili legalmente le persone fisiche dotate di incarichi dirigenziali all'interno delle organizzazioni indagate nel caso in cui si identifichino delle responsabilità, le quali comportano, oltre alle inchieste giudiziarie, l'adesione presso corsi specifici di valutazione del rischio cibernetico e la promozione di percorsi di formazione analoghi per tutti i dipendenti dell'ente presso il quale si esercita la propria professione.

Ulteriore regolamento europeo rilevante in materia di sicurezza informatica, in modo specifico in riferimento ai prodotti connessi[50], è noto come Cyber Resilience Act, presentato per la prima volta al vaglio delle istituzioni dell'Unione Europea nel 2022 e successivamente pubblicato in data 20 dicembre 2023, in seguito ad una serie di modifiche inerenti all'ambito di applicazione ed alle novità dell'industria digitale. L'atto normativo è finalizzato in primo luogo alla promozione e diffusione della cultura della *cybersicurezza* non soltanto tra utenti, ma anche e soprattutto nei riguardi di fornitori ed altri soggetti coinvolti all'interno della *supply chain*, garantendo dunque l'abbattimento delle principali vulnerabilità dei moderni apparecchi, i quali risultino pertanto distinti dagli acquirenti e dai mercati in base alla capacità tutela dell'informazione. È significativo evidenziare come la responsabilizzazione del produttore si estenda sino all'epilogo del ciclo di vita di un prodotto dotato di componenti digitali, il quale per la collocazione sul mercato necessiterà del marchio CE, sinonimo di conformità ai requisiti posti dalla documentazione approvata dall'Unione Europea e, di conseguenza, garanzia di *cybersecurity* nei confronti del cliente. Inoltre, è prevista in allegato al prodotto oggetto del commercio una serie di indicazioni riguardanti l'utilizzo maggiormente appropriato ed al netto di potenziali rischi. Infine, il regolamento fornisce una definizione dettagliata di *software* libero e *open source*, così descritto "Per software libero e open source si intende il software il cui codice sorgente è apertamente condiviso e la cui licenza prevede tutti i diritti per renderlo liberamente accessibile, utilizzabile, modificabile e re-distribuibile. Il software gratuito e open source viene sviluppato, mantenuto e distribuito apertamente, anche tramite piattaforme online. In relazione agli operatori economici soggetti al regolamento, solo il software gratuito e open source reso disponibile sul mercato e quindi fornito per la distribuzione o l'utilizzo nel corso di

[50] Per prodotti connessi si intendono dispositivi elettronici tra essi collegati e capaci di comunicare, in tal modo generando un complesso *network* tale da unire componenti eterogenee dalle funzioni molteplici.

un’attività commerciale” (Cyber Resilience Act, 12 Marzo 2024).
La strategia in ambito digitale delle istituzioni europee, fondata sulla protezione dei dati ed il rispetto di diritti fondamentali degli utenti tramite l’efficientamento delle procedure di *cybersecurity,* risulta perseguita tramite l’AI Act, regolamento europeo in materia di intelligenza artificiale e diritti o doveri previsti per i soggetti appartenenti a tale ambito. Tale atto giuridico, approvato recentemente dal Parlamento Europeo in data 13 Marzo 2024, si configura come la prima legge trasversale al mondo riguardante l’*artificial intelligence*. La normativa in analisi mira, in primo luogo, alla costituzione di un mercato unico per l’AI, che consenta la circolazione libera di sistemi conformi alla normativa, pertanto dotati di affidabilità e trasparenza tali da incrementare in modo significativo la fiducia nei confronti di questo tipo di strumenti, favorendo gli investimenti e le collaborazioni imprenditoriali, scientifiche ed istituzionali al fine di generare innovazione utile alla prevenzione del rischio ed all’avanzamento in termini di ricerca. L’intelligenza artificiale si qualifica come strumento idoneo alla realizzabilità di notevoli progressi nel contesto sociale, tecnologico ed economico, bensì può eventualmente esporre gli utenti ed i dispositivi a minacce di carattere informatico e lesive di diritti strettamente personali, motivazione per la quale l’AI Act fornisce una classificazione dei sistemi in base all’aleatorietà per gli individui e la collettività. Il primo livello, partendo dal basso verso l’alto, è definito minimo, i quali non hanno effetti diretti nei riguardi di diritti fondamentali o della sicurezza degli utenti, ragione per cui sono svincolati da peculiari obblighi normativi, garantendo margini di controllo alle persone nella speranza di incoraggiare sperimentazioni e, di conseguenza, sviluppo in ossequio alle normative generali in materia. In seguito, si fa capo al nucleo di rischio limitato, capace di generare impatto moderato su diritti e volontà degli individui, per questo sottoposti a requisiti di trasparenza, i quali consentano ai fruitori di sistemi IA di essere pienamente consapevoli dell’interazione con quest’ultimi e delle correlate caratteristiche e limitazioni tramite processi informativi chiari, comprensibili ed accessibili. All’interno della scala gerarchica descritta, si prospetta successivamente il profilo del rischio elevato, in grado di dar luogo ad implicazioni sistemiche nei confronti dei diritti fondamentali degli utenti, ciò comporta l’imposizione a riguardo di requisiti stringenti per la collocazione di tali strumenti sul mercato, come obblighi di registrazione, tracciabilità e segnalazione del rischio assoggettate al giudizio di enti

indipendenti legittimati al rilascio o ritiro di specifici certificati. In ultima istanza, in cima alla graduatoria in termini di pericolosità di profila il rischio inaccettabile, potenzialmente costitutivo della violazione di principi fondamentali dell'Unione Europea, quali dignità umana e democrazia, dunque associati a rigorose restrizioni o divieti assoluti. Inoltre la creazione di un complesso normativo armonizzato per gli Stati membri dell'Unione Europea in riferimento all' intelligenza artificiale, incrementandone la competitività nello scenario internazionale tramite l'introduzione di iniziative progressiste come l'istituzione di un comitato europeo per l'AI che si consolidi come strumento di assistenza per la Commissione nel rinnovamento dell'AI Act tramite la formulazione di raccomandazioni e pareri in materia sostenuti da centri di competenza specializzati ed aggiornati nei riguardi delle *best practices* del settore. Per quanto concerne la definizione del concetto di intelligenza artificiale risulta essere una delle tematiche maggiormente discusse nel corso dell'*iter* legislativo della normativa, nonché una delle più rilevanti, implicando il delineamento delle componenti sottostanti tale regolamento. Dunque da una prima proposta della Commissione, contenente una descrizione del fenomeno flessibile ed adattabile associata ad un elenco di approcci per lo sviluppo in materia, si è giunti all'attuale definizione, conseguente la proposta definitoria dell'OCSE[51], secondo la quale l'*artficial intelligence* si identifica come "un sistema automatizzato progettato per funzionare con diversi livelli di autonomia e che può mostrare capacità di adattamento dopo l'installazione e che, per obiettivi espliciti o impliciti, deduce, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali" (articolo 3, AI ACT, 13 Marzo 2024). Si noti, in aggiunta a quanto precedentemente analizzato, come i requisiti della normativa siano applicabili nei confronti di fornitori, operatorii soggetti terzi appartenenti alla catena di valore dell'intelligenza artificiale, come importatori, distributori, fabbricanti e rappresentanti autorizzati, a patto che quest'ultimi offrano servizi o utilizzino output prodotti dall'AI in UE, a prescindere dal fatto che siano collocati effettivamente all'interno di Stati membri. Parallelamente l'applicazione dell'AI Act non è prevista per sistemi operanti

[51] L'OCSE, acronimo di Organizzazione per la Cooperazione e lo Sviluppo Economico, è un ente internazionale specializzato nell'ambito economico e costituito da paesi sviluppati aventi in comune un sistema di governo democratico ed un'economia di mercato. Essa svolge prevalentemente il ruolo di assemblea consultiva per tematiche politiche, commerciali e di coordinamento.

nel settore militare, di difesa o di sicurezza nazionale, così come esclusi saranno strumenti attivi per scopi di ricerca, prova e sviluppo scientifico, rilasciati con licenze *free e open source* o per attività non professionali puramente personali. Come conclusione in merito, è fondamentale porre in rilievo il cosiddetto "Brussels effect", tramite il quale il primo progetto trasversale riguardante l'*artificial intelligence* nel panorama mondiale, si configura come emblema di riferimento in ottica internazionale per tutela dei diritti fondamentali ed il consolidamento di una visione prettamente umano-centrica, essenza delle normative europee inerenti alla *data economy.*

3.3 Autorità competenti ed organismi di controllo

Il progressivo ampliamento della necessità di misure di *cybersecurity* per la tutela di utenti, dispositivi ed infrastrutture informatiche da potenziali minacce di attacco *hacker* ha indotto le istituzioni competenti in materia di regolamentazione a legittimare l'introduzione di autorità specializzate in materia di vigilanza.

In primo luogo si intende analizzare nel dettaglio l'ACN, acronimo di Agenzia per la Cybersicurezza Nazionale, costituita in data 4 agosto 2021 in seguito alla pubblicazione in Gazzetta Ufficiale della legge di conversione n.109 del decreto legge 14 giugno 2021 n.82. Tale ente costituisce uno strumento tramite il quale il Governo Draghi all'epoca mirava all'affermazione dei principi di sicurezza informatica tramite la composizione di una solida consapevolezza della pericolosità del rischio cibernetico da parte del settore pubblico e privato, come attuazione del Piano Nazionale di Ripresa e Resilienza, noto ai più come PNRR[52], il quale colloca la *cybersicurezza* a fondamento della transizione digitale, prevedendo in tale ambito un finanziamento di oltre 620 milioni di euro previsti per l'efficientamento delle infrastrutture tecnologiche e per la sicurezza nazionale. L'ente è istituito in capo alla Presidenza del Consiglio dei Ministri e sottoposto al controllo diretto del COPASIR[53], mentre la composizione prevede la possibilità di assunzione di personale *ad hoc* non appartenente alla Pubblica

[52] Il PNRR è il piano approvato nel 2021 dal governo italiano per far ripartire l'economia italiana in seguito alla pandemia di Covid-19, favorendo lo sviluppo digitale, la transizione ecologica, la mobilità sostenibile, l'istruzione e ricerca, l'inclusione e la salute. Tale piano è parte integrante del programma dell'Unione Europea "Next Generation EU da 750 miliardi d'euro.

[53] Il COPASIR, ovvero Comitato Parlamentare per la Sicurezza della Repubblica, si identifica come organo del Parlamento della Repubblica Italiana per la vigilanza dei servizi segreti italiani, del Sistema di informazione per la sicurezza della Repubblica o altri organi della Pubblica Amministrazione.

Amministrazione. L'istituzione dell'ACN non si limita all'avanzamento delle competenze nazionali di prevenzione, rilevamento e mitigazione delle minacce *cyber* tramite il coinvolgimento di organizzazioni essenziali quali il Computer Security Incident Response Team, al secolo CSIRT, ed un Centro per la valutazione e certificazione nazionale, ma si estende all'innovazione nel contesto industriale, tecnologico e scientifico nella prospettiva di autonomia strategica nazionale nel settore, predisponendone pianificazione di coordinamento e divenendone autorità nazionale di certificazioni. Inoltre, l'Agenzia si predispone ad essere interlocutore unico nazionale per soggetti pubblici e privati in materia ispettiva e di sicurezza nazionale cibernetica, delle reti e dei sistemi informativi, in ossequio alla direttiva NIS, e delle infrastrutture di comunicazione elettronica, rivelandosi, peraltro, competente in riferimento all'accertamento delle violazioni ed al fine di comminare le sanzioni previste. Il decreto istitutivo dell'ACN prevede, in seguito, la fondazione del Comitato Interministeriale per la Cybersicurezza, anche noto come CICS, dotato di funzioni di consulenza, proposta e deliberazione per le politiche di *cybersecurity* e la salvaguardia della sicurezza cibernetica nazionale, monitorando l'attuazione delle specifiche strategie del Paese in materia. Infine è prevista l'introduzione dell'Nsc, dunque Nucleo per la sicurezza cibernetica, abilitato alla proposta di misure di *cybersicurezza* in Italia ed Europa, alla promozione delle strategie operative e del coordinamento interministeriale ed alla condivisione di informazioni di attualità inerenti a violazioni dell'integrità delle infrastrutture digitali.

Per quanto concerne l'ambito specifico della protezione dei dati personali, si ritiene doveroso esplicitare le funzioni del Garante della Privacy, ente amministrativo indipendente istituito tramite la legge in materia di privacy n.675 del 1996, successivamente sostituita dal decreto legislativo n.196 del 2003, ,meglio noto come Codice della Privacy. La funzione primaria di tale organizzazione risulta essere la tutela del trattamento dei dati personali nel rispetto della dignità dell'individuo, perseguita mediante il monitoraggio della trasmissione di informazioni, la promozione dei principi costituenti la materia e l'erogazione di sanzioni amministrative e penali. Nella fattispecie di violazione dei diritti della persona l'interessato ha il dovere di rivolgersi in prima battuta al responsabile o titolare del trattamento dei dati e, trascorsi 30 giorni da tale comunicazione nel caso in cui non sia pervenuto o risulti insoddisfacente il

riscontro, ha la possibilità di avvisare direttamente il Garante della Privacy, al quale ci si può rivolgere in prima istanza nel caso in cui il decorso della tempistica appena menzionata comporti un pregiudizio imminente ed irreparabile assoggettato ad onere della prova. In modo dettagliato, l'ente in analisi può essere reperito tramite una triplice modalità: segnalazione, che si presenta come gratuita ed al netto di peculiari formalità, prevedendo la descrizione delle componenti utili ad un eventuale intervento; reclamo, formulato in ossequio alle istruzioni del Garante e richiedente il pagamento dei diritti di segreteria[54]; ricorso, dotato di effetti giuridici e firma autenticata, contenente i requisiti scriminati dall'art.147 del Codice della Privacy e fonte del pagamento di diritti di segreteria, nonché delle spese del procedimento a carico della parte soccombente in giudizio. In aggiunta a quanto appena esplicitato, è opportuno segnalare come il Garante della Privacy sia competente in materia di richieste al Parlamento e ad ulteriori istituzioni di progresso in termini normativi ed amministrativi, formulando pareri e consulenze ove ritenuto necessario e fornendo una relazione annuale al Governo ed alle Camere inerente all'attività compiuta. Infine, si pone rilievo nei riguardi del codice etico dell'ente in esame, il quale ha la funzione di orientare la deontologia dei componenti dell'Ufficio del Garante all'adozione di assoluta imparzialità e trasparenza nell'esercitare la propria professione al fine di garantire l'ossequio agli obblighi di riservatezza evitando potenziali conflitti di interesse. In modo particolare tali dipendenti non sono legittimati alla strumentalizzazione delle informazioni assunte per l'appagamento di interessi privati, così come non è consentito rilasciare dichiarazioni inerenti agli atti ed ai provvedimenti di pertinenza dell'ente previa comunicazione alle parti interessate, avendo la capacità di attuare il principio della parità di trattamento in riferimento alla tempestività con la quale le notizie vengono trasmesse salvaguardando il rapporto lavorativo con la stampa ed i fornitori di informazione.
Nel proseguimento della conduzione dell'*excursus* di carattere informativo in riferimento ai principali organismi di controllo in materia di sicurezza informatica, si ritiene opportuno far riferimento all' Agenzia dell'Unione Europea per la cibersicurezza in passato nota come ENISA, acronimo di European Network and Information Security

[54] I diritti di segreteria costituiscono un corrispettivo versato al Comune o alla Provincia al fine di ottenere una prestazione non prevista in favore della comunità indistinta, bensì in modo specifico ed occasionale nei riguardi del richiedente. Sono previsti nello specifico per pratiche demografiche, autorizzazioni edilizie o certificati di destinazione urbanistica tra gli altri.

Agency, costituita nel lontano 2004, epoca nella quale le minacce *hacker* non avevano ancora acquisito la sostanziale portata ad oggi di dominio pubblico, come testimoniato dalla decisione di collocare le prime due sedi dell'ente in Grecia, a considerevole distanza dai più potenti centri decisionali europei. Oltre a ciò, originariamente l'istituto rappresentava un mandato a termine di soli cinque anni, per poi essere qualificato, in seguito a numerose proroghe, come agenzia permanente nel 2019 data la rilevanza acquisita con il decorso degli anni nella definizione di una strategia comune di *cybersecurity.* Le funzioni esercitate da tale organo si denota essere molteplici e variegate, a partire da un ruolo di estrema significatività in termini di consulenza e delibera di istruzioni operative per gli Stati membri, supportati nell'individuazione delle priorità in tema di finanziamento per la ricerca e lo sviluppo e dei criteri comuni per l'unificazione dei sistemi nazionali di rilascio delle certificazioni di sicurezza informatica, aspetti essenziali per il flusso dinamico di informazioni all'interno del commercio transfrontaliero apportando benefici nell'interesse di consumatori, attività imprenditoriali ed istituzioni europee. Si evidenzia, poi, come in capo ad ENISA si annoveri la stesura dell'ECSF, dunque Quadro Europeo delle Competenze in materia di Cybersicurezza, avente come obiettivo l'avanzamento della cultura europea in riferimento alla sicurezza informatica tramite l'impiego di un linguaggio comune a tutte le comunità come strumento funzionale al progresso delle propsettive nell'ambito digitale rappresentando una sorta di tramite tra la domanda professionale di *cybersecurity* e l'offerta formativa tra gli Stati membri. In tal senso l'ECSF si configura come compromesso tra cittadini, datori di lavoro e fornitori di programmi di formazione utile all'analisi di competenze, capacità e potenzialità dei lavoratori nel contesto della sicurezza cibernetica, tramite le quali è stato possibile delineare 12 profili professionali tipici tra cui: il *Chief Information Security Officer*, manager della sicurezza dell'informazione; il *Cyber Incident Responder*, competente in caso di incidenti; il *Cybersecurity Researcher*, dunque ricercatore in *cybersicurezza*. In questa prospettiva tale documento si profila di particolare rilevanza nell'identificare competenze critiche ritenute essenziali dal mercato del lavoro, armonizzando i percorsi di istruzione e sviluppo professionale e garantendo maggiore comunicazione e coordinamento tra le parti coinvolte all'interno della *supply chain*. Nel corso degli anni la collaborazione di ENISA con istituzioni nazionale ed europee ha favorito l'elaborazione ed il progresso di

numerosi *iter* di matrice educativa in materia di *cybersecurity* in ossequio ai requisiti esplicitati dal Quadro Europeo.

4. Prevenzione e tutela da cyber risk

Il percorso analitico in materia di *cybersecurity*, sino ad ora tracciato, ha consentito di evincere cosa si intende per rischio cibernetico, quali sono le metodologie e gli approcci maggiormente impiegati al fine minimizzare le potenzialità di tale fenomeno e le forme di regolamentazione realizzate nel tentativo di disciplinare in maniera coordinata un settore in continua evoluzione come quello in analisi. Pertanto, si ritiene, a tal punto, opportuno approfondire le procedure mirate alla prevenzione, intese come iniziative precauzionali e prudenziali di natura preliminare rispetto all'effettiva e pratica salvaguardia dei contenuti informatici, prestabilite nell'intento di ridurre gli effetti catastrofici delle operazioni di *cybercrime*. Albert Einstein affermava che "Gli intellettuali risolvono i problemi; i geni li prevengono", aforisma dal quale è possibile dedurre la sfida maggioremente intrigante per la dottrina nell'ambito della sicurezza informatica: l'assunzione di competenze tali da porre in essere infrastrutture digitali oggetto di costante monitoraggio, essenziale per l'efficientamento di sistemi di segnalazione simultanea di eventuali minacce, la cui materializzazione non sia tale da compromettere l'utlizzo di specifici servizi multimediali o l'accesso a determinate informazioni sensibili contenute negli archivi digitali attraverso la realizzazione di procedure preventive funzionali al ridimensionamento della perdita in termini economici, personali o reputazionali. In tale prospettiva si ricorda in modo dettagliato come una fuga di dati possa comportare non soltanto la dispersione di ingenti somme di denaro per i titolari delle informazioni indebitamente acquisite attraverso il pagamento di riscatti o tramite il crollo dei ricavi causato dall'interruzione di un'attività, ma le relative conseguenze possono estendersi sino alla violazione dell'integrità dei contenuti, passando per l'indisponibilità dell'accesso a piattaforme personali, comportando, dunque, nel caso in cui si sostanzi la lesione nei confronti di professionisti o complessi imprenditoriali, della dispersione totale o parziale della propria clientela, verificandosi una spiacevole *customer experience* dettata dalla disseminazione del vantaggio competitivo in favore dei concorrenti. Dunque, è, in tale ottica, lapalissiano comprendere quanto la profilassi cautelare sia imprescindibile nel corso dell'epoca contemporanea nel contesto pubblico e privato.

4.1 Cybersecurity assessment

L'esponenziale progresso delle operazioni di *cybercrime* nel corso degli ultimi anni ha reso la *cybersicurezza* una disciplina di estremo valore per la competitività e la distinzione di una particolare compagnia rispetto alle concorrenti, motivazione per quale si è ritenuto doveroso stabilire una procedura secondo cui stimare le capacità di tutela del proprio ente rispetto ai rischi di matrice cibernetica tipici del settore di appartenenza. Tale pratica prende il nome di *cybersecurity assessment*, intesa come branca di particolare utilità nel fornire a privati, imprese e istituti di pubblica amministrazione stimoli ulteriori all'adozione delle *best practices* del mondo informatico e, di conseguenza, idonea alla realizzazione delle strategie finalizzate all'avanzamento del processo di transizione digitale. Nello specifico il Framework nazionale per la cybersecurity e la data protection[55] delinea questo fenomeno come costituito da una prima procedure preliminare definita contestualizzazione, all'interno della quale si sostanzia uno studio delle condizioni di sicurezza della propria attività e dei modelli di riferimento circostanti in maniera tale da identificare il corrente *status* in termini di capacità di salvaguardia dei propri *asset* ed la relativa distanza in termini di preparazione e competenze rispetto ai detentori delle *best practices*, realizzando in questo modo il procedimento di *gap analysis*, funzionale ad una fase di pianificazione esplicitata tramite la stesura di un programma di allineamento ai *target* individuati. La qualità di tale procedura è determinata dal rispetto delle tempistiche definite per l'azione implementativa, così come dal graduale raggiungimento di obiettivi *mid-term* nel breve periodo. In modo ancor più specifico, è possibile distinguere tra una duplice alternativa in termini di *cybersecurity assessment*: qualitativo, pertanto orientato dalla valutazione di componenti di natura soggettiva o difficilmente misurabili e caratterizzato da tempistiche brevi ed investimenti circoscritti; quantitativo, approccio sostanzialmente oggettivo tramite il quale dar luogo a precisi rilevamenti mediante l'impiego di metriche specificamente previste che richiedono un monitoraggio periodico, nonché costi generalmente più elevati. Si ritiene essenziale porre in rilievo come tali metodologie non vadano intese come alternative ed esclusive, bensì debbano essere alla base di un'integrazione fondametale per la propria esaustività. Una delle principali

[55] Il Framework nazionale per la cybersecurity e la data protection, ispirato al Cybersecurity Framework del NIST, si identifica come insieme di requisiti ed indicazioni in materia di sicurezza cibernetica, desunti dalla collaborazione tra organizzazioni private, istituti pubblici e figure accademiche.

problematiche riscontrate a riguardo si denota esser rappresentata dalla scarsità di collaborazione ed armonizzazione tra i *provider* di sistemi di *cybersecurity assessment*, dettate dallo sviluppo di procedure chiuse entro la disponibilità esclusiva in termini di offerta da parte degli sviluppatori, condizione che comporta un elevato tesso di eterogeneità all'interno dei mercati, dando luogo a difficoltà sostanziali nella comparazione dei vari servizi offerti alla clientela, la quale, pur di intercettare continuità in termini di interpretazioni dei principi informatici, tende a rivolgersi nel corso del tempo alla medesima organizzazione in maniera continuativa portando, così, all'origine di un processo di *lock-in*, ridimensionando in tal senso le potenzialità di progresso nei riguardi di tale disciplina. Per la ragione appena esplicata, è stato previsto lo sviluppo di un approccio di *assessment* interamente accessibile ed incentrato sull'uso del Framework Nazionale, dunque suddiviso in tre fasi operative essenziali: la contestualizzazione, consistente in un'interpretazione della realtà circostante tramite l'impiego di prototipi di supporto quali normative o *standard* tecnici, utile alla definizione delle priorità e dei *target* in termini di sicurezza informatica; la misura, realizzata per mezzo della somministrazione assistita di un questionario compilato dai professionisti competenti in materia, chiamati ad esprimersi riguardo copertura e maturità , chiamati ad esprimersi riguardo copertura e maturità dei propri programmi di prevenzione, in modo da dedurre la distanza dal profilo auspicato; la valutazione, nel corso della quale si analizzano i risultati ottenuti nello *step* precedente, per poi proiettarli nell'ottica di riutilizzo e versatilità in molteplici contesti, tra cui la *compliance* e la gestione del rischio. In tale prospettiva si rende possibile una procedura essenziale di comparazione rispetto ai propri *competitor*, la quale si rivela di particolare importanza nella formazione dei processi di *decision making*[56], i quali implicano un impatto considerevole a livello tecnico, esecutivo e dirigenziale ponendo in essere una sorta di *rating* in materia di *cybersicurezza* nel dettaglio delle singole componenti operative, componenti operative, la cui interpretazione complessiva garantisce una visione totale dello *status* di tutela dell'ente in esame. In sostanza la finalità ultima della

[56] Con l'espressione *decision-making*, si fa sostanzialmente riferimento al processo decisionale inteso come fenomeno cognitivo alimentato da elementi consci ed inconsci alimentato da elementi consci ed inconsci funzionali all'acquisizione di una scelta tra più opzioni da parte di un individuo o un collettivo. Tale disciplina ha acquisito estrema rilevanza nell'ambito del management aziendale, ma risulta applicabile nella quotidianità.

materia oggetto di descrizione risulta essere l'adozione di contromisure idonee alla salvaguardia cautelare delle infrastrutture digitali, dei contenuti trasmessi e delle modalità di accesso tramite l'assunzione di protcolli efficienti di *cybersecurity,* che espongano alla luce le principali vunerabilità dei sistemi di protezione delle organizzazioni in modo da indirizzare l'allocazione delle risorse nell'interesse di tutti i soggetti coinvolti nella catena di approviggionamento dell'informazione. Da questo punto di vista la coesione di una moltitudine di, apparentemente, semplici iniziative , quali l'identificazione delle principali minacce del settore di appartenenza, l'assunzione delle necessarie contromisure e l'implementazione delle stesse tramite il progressivo monitoraggio dei fenomeni di attualità, costituisce una preziosa fonte di comprensione effettiva della condizione delle proprie strutture preventive, la quale favorisce la pianificazione e realizzazione di opportune strategie operative indirizzate dalla quantificazione della qualità dei dati da proteggere. Infatti, è fondamentale, per la prospettiva futura della trasformazione delle aziende all'indirizzo del mondo digitale, evincere il valore sostanziale dell'abbattimento dei costi correlati ad incidenti di sicurezza in grado di minare irretroattivamente la produttività di un ente imprenditoriale e del mercato nel quale esso esercita la propria funzione a seconda, chiaramente, delle relative dimensioni e criticità.

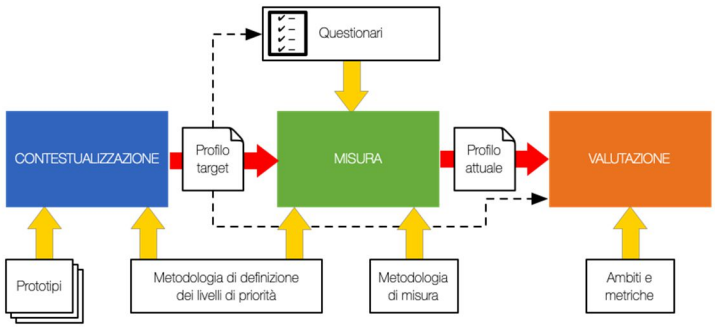


Figura 11: cybercesecurity assessment nel Framework Nazionale [57]

4.2 Cyber risk management

Nel corso del recente passato, in modo particolare in seguito alla propagazione della pandemia da Covid-19, si è assistito un incremento esponenziale dell'utilizzo di dispositivi tecnologici da parte di giovani studenti e professionisti affermati, legati

[57] Fonte: Framework Nazionale per la Cybersecurity e la Data Protection, 2015, "Metodologia per il cybersecurity assesment"

all'utilizzo di *smartphone* e *computer* quasi ininterrottamente durante la giornata tra l'esercizio dei propri doveri e l'intrattenimento nel tempo libero. Tali presupposti hanno attribuito un ruolo pivotale ad una disciplina peculiare quale il *cyber risk management*, incentrata rispetto all'osservazione ed al ridimensionamento dei rischi di natura cibernetica associati all'utilizzo di apparecchi multimediali. Dal punto di vista strettamente normativo, utile all'identificazione della tematica in un'ottica maggiormente estesa, a primo impatto, si fa riferimento alla normativa ISO 3100, intitolata "Linee guida per la Gestione del Rischio", riguardante l'ambito complessivo del *risk management*. Tale *stantard* di regolamentazione si qualifica come misura finalizzata al montenimento del valore all'interno delle organizzazioni, realizzato tramite la gestione del rischio, impiegata al fine di minimizzare l'effetto negativo delle minacce e ponendo i presupposti per lo sfruttamento delle opportunità di crescita e sviluppo. Il documento citato delinea la gestione del rischio come pratica essenzialmente caratterizzata dalla valutazione complessiva di un complesso imprenditoriale, valutandone l'ambiente circostante e le criticità interne tramite un processo di coinvolgimento delle parti interessate, in modo da acquisire consapevolezza delle vulnerabilità e, dunque, dei cambiamenti da intraprendere all'interno della fase applicativa di strategie mirate alla realizzazione di obiettivi peculiari. In tale ottica, il *risk management* si configura come pratica in progressiva evoluzione, essendo orientata da fattori culturali e settoriali correlati all'ente considerato e, in modo particolare, in maniera coordinata con le ulteriori componenti di *governance* della dirigenza. Si evidenzia l'importanza dell'integrazione di tale procedura rispetto alle ulteriori mansioni perseguite dall'azienda, in mododa poter porre in essere un sistema di pianificazione che coinvolga in modo chiaro ed opportuno i singoli dipendenti, incentivando il coinvolgimento da parte degli stessi al fine di implementare, ove necessario, i propri programmi tramite verifiche costanti del sistema di gestione del rischio. Pertanto la consultazione con il personale si profila come *step* imprescindibile nel rendere il sistema di gestione del rischio perennemente all'avanguardia, sostenendolo mediante strategie di comunicazione che eplicitino la sussistenza, la pericolisità e l'eventuale tollerabilità dei rischi, in modo tale da desumerne il potenziale impatto finanziario e/o operativo e, di conseguenza, sostanziando il processo di ponderazione del rischio atto a prioritizzare le minacce maggioremente dannose e

probabili, definendone il relativo trattamento e ripotordanone le principali caratteristiche nel corso della stesura del registro dei rischi da conservare presso l'organizzazione.

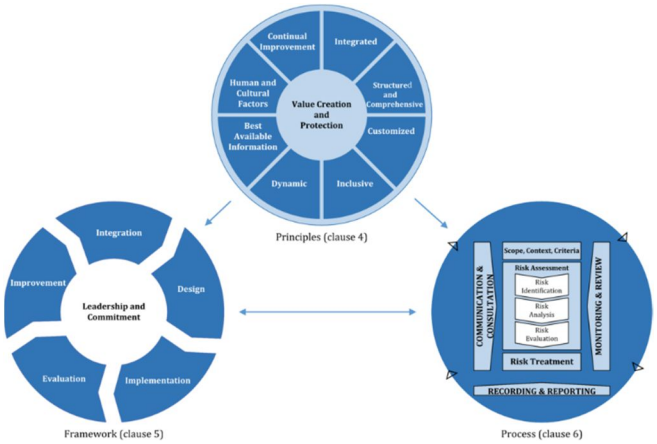


Figura 12: risk management secondo l'ISO 31000[58]

Focalizzando il discorso sino ad ora condotto, è possibile constatare come, nello specifico, il *cyber risk management* sia di recente oggetto di analisi tramite l'impiego di modelli semi-quantitativi, caratterizzati da costi moderati e da un tasso di oggettività piuttosto elevato. Tali strumenti prevedono l'impiego di particolari indici ottenuti tramite la valutazione di determinate variabili quali la frequenza degli attacchi, gli eventuali effetti rispetto agli *asset* e la stima approssimativa delle perdite attese, consentendo l'allocazione della fattispecie analizzata all'interno di distinte categorie di rischio, tarate mediante l'utilizzo di calcoli matematici. La collazione all'interno di una specifica classe di rischio evidenzia lo *status* della *governance* della struttura posta a tutela dei contenuti informatici di una certa organizzazione esposta generalmente a differenti tipologie di minacce di natura cibernetica, la cui classificazione si configura come essenziale al fine di dar luogo ad una gestione mirata, sostenuta tramite investimenti atti alla difesa preventiva di un complesso imprenditoriale, di un privato o di una istituzione, il cui costante monitoraggio per mezzo di piattaforme specializzate nella registrazione di dati funzionali alla redazione di *report* analitici, impiegati dal *top management* per la definizione di strategie improntate sia sul fronte economico che operativo. La procedura di gestione del rischio può essere resa ulteriormente efficace ed economica nella misura in cui le informazioni raccolte provengano da molteplici

[58] Fonte: International Organization for Standardization, Maggio 2018, "ISO 31000: Risk Management-Guidelines

dipartimenti aziendali o da attività imprenditoriali distinte in modo da favorire un procedimento di collaborazione mirata allo sviluppo di soluzioni innovative e garantite poste a tutela, in modo particolare, dei fattori di maggiore esposizione al *cybercrime*, ovvero l'individuo e la catena di approvigionamento. In tal senso si prospetta particolarmente rilevante il consolidamento di una cultura di *cybersicurezza* aziendale strutturata, sostenuta da solide *skills* ed *expertise* da parte del personale in modo da minimizzare la pericolosità di attacchi *hacker*, rispetto ai quali è opportuno che l'azienda sia coperta dal punto di vista strettamente finanziario. Nella prospettiva oggetto di analisi il ruolo del *cyber risk manager* si prospetta assolutamente centrale per le aziende moderne, intenzionate a tutelare la propria produttività attribuendo valore alla specializzazione dei propri professionisti nel minimizzare il potenziale impatto di crimini di natura informatica. Tale figura professionale risulta dotata di competenze peculiari e dettagliate in materia di *cybersecurity*, a differenza ad esempio di un comune *risk manager* necessariamente provvisto di conoscenze tarsversali in riferimento a diversi compartimenti dell'impresa come questioni assicurative, legali ed economiche. Inoltre, è fondamentale che il *cyber risk manager* sia pienamente consapevole delle vulnerabilità fronteggiate dall'ente che rappresenta, in modo da poter sviluppare sistemi di prevenzione idonei al ridimensionamento del rischio cibernetico ed all'orientamento del resto del personale, in modo da erigere capacità tali da fronteggiare responsabilmente possibili fasi di crisi digitale. Una curiosità in riferimento a questa figura è rappresentata dal fatto che, trattandosi di un ruolo particolarmente specializzato e piuttosto progressista all'interno del nostro paese, sia associata ad una retribuzione piuttosto redditizia, come testimoniato dal *report* di Glassdor[59], essendo a giudizio degli esperti una delle professioni maggiormente richieste da qui ai prossimi 5 anni, in quanto elemento chiave per il successo e la sopravvivenza dell'impresa, nonché componente pivotale per gestire efficientemente l'adozione della tecnologia come processo cardine della trasformazione aziendale come riportato all'interno del "Future of Jobs Report 2023", a cura del World Economic Forum. La tematica dell'onerosità dell'assunzione di tali individui costituisce una seria problematica di solvibilità per aziende di medie o piccole dimensioni, colmabile attraverso il coinvolgimento di vantaggi diversificati,

[59] Glassdor si configura come sito Internet e *social network* presso il quale dipendenti o ex dipendenti di una particolare organizzazione forniscono, in maniera anonima, informazioni riguardanti gli enti presso cui hanno fornito prestazioni lavorative.

come i premi di rendimento o le opportunità di apprendimento continuo, oltre alla garanzia di un ambiente lavorativo flessibile entro il quale possono enuclearsi possibilità di crescita rapida. Ulteriore complicazione è dettata dalla scarsità di competenze interne tali da esercitare le scelte più rimunerative per gli interessi specifici dell'azienda, la quale viene pertanto indotta a consultare agenzie di *recruiting* per una selezione del personale adeguata alle caratteristiche del proprio complesso organizzativo. Infine, si pone in evidenza che un ottimo *cyber risk manager* debba essere dotato di *hard skill*, tra le quali una dettagliata conoscenza delle risorse IT dell'infrastruttura aziendale per la definizione di strategie di prevenzione commisurate all'ente di riferimento, supportando adeguatamente quest'ultimo in caso di risposta ad iniziative di *cybercrime.* Allo stesso tempo è necessario che vengano poste in risalto anche *soft skills*, come la capacità di comunicazione efficace, funzionale alla collaborazione in *team* finalizzata all'integrazione tra gli obiettivi operativi e finanziari, associati alle finalità di sicurezza enfatizzando competenze interpersonali, pensiero analitico e risoluzione dei problemi.

4.3 Cyber insurance

Nel corso degli ultimi anni il percorso di transizione digitale intrapreso dalla stargrande maggioranza delle aziende ha attribuito particolare rilevanza ad uno strumento essenziale per la salvaguardia e la prevenzione da iniziative di cybercrime: la *cyber insurance.* Quest'ultima si configura come polizza assicurativa posta a tutela dei dispositivi rispetto a rischi di natura cibernetica, dinanzi ai quali si predispongono coperure di natura finanziaria nel caso in cui si realizzino fenomeni dannosi quali interruzione dei servizi, estorsioni informatiche o furto di dati. È doveroso segnalare come l'assicurazione cibernetica debba essere modellata in riferimento alle caratteristiche principali di una specifica tipologia di attività imprenditoriale, rispetto alle cui esigenze si sostanzia la variabilità di tali elementi in termini di costi e copertura. Parallelamente è opportuno analizzare le particolarità generalmente caratterizzanti le singole assicurazioni informatiche, la prima delle quali risulta essere la responsabilità civile, la quale tutela il soggetto assicurato nella fattispecie in cui egli sia ritenuto legalmente responsabile per danni cagionati a terzi in seguito a violazioni della sicurezza informatica. Altro elemento costituente è rappresentato dalla copertura dei costi di ripristino, a difesa dei sistemi informatici tramite la garanzia di riparazione dei

danni e pulizia delle reti violate, nonché, eventualemente, dei costi di consulenza informatica, l'acquisto di nuove componenti ed il ripristino dei dati. Inoltre, è previsto che lo strumento in esame sia posto a copertura delle perdite finanziarie dirette causate da violazioni della sicurezza *cyber* o da ulteriori casistiche digitali come le interruzioni dei servizi *online* o l'inattività aziendale causati da crimini digitali. In aggiunta, si fa riferimento alla copertura di eventuali estorsioni informatiche che si verificano nel caso di riscatti percepiti per la restituzione di dati ottenuti impropriamente tramite l'impiego di *virus* quali il *ransomware*, rispetto ai quali la *cyber insurance* di norma prevede il pagamento della cifra richiesta o di assistenza per la risoluzione della problematica citata. Ulteriore componente costitutiva è la protezione legale nella fattispecie di iniziative ispettive legate alla violazione della sicurezza digitale, circoscrivendo, potenzialmente, spese legali, multe e sanzioni deliberate dalle autorità competenti. Ultimo elemento comune alla maggioranza delle assicurazioni cibernetiche è l'offerta di servizi per la gestione delle crisi, al fine di disporre preventivamente modalità di risposta all'incidente, programmi di consulenza nell'ambito della comunicazione, ma soprattutto i mezzi per l'identificazione delle cause scatenanti ed i relativi piani di natura correttiva. Dunque, si evidenzia la rilevenza assoluta dell'acquisizione di una polizza assicurativa adatta ai requisiti di *performance* finanziaria o operativa di enti assolutamente eterogenei, essendo di recente ogni singola tipologia di azienda, in peculiari modalità, investita dall'affermazione della *digital economy*, risultando, quindi, coinvolte attività imprenditoriali dalle più svariate dimensioni, operanti in settori differenti quali la sanità, la finanza o la Pubblica Amministrazione. Nonostante la moltitudine di ragioni esplicitate in favore dell'adozione di una *cyber insurance*, quest'ultima può risultare eccessivamente onerosa per enti dotati di un *budget* limitato, analisi che risulta generalmente suffragata da una sottovalutazione o semplice incomprensione del rischio cibernetico conseguente alla mancata esperienza pregressa di iniziative di *cybercrime* ma anche, alternativamente, determinata da una eccessiva fiducia nei riguardi delle startegie di sicurezza digitale interne. In tale prospettiva, si verificano, poi, casistiche di distacco dall'assicurazione informatica motivate dall'assenza di competenze tali da apprenderne l'utilità o le procedure di applicazione, fattsipecie che possono indurre il personale ad acquisire un apporoccio diffidente rispetto a tale strumento trascurandone l'utilità, ragione per la quale diviene di

fondamentale importanza la regolamentazione di casi particolari, come nel settore finanziario ed ospedaliero, di imporre in termini normativi la conformità ad una specifica tipologia di *cyber insurance.* Infine si ricorda che la richiesta di indennizzo presso la compagnia assicurativa preveda l'illustrazione di documentazioni specifiche come richieste di riscatto, rapporti periodici ed analisi forensi sostenute tramite l'applicazione di programmi e tecnologie funzionali al perenne monitoraggio dello *status* di *cybersecurity* aziendale.

Secondo quanto riportato all'interno del rapporto Clusit 2022, nel corso di tale anno in Italia le imprese dotate di *cyber insurance* ammontavano soltanto al 27% del totale, dunque neppure un'azienda su tre si rivelava opportunamente strutturata in termini di prevenzionerispetto a possibili minacce di natura informatica. Bensì la statistica maggiormente preoccupante è rappresentata della mancanza di infrastrutture e strategie adeguate persino all'acquisizione di una polizza assicurativa nell'ambito cibernetico per il 40% delle attività imprenditoriali del paese, dato sostanzialmente preoccupante che pone in risalto l'impossibilità di predisporre condizioni tali da sostenere un livello di aggiornamento quantomeno concorrente rispetto a quello dei *cyber risks* a causa di sistemi informatici evidentemente sottodimensionati ed obsoleti. Si prospetta, dunque, imprescindibile fornire alle aziende evidenze tali da evincere l'importanza dell'omologazione a particolari requisiti di assicurazione cibernetica, in relazione alla quale, malgrado siano divenuti maggiormente gravosi i premi assicurativi, è fondamentale mettere in rilievo la convenienza di una strategia preventiva di gestione del rischio, in seguito alla valutazione effettiva degli esponenziali costi nel caso di violazione dei dati, ridimensionando le tempistiche di risposta e minimizzando l'impatto potenzialmente catastrofico della realizzazione di attacchi *hacker* in tal modo salvaguardando l'integrità finanziaria e reputazionale dell'impresa per la continuità e la sopravvivenza aziendale.

Secondo alcuni esponenti del settore, malgrado un progressivo ampliamento in riferimento all'adozione di sistemi di *cyber insurance* sul fronte pubblico e privato, le organizzazioni devono tutelarsi in maniera ulteriore ed ancor più dettagliata divenendo in grado di istituire programmi di risoluzione dei rischi cibernetici autonomamente tramite l'utilizzo di ulteriori forme di assicurazione informatica. All'interno del novero di quest'ultime si fa riferimento, in prima istanza, al *patching*, ovvero un sistema di

gestione delle *patch* di sicurezza, in sostanza aggiornamenti *software* tempestivi, conseguenti l'introduzione di funzionalità innovative, finalizzati alla riparazione di vulnerabilità inerenti i sistemi operativi, le applicazioni o ulteriori componenti del *software,* in modo tale da difendere le infrastrutture informatiche da azioni di *cybercrimine*, porteggendo in maniera efficiente le proprie risorse ed evitando, pertanto, prolungate ed onerose tempistiche di inattività in termini operativi. Ulteriore tipologia di azione preventiva dinanzi alle minacce di tipo informatico è certamente le formazione del personale, come palesato in modo irreprensibile all'interno del IBM Cyber Security Intelligence Index Report riguardante i dati raccolti nel corso del 2021, dove si qualifica la negligenza umana come principale fonte di violazioni della sicurezza informatica nel 95% dei casi registrati, motivazione per la quale sostanziali investimenti in termini di formazione si identificano utili alla definizione di contromisure rispetto ai più frequenti errori di salvaguardia dell'informazione, sostenendo l'impiego di password resistenti, il ridimensionamento dei casi di *phishing* e la difesa delle criticità essenziali per l'attività aziendale. Inoltre, si rivela di particolare importanza l'implementazione dei programmi di *disaster recovery*, incrementando la tempestività di reazione ad eventuali crisi informatiche mediante l'introduzione e l'avanzamento progressivo di procedure predisposte *ex ante* al fine di valutare opportunamente i gradi di responsabilità dei soggetti coinvolti ed i successivi piano risolutivi da mettere in pratica. Come epilogo, si fa capo alla necessità di potenziamento dei sistemi di *backup*, intesi come strumenti funzionali alla replica di particolari informazioni da impiegare nel caso di recupero o ripristino dei dati stessi a seguito di eventi inattesi o volontari come la manutenzione del sistema, pertanto tutelando gli *asset* di un peculiare complesso digitale seguendo modalità estremamente rapide e strategiche.

4.4 Cyber resilience

L'epilogo del tragitto in tal sede condotto in materia di prevenzione risulta essere ultimato tramite il riferimento alla *cyber resilience*, tematica di estrema rilevanza nell'individuare un ulteriore canale secondo cui consentire ad un complesso aziendale di apprendere dalle fasi di maggiore esposizione del proprio settore operativo e finanziario alle minacce informatiche, dando luogo ad una consapevolezza e competenza tali da garantire il prosieguo delle attività. Infatti, il concetto in esame si configura come la capacità di fronteggiare, con il minimo danno percepito, periodi potenzialmente critici

per un'attività , un privato o un istituto della Pubblica Amministrazione, la cui fluidità in termini produttivi risulta generalmente minata da fattispecie peculiari come congiunture economiche negative, calamità naturali e rischi di natura cibernetica, rispetto ai quali diviene fondamentale, dunque, istituire delle infrastrutture di sicurezza digitale tali da garantire la continuità aziendale mediante l'impiego delle conoscenze acquisite al fine di ridimensionare o evitare del tutto tempistiche di inattività. In questa prospettiva si pone in rilievo il beneficio che la resilienza cibernetica apporta in termini di *brand reputation*, ponendo in essere operazioni efficaci ed efficienti funzionali alla definizione di un vantaggio competitivo rispetto ai propri *competitor* tale da implementare il procedimento di *value creation*, in modo da delineare i presupposti per disporre di un'attrattiva *customer experience* che sia adeguata a conquistare la fiducia e la fedeltà del cliente. Quest'ultima, non a caso, può risultare facilmente dispersa in caso di ingenti perdite finanziarie, le quali si rivelano piuttosto frequenti nel caso di realizzazione di un'iniziativa di *cybercrime*, come riportato dal "Cost of a data Breach Report 2021" del Ponemon Institute[60], dove si evidenzia un impatto negativo medio in caso di violazione dei dati dall'ammontare di 4.24 milioni di dollari. In aggiunta a quanto appena illustrato, si evidenzia l'importanza dello *stakeholders engagement* nel processo di sviluppo delle misure di *cyber resilience* tramite il coinvolgimento diretto del personale e dei componenti della *supply chain*, tra i quali *partner* ed acquirenti, costituendo in tale ottica una struttura gnoseologica, deontologica ed empirica tale da progredire nella *governance* del rischio, respingendo gli attacchi *hacker* e tutelando gli *asset* infomrativi attraverso l'interazione tra meccanismi di controllo preventivi, ispettivi e correttivi. Pertanto, in questa direzione, si prospetta possibile dar luogo ad un bilanciamento tra *cyber risks* ed eventuali opportunità da cogliere, valutando l'economicità e, di conseguenza, la fattibilità di specifiche iniziative di prevenzione o, eventualmente, di tecnologie per il monitoraggio e la risposta a breve termine rispetto ad eventuali criticità di matrice digitale. La composizione idonea di un modello efficiente di *cyber resilience* presenta una struttura analoga al ciclo di vita delineato dall' Information Technology Infrastructure Library, anche noto come ITIL, ente impegnato

[60] Il Ponemon Institute è un ente indipendente impegnato nella ricerca e nello sviluppo in materia di gestione responsabile dell'informazione e di pratiche di *management* della *privacy* per aziende e governi. In modo particolare, annualmente in collaborazione con IBM l'organizzazione fornisce uno studio riguardante i *data breach*.

nella fornitura di linee guida nel settore dell'IT *Service Management*. Dunque, è previsto, in primo luogo, la definizione di una particolare strategia che consenta l'esaltazione delle principali criticità dell'organizzazione ed al contempo l'identificazione delle vulnerabilità maggiormente impattanti, in tale ottica dando luogo ad una precisa definizione degli obiettivi cui l'ente aspira. Una volta delineato il fine ultimo dell'attività diviene essenziale progettare oculatamente peculiari dipartimenti di controllo, analizzando per ciascuno le competenze necessarie ed individuando, quindi, soggetti predisposti all'assunzione di *leadership* e conseguenti responsabilità. Vi è, in seguito, una fase di transizione che conduce all'osservazione della componente operativa, nel corso della quale si sostanzia il monitoraggio e l'avanzamento delle procedure di gestione e prevenzione di eventi accidentali o intenzionali, al fine di verificarne l'effettiva efficienza. Tale complesso lineare di azioni permette di evincere le modifiche da apportare, traendo beneficio dall'apprendimento empirico, utile all'individuazione dei compartimenti aziendali da implementare e rafforzare. In modo ancor più approfondito, è possibile precisare come la resilienza cibernetica possa essere orientata da un duplice approccio: per processi, secondo il quale quest'ultimi sono considerati come attività aventi un particolare obiettivo e coordinate tra loro al fine di garantire la *business continuity*, che viene testata ipotizzando l'indisponibilità di specifiche informazioni, valutandone gli effetti in riferimento alle singole componenti dell'organizzazione; per servizi, il quale prevede la condivisione e l'applicazione di risorse e conoscenze per più di un singolo processo, motivazione per la quale è considerato essere veicolo di maggiore totalità di servizio nei confronti del cliente, attribuendo, peraltro, maggiore dettaglio nella sperimentazione delle conseguenze prodotte da eventuali calamità potenzialmente dannose. Appartenente a tale ultima metodologia risulta essere il *customer journey*, caratterizzato dalla valutazione della fase in cui l'acquirente interagisce con l'azienda al fine di usufruire di un particolare servizio offerto da quest'ultima, osservandone, in maniera scrupolosa, la capacità di apportare soddisfazione al cliente anche nell'eventualità di possibili congiunture sfavorevoli, salvaguardando, dunque, un livello minimo di operatività da parte dell'ente. Proiettando lo sguardo analitico sino ad ora impiegato, si ritiene doveroso evidenziare come in attualità si evidenzi una forbice di *cyber inqueity* in Italia, costituita dall'ampio divario che si sta costituendo tra complessi organizzativi virtuosi in termini di resilienza

digitale ed attività dotate di minori *budget* o competenze, le quali presentano come drastico effetto l'impreparazione dinanzi ad eventuali minacce informatiche e, difatti, l'aleatorietà della propria sopravvivenza. In tale prospettiva, si identificano imprescindibili al processo di transizione digitale i fondi predisposti dall'Unione Europea aventi come obiettivo la realizzabilità dei programmi pubblici e privati per massimizzare l'armonizzazione in termini di sicurezza e prevenzione cibernetica, richiedenti sostanziose capitalizzazioni, come nel caso del programma Digital Europe, veicolo di un finanziamento da oltre 7.5 miliardi di euro per l'adozione di moderne tecnologie digitali nell'economia e nella società, stimolando in tal senso il progresso dell'innovazione informatica.

5. Quantificazione cyber risk

Un fenomeno aleatorio ed in continuo mutamento come il rischio cibernetico richiede, al fine della realizzazione di un efficiente ridimensionamento, non soltanto l'acquisizione di una vasta varietà di competenze di carattere gnoseologico e deontologico pertinenti il settore della *cybersecurity*, ma necessita di procedimenti funzionali alla ricerca di oggettività in un contesto così dinamico ed imprevedibile. Per tale motivazione si configura di estrema rilevanza il processo di *cyber risk quantification*, metodologia desunta dal variegato ambito del *risk management* ed impiegata in modo da porre in essere valutazioni di carattere analitico in riferimento alla potenziale esposizione di attività imprenditoriali, istituzionali o privati alle minacce di matrice informatica, indicizzando quest'ultime al variare di componenti quali l'eventuale impatto economico e reputazionale, la probabilità di compimento e l'applicazione di misure di prevenzione e tutela associate alla tipologia di rischio digitale in esame. Tale pratica si rivela fondamentale in quanto rappresenta una misura di salvaguardia delle informazioni ulteriore, pertanto utile ad incentivare il tasso di sicurezza e resilienza all'interno degli enti in esame, ponendo in tal modo barriere ulteriori per gli individui ed i relativi diritti o interessi, ma, soprattutto, per le organizzazioni di dominio privato o pertinenti la Pubblica Amministrazione, capaci mediante questi indicatori matematici di fornire una direzione precisa alle scelte dirigenziali, dirette ad esempio alla massimizzazione dell'investimento in termini di

ROI[61]. La definizione delle iniziative di *cybercrime* rispetto alle quali porre in essere maggiore misure cautelari risulta delineata gerarchicamente all'interno di specifici piani di *remediation,* ottenuti in seguito alla quantificazione di strumenti derivanti dal monitoraggio standardizzato del perimetro interno ed esterno al complesso aziendale in analisi in ossequio all'opportuna *compliance* nei riguardi di requisiti richiesti da normative nazionali, transfrontaliere o internazionali. In riferimento all'ambito interno si ritiene di particolare utilità l'adozione di un approccio *inside-out* per la definizione di indici di rischio cibernetico, inerenti peculiari domini di natura tecnologica appartenenti ad aree di aleatorietà scriminate dagli *standard* internazionali come GDPR e NIST. Parallelamente, il contesto esterno richiede un modello *outside-in*, in base al quale si pone in essere la valutazione delle principali vulnerabilità riguardanti *asset* collegati ad un dato dominio. In modo ancor più approfondito, si ricorda come il processo matematico in analisi debba osservare con particolare meticolosità l'esposizione al *cyber risk* derivante dagli *endpoint*, intesi come uno dei *target* di maggior criticità nello sviluppo dell'intera *supply chain*, dunque ponendo come oggetto del monitoraggio non soltanto il personale dell'organizzazione, ma anche fornitori, *partner* e clienti, veicoli di catastrofiche minacce cibernetiche.

5.1 Introduzione al frequency-severity method

Il modello selezionato ai fini della quantificazione del rischio cibernetico è definito *frequency-severity,* binomio che letteralmente sta per metodo frequenza-gravità, dove quest'ultima può essere interpretata come perdite di matrice monetaria o economica. Si prospetta, pertanto, indispensabile fornire una precisa definizione della tipologia di approccio analitico individuata, secondo la quale il modello *frequency-severity* si identifica innanzitutto come una procedura di matematica attuariale, inerente a fattispecie che possono essere incerti nel sostanziarsi o nella tempistica secondo cui verificarsi, analizzandone l'intensità e la frequenza tramite l'impiego di risultanze statistiche utili all'implementazione delle semplici probabilità. In modo specifico, l'*iter* numerico oggetto della corrente analisi si configura come funzionale alla

[61] Il Return on Investment, anche noto come indice di redditività del capitale investito, è dato dal rapporto tra il risultato operativo ed il capitale investito netto, fornendo indicazioni in riferimento all'efficienza economica della gestione caratteristica, ovvero la sezione del Conto economico inerente costi e ricavi riguardanti la gestione tipica per la realizzazione dell'oggetto dell'impresa.

determinazione della quantità attesa di realizzazioni di particolari fenomeni e del relativo costo medio sostenuto da soggetti definiti "*insurers"*, dunque in riferimento al tema in analisi riconducibili ai sistemi o responsabili di *cybersecurity*. L'applicazione del procedimento descritto prevede l'utilizzo di dati relativi al passato per il calcolo del numero medio di casi verificati e del costo medio di ognuno di essi, per poi porre in relazione queste due grandezze. Dunque, il concetto di *frequency* indica il numero di realizzazioni attese da parte dell'*insurer* entro un certo periodo di tempo ed è dato dal rapporto tra il numero di realizzazioni o violazioni di un determinato fenomeno e l'esposizione al rischio analizzato, pertanto maggiore è la frequenza più il fenomeno in esame si verificherà frequentemente. Parallelamente il termine *severity* è riferito in modo dettagliato al costo derivante dal realizzarsi di un particolare evento, come le perdite derivanti dall'esecuzione di un'iniziativa di cybecrime, cifra che viene generalmente calcolata come rapporto tra le perdite riscontrate ed il numero di fenomeni registrati, indice poi confrontato al costo medio ottenuto tramite l'analisi degli *historical data*, per cui un livello di *severity* risulta elevato nel caso in cui risulti maggiore rispetto al costo medio e poco impattante quando è inferiore a quest'ultimo. Al fine di garantire la comprensione effettiva ed esaustiva dei concetti appena descritti si fornisce un semplicissimo esempio pratico: le assicurazioni automobilistiche, riguardo le quali è possibile constatare in riferimento alla densità abitativa di un determinato luogo geografico come in correlazione positiva rispetto alla frequenza di incidenti e negativa nei riguardi della gravità degli stessi. Difatti, si evince in tal prospettiva che un contesto urbano densamente popolato sarà probabilmente oggetto di sostanziose congestioni stradali, causa di sinistri numerosi, ma relativamente poco cari, a differenza di un ambito prettamente rurale, dotato di popolazione largamente distribuita, all'interno del quale si ipotizza una frequenza inferiore di incidenti, bensì una rilevanza maggiore in termini economici e di sanità, dettata da velocità superiori su strade più libere. A conclusione dell'excursus analitico in analisi è previsto il prodotto tra *frequency* e *severity* al fine di ottenere le perdite attese in futuro. Si ritiene rilevante porre in rilievo il fatto che la dipendenza dell'approccio in analisi da dati relativi al passato ha come logica conseguenza una minore influenza posta in essere da eventuali periodi maggiormente recenti caratterizzati da una significativa volatilità, per tale motivazione rivelandosi meno alterato in seguito ad eventuali fluttuazioni di quest'ultima. Dunque il

calcolo del *frequency-severity index* si rivela prezioso nella quantificazione di eventuali perdite derivanti ad esempio da violazioni della *cyber insurance,* in modo da stimare in modo analitico la quantità di riserve da risparmiare ogni singolo esercizio al fine di garantire la copertura di potenziali future spese, manifestandosi, quindi, come un metodo fondamentale per la programmazione di mirate strategie finanziarie, oggetto di costante monitoraggio al fine di operare, ove necessario, le opportune modifiche in termini di costi o risparmi. Il *frequency-severity approach* si considera di particolare rilevanza in quanto maggiormente dettagliato e preciso rispetto ad altri modelli per la definizione dei costi attesi in riferimento all'ambito *insurance* come il *loss ratio method* e l'*extended loss ratio method*, entrambi particolarmente più semplici ed approssimativi, caratteristiche potenzialmente veicolo di minore copertura e prevenzione finanziaria in termini di riserve e, di conseguenza, motivo di maggiore esposizione al rischio di instabilità ed insolvibilità futura conseguente ad eventuali calamità negative, tra cui la realizzazione di operazioni di *cybercrime.*

Nell'intento di fornire una prima formulazione definita in riferimento al *frequency-severity method* si intende, anzitutto, far riferimento ad un assicuratore, il quale è incaricato di tutelare un particolare *database,* posto in capo ad uno specifico *policyholder,* in modo da monitorarne in modo costante all'interno di un predeterminato lasso di tempo le relative *closed claims*, ovvero segnalazioni o violazioni, valutate opportunamente mediante l'impiego di una procedura di carattere stocastico, privato di un preciso riferimento temporale relativo all'avvio di una determinata *policy* e mirato ad una duplice finalità: il *ratemaking*[62] e la *reinsurance*[63]. Dunque la notazione che si ritiene necessario fornire, in riferimento alle singole *policy* $\{i\}$, le variabili osservabili risultano essere:

- N_i, inteso come numero di *claims*
- y_{ij}, dove $j = 1, \dots, N_i$, riguarda la perdita conseguente ad ogni singola *claim*
- $S_i = y_{i1} + \cdots + y_{iN_i}$, ovvero il valore complessivo delle singole *claims*

Si suppone inoltre per ipotesi che l'insieme $\{y_{ij}\}$ sia vuoto nel caso in cui $N_i = 0$.

[62] Il *rate-making*, anche noto come *insurance pricing*, consiste sostanzialmente in un processo di definizione dei tassi forniti dalle compagnie assicurative, in modo da garantire trasparenza ed adeguatezza all'interno di un settore altamente competitivo come quello delle assicurazioni.

[63] La *re-insurance*, anche conosciuta come riassicurazione finanziaria, indica il procedimento secondo il quale una data compagnia assicurativa si libera di una parte del rischio assunto dai propri clienti, attribuendo quest'ultimo ad un'altra di secondo livello, definita pertanto riassicuratore.

Nel caso in cui si faccia, invece, riferimento ad un particolare esercizio contabile, ad esempio della durata di un singolo anno, il campionamento di potenziali variabili si rivela essere costituito come segue:

- S_i,in modo che sia disponibile esclusivamente il valore aggregato delle perdite, come nella fattispecie pratica di analisi dei costi derivanti da assicurazioni commerciali
- (N_i, S_i), in modo che sia reperibile sia la numerosità che il peso delle perdite complessive
- $\left(N_i, y_{i1}, \dots, y_{iN_i}\right)$, in modo che si possa analizzare in modo dettagliato le informazioni riguardanti ogni singola *claim*, in modo da poter interpretare opportunamente le varie perdite ad esse relative. Si consideri $y_i = \left(y_i, \dots, y_{N_i}\right)'$ come il vettore delle singole perdite derivanti da *claims*.

A tal punto al fine di ricondurre la distribuzione a componenti di *frequency* e *severity*, si impiegano concetti pertinenti la probabilità condizionata[64]. Dunque impiegando il terzo modulo, si rende possibile eliminare la variabile $\{i\}$ in modo tale da scomporre la distribuzione delle variabili dipendenti come segue:

$$f(N, y) = f(N) \times f(y|N)$$

$$joint\ distribution = frequency \times conditional\ severity$$

dove $f(N, y)$ indica la *joint distribution*, anche nota semplicemente come distribuzione congiunta[65], di (N, y). Come evidente dalla formula sopra esplicitata, tale distribuzione congiunta è data dal prodotto di due componenti:

- *frequency*, in quanto $f(N)$ *indica* la probabilità di ottenere N *claims*
- *conditional severity*, dato che $f(y|N)$ la densità condizionata del vettore y dato N

Il secondo modulo presenta una struttura analoga, l'eccezione è costituita dal fatto che il vettore delle perdite individuali y è sostituito dalla perdita aggregata S. Inoltre, è possibile scomporre la prima formula rimuovendo lo *zero event* mediante la notazione $r_i = I(S_i > 0)$ relativamente alla *frequency* e ponendo come condizione per la *severity* $r_i = 1$.

---

[64] Per probabilità condizionata, anche nota come probabilità a posteriori, si intende la probabilità che si verifichi un evento E, definito condizionato, sapendo che un secondo evento F si è già realizzato, per questo detto condizionante, la cui probabilità è necessario sia diversa da zero. Si indica con $P(E|F)$.

[65] La distribuzione congiunta di due variabili aleatorie X e Y, definite all'interno del medesimo spazio di probabilità, è data dalla distribuzione di probabilità associata al vettore (X, Y). Essa si definisce bi-variata nel caso in cui si considerino due sole variabili, multivariata nel caso in cui siano più di due variabili.

In tale prospettiva l'impiego della probabilità condizionata al fine di realizzare un processo di decomposizione dei moduli si rivela un metodo di particolare utilità nell'individuare rapporti di dipendenza tra le variabili, costituendo, dunque, un'ottima base analitica per lo sviluppo di un progetto con finalità pratiche, discostandosi dalla richiesta di indipendenza delle componenti di *frequency* e *severity* come tradizionalmente avviene in ossequio alla letteratura delle scienze attuariali. Quindi impiagando la distribuzione congiunta $f(N, y)$ è possibile interpretare il concetto di dipendenza secondo molteplici varianti tra cui la considerazione di una variabile latente avente impatto su frequenza e gravità o le copule per correlazioni non lineari.
Una tipologia di approccio prettamente di carattere empirico e costituita da componenti di *frequency* e *severity* è certamente il modello lineare generalizzato, meglio noto come GLM, dotato di una flessibilità tale da costituire una sorta di congiunzione tra modelli improntati sulla frequenza ed altri incentrati rispetto alla gravità. Il GLM si differenzia dal classico modello lineare nell'ambito della regressione lineare, caratterizzato da una variabile endogena distribuita in modo normale, in quanto caratterizzato dalla presenza di una variabile endogena casuale la cui distribuzione può essere, tra le altre, esponenziale, di Poisson o binomiale. Pertanto, si introduce una generica variabile dipendente y_i, al netto di specifica se essa rappresenti una componente di *frequency* o *severity*, si ragiona in termini logaritmici in riferimento alla funzione media, che risulta essere $E\ y_i = \exp\ (x_i'\beta)$. In particolari condizioni, la funzione media risulta correlata proporzionalmente alla variabile *exposure*, o esposizione, indicata nel modo seguente E_i, la quale al fine di essere integrata necessita la definizione della variabile esplicativa $\ln E_i$ ed attribuendo al corrispondente coefficiente di regressione il valore unitario, tale concetto è noto come *offset.* In tale ottica la funzione risultante è data da:

$$ln\mu_i = lnE_i + x_i'\beta$$

Inoltre si evince come il metodo multivariato del GLM sia generalmente impiegato in casi pratici, in quanto la generalizzazione del modello lineare è ultimata al fine di favorire l'adattamento e l'inserimento di più fattori all'interno di una certa mole di dati, ponendo particolare attenzione alla variabilità in seguito all'introduzione dell'*exposure*. Il concetto di esposizione è funzionale al calibrare la rilevanza di eventuali perdite in termini finanziari e, secondo una prospettiva di natura prettamente statistica, si rivela essere una variabile di *rating* di un'importanza tale da essere considerata all'interno di

tale settore uno degli strumenti principali essendo spesso impiegato per la definizione e composizione di premi assicurativi o potenziali perdite. Si evidenzia come l'*exposure* debba essere caratterizzata da specifiche peculiarità, tra le quali si annovera, in primo luogo, l'accuratezza analitica nella quantificazione della vulnerabilità alla potenziale perdita, in modo tale da rendere quest'ultima chiaramente esplicitata, nella fase di istituzione della *policy*, all'indirizzo di *insurer* ed *insured* al netto di manipolazioni, garantendo, peraltro, la valutazione degli antecedenti livelli di esposizione nel settore di riferimento, nonché, per particolari attività, l'individuazione di una proporzionalità rispetto all'inflazione, così minimizzando la sensibilità dei tassi ad eventuali fluttuazioni del valore della moneta nel corso del tempo. Si puntualizza come, generalmente, nel caso di utilizzo di un *frequency-severity method*, il concetto di esposizione si rivela essere proporzionalmente correlato alla frequenza, a differenza della variabile gravità rispetto ad esso indipendente. L'eccezione di quanto appena enunciato è rappresentata dai particolari settori, precedentemente citati, i quali presentando una particolare tipologia di *exposure* proporzionale all'inflazione presentano un andamento peculiare essendo quest'ultima proporzionale alla *severity*, ma non alla *frequency*.

5.2 Definizione teorica dei modelli frequency-severity selezionati

In tale sezione si intende partire dalla prima delle tre variabili dipendenti introdotte nel paragrafo precedente, ove l'unica oggetto di interesse risulta essere la quantità totale di *claims* rispetto ad una specifica *policy*, considerando, in prima istanza, *dataset* caratterizzati in larga parte dall'assenza di *claims*, corrispondente in termini numerici al valore nullo. Al fine di analizzare opportunamente quest'ampia porzione di *claims* dal valore zero, si introduce il *two-part model*, tipologia specifica di approccio *frequency-severity* costituita da una duplice sezione, la prima delle quali inerente all'eventualità di realizzazione di un particolare evento, mentre la seconda riguardante il peso e la rilevanza di quest'ultimo. In modo dettagliato, le variabili costituenti tale procedura risultano essere le seguenti:

- r_i, intesa come variabile binaria espressione della verifica o meno della *claim*
- i, riguardante la quantità di componenti dotate di *insurance*
- y_i, inerente il valore della *claim*

Si pone in rilievo come l'utilizzo del *two-part model* prevede, anzitutto, l'osservazione della *frequency*, rispetto alla quale risulta condizionata la *severity:*

- Dunque si prevede l'impiego di un modello di regressione binario con r_i variabile dipendente e x_{1i} inerente alle variabili esplicative, il cui corrispondente gruppo di coefficienti di regressione è rappresentato da β_1. Il modello *logit* è un tipico esempio di approccio di regressione binaria.
- Nell'ipotesi in cui $r_i = 1$, si sviluppa un modello di regressione con variabile dipendente y_i ed in qualità di insieme di variabili esplicative x_{2i}, il cui corrispondente gruppo di coefficienti di regressione è dato da β_2. Una tipologia classica di *severity model* è rappresentata dalla funzione gamma di *link* logaritmico.

Si ritiene doveroso precisare come possano sussistere sovrapposizioni in termini di variabili esplicative, le quali possono rilevarsi appartenenti sia ad x_1 che a x_2. Inoltre, generalmente, si assume che β_1 e β_2 risultino privi di correlazioni di modo che la probabilità congiunta si configuri suddivisa in due componenti, il cui andamento si sviluppa separatamente.

Ulteriore metodologia è rappresentata dal *tobit model,* secondo il quale gestire un'ampia quantità di valori nulli all'interno di uno specifico *dataset* è realizzare l'assunzione che la variabile dipendente sia censurata a zero, introducendo dunque un modello di regressione censurata, secondo la quale è previsto il riferimento ad una variabile inosservata o latente y^*, che, per ipotesi, presenta un modello di regressione lineare del seguente formato:

$$y_i^* = x_i'\beta + \varepsilon_i$$

Dunque le possibili risposte risultano essere consurate o limitate in quanto si osserva $y_i = max(y_i^*; 0)$. Generalmente il modello è applicando assumendo una distribuzione normale per i disturbi ε_i ed impiegando il metodo della massima verosimiglianza[66].

L'estensione di tale modello si configura funzionale al limitare la variazione di componenti sensibili al mutare delle *policy*, motivazione per la quale all'interno dei modelli di natura attuariale si definisce d_i come dato deducibile che varia a seconda del *policyholder* di riferimento.

Malgrado l'utilità di tale approccio, è necessario evidenziarne gli aspetti negativi, primo dei quali il fatto che si basi sull'assunzione di distribuzione normale della risposta

[66] Il metodo della massima verosimiglianza è una procedura matematica applicata in statistica al fine di ottenere uno stimatore, ovvero una funzione che associa ad ogni possibile campione un certo valore del parametro in esame. Tale approccio è definito dalla probabilità di riscontrare una specifica realizzazione campionaria, la quale risulta essere condizionata dai valori assunti dai parametri statistici stimati.

latente, nonché l'evidenza che un'unica variabile latente orienti decisamente sia la magnitudine della risposta che la censura. A tal proposito, si annoverano molteplici congiunture all'interno delle quali la limitazione del valore costituisce una scelta o iniziativa, parallelamente condotta rispetto alla magnitudine.
Variando la prospettiva e mirando quest'ultima rispetto alla seconda e terza tipologia di variabili dipendenti osservate nel primo paragrafo di tale capitolo, a partire dalla seconda variante illustrata, in riferimento alla quale si annoverano la quantità e la gravità in termini aggregati delle *claims,* ovvero (N_i, S_i). Dunque, il modello *frequency-severity* a due *step* assume la seguente struttura:
- Si impiega un modello di regressione per dati di conteggio, ove N_i costituisce la variabile dipendente e x_{1i} rappresenta il gruppo di variabili esplicative, il cui corrispondente insieme di coefficienti di regressione è dato da β_1. In tal caso un'applicazione pratica è riconducibile al modello di Poisson o di Pascal.
- Ipotizzando $N_i > 0$, si utilizza la procedura GLM con variabile dipendente S_i/N_i e x_{2i} come insieme di variabili esplicative, il cui relativo gruppo di coefficienti lineari è dato da β_2. Modelli esplicativi in questa fattispecie risultano essere la regressione gamma di collegamento logaritmico dotata di un parametro di dispersione proporzionale a $1/N_i$.
Per quanto concerne la terza tipologia di variabili dipendenti di cui sopra, si analizzano le singole *claims* disponibili tramite il vettore $y_i = (y_{i1}, \dots, y_{iN_i})'$. Nella casistica in analisi, il modello segue questo *diktat*:
- il primo *step* risulta essere il medesimo in riferimento al modello di regressione per dati di conteggio
- il secondo passaggio inerente alla *severity* varia, in quanto si assume che $N_i > 0$, bensì in tal ottica si seleziona un modello di regressione con variabile dipendente y_i ed insieme di variabili esplicative x_{2i}, alle quali risulta associato il gruppo di coefficienti lineari β_2. I modelli riconducibili a quanto appena enunciato sono la regressione lineare con *claims* logaritmiche in qualità di variabili dipendenti, la regressione gamma e modelli lineari misti, per i quali è previsto l'utilizzo di un'intercetta *subject-specific* finalizzata a rispettare l'eterogeneità tra *policyholders*.
L'excursus sino ad ora condotto in materia di modelli *frequency-severity*, induce alla valutazione dell'approccio Tweedie GLM, frutto dell'unione tra distribuzioni di natura

continua, come la gamma e la normale, ed altre di tipo discreto, tra cui la binomiale e la Poisson. Tale modello è caratterizzato da un'ampia quantità di *claims* dal valore nullo ed una componente continua prevista per il totale dei valori positivi in riferimento ad una o più *claims*. Dunque, la distribuzione in esame si configura come una formula di sommazione di Poisson riguardante variabili gamma casuali. In modo ancor più specifico, si assume che N sia dotata di una distribuzione di Poisson con media λ e che rappresenti il numero di *claims*, mentre y_i costituisce una sequenza di variabili indipendenti ed identicamente distribuite, pertanto non dipendenti da N e ciascuna provvista di una distribuzione gamma con parametri α e γ, in modo da simboleggiare il peso delle *claims*. Pertanto, $S_N = y_1 + \cdots + y_N$ si riconosce come sommazione di Poission in riferimento a variabili gamma. Al fine di comprendere in modo esaustivo la natura mista della distribuzione Tweedie, si ricorda anzitutto come il calcolo della probabilità di *zero claims* è data da:

$$Pr(S_N = 0) = Pr(N = 0) = e^{-\lambda}$$

La funzione di distribuzione può essere ottenuta impiegando valori attesi condizionati, come segue:

$$Pr(S_N \leq y) = e^{-\lambda} + \sum_{n=1}^{\infty} Pr(N = n)\,\Pr(S_n \leq y) \quad con\ y \geq 0$$

Considerando che la somma di variabili gamma indipendenti ed identicamente distribuite fornisce come risultato una variabile gamma, si evince come S_n, non S_N, sia caratterizzata da una distrubuzione gamma di parametri $n\alpha$ e γ. Pertanto, per $y > 0$, la densità della distribuzione Tweedie risulta essere la seguente:

$$f_s(y) = \sum_{n=1}^{\infty} e^{-\lambda} \frac{\lambda^n}{n!} \frac{\gamma^{n\alpha}}{\Gamma(n\alpha)} y^{n\alpha-1} e^{-y\gamma}$$

Tale ultima formula, ad una prima analisi, può risultare apparentemente priva delle caratteristiche tipiche delle funzioni lineari esponenziali. Dunque al fine di dimostrare tale relazione, si introducono attese reiterate per il calcolo dei momenti statistici[67]:

$$E\ S_N = \lambda \frac{\alpha}{\gamma} \quad e \quad VarS_N = \frac{\lambda\alpha}{\gamma^2}(1 + \alpha)$$

[67] Il momento statistico è uno strumento impiegato al fine di analizzare le caratteristiche di una particolare distribuzione; dunque, supponendo X come variabile casuale di interesse, i momenti sono ottenuti come valori attesi di X. Sono utili all'interpretazione dei dati e tra i più comuni si annoverano la media, la varianza e la simmetria.

A tal punto si introducono i parametri $\mu, \phi\ e\ \rho$ mediate le seguenti relazioni:

$$\lambda = \frac{\mu^{2-\rho}}{\phi(2-\rho)}, \quad \alpha = \frac{2-\rho}{\rho-1}, \quad e \quad \frac{1}{\gamma} = \phi(p-1)\mu^{p-1}$$

Dunque riprendendo inserendo i parametri appena introdotti all'interno della funzione precedentemente esplicitata come densità della distribuzione Tweedie:

$$f_S(y) = \exp\left[-\frac{1}{\phi}\left(\frac{\mu^{2-\rho}}{2-\rho} + \frac{y}{(\rho-1)\mu^{\rho-1}}\right) + S(y,\rho,\phi)\right]$$

All'interno di tale formula si fa notare quanto segue:

$$expS(y,\rho,\phi) = \frac{1}{y}\sum_{n=1}^{\infty} \frac{\left(\frac{y^{\alpha}}{\phi^{1/(\rho-1)}(2-\rho)(\rho-1)^{\alpha}}\right)^{n}}{n!\,\Gamma(n\alpha)}$$

Dunque si può concludere che la distribuzione tweedie è parte della famiglia delle distribuzioni lineari esponenziali. Una semplice conclusione dimostra che:

$$E\ S_N = \mu \quad e \quad Var\ S_N = \phi\mu^{\rho}$$

dove è opportuno precisare che $1 < \rho < 2$. Pertanto, si può concludere come la distribuzione Tweedie possa essere considerata come una sorta di scelta intermedia tra le distribuzioni Poisson e gamma.

Infine, si precisa come all'interno dell'approccio Tweedie GLM, è possibile impiegare $x_{i,T}$ come insieme di covarianze, il cui relativo gruppo di coefficienti lineari è simboleggiato come β_T, ipotizzando la seguente correlazione di natura logaritmica $\mu_i = exp(x'_{i,T}\beta_T)$. Per quanto concerne la specifica della funzione di distribuzione, non è possibile formulare un'espressione chiusa, bensì è possibile computare quest'ultima in maniera diretta e pratica mediante l'utilizzo della funzione `ptweedie` della piattaforma R.

Alternativamente al modello Tweedie è possibile dar luogo all'applicazione di un approccio caratterizzato dall'interpretazione di componenti *frequency-severity*, impiegando per la frequenza un modello di regressione di Poisson al fine di registrare il numero di *claims* in riferimento all'i-esimo individuo, ottenendo dunque analiticamente la funzione di collegamento logaritmica che segue:

$$N_i \sim Poisson(\lambda_i) \quad \lambda_i = exp(x'_{i,F}\beta_F)$$

dove $x'_{i,F}$ rappresenta un insieme di covarianze impiegate nel modello di frequenza, mentre β_F costituisce il correlato gruppo di coefficienti di regressione.

Parallelamente, per quanto riguarda la componente *severity* si può selezionare una regressione gamma associata ad una funzione di collegamento logaritmico al fine di stabilire formule analitiche per il calcolo delle perdite per singola *claim,* così ricavando:

$$y_{ij} \sim gamma(\alpha, \gamma_i), \quad dove \quad \frac{\alpha}{\gamma_i} = E \quad y_{ij} = exp\left(x'_{i,S}\beta_S\right)$$

per $j = 1, \dots, N_i$. Quindi, come esplicitato nel caso della procedura inerente all'elemento *frequency*, $x'_{i,S}$ costituisce l'insieme di covarianze di riferimento all'interno dell'approccio riguardante la *severity*, così come β_S simboleggia l'associato gruppo di coefficienti di regressione. Si evince, pertanto, come i modelli *frequency* e quelli *severity* non necessitano dell'applicazione delle medesime covarianze.
Al fine di ottenere il valore della perdita aggregata è essenziale porre in relazione ed unire le componenti di *frequency* e *severity* come illustrato:

$$S_{N,i} = y_{ij} + \cdots + y_{i,N_i}$$

tale espressione ha come media quanto segue:

$$E\ S_{N,i} = E\ N_i \times E\ y_{ij} = exp\left(x'_{i,F}\beta_F + x'_{i,S}\beta_S\right)$$

mentre la relativa varianza è ottenuta analiticamente come:

$$VarS_{N,i} = \lambda_i \frac{\alpha}{\gamma_i^2}(1+\alpha) = \exp\left(x'_{i,F}\beta_F + 2x'_{i,S}\beta_S + ln(1 + 1/\alpha)\right)$$

Si pone in rilievo l'evidenza che all'interno di un modello *frequency-severity*, i due parametri λ_i e γ_i fluttuano al variare dell'elemento i. Dunque nel caso in cui si intenda computare la distribuzione della funzione è possibile fare ricorso al modello Tweedie per la variabile S_N applicando la funzione `ptweedie` presente nel *software* R, ovvero invertendo le relazioni precedentemente esplicate, in seguito all'introduzione dei parametri $\mu, \phi\ e\ \rho$, nel seguente formato:

$$\rho = \frac{\alpha + 2}{\alpha + 1}, \quad \mu_i = \lambda_i \frac{\alpha}{\gamma_i}, \quad e \quad \phi_i \mu_i^{\rho} = \lambda_i \frac{\alpha}{\gamma_i^2}(1+\alpha)$$

Si pone in evidenza come nel caso di applicazione della formula pertinente il modello *frequency-severity*, il parametro di scala[68] ϕ dipende da i.

[68] Per parametro di scala, o *scale parameter*, si intende una peculiare tipologia di parametro numerico della famiglia parametrica delle distribuzioni di probabilità. All'aumentare di quest'ultimo si ottiene come effetto un maggiore ampliamento della distribuzione in esame.

5.3 Applicazione numerica del frequency-severity method

La definizione del modello *frequency-severity*, ed in modo particolare delle principali tipologie di approccio specifiche ad esso correlate, consente, a tal punto del cammino di carattere analitico sino ad ora condotto di presentare delle applicazioni di carattere pratico e numerico inerenti la tematica principale dell'elaborato di tesi in esame: il *cyber risk* e, in modo particolare, nel corso di tale fase, la quantificazione di quest'ultimo tramite l'interpretazione delle procedure matematiche e statistiche appena approfondite in una prospettiva di adattamento alla moltitudine di dati ed informazioni raccolti nel corso della stesura del documento in materia di rischio cibernetico.
In primo luogo, si intende sviluppare un approccio orientato dal *generalized linear model* ed incentrato rispetto alla tematica delle *relativities* dando luogo alla definizione di un particolare *dataset* caratterizzato dalla presenza di quattro variabili principali, prima delle quali indicata con `LossLAE`, dall'inglese *loss and loss adjustment expenses*, dunque riguardante le perdite e le spese generate dal contenimento di quest'ultime, variabile che può essere quindi valutata come una componente *severity*. Il valore di quest'ultima, dedotto tramite il riferimento costante al Rapporto Clusit 2024, 2023 e 2022, si ipotizza essere influenzato da due elementi fondamentali, ovvero l'anno di riferimento, che verrà indicato con `YOR`, dunque *year of refererence*, ed il continente di provenienza della fattispecie oggetto d'analisi, simboleggiato da `Terr`, espressione di *territories*, i cui riferimenti saranno rappresentati dagli agglomerati transnazionali maggiormente lesi da rischi di natura cibernetica, quindi nell'ordine Asia, Europa ed America. Si pone in evidenza come la singola combinazione delle due variabili appena introdotte, cioè `YOF` e `Terr`, fornisca la quantità di violazioni determinate dalla concretizzazione di iniziative di *cybercrime*, indicata come `Exposure`, e oggetto di valutazione come componente di *frequency*. Si precisa che nel corso dell'applicazione del modello GLM in analisi è previsto l'utilizzo delle piattaforme R ed Excel al fine di ottenere vantaggio dalle rispettive molteplici funzionalità in modo da semplificare l'apprendimento delle tematiche di riferimento.

YOR	**Terr**	**Exposure**	**LossLAE**
2021	Asia	242	4,66*10^17
2022	Asia	196	6,52*10^17

2023	Asia	246	9,45*10^17
2021	Europa	436	1,40*10^18
2022	Europa	599	1,96*10^18
2023	Europa	644	2,42*10^18
2021	America	918	2,21*10^18
2022	America	941	3,10*10^18
2023	America	1226	4,62*10^18

Figura 13:tabella costruita su Excel per la definizione numerica delle variabili descritte[69]

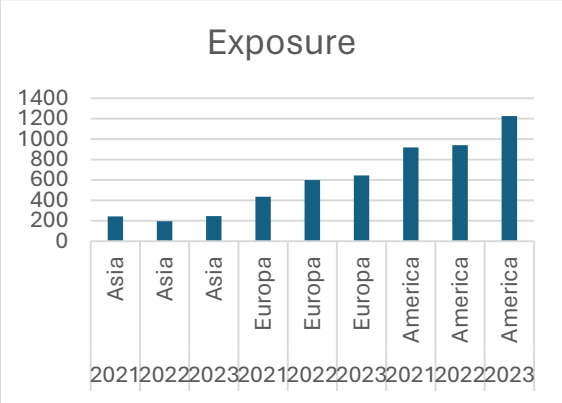


Figura 14:crescita exposure 2021/2023[70]

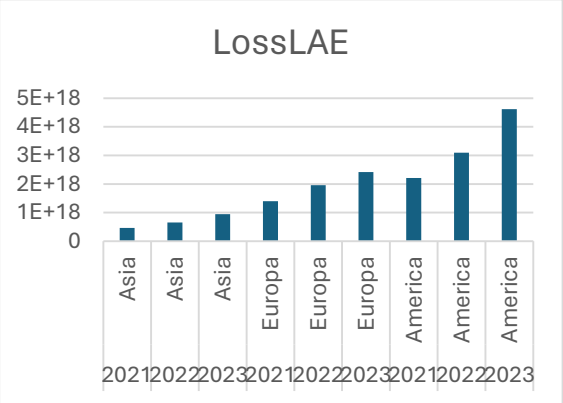


Figura 15:crescita perdite 2021/2023[71]

Si osservi come l'obiettivo che si intende realizzare è applicare il modello GLM ai dati appena forniti considerando `LossLAE` come variabile dipendente, in modo da analizzare ed interpretare l'impatto dell'annata e del territorio di riferimento rispetto alle perdite registrate.

A tal punto è possibile introdurre due fattori e concretizzare la stima di un modello lineare generalizzato applicando una distribuzione gamma con funzione di collegamento di matrice logaritmica. Si specifica come, in riferimento agli *output* derivanti dalle operazioni condotte all'interno della piattaforma R, il comando `relevel` consente di fornire una chiara indicazione riguardo il *refernce level* selezionato. In modo specifico

[69] Fonte: Excel, dati acquisiti da: Clusit-Associazione Italiana per la Sicurezza Informatica, "Rapporto 2022 sulla sicurezza ICT in Italia"; "Rapporto 2023 sulla sicurezza ICT in Italia"; "Rapporto 2024 sulla sicurezza ICT in Italia"

[70] Fonte: Excel, tramite l'interpretazione del *dataset* fornito e l'impiego della funzione grafico

[71] Fonte: Excel, tramite l'interpretazione del dataset fornito e l'impiego della funzione grafico

all'interno del progetto numerico in analisi, i *reference levels* risultano rappresentati dal 2022 come annata (`YOR=2022`) e dall'Europa come continente (`Terr=Europa`). Inoltre, l'esposizione logaritmica è impiegata come variabile *offset* in modo tale che la combinazione di due variabili categoriche comporti maggiori perdite attese nel caso di un più elevato valore di *exposure*. Si illustrano di seguito le singole operazioni e relativi comandi eseguiti sul *software* R:

```
> library(readxl)
> TESI<-read_excel("TESI.xlsx")
> View(TESI)
> Tesi$Terr=factor(Tesi$Terr)
> Tesi$Terr=relevel(Tesi$Terr,ref="Europa")
> Tesi$YOR=factor(Tesi$YOR)
> Tesi$YOR=relevel(Tesi$YOR,ref="2022")
> summary(glm(LossLAE~YOR+Terr,offset=log(Exposure),data =
Tesi,
+ family = Gamma(link = "log")))
Call:
glm(formula = LossLAE ~ YOR + Terr, family = Gamma(link =
"log"),
data = Tesi, offset = log(Exposure))
Deviance Residuals:
 1         2         3         4         5         6
-0.17861   0.07948   0.08416   0.17444  -0.09488  -0.09586
7         8         9
-0.01667   0.01026   0.00627
Coefficients:

             Estimate Std. Error t value Pr(>|t|)

(Intercept) 35.8186     0.1143 313.445 6.22e-10 ***

YOR2021      -0.2848     0.1252  -2.275   0.0853 .

YOR2023       0.1394     0.1252   1.113   0.3279

TerrAmerica  -0.0988     0.1252  -0.789   0.4741
```

```
TerrAsia      -0.1563     0.1252  -1.249   0.2799
---
Signif. codes:
0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
(Dispersion parameter for Gamma family taken to be
0.0235054)
Null deviance: 0.386185  on 8  degrees of freedom
Residual deviance: 0.094342  on 4  degrees of freedom
AIC: 750.76
Number of Fisher Scoring iterations: 5
```

Le stime inerenti ai parametri possono essere facilmente convertite in *relativities* tramite l'impiego della potenza del numero di Nepero *e* come segue:

Variabile	**Stima del parametro**	**Relativity (stima esponenziale del parametro)**
Intercetta	35,8186	3,5960*10^15
YOR2021	-0,2848	0,7522
YOR2022	0	1
YOR2023	0,1394	1,1496
TerrAsia	-0,1563	0,8553
TerrEuropa	0	1
TerrAmerica	-0,0988	0,9059

Figura 16:tabella ottenuta tramite R inerente alla definizione dei parametri ed alla relativa potenza di e[72]

Dunque, una volta in possesso di *relativities* e *exposures*, diviene immediato ultimare il calcolo riguardante le attese. Nello specifico, in riferimento ad un'annata più prossima come il 2023 all'interno del continente maggiormente minato da iniziative di cybercrime, quello Americano, dove l'*exposure* presenta valore corrispondente a 1226, il valore ottenuto tramite l'impiego del modello è computato come segue:

[72] Fonte: R, tramite interpretazione del *dataset* precedentemente fornito e conseguente applicazione dei comandi R

$$exposure_{YOR,Terr} \times relativity_{intercetta} \times relativity_{YOR} \times relativity_{Terr} = fitted\ amount$$

$$1226 \times 3{,}5960 * 10^{15} * 1{,}1496 \times 0{,}9059 = 4{,}5913 * 10^{18}$$

Il valore ottenuto analiticamente mediante l'impiego del modello GLM si rileva particolarmente prossimo al valore effettivo del corrispondente livello di `LossLAE` $4{,}62 * 10^{18}$.

La comparazione tra tutti i valori effettivi e quelli generati dall'applicazione dell'approccio GLM, o la devianza nulla rispetto a quella residuale, o ancora analizzando *t-values* e *p-values,* evidenzia l'utilità e la funzionalità del processo di adattamento dei dati rispetto al modello selezionato, ponendo in rilievo la necessità di implementazione di semplici metodi univariati per l'identificazione delle *relativities*, ragione per la quale, come dimostrato, risulta per applicazioni di matrice numerica di maggiore beneficio l'utilizzo di un metodo multivariato come il GLM. Si ricordi come l'impiego di un modello di questo genere sia finalizzato all'adattamento di molteplici fattori ad un particolare *dataset*, in modo che quest'ultimi non risultino isolati.

Considerazioni complessive e conclusive

Il percorso gnoseologico sino ad ora tracciato mira a sostanziarsi come un viaggio all'interno del mondo del rischio cibernetico, nel corso del quale si auspica di aver sollecitato la curiosità e la conoscenza del lettore rispetto ad una delle tematiche che si candida ad essere preminente in prospettive particolarmente prossime, in sostanza in un immediato futuro. Per tale motivazione si è inteso esplorare le fasi salienti dell'evoluzione della tematica del *cyber risk* e delle correlate misure di tutela e prevenzione, meglio note come strumenti di *cybersecurity*. Si precisa come l'approccio applicato nel corso della stesura dell'intero elaborato sia di natura strettamente economica e, per questa ragione, finalizzato a generare una sorta di richiamo dell'appassionante percorso formativo condotto, il cui epilogo è rappresentato dal documento in esame. Dunque si auspica che quanto analizzato possa rievocare non soltanto chiari riferimenti all'ambito della matematica finanziaria, materia di riferimento, come è possibile evincere dalla sezione conclusiva del testo, nella quale è opportuno annoverare, nel corso dell'approfondimento di modelli teorici, in partenza, e pratici, in proiezione, anche l'utilizzo di tecniche e nozioni di natura matematica e

statistica, ma anche brevi digressioni, correlate alle informazioni oggetto di studio ed estese su una molteplicità di contesti variegati, tra gli altri, il diritto privato e commerciale, la pianificazione ed il controllo di gestione aziendale e l'informatica, richiamando, peraltro, tratti essenziali della storia dell'economia e dell'impresa. Ebbene proprio lo sviluppo della transizione digitale e dei meccanismi da essa derivanti, come l'implementazione dei più innovativi programmi di sicurezza cibernetica, ha rappresentato e, sicuramente, rappresenterà una fonte pivotale di crescita e sviluppo per singoli individui ed intere nazioni, a patto che se ne comprendano i rischi associati ed i relativi limiti in termini di utilizzo. Diviene dunque chiaro ed evidente evincere il fine ultimo che si è inteso perseguire sin dalla prima battitura dell'elaborato in esame: promuovere l'adozione consapevole, responsabile e proattiva della tecnologia nel rispetto dei diritti inalienabili e fondamentali dell'essere umano, nonché del relativo ingegno e creatività.

Bibliografia

Accenture. (2018, Agosto 7). *Accenture Mid-Year Threatscape Report identifies five global threats.* Retrieved from Accenture: https://newsroom.accenture.com/news/2018/accenture-mid-year-threatscape-report-identifies-five-global-cybersecurity-threats

Accenture. (2019). *Technology Vision 2019 Executive Summary.* Retrieved from Accenture: https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-additional-pages-1/pdf/pdf-94/accenture-techvision-2019-exec-summary.pdf

Accenture. (n.d.). *Securing the digital economy* . Retrieved from Accenture: https://insuranceblog.accenture.com/series/securing-the-digital-economy

Agenda Digitale. (n.d.). *Intelligenza Artificiale.* Retrieved from Agenda Digitale: https://www.agendadigitale.eu/tag/intelligenza-artificiale/

Agenzia per l'Italia digitale. (n.d.). *Chi siamo| Agenzia per L'Italia digitale.* Retrieved from Agenzia per l'Italia digitale: https://www.agid.gov.it/it/agenzia/chi-siamo

Agenzia per l'Italia digitale. (n.d.). *Misure minime di sicurezza ICT per le pubbliche amministrazioni.* Retrieved from Agenzia per l'Italia digitale: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict#:~:text=Le%20misure%20minime%20di%20sicurezza,le%20minacce%20informatiche%20pi%C3%B9%20frequenti.

Agicap. (2024, Aprile 16). *Return on investment (ROI): cos'è e come calcolarlo.* Retrieved from Agicap: https://agicap.com/it/articolo/return-on-investment/

Agostinelli, A. (n.d.). *Cos'è la digital economy e a che punto siamo in Italia*. Retrieved from Aldo Agostinelli: https://aldoagostinelli.com/digital-economy/

Akamai. (n.d.). *Che cos'è il cloud?* Retrieved from Akamai: https://www.akamai.com/it/glossary/what-is-the-cloud

Allianz. (n.d.). *Allianz Commercial - your partner in business insurance*. Retrieved from Allianz: https://commercial.allianz.com/about-us/about-allianz-commercial.html

Alteredu. (n.d.). *Cyber Risk Manager: chi è? Cosa fa? Quanto guadagna?* Retrieved from Altereudo: https://www.alteredu.it/cyber-risk-manager-chi-e-cosa-fa-stipendio/#:~:text=Il%20Cyber%20Security%20Risk%20manager,e%20renderli%20il%20meno%20impattanti

ANIA. (n.d.). *IL RISCHIO CYBER CONOSCERLO DI PIÙ PER PROTEGGERSI MEGLIO*. Retrieved from ANIA: https://www.ania.it/documents/35135/144872/Il-rischio-cyber-conoscerlo-di-piu-per-proteggersi-meglio-Position-paper.pdf/79d04d00-5449-2741-5009-bf42c5c803b3?version=1.0&t=1575898452596

ANSA. (2021, Novembre 10). *Cybercrime emergenza globale, danni oltre 6% Pil mondiale*. Retrieved from ANSA.it: https://www.ansa.it/sito/notizie/tecnologia/hitech/2021/11/09/-cybercrime-emergenza-globale-danni-oltre-6-pil-mondiale-_bf3e3248-8807-4846-82de-431e2f7405f2.html

ANSA. (2022, Marzo 10). *Clusit, emergenza cybercrime vale 4 volte Pil italiano*. Retrieved from ANSA.it: https://www.ansa.it/sito/notizie/tecnologia/internet_social/2022/03/07/cybercrimeper-clusit-emergenza-vale-4-volte-pil-italiano_721a6787-8094-445f-b0d6-e23f8ec30e34.html

ANSA. (n.d.). *Agenzia Ansa - presentation page*. Retrieved from ANSA.it: https://www.ansa.it/amphtml/ansa.amp.html

Aranzulla, S. (n.d.). *Come rootare il telefono*. Retrieved from Salvatore Aranzulla: https://www.aranzulla.it/come-rootare-il-telefono-940520.html

Ardesia. (2023, Agosto 31). *Com'è nato internet?* Retrieved from Ardesia: https://www.ardesia.it/come-nato-internet/

Augeos. (2022, Giugno 21). *Rischio operativo: cos'è e come gestirlo per evitare perdite*. Retrieved from Augeos: https://blog.augeos.it/rischio-operativo-come-evitare-perdite-correggendo-in-anticipo-i-processi

Ballejos, L. (2024, Marzo 18). *Cos'è la sicurezza degli endpoint e come funziona?* Retrieved from ninja.com: https://www.ninjaone.com/it/blog/cose-la-sicurezza-degli-endpoint-e-come-funziona/?utm_source=google&utm_medium=cpc&utm_campaign=EU_ITA_PS_Feature_Endpoint_Management_Dynamic&utm_content=homepage&utm_term=&utm_matchtype=&utm_device=c&utm_adposition=&utm_g

Balocco, V. (2023, Agosto 1). *Cybersecurity, la sfida del futuro è renderla più democratica. Fastweb in campo.* Retrieved from CorCom: https://www.corrierecomunicazioni.it/digital-economy/cybersecurity-la-sfida-del-futuro-e-renderla-piu-democratica-fastweb-in-campo/

Banca d'Italia. (2006, Luglio). *RISCHI OPERATIVI (Metodi Avanzati - AMA)* . Retrieved from Banca d'Italia: https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2006/basilea2/Rischi_operativi_metodi_avanzati_AMA.pdf

Barbera, A. (n.d.). *Vademècum sulla privacy (legge 675/96 e successive modifiche ed integrazioni).* Retrieved from Diritto.it: https://www.diritto.it/vademecum-sulla-privacy-legge-675-96-e-successive-modifiche-ed-integrazioni/

Bisceglia, M. (n.d.). *Decision making: come prendere le decisioni?* Retrieved from Serenis: https://www.serenis.it/articoli/decision-making/

Bissell, K., & Ponemon, L. (n.d.). *The cost of crybercrime*. Retrieved from PR Newswire: https://mma.prnewswire.com/media/882924/Accenture_Cybercrime_Costs_Canadian_Companies_more_than_US_9M_La.pdf?p=original

Brocardi.it. (n.d.). *Articolo 38 Disposizioni di attuazione del codice di procedura penale.* Retrieved from Brocardi.it: https://www.brocardi.it/disposizioni-per-attuazione-codice-procedura-penale/titolo-i/capo-iv/art38.html

Brolli, M. (2021, Maggio 12). *WannaCry: il ransomware che cambiò il mondo.* Retrieved from Red Hot Cyber: https://www.redhotcyber.com/post/la-storia-di-wanna-cry/

Campara, F. (2022, Novembre 2). *Cyber risk management: un nuovo modello di protezione dati per l'azienda di domani.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/soluzioni-aziendali/cyber-risk-management-un-nuovo-modello-di-protezione-dati-per-lazienda-di-domani/

Cataleta, A., Longo, A., & Natale, R. (2024, Aprile 5). *GDPR, tutto ciò che c'è da sapere per essere in regola*. Retrieved from Agenda Digitale: https://www.agendadigitale.eu/sicurezza/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/

Cetrom. (2022, Giugno 6). *The Importance of Mitigating Human Error in Cybersecurity.* Retrieved from Cetrom: https://www.cetrom.net/resources/blog/importance-of-mitigating-human-error-in-cybersecurity#:~:text=A%20global%20study%2C%20the%20IBM,cybersecurity%20breaches%20would%20not%20have

Check Point. (n.d.). *Che cos'è il Modello di Responsabilità Condivisa?* Retrieved from Check Point: https://www.checkpoint.com/it/cyber-hub/cloud-security/what-is-aws-shared-responsibility-model-and-how-it-works/#:~:text=Il%20Modello%20di%20Responsabilit%C3%A0%20Condivisa%20descrive%20le%20responsabilit%C3%A0%20di%20sicurezza,cloud%20e%20del%20cliente%2

Check Point. (n.d.). *Cos'è la sicurezza informatica?* Retrieved from Check Point: https://www.checkpoint.com/it/cyber-hub/cyber-security/what-is-cybersecurity/

Cloud Flare. (n.d.). *Che cos'è un attacco DDoS?* Retrieved from Cloud Flare: https://www.cloudflare.com/it-it/learning/ddos/what-is-a-ddos-attack/

Clusit – Associazione Italiana per la Sicurezza Informatica. (2023, Marzo). *Registrazione della sessione di presentazione del Rapporto Clusit 2023.* Retrieved from Clusit – Associazione Italiana per la Sicurezza Informatica: https://clusit.it/blog/registrazione-della-sessione-di-presentazione-del-rapporto-clusit-2023/

Clusit. (2022). *Rapporto Clusit 2022 sulla sicurezza ICT in Italia.* Retrieved from Clusit: https://www.saccani.net/wp-content/uploads/2022/03/Rapporto-Clusit-marzo-2022_b_web.pdf

Clusit. (2024). *Rapporto Clusit 2024 sulla sicurezza ICT in Italia.* Retrieved from Clusit: file:///C:/Users/andre/Downloads/Rapporto_Clusit_2024_web%20(1).pdf

CLUSIT. (n.d.). *CLUSIT – Associazione Italiana per la Sicurezza Informatica.* Retrieved from CLUSIT: https://clusit.it/chi-siamo/

Commissariato di Polizia Postale. (2024, Febbraio 6). *Safre Internet Day.* Retrieved from Commissariato di Polizia Postale online Sportello per la sicurezza degli utenti del web: https://www.commissariatodips.it/docs/report_safer_internet_day_2024.pdf

Concas, A. (2023, Settembre 25). *Il Garante per la protezione delle informazioni personali - Scheda di Diritto.* Retrieved from Diritto.it: https://www.diritto.it/garante-protezione-informazioni-personali-scheda/

Cooper, V. (2024, Aprile 1). *Le 10 principali tendenze e previsioni sulla sicurezza informatica per il 2024.* Retrieved from Splashtop: https://www.splashtop.com/it/blog/cybersecurity-trends-and-predictions-2024

Crisantemi, M. (2023, Novembre 9). *Rapporto Clusit, in Italia attacchi in crescita e manifatturiero sempre più nel mirino.* Retrieved from Innovation Post : https://www.innovationpost.it/attualita/rapporto-clusit-in-italia-attacchi-in-crescita-e-manifatturiero-sempre-piu-nel-mirino/

CSIS Center for Strategic and International Studies . (n.d.). *About CSIS.* Retrieved from CSIS Center for Strategic and International Studies : https://www.csis.org/about

CSIS Center for Strategic and International Studies. (2014, Giugno). *Net Losses: Estimating the Global Cost of Cybercrime.* Retrieved from CSIS Center for Strategic and International Studies: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/140609_rp_economic_impact_cybercrime_report.pdf

Cyber Security 360. (2018, Maggio 31). *Attacco Man-in-the-middle, tutti i modi possibili e come difenderci.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/nuove-minacce/attacco-man-in-the-middle-tutti-i-modi-possibili-e-come-difenderci/

Daga, M. C. (2023, Aprile 20). *Phishing: il punto della giurisprudenza per individuare le responsabilità di banche e utenti.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/legal/phishing-il-punto-della-giurisprudenza-per-individuare-le-responsabilita-di-banche-e-utenti/

De Angelis, D. (2017, Ottobre 24). *Come il Morris Worm ha cambiato per sempre la storia di internet.* Retrieved from VICE: https://www.vice.com/it/article/43a97g/come-il-morris-worm-ha-cambiato-per-sempre-la-storia-di-internet

De Tommasi, A. (2022, Febbraio 17). *Cybersecurity: i cinque trend che influenzeranno il futuro del settore.* Retrieved from ANSA: https://www.ansa.it/ansa2030/notizie/asvis/2022/02/17/cybersecurity-i-cinque-trend-che-influenzeranno-il-futuro-del-settore_0cc88fef-91ee-4152-b14c-1edc14aee8a3.html

Defence Tech. (2022, Gennaio 14). *1° ATTACCO HACKER DELLA STORIA.* Retrieved from Defence Tech: https://www.defencetech.it/2022/01/14/1-attacco-hacker-della-storia/

Desirò, G. (n.d.). *ITSEC: i criteri europei per la valutazione della sicurezza informatica*. Retrieved from Privacy.it: https://www.privacy.it/archivio/desiro200406.html

Di Francesco, G. (2023, Novembre 9). *L'industria assicurativa e la sfida del rischio cyber: la chiave per affrontarla in modo efficace.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/soluzioni-aziendali/lindustria-assicurativa-e-la-sfida-del-rischio-cyber-la-chiave-per-affrontarla-in-modo-efficace/

Di Sabatino, G. (2023, Aprile 27). *Cloud security: cos'è e come implementarla per mettere in sicurezza dati, applicazioni e infrastrutture.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/soluzioni-aziendali/cloud-security-cose-e-come-implementarla-per-mettere-in-sicurezza-dati-applicazioni-e-infrastrutture/

Dipartimento del Tesoro. (n.d.). *OCSE - Organizzazione per la cooperazione e lo sviluppo economico.* Retrieved from Dipartimento del Tesoro: https://www.dt.mef.gov.it/it/attivita_istituzionali/rapporti_finanziari_internazionali/organismi_internazionali/ocse/

doxee. (2022, Giugno 10). *Settore Healthcare: caratteristiche ed evoluzione di un settore in salute.* Retrieved from doxee: https://www.doxee.com/it/blog/marketing/caratteristiche-settore-healthcare/

Dragoni, G. (2023, Giugno 6). *Cos'è il Social Engineering, come difendersi e come riconoscerlo.* Retrieved from Osservatori.net: https://blog.osservatori.net/it_it/social-engineering-come-difendersi

Egan, R., Cartagena, S., R.Mohamed, Gosrani, V., Grewal, J., M.Avharyya, . . . Ang, K. (2018, Maggio 28). *Cyber operational risk scenarios for insurance companies*. Retrieved from Institute and Faculty of Actuaries: https://www.actuaries.org.uk/system/files/field/document/Sessional%20paper%20-

%20Cyber%20operational%20risk%20scenarios%20for%20insurance%20companies_0.pdf

Egidi, L. (2021/2022). *Modelli Lineari Generalizzati (GLM): parte I*. Retrieved from Università di Trieste Corso di laurea magistrale in Scienze Statistiche ed Attuariali: https://moodle2.units.it/pluginfile.php/405454/mod_resource/content/5/lucidi_2021.22_A.pdf

Entrust. (n.d.). *Che cos'è Common Criteria?* Retrieved from Entrust: https://www.entrust.com/it/resources/learn/common-criteria

EUR-Lex. (n.d.). *Gazzetta ufficiale dell'Unione europea*. Retrieved from EUR-Lex: https://eur-lex.europa.eu/oj/direct-access.html?locale=it

European Union. (n.d.). *Agenzia dell'Unione europea per la cibersicurezza (ENISA)*. Retrieved from European Union: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_it

F. O. (2010, Gennaio 22). *Basilea II*. Retrieved from Borsa Italiana: https://www.borsaitaliana.it/notizie/sotto-la-lente/basileaii.htm

Fabio, D. F. (2022, Dicembre 9). *Enisa: "Nasce il quadro europeo delle competenze di cybersecurity, ecco perché è importante"*. Retrieved from Agenda Digitale: https://www.agendadigitale.eu/sicurezza/cybersicurezza-arriva-il-quadro-europeo-delle-competenze-ecco-perche-e-importante/

Forcepoint. (n.d.). *Che cos'è la sicurezza di rete?* Retrieved from Forcepoint: https://www.forcepoint.com/it/cyber-edu/network-security

Forte, S. (2022, Giugno 23). *La valutazione del rischio cibernetico*. Retrieved from Ordine degli Attuari: https://www.ordineattuari.it/media/317686/forte_seminario_ona_23_6_2022_cyber_risk.pdf

Framework Nazionale per la Cyber Security e la Data Protection. (n.d.). *Framework Nazionale per la Cyber Security e la Data Protection*. Retrieved from Metodologia per il cybersecurity assessment: https://www.cybersecurityframework.it/

Frareg. (n.d.). *Certificazione BS 7799 sulla sicurezza informatica*. Retrieved from Frareg: https://www.frareg.com/it/dossier/certificazione-bs-7799-sulla-sicurezza-informatica/

Frees, E. W., Derrig, R. A., & Meyers, G. (2014). *Predictive Modeling Applications in Actuarial Science*. Cambridge University Press. Retrieved from https://doi.org/10.1017/CBO9781139342674.006

FreshBooks. (2023, Febbraio 20). *Frequency Severity Method: Definition & Overview*. Retrieved from FreshBooks: https://www.freshbooks.com/glossary/small-business/frequency-severity-method

Gallotti, C. (2021, Febbraio 26). *Storia delle norme, degli standard e delle linee guida della cybersecurity.* Retrieved from Cybersecurity Italia: https://www.cybersecitalia.it/storia-delle-norme-degli-standard-e-delle-linee-guida-della-cybersecurity/9160/

Gartner. (n.d.). *Gartner at a Glance.* Retrieved from Gartner: https://emt.gartnerweb.com/ngw/globalassets/en/about/documents/gartner-at-a-glance.pdf?_gl=1*c00adm*_ga*MTk5MDU2NDE2OC4xNzAyOTgzMTcx*_ga_R1W5CE5FEV*MTcwMjk4MzE3MC4xLjEuMTcwMjk4NDA0OS4zNy4wLjA.

Generali. (n.d.). *Come proteggersi dal Cyber Risk*. Retrieved from Generali: https://www.generali.it/magazine/business/cyber-risk#:~:text=Il%20Cyber%20Risk%20%C3%A8%20il,per%20esempio%20gli%20attacchi%20hacker).

Generali Group. (n.d.). *Carlo Ferraresi nominato Presidente del CRO Forum*. Retrieved from Generali Group: https://www.generali.com/it/media/News/2023/Carlo-Ferraresi-appointed-Chairman-of-the-CRO-Forum#:~:text=Gli%20obiettivi%20del%20CRO%20Forum,requisiti%20normativi%20e%20regolamentari%20ed

Glassdor. (2024, Maggio 2). *Stipendi per Cyber Security Manager, Italia*. Retrieved from Glassdor: https://www.glassdoor.it/Stipendi/cyber-security-manager-stipendio-SRCH_KO0,22.htm#:~:text=Stipendi%20per%20Cyber%20Security%20Manager%2C%20Italia&text=Quanto%20%C3%A8%20precisa%20una%20paga,stima%20della%20retribuzione%20nel%20tempo

Goyal, C. (2024, Aprile 29). *Moments in Statistics – A Must Known Statistical Concept for Data Science.* Retrieved from Analytics Vidhya: https://www.analyticsvidhya.com/blog/2022/01/moments-a-must-known-statistical-concept-for-data-science/

GPDP- Garante per la Protezione dei Dati Personali. (1996, Dicembre 31). *Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.* Retrieved from GPDP- Garante per la Protezione dei Dati Personali: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335#:~:text=La%20presente%20legge%20garantisce%20che,giuridiche%20e%20di%20ogni%20altro

Guzzo, A. (2010, 02 18). *I piani di sicurezza secondo lo standard di riferimento.* Retrieved from diritto.it: https://www.diritto.it/wp-content/uploads/2010/02/pdf_28936-1.pdf

He, O. (2023, Dicembre 26). *Cos'è la Commissione Elettrotecnica Internazionale (IEC).* Retrieved from RayZeek: https://www.rayzeek.com/it/glossary/che-cose-la-commissione-elettrotecnica-internazionale-iec

HSC System. (2021, Agosto 24). *SICUREZZA DIGITALE: L'IMPORTANZA DELLA CYBER SECURITY OGGI.* Retrieved from HSC System:

https://www.hscsystem.it/blog/sicurezza-digitale-l-importanza-della-cyber-security-oggi

IBM. (2022). *X-Force Threat Intelligence Index 2022.* Retrieved from IBM : https://www.ibm.com/downloads/cas/ADLMYLAZ

IBM. (2023). *Report Cost of a Data Breach 2023.* Retrieved from IBM: https://www.ibm.com/it-it/reports/data-breach

IBM. (n.d.). *Cos'è a cybersecurity?* Retrieved from IBM: https://www.ibm.com/it-it/topics/cyber-resilience

IBM. (n.d.). *Cos'è il NIST Cybersecurity Framework?* Retrieved from IBM: https://www.ibm.com/it-it/topics/nist

IBM. (n.d.). *Cos'è un malware?* Retrieved from IBM: https://www.ibm.com/it-it/topics/malware

IBM. (n.d.). *IBM-Italia.* Retrieved from IBM: https://www.ibm.com/it-it

IBM Security. (2021, Luglio). *Cost of a data breach report 2021*. Retrieved from IBM Security: https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF

Ierinò, A., Tonussi, G., Natta, A., De Nardi, M., & De Menna, D. (2023, Aprile 4). *Cyber Resilience: strategie e tecnologie per proteggere i servizi dalle minacce informatiche.* Retrieved from NTT Data: https://it.nttdata.com/insights/blog/cyber-resilience-strategie-protezione-attacchi-informatici

Internazionali, B. d. (2006, Giugno). *Bank for International Settlements.* Retrieved from bcbs128ita.pdf: https://www.bis.org/publ/bcbs128ita.pdf

Internet4Things. (2020, Agosto 31). *Cosa si intende per connected products, come questi stanno guidando la trasformazione digitale.* Retrieved from Internet4Things: https://www.internet4things.it/iot-library/cosa-si-intende-per-connected-products-come-questi-stanno-guidando-la-trasformazione-digitale/

IONOS Italia. (2020, Luglio 20). *HTTPS: cosa significa e perché è così importante.* Retrieved from IONOS Italia: https://www.ionos.it/digitalguide/hosting/tecniche-hosting/cose-https/

IONOS Italia. (2022, Settembre 6). *Cos'è ISO? Una spiegazione sullo standard e il certificato ISO.* Retrieved from IONOS Italia: https://www.ionos.it/digitalguide/server/know-how/cose-iso/

ISO. (2018, Maggio). *ISO 31000:2018 (en) Risk Management-Guidelines.* Retrieved from ISO: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO-International Organization for Standardization. (n.d.). *ISO/IEC 27018:2019.* Retrieved from ISO-International Organization for Standardization: https://www.iso.org/standard/76559.html

IT impresa. (2021, Agosto 28). *Cyber Crime: Cos'è, Tipologie, Esempi, Situazione in Italia*. Retrieved from IT impresa: https://www.it-impresa.it/blog/cyber-crime/

IT impresa. (2021, Settembre 2). *Qubit, una tecnologia rivoluzionaria che ci porta nel futuro.* Retrieved from IT impresa: https://www.it-impresa.it/blog/qubit/

IT impresa. (2023, Dicembre 18). *Cyber Warfare: cos'è, tipologie, esempi e come combatterla*. Retrieved from IT impresa: https://www.it-impresa.it/blog/cyber-warfare/

Izrael, N. (2023, Dicembre 1). *Cybersecurity, i trend 2024: l'IA cambia tutto.* Retrieved from Agenda Digitale : https://www.agendadigitale.eu/sicurezza/trend-2024-cosi-lia-cambiera-cybersecuity-lavoro-e-spionaggio/

Kagan, J., & Howard, E. (2023, Settembre 28). *Frequency-Severity Method: Definition and How Insurers Use It*. Retrieved from Investopedia: https://www.investopedia.com/terms/f/frequencyseverity-method.asp

Kaspersky. (n.d.). *Che cos'è il ransomware WannaCry?* Retrieved from Kaspersky: https://www.kaspersky.it/resource-center/threats/ransomware-wannacry

Klugman, S. A., Panjer, H. H., & Willmot, G. E. (2019, Maggio 28). *Loss Models: From Data to Decisions*. John Wiley & Sons Inc.

Klusaitè, L. (2023, Gennaio 11). *La storia della cybersecurity.* Retrieved from Nord VPN: https://nordvpn.com/it/blog/la-storia-della-cybersecurity/#:~:text=La%20cybersecurity%20si%20evolve&text=A%20met%C3%A0%20anni%202000%20vennero,che%20inviano%20e%20ricevono%20online.

La Stampa. (2024, Gennaio 16). *Allianz Risk Barometer: il cyber è il principale rischio aziendale a livello globale per il 2024.* Retrieved from La Stampa: https://finanza.lastampa.it/News/2024/01/16/allianz-risk-barometer-il-cyber-e-il-principale-rischio-aziendale-a-livello-globale-per-il-2024/MTkxXzIwMjQtMDEtMTZfVExC

Lima, E. (2024, Gennaio 8). *Cybersecurity, in vigore le nuove regole Ue. Ecco cosa cambia*. Retrieved from CorCom: https://www.corrierecomunicazioni.it/digital-economy/cybersecurity-in-vigore-le-nuove-regole-ue-ecco-cosa-cambia/

Livelli, F. M. (2024, Gennaio 23). *La Direttiva NIS2 avanza: come prepararsi in questi 9 mesi.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-ce-il-nuovo-regolamento-ue-cosi-aumenta-il-livello-comune-di-sicurezza/

Livelli, F. M. (2024, Marzo 11). *Risk management: cos'è e come trasforma i rischi in opportunità.* Retrieved from Agenda Digitale: https://www.agendadigitale.eu/industry-4-0/risk-management-cose-e-come-trasforma-i-rischi-in-opportunita/

Longo, A., & Tarsitano, P. (2021, Agosto 8). *Ecco l'Agenzia per la cybersicurezza nazionale: come cambia la sicurezza cibernetica dell'Italia.* Retrieved from Agenda Digitale:

https://www.cybersecurity360.it/cybersecurity-nazionale/ecco-lagenzia-per-la-cybersicurezza-nazionale-come-cambia-la-sicurezza-cibernetica-dellitalia/

McAfee. (n.d.). *Cos'è un malware?* Retrieved from McAfee: https://www.mcafee.com/it-it/antivirus/malware.html

McAfee. (n.d.). *McAfee è il miglior antivirus del 2023.* Retrieved from McAfee: https://www.mcafee.com/it-it/antivirus.html

Merchants Insurance Group. (2022, Marzo 8). *What is "Ratemaking" and Why is it Important for Insurance Consumers?* Retrieved from Merchants Insurance Group: https://www.merchantsgroup.com/blog/what-is-ratemaking-and-why-is-it-important-for-insurance-consumers/

Meta, F. (2017, Dicembre 19). *Wannacry, Usa attaccano Corea del Nord: "Responsabile dell'attacco".* Retrieved from CorcCom: https://www.corrierecomunicazioni.it/cyber-security/wannacry-usa-attaccano-corea-del-nord-responsabile-dellattacco/

Microsoft . (n.d.). *Data Security Index: Trends, insights, and strategies to secure data*. Retrieved from Microsoft: https://info.microsoft.com/ww-landing-data-security-index.html?lcid=en-us

Musa Formazione. (2021, Luglio 22). *Trattamento dati personali: cosa dice la normativa*. *La legge 675 96 art 13.* Retrieved from Musa Formazione: https://www.musaformazione.it/trattamento-dati-personali-cosa-dice-la-normativa-la-legge-675-96-art-13/

National Institute of Standards and Technology. (2012, Aprile). *NIST/SEMATECH e-Handbook of Statistical Methods*. Retrieved from National Institute of Standards and Technology: https://www.itl.nist.gov/div898/handbook/

NQA. (n.d.). *ISO 27018: Protezione delle Informazioni di Identificazione Personale*. Retrieved from NQA: https://www.nqa.com/it-it/certification/standards/iso-27018

Openpolis. (2023, Settembre 12). *Cos'è il Copasir, comitato parlamentare per la sicurezza della repubblica*. Retrieved from Openpolis: https://www.openpolis.it/parole/cose-il-copasir-comitato-parlamentare-per-la-sicurezza-della-repubblica/

Openpolis. (2023, Febbraio 28). *Cos'è il Pnrr, piano nazionale ripresa e resilienza*. Retrieved from Openpolis: https://www.openpolis.it/parole/cose-il-pnrr-piano-nazionale-ripresa-e-resilienza/

Openpolis. (28, Dicembre 2021). *L'Enisa e la strategia europea di cibersicurezza.* Retrieved from Openpolis: https://www.openpolis.it/lenisa-e-la-strategia-europea-di-cibersicurezza/

Oracle. (n.d.). *Che cos'è il Deep Learning?* Retrieved from Oracle: https://www.oracle.com/it/artificial-intelligence/machine-learning/what-is-deep-learning/

Osservatori.net. (n.d.). *Record per il mercato italiano della cybersecurity: 2,15 miliardi di euro, +16%*. Retrieved from Osservatori.net: https://www.osservatori.net/it/ricerche/comunicati-stampa/cybersecurity-italia-mercato-crescita#:~:text=A%20testimonianza%20dell'interesse%2C%20nel,pari%20allo%200%2C10%25).

Padovan, D. (2023, Giugno 21). *Sicurezza delle informazioni: i tre principi per gestire il cyber risk*. Retrieved from Agenda Digitale: https://www.agendadigitale.eu/sicurezza/sicurezza-delle-informazioni-i-tre-principi-per-gestire-il-cyber-risk/

Pain, D., & Anchen, J. (2017, Gennaio 24). *Cyber: getting to grips with a complex risk*. Retrieved from Swiss Re: https://www.swissre.com/dam/jcr:995517ee-27cd-4aae-b4b1-44fb862af25e/sigma1_2017_en.pdf

Panda Security. (n.d.). *Panda Security Sito Ufficiale*. Retrieved from Panda Security: https://www.pandasecurity.com/security-promotion/?reg=IT&lang=it&track=109162&campaign=dome2001&option=yearly&coupon=30OFFMULTIP&gad_source=1&gclid=Cj0KCQjwlN6wBhCcARIsAKZvD5iur-pUxhLG7ER1jjCOmlmnG4w2ikBn2gl1DHut3THNjBubK7dSf3oaAv45EALw_wcB

Panetta, R. (2024, Marzo 12). *Ai act: cos'è e come plasma l'intelligenza artificiale in Europa*. Retrieved from Agenda Digitale: https://www.agendadigitale.eu/cultura-digitale/ai-act-ci-siamo-ecco-come-plasmera-il-futuro-dellintelligenza-artificiale-in-europa/

Pivato, C. (2019, Novembre 13). *Lo spam: cos'è e come difendersi, anche alla luce del GDPR*. Retrieved from Cyber Security 360 : https://www.cybersecurity360.it/soluzioni-aziendali/lo-spam-cose-e-come-difendersi-anche-alla-luce-del-gdpr/

Politini, S. (2024, Marzo 27). *Chi è il cybersecurity manager, e perché è strategico per il business*. Retrieved from People & Change 360: https://www.peoplechange360.it/people-strategy/competenze-digitali/cybersecurity-manager-identikit-cosa-fa-figura-strategica/

Ponemon Institute. (n.d.). *Why we are unique*. Retrieved from Ponemon Institute: https://www.ponemon.org/about/why-we-are-unique.html

Principali, L. (2022, Febbraio 11). *Certificazioni cyber: l'evoluzione dei requisiti e l'impatto sull'ecosistema*. Retrieved from Agenda Digitale: https://www.agendadigitale.eu/sicurezza/certificazioni-cyber-levoluzione-dei-requisiti-e-limpatto-sullecosistema/

PrivacyDati.it. (n.d.). *https://privacydati.it/faq-privacy-gdpr/garante-privacy-dati-gdpr*. Retrieved from PrivacyDati.it: Chi è il Garante per la protezione dei dati personali e quali sono i suoi compiti?

Proofpoint. (n.d.). *Che cos'è la Mobile Security?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/mobile-security

Proofpoint. (n.d.). *Che cos'è una Botnet?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/botnet

Proofpoint. (n.d.). *Che cos'è il phishing?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/phishing#:~:text=Per%20phishing%20si%20intende%20quel,accesso%20o%20altri%20dati%20sensibili.

Proofpoint. (n.d.). *Che Cos'è la Cybersecurity/Network Security?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/cybersecurity-network-security

Proofpoint. (n.d.). *Che cos'è la IoT Security?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/iot-security

Proofpoint. (n.d.). *Cosa sono i dati PII (Personally Identifiable Information)?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/personal-identifiable-information#:~:text=L'acronimo%20PII%20sta%20per,furto%20da%20parte%20dei%20cybercriminali.

Proofpoint. (n.d.). *Cos'è un ransomware?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/ransomware

Proofpoint. (n.d.). *DLP (Data Loss Prevention).* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/dlp

Proofpoint. (n.d.). *Haktivism cos'è? Chi sono gli Hacktivist?* Retrieved from Proofpoint: https://www.proofpoint.com/it/threat-reference/hacktivism

Querzioni, L. (2021, Novembre 12). *Cybersecurity assessment: come si misura l'efficacia del livello di sicurezza.* Retrieved from Agenda Digitale: https://www.agendadigitale.eu/sicurezza/cybersecurity-assessment-come-si-misura-lefficacia-del-livello-di-sicurezza/

Rappresentanza ONU GInevra. (n.d.). *World Economic Forum (WEF).* Retrieved from Rappresentanza ONU Ginevra: https://italiarappginevra.esteri.it/it/litalia-e-ooii/commercio-internazionale/world-economic-forum-wef/

Razzini, A. (2024, Febbraio 13). *Il Cyber Resilience Act si aggiorna: ecco i nuovi requisiti fondamentali e i prodotti coinvolti.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/legal/il-cyber-resilience-act-si-aggiorna-ecco-i-nuovi-requisiti-fondamentali-e-i-prodotti-coinvolti/

Remer, P. (2019, Settembre 6). *Diritti di segreteria.* Retrieved from La legge per tutti: https://www.laleggepertutti.it/299559_diritti-di-segreteria

Russell, D., & Vanover, R. (2023, Febbraio 27). *La cyber insurance non può farcela da sola: le altre "assicurazioni" che allontanano la minaccia cyber.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/soluzioni-aziendali/la-cyber-

insurance-non-puo-farcela-da-sola-le-altre-assicurazioni-che-allontanano-la-minaccia-cyber/

S&P Global Ratings. (2023, Agosto 3). *Cyber Risk Insights: New Regulations Will Increase*. Retrieved from S&P Global Ratings: https://img.corrierecomunicazioni.it/wp-content/uploads/2023/08/08112919/RatingsDirect_CyberRiskInsightsNewRegulationsWillIncreaseResilienceAtACost_55652763_Aug-07-2023.pdf

S&P Global Ratings. (n.d.). *S&P Global Ratings*. Retrieved from Forum per la Finanza Sostenibile : https://finanzasostenibile.it/soci/sp-global-ratings/

Saetta, B. (2020, Marzo 2). *Dati biometrici*. Retrieved from Protezione Dati Personali: https://protezionedatipersonali.it/dati-biometrici

SealPath. (2024, Gennaio 31). *I TREND DELLA SICUREZZA INFORMATICA PER IL 2024 SECONDO GLI ESPERTI*. Retrieved from Ingecom: https://www.ingecom.net/it/blog/304/i-trend-della-sicurezza-informatica-per-il-2024-secondo-gli-esperti/

Telmon, C. (2024, Marzo 12). *Cyber Resilience Act, il Parlamento UE approva: perimetro di applicabilità e impatti*. Retrieved from Cyber Security 360: https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-resilience-act-il-parlamento-ue-approva-perimetro-di-applicabilita-e-impatti/

Tetto, P. (2016, Maggio). *Il Cyber Risk: cos'è e come difendersi*. Retrieved from Rivista Microcredito: https://rivista.microcredito.gov.it/opinioni/archivio-opinioni/892-il-cyber-risk-cos-e-e-come-difendersi.html

The Hacker News. (2021, Febbraio 4). *Why Human Error is #1 Cyber Security Threat to Businesses in 2021*. Retrieved from The Hacker News: https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html#:~:text='Human%20error%20was%20a%20major,in%2095%25%20of%20all%20breaches.&text=Mitigation%20of%20human%20error%20must,cyber%20business%20security%20in%202021.

The Innovation Group. (2015, Novembre 11). *IMPATTO ECONOMICO DEL CYBERCRIME SULLE AZIENDE E SULLE NAZIONI*. Retrieved from The Innovation Group: https://channels.theinnovationgroup.it/cybersecurity/impatto-economico-del-cybercrime-sulle-aziende-e-sulle-nazioni/

Treccani. (n.d.). *IBM nell'enciclopedia Treccani*. Retrieved from Treccani: https://www.treccani.it/enciclopedia/ibm/

Treccani. (n.d.). *Riassicurazione*. Retrieved from Treccani: https://www.treccani.it/enciclopedia/riassicurazione_(Dizionario-di-Economia-e-Finanza)/

Treccani. (n.d.). *Verosimiglianza massima, metodo della*. Retrieved from Treccani: https://www.treccani.it/enciclopedia/verosimiglianza-massima-metodo-della_%28Dizionario-di-Economia-e-Finanza%29/

Ufficio Brevetti. (n.d.). *Il Marchio CE. Cosa significa e quando è obbligatorio.* Retrieved from Ufficiobrevetti.it: https://ufficiobrevetti.it/faq/marchio-ce-cosa-significa-e-quando-e-obbligatorio/

Unione Europea. (2018, Maggio 23). *REGOLAMENTO GENERALE.* Retrieved from Garante per la protezione dei dati personali: https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018

UniverseIT, Redazione. (n.d.). *Sicurezza delle applicazioni: cos'è, tipologie e come testarle.* Retrieved from UniverseIT: https://universeit.blog/sicurezza-delle-applicazioni/

Università degli Studi di Perugia. (n.d.). *Diapositiva 1.* Retrieved from Università degli Studi di Perugia : https://www.dinomolli.it/Modulo_C/PDF_Singoli/8_10a.pdf

Università Politecnica delle Marche. (n.d.). *Metodo della massima verosimiglianza.* Retrieved from UNIVPM: https://www2.econ.univpm.it/servizi/hpp/lucchetti/didattica/matvario/MLLN.pdf

Valentini, A. (2020, Agosto 31). *Identity Management: cos'è, a cosa serve, i consigli degli esperti.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/soluzioni-aziendali/identity-management-cose-a-cosa-serve-i-consigli-degli-esperti/

Valentini, A. (2023, Giugno 20). *Quantificazione e gestione del rischio cyber: concentrarsi sulle priorità.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/soluzioni-aziendali/rischio-cyber-gestire-e-allineare-obiettivi-strategici-organizzazione/

Valentini, A. (2024, Aprile 29). *I fattori decisivi di un'organizzazione cyber resiliente.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/outlook/i-fattori-di-unorganizzazione-cyber-resiliente/

Valore BF. (2023, Febbraio 13). *Cyber Risk: cos'è e come difendersi*. Retrieved from Valore BF : https://www.valorebf.it/cyber-risk-cose-e-come-difendersi/

Versaci, M. B., & Pauri, A. (2024, Gennaio 10). *Cyber security, c'è il nuovo Regolamento UE: così aumenta il livello comune di sicurezza.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-security-ce-il-nuovo-regolamento-ue-cosi-aumenta-il-livello-comune-di-sicurezza/

Verxo. (2015, Luglio). *Rischio informatico: cosa si intende*. Retrieved from Verxo: https://www.verxo.it/rischio-informatico-cosa-si-intende/

Wabbi. (n.d.). *About Us- Wabbi.* Retrieved from Wabbi: https://wabbisoft.com/about_us/

Webristle. (2023, Novembre 22). *Cyber Insurance: cos'è e perché è fondamentale.* Retrieved from Webristle: https://www.webristle.com/2023/11/22/cyber-insurance-cose-e-perche-e-fondamentale/

World Economic Forum. (2023, Aprile 30). *The Future of Jobs Report 2023*. Retrieved from World Economic Forum: https://www.weforum.org/publications/the-future-of-jobs-report-2023/

World Economic Forum. (2024). *The Global Risks Report 2024.* Retrieved from World Economic Forum: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Wüest, C. (2024, Febbraio 7). *Mitigare i rischi del ransomware con le assicurazioni informatiche: il rapporto costi-benefici.* Retrieved from Cyber Security 360: https://www.cybersecurity360.it/soluzioni-aziendali/mitigare-i-rischi-del-ransomware-con-le-assicurazioni-informatiche-il-rapporto-costi-benefici/

Yan, J. (2017, Maggio). *Loss Cost Modeling vs Frequency and Severity Modeling.* Retrieved from Deloitte: https://www.casact.org/sites/default/files/presentation/spring_2017_presentations_c-12_yan.pdf

Zero Uno. (2016, Ottobre 5). *WAF significa Web Application Firewall: che cos'è, come funziona e a cosa serve.* Retrieved from Zero Uno: https://www.zerounoweb.it/cloud-computing/waf-significa-web-application-firewall-che-cos-e-come-funziona-e-a-cosa-serve/

Zscaler. (n.d.). *Cosa si intende per zero trust?* Retrieved from Zscaler: https://www.zscaler.it/resources/security-terms-glossary/what-is-zero-trust